Guest Internet
Managed WiFi

PRODUCT DOCUMENTATION

Manage a public Internet WiFi service for one or many locations through one cloud screen. Optionally monetize the Internet WiFi service.

January 2025

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

+786 722-0424
guest-internet.com
support@guest-internet.com

This document is divided into the following sections:

	Page
Overview	4
Products	15
Wizard	56
Admin interface	63
Status	63
Management	69
Advanced settings	97
Cloud management	175
Additional information	199

If you cannot find an answer for your question in these sections, please contact us through our technical support page.

https://guest-internet.com/guest_internet_hotspot_support.php

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

IMPORTANT NOTICES

Federal Communications Commission (FCC)
Supplier's Declaration of Conformity (SDoC)

47 CFR § 2.1077 Compliance Information

Product Identifiers: **GIS-R2, GIS-R4, GIS-R6, GIS-R10, GIS-R20, GIS-R40**

Responsible Party – U.S. Contact Information

Guest Internet Solutions
Fire4 Systems Inc.
6073 NW 167th ST, Unit C15
Hialeah, FL 33015
Tel: +1-786-358-5406
Email: support@guest-internet.com
Website: www.guest-internet.com

FCC Compliance Statement

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

Interfaces With 3rd Party Systems and Services

Guest Internet provides interfaces with the third-party systems, PayPal, OpenDNS and DynDns. The interfaces are provided "AS IS". Guest Internet makes no warranties, express or implied, as to the correct functioning of Guest Internet products with the third-party interfaces and hereby disclaims all implied warranties, including any warranty of merchantability and warranty of fitness for a particular purpose.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Guest Internet Product Documentation

Overview.

Guest Internet products are specialized network appliances that have been designed to address the requirements of three market segments:

- Managed WiFi.
- Mobile Broadband.
- Internet WiFi hotspots.

Unfortunately there is no one-product-fits-all for these three market segments and so Guest Internet manufacturers groups of products where each group is specialized for a market segment.

The Pro range of products, GIS-R10, GIS-R20 and GIS-R40 have the features needed for the managed WiFi market and are installed by many Managed Service Providers (MSP's) and are used to deliver the MSP services to many types of businesses.

The wireless range of products, GIS-K1, GIS-K3, GIS-K5 and GIS-K7 have features for the mobile broadband market as they can be used to build cellular WiFi networks with roaming. Wireless Internet Service Providers (WISPs) install the K-series of products to sell Internet access with the sale of vouchers or with on-line credit card payments.

The business range of products, GIS-R2, GIS-R4 and GIS-R6 have features that are required for the Internet WiFi Hotspot market and are used together with one or many wireless access points to cover a large area. Many types of locations that include hospitality, retail and government buildings provide an Internet WiFi Hotspot service.

There is also crossover between the product ranges. For example, an international airport IT department may install a public WiFi Internet system (Internet WiFi Hotspot), or the airport may outsource the WiFi system to a MSP (Managed WiFi).

What is Wi-Fi?

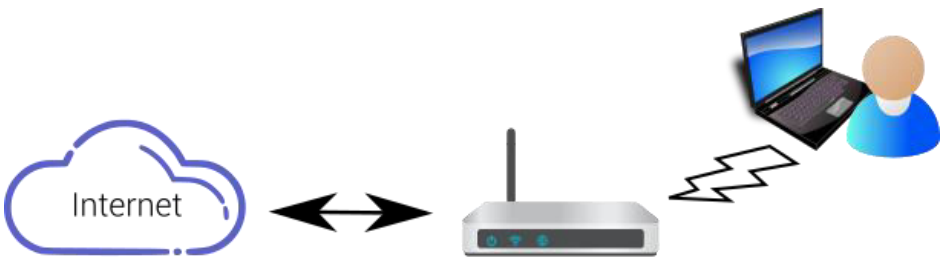
In order to explain Internet Wi-Fi, we first need to clarify **What is Wi-Fi?**

Wi-Fi stands for **Wireless Fidelity** and it is the technology used by laptops, tablets, mobile phones and other devices to connect to the Internet without wires.

The Internet is delivered via a DSL or cable connection to a **wireless router**.

A **wireless router** is an electronic device that sends data from the Internet cable to a device through radio signals instead of another cable.

So, an **Internet Wi-Fi** is a wireless connection for any device (computers, laptops, tablets, smartphone, etc.).



DSL/Cable router with WiFi wireless
A password is required to connect

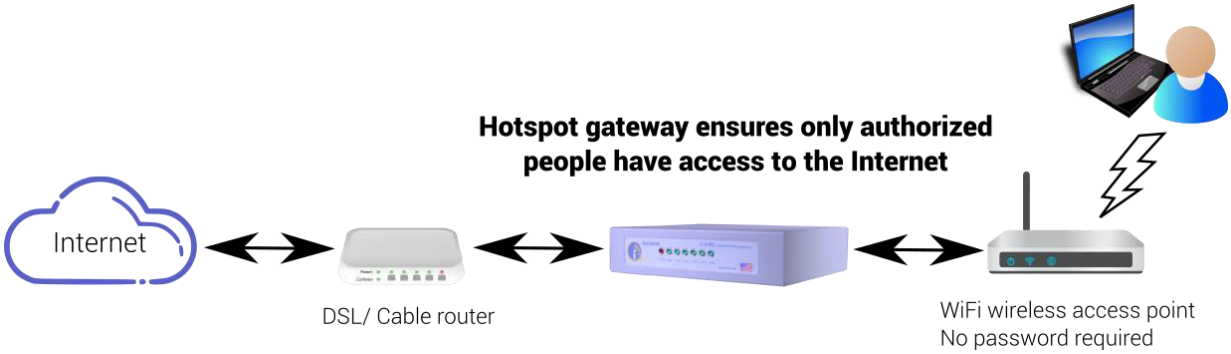
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Most homes and offices have a wireless router that provides Internet access. The wireless router has a password (WEP or WPA key), therefore devices can only connect to the Internet when the password is provided.

What is Wi-Fi Hotspot?

Essentially **Wi-Fi Hotspot** is similar to **Internet Wi-Fi**, however it differs in a few aspects:

- The wireless WiFi does not have an encryption password, therefore anyone with a mobile device, smart-phone, tablet or laptop can connect to the network, and it is typically installed in **public locations**;
- Access to the Internet is controlled by a **Gateway** so that only users who have been given authorization can connect to the Internet.



The **wired router** gets Internet connection from the **Internet Service Provider (ISP)**, the **Gateway** is connected to the wired router in order to control who can connect and a **wireless access point** is connect to the gateway so it can pass the Wi-Fi signal to devices.

What is Managed WiFi?

Managed WiFi is a service that a business called a managed Service Provider (MSP) offers to another business, or else the IT department of a large business provides a Managed WiFi service for all departments and subsidiaries of the business. An Internet Service provider (ISP) can also provide a managed WiFi service for a residential or business customer.

In any business network the WiFi is the weakest link and so it is desirable that a business puts the management of the WiFi network into the hands of experts.

- If a WiFi problem occurs the business may have to stop operations.
- An intruder might access the WiFi network using a laptop computer from the parking lot.
- Managed WiFi is very important for any business that has no or limited IT staff. Most small business have no IT staff and rely on an IT services business for their computer and network requirements.

Managed Wifi is an outsourced service that might include many or all of the following services:

- Site survey to plan the wireless WiFi network installation to ensure adequate coverage, and to provide contingency in the case of ISP failure, that might include having two ISP's with load balance and fail-over.
- WiFi network product evaluation, selection and acquisition.
- Installation of the WiFi network and verification of correct operation.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

- Designing a security policy to ensure the security of the data.
- Segmenting the WiFi network to separate departments, environments, to ensure data security.
- Implementing security features such as intrusion detection to prevent hacking, a denial of service attack, or ransomware attack.
- Incident response plan in case of a data breach.
- Configuration of the WiFi network based on the parameters provided by the customer, that might include setting data speed and download limits or blocking access to websites.
- Authenticating users onto the network and ensuring that no unauthorized personnel have access, with differential access rules for staff and also for guests of the business.
- A hospitality business can provide isolated WiFi access for staff, free basic Internet WiFi for guests and charge for high-speed guest WiFi.
- Monitoring network components for failure (wireless access points, etc) with alarm and initiating a process to quickly replace the defective product.
- Testing the network to ensure that no rough products (wireless routers, etc.) have been connected.
- Remove configuration changes to any device in the network, for example change a wireless access point SSID.
- User training for staff that will be accessing the network.
- Cloud management that permits the Managed WiFi provider to provide 24/7/365 support coverage for the customer.
- Monitoring and reporting of the network performance to inform the customer of any situations that might cause a problem and require maintenance.
- Upgrading and expanding the network design and installation to meet the growth requirements of the customer can be done quickly as the Managed WiFi provider will have a stock of materials.

It is possible that the managed WiFi services are divided between several suppliers, for example

- Supplier 1: Designs the infrastructure and prepares the site survey to indicate where wireless access points are installed.
- Supplier 2: Installs the infrastructure following the network design and verify that the network is functional to specification.
- Supplier 3: Operates the network, sets and manages authentication rules, monitors user accesses, and monitors devices for failure.

Managed WiFi has several benefits for the customer:

- Access to WiFi experts who will improve network quality and operations and will assume responsibility for the performance of the network, meeting business objectives and improving cost management.
- Improved network performance through data circuit management.
- Improved security to protect the business data with reduced risk of attack.
- Improved user support leading to workplace efficiency improvements.
- Shorter downtime when a WiFi network problem occurs.
- Eliminating network design errors will reduce cost of network ownership.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

- If the business provides WiFi for guests, such as a hotel, then improving the guest WiFi performance will lead to better reviews.

There are disadvantages when implementing Managed WiFi with an outsource supplier.

- The customer looses some control of the network environment as this is now outsourced to a third party supplier.
- The cost of network installation and/or operation may be higher than an in-house solution however the higher cost will translate in cost savings with better data security, improved reliability with less downtime and improved staff efficiencies through education and training.

Guest Internet products have the features that MSP's and IT departments need to provide a Managed WiFi service and so many MSP's install Guest Internet products at their customers locations to provide the Managed WiFi service.

What is Mobile Broadband?

A mobile broadband is a wireless Internet service that is provided in public areas as a free or paid service. The mobile broadband service is provided by a wireless connection, called **WiFi.**

Mobile broadband WiFi provides a wireless connection for mobile devices; smart-phones and tablets, and is used by people who are at a location for a short time, like an airport or a hotel.

Some examples of mobile broadband in public areas are listed below.

- Municipal and state parks and campgrounds, municipal sports arenas.
- Municipal offices that open to the public.
- Municipal WiFi in the public areas of villages, towns and cities.

Some examples of mobile broadband service provided by businesses are listed below.

- RV parks and campgrounds.
- Airports.
- Internet cafes, restaurants, coffee bars, retail stores.
- Motels, hotels, and resorts.
- Sporting events, team games, sports clubs, and gymnasiums.
- Shopping malls.
- Marinas.
- Schools and colleges.
- Churches.
- Trade shows.

In some cases the mobile broadband service is provided without charge as this is part of the services provide to the public by businesses. Hotels and motels provide free Internet access and guests expect to have free WiFi.

Some mobile broadband Internet providers charge a fee for use of the WiFi Internet; this is the case with many airports, especially International airports.

There are situations where the mobile broadband service is both free and paid. One example of this is hotels where free WiFi is offered to guests at a slow download and upload speed. If the

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

guest wants faster download and upload speeds then the guest can purchase the fast service using a credit card.

A mobile broadband user should always remember that using a public broadband service has risks and the user should always make encrypted connections to websites (https://) or else install reliable VPN software before using a mobile broadband service.

What does a Gateway do?

A **Gateway** is a device that provides access control that allows the user to connect to the Internet if the user meets the programmed criteria. The access control includes authentication, authorization and accounting of a wired or wireless network user to access an external network.

The Gateway has different types of access methods which are selected according to the business' requirements in order to control who has access to the network:

- User agrees to the terms and conditions of use
- Business provides a code (paid or free) to the user
- User provides personal information (e.g. name, phone number, email address...) in order to connect to the Internet

It is possible to combine some of these options. For example: provide a free and slow Internet, and then charge for a high speed Internet access.

The Gateway can control the download speed of each user. This is necessary so that the **bandwidth** (the amount of data that can be carried from one point to another in a given time period - usually a second) available from the DSL or cable provider can be shared equally between all users.

The Gateway has many other features that help the business owner provide guests and visitors with a good reliable Internet service, while ensuring that the business is not put at risk. A few features are:

- Limit the number of data bytes that a user can download
- Charging a customer for Internet use via PayPal or Credit/Debit card
- Monitoring the use of the Hotspot with reports on connected users, usage and billing
- Generation of codes
- Setting the Hotspot to be available during certain hours
- Custom login page, the first thing the guest sees when trying to connect to the Internet
- The Gateway can send an email to the Hotspot manager with reports, notifications and guest's information
- The Gateway can have a firewall that prevents any Hotspot users to connect to the business' computers, to prevent hacking
- The Gateway can block users who are abusing the service and allow approved devices to connect directly to the Internet
- The Gateway can have a printer connected that prints access codes onto tickets

In addition to the features listed above, the Gateway can also have **Cloud management**. Cloud management is a tool that permits one or many Gateways to be managed via Cloud service. This is very useful for two types of applications:

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

- When a business chain has many locations that provide Internet Wi-Fi for guests, then all Gateways installed on the premises of each location can be managed by one member of staff at a central IT facility
- When a business uses an IT service provider to take caare of all IT issues

What are the dangers of providing Internet access for guests?

Most retail business have a **Point of Sale (PoS)** on the premises and many business owners are aware of the danger of hacking that can occour if the PoS is connected directly to the Internet without protection of a firewall. However there are other risks of having the PoS hacked that the business owner may not be aware of. One situation might occur when the business provides Wi-Fi Internet Hotspot access for the customer.

By connecting a Wi-Fi wireless unit directly to the same network as the PoS, any user of the public Wi-Fi is able to access the PoS. An exeperienced credit card thief can steal the credit card information from the PoS in a few minutes, without the need to enter the premises.

Business owners should be aware that a Wi-Fi wireless unit should never be connected directly to the PoS network. The **credit card company rules (PCI DSS)** requires that a public Wi-Fi wireless unit is connected via one of the two methods:

1. The Wi-Fi wireless unit should be connected to a second independent Internet circuit (DSL), or
2. The Wi-Fi wireless unit should anly be connected to the PoS network through a second firewall

How to eliminate risks when installing a Wi-Fi Hotspot for guests?

By providing an open Wi-Fi wireless unit the retail business owner is also exposed to risks in addition to those of having credit card information stolen from the PoS.

The public Wi-Fi may be used to share copyrighted material and when that happens the business owner will receive a **DMCA Notice** from the ISP, advising that illegal file sharing must stop, or else the Internet service will be disconnected. The retailer relies on the Internet service to process credit cards, and so the disconnection of the Internet service will prevent the retailer processing credit card payments.

The public Wi-Fi Internet service can be abused in other ways. Customers can occupy coffee shop tables while using the free service without purchasing products, thereby reducing the profitability of the business. Customers can also download very large files (e.g. videos) which will result in other customers getting a very low Wi-Fi service, and creating a delay to process credit cards, slowing the checkout process.

A Internet Hotspot Gateway will solve the business Wi-Fi problems. The Gateway has a **firewall** (a network security system designed to prevent unauthorized access to or from a private network) which prevent Wi-Fi users getting access to the PoS and other business computers. The Gateway also has control mechanisms that prevent illegal file sharing, and also prevents any customer using all the available Internet bandwidth capacity.

The Gateway can also limit the time that a customer can connect to the Internet, preventing a coffee shop or restaurant being occupied by customers who are not purchasing products. The Gateway can also provide a limited time code to each customer at the check out point.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Why choose Guest Internet?

Guest Internet is market leading Internet Hotspot Gateway with content control. Our low cost Internet Hotspot Gateway has no extra charges or monthly fees and provides the following:

- Free lifetime support
- The ability to fully manage public Internet access:
- Different types of login (agree with disclaimer, email login, login with a code and login via social media)
- Setting limits to all the users or to individual codes - time limit, speed limit and data limit
- Manage units remotely with a free Cloud service
- Display a custom login page with promotional content to customers
- Charge for access
- Collect data about customers for marketing

We Make a Wi-Fi Hotspot Work Better

Add our Hotspot gateway to improve your Wi-Fi Hotspot:

- Plug & play installation with easy to use wizard
- Display a login page with your logo and adverts
- Require use of individual or group login codes
- Credit card & PayPal billing and reporting
- Built-in firewall
- Illegal downloads and web sites can be blocked
- Speed control shares bandwidth
- Access can be blocked outside of business hours
- No extra charges or monthly fees

We offer a very simple and low cost way to add important features for any Wi-Fi Hotspot.

We make a range of products: from a 25 users product for a bar or restaurant, up to a 2000+ users product suitable for a large resort.

Product features have been designed to protect your business from the consequences of data theft, and to give your guests and visitors a great Internet service.

Our products make great financial sense: low cost products ensure that you get a fast return on investment.

Plug and play installation

Our products do not require a computer specialist to install them. With the easy to follow setup wizard, any person who runs a business and uses a computer already has the skills required.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

10,000 access codes

Up to 10,000 access codes can be generated at one time. As access codes expire then new codes can be generated. Access codes have many features/limits such as duration, single/multi user per code, and download/upload speeds.

Credit card billing and reporting

Credit card billing can be configured for commercial Hotspots. A PayPal account is required and the account information must be entered during the configuration process. All payments go directly to your PayPal account.

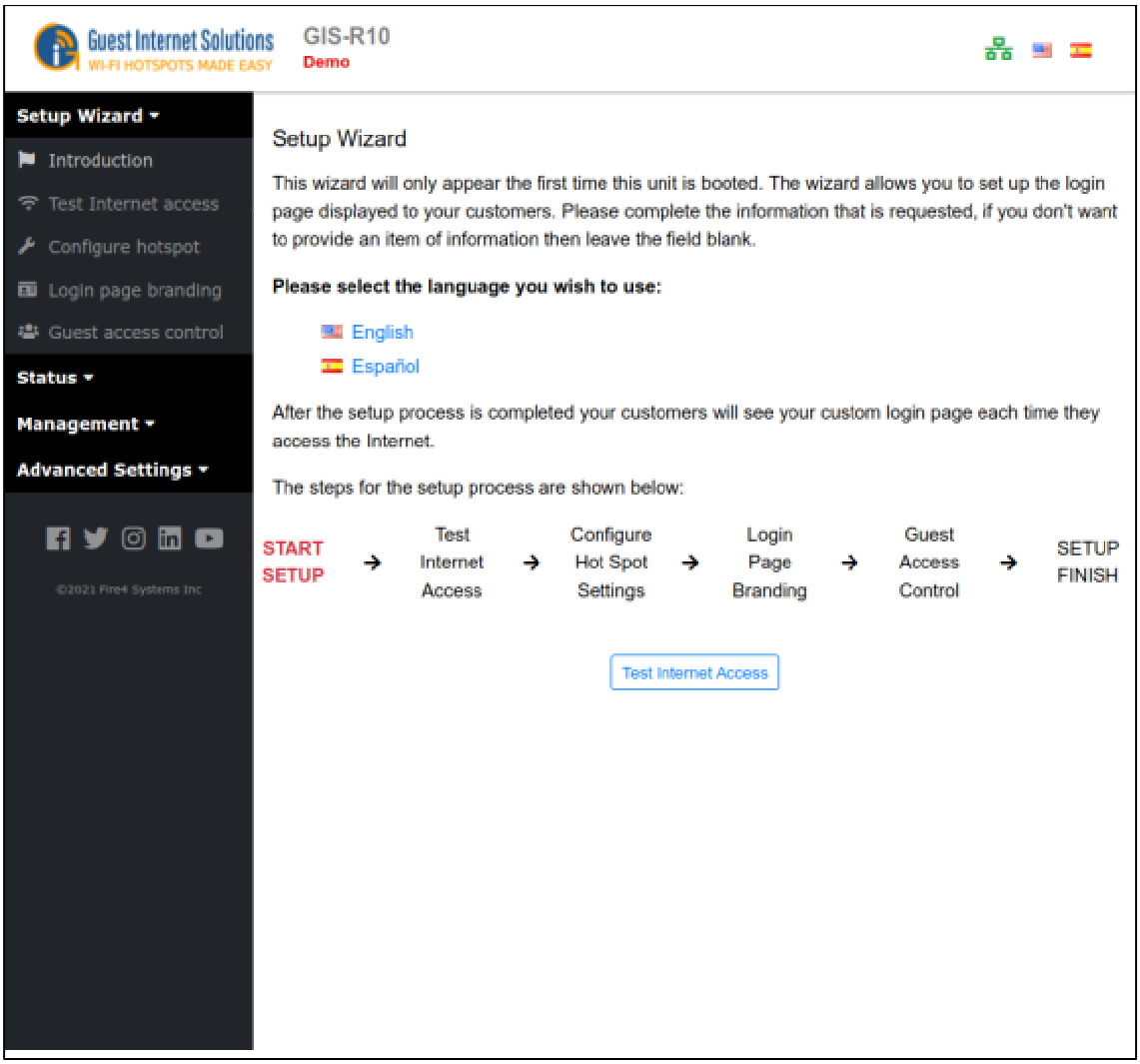
Illegal downloads are blocked

Some guests and visitors have file sharing software installed in their computers. When the files are copyrighted (music MP3's or videos) the sharing of files is illegal. File sharing can be identified by organizations like the RIAA who are then suing DSL customers. Our higher performance products block file sharing to prevent the Hotspot operator being at risk of DSL disconnection and lawsuits.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Very easy to use

Connect the product to your router or cable modem then connect a computer to the product. Just answer the questions that appear on the screen in the setup wizard:



The wizard checks your Internet connection then creates your custom login page and selects the correct features for your business.

You now have a Wi-Fi Hotspot to provide Internet for your guests.

Login page: use for advertising

Twelve different login pages are already installed in all our products. In addition you can upload your own background photo or design a login page with advertising using HTML. Promote specials to increase sales, or provide a discount coupon to encourage return visits. Read more about login pages

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Speed control shares bandwidth

One of the problems with Wi-Fi Hotspots is that some guests abuse the service by downloading very large files. This slows Internet access for all the other guests, and also for the business computers if one DSL or cable connection is used for all services. Our speed control ensures that each guest gets a fair share of the total bandwidth available and prevents anyone downloading a large file from slowing the Internet service for other guests.

Built-in Firewall

All our products have a firewall which prevents Wi-Fi Hotspot users accessing any computer that is connected to the same DSL or cable. The firewall prevents a hacked getting access to a Point of Sale (PoS) terminal to prevent the theft of credit card information. Our product firewall technology complies with the credit card industry PCI DSS requirements to protect PoS and computers that contain credit card information..

Web sites can be blocked

Our products have a feature called content filtering. This blocks access to adult and similar websites, ensuring that web surfing is family friendly. In addition to serving as a parental control content filtering prevents anyone viewing unpleasant website in public places. Content filtering ensures that you will not get any complaints from guests who have been offended by the Wi-Fi Hotspot service. In addition to website category blocking our products also have a domain/IP white list and black list.

New features to be included with this software generation

The new features listed below have been requested by our customers and will be introduced during Q1 and Q2 of 2022.

The Guest Internet admin pages and login pages are now responsive and adapt to any size of display, from a small mobile phone to a large desktop computer.

Access codes can now have the start date and time specified

Send email messages via the Cloud. Users have had problems with SMTP service and the use of Gmail. A Cloud messaging service has been added to easily send gateway emails.

Roaming between hotspots: User MAC addresses will be shared between gateways so that after a user logs in on one gateway, that user will remain logged in on other gateways.

VLAN settings on the LAN ports: VLAN tagging will be added to the LAN ports. The primary purpose is to allow guests and staff to share the same wireless access points (AP's) providing APs can support duplicate SSID's each on a different VLAN. Guests will be directed to the login page while staff will bypass the gateway.

Max speed settings on each LAN port: For division of speed, for example 1Gb/s comes into the WAN, then set LAN1 at 800Mb/s maximum for guests and LAN2 at 200Mb/s maximum for the conference area to guarantee bandwidth for each area. A new LAN max speed setting will be added to the LAN port configuration.

High availability. Install two GIS products and have failover if one product fails: Implemented using the cloud where the cloud can share settings and logins.

PMS support: implementation of a REST API (https://restfulapi.net/) as part of the cloud services as a standard API format for PMS integration. This implementation will have the same features as the current http implementation but via the cloud, not via the gateway as with the current API.

See a demo of the new generation firmware here: https://demo.guest-internet.com/admin/

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Features eliminated from this new software generation

Emails are now sent using either the ISP SMTP server or using the GIS Cloud service. Email transmission methods using Gmail, Yahoo, AOL, Hotmail and Outlook have been removed due to the increasing security requirements of these services leading to frustration for our customers.

Social media login using Facebook has been eliminated from this generation of software for two reasons. First, the feature uses the Facebook Hotspot API and Facebook made changes to increase the security of the API which made the feature very difficult to use, our new customers had to purchase a domain name and security certificate and create a website to use the feature. Second, even when our customers followed the new Facebook API rules, Facebook could and did block access to the API as determined by their automated algorithm for an unstated reason, with no means of recourse.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Products

GIS Wireless Gateway Products with the New Generation firmware

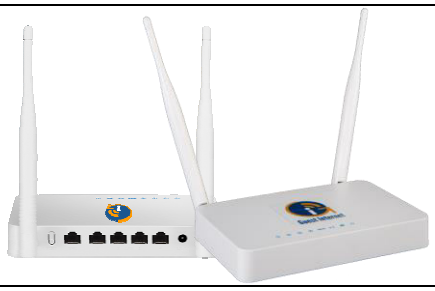
	GIS-K1	GIS-K3	GIS-K5	GIS-K7
Core GIS Features	•	•	•	•
Customer Data Collection	•	•	•	•
PCI compliant Firewall	•	•	•	•
PayPal® & Credit Card Billing	•	•	•	•
Internet por ficha	•	•	•	•
FREE Cloud management	•	•	•	•
Indoor installation	•		•	
Outdoor installation		•		•
Antenna type omni-directional	•		•	•
Antenna type directional		•		
Power over Ethernet (PoE)		•	•	•
WAN Port 10/100	•	•	•	•
LAN port(s) 10/100	4	1	1	0
Wireless (WiFI) technology	11n	11n	11n	11n
Wireless (WiFI) data speed	300Mb/s	300Mb/s	300Mb/s	300Mb/s
User limit**	none	none	none	none
Throughput (Mbps)***	75	100	100	100

**There are no limits on the number of users; user capacity is dependent on type and quantity of user traffic, backhaul bandwidth and gateway options.

***Throughput is dependent on network infrastructure, backhaul bandwidth and gateway options.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS Wireless Hotspot Gateway Product Links

Product	Range	Photo	Datasheet
GIS-K1	Wireless		https://guest-internet.com/GIS-K1_product_page.php
GIS-K3	Wireless		https://guest-internet.com/GIS-K3_product_page.php
GIS-K5	Wireless		https://guest-internet.com/GIS-K5_product_page.php
GIS-K7	Wireless		https://guest-internet.com/GIS-K7_product_page.php

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS Business Gateway and PRO Gateway Products

	Business Gateways			PRO Gateways		
	GIS-R2	GIS-R4	GIS-R6	GIS-R10	GIS-R20	GIS-R40
Core GIS Feature	•	•	•	•	•	•
Customer Data Collection	•	•	•	•	•	•
Advanced Firewall		•	•	•	•	•
PayPal® & Credit Card Billing		•	•	•	•	•
Internet por ficha	•	•	•			
FREE Cloud management	•	•	•	•	•	•
Rack-mountable (1U)			•	•	•	•
Processor architecture	32 bit 2-core	32 bit 2-core	32 bit 2-core	64 bit 2-core	64 bit 2-core	64 bit 4-core
WAN Ports Gb Load balance/Failover	1	1	2	2	2	4
LAN Ports Gb	4	4	3	4	4	2
User limit**	none	none	none	none	none	none
Throughput (Mbps)***	100	150	200	400	600	800

** There are no limits on the number of users; user capacity is dependent on type and quantity of user traffic, backhaul bandwidth and gateway options.

***Throughput is dependent on network infrastructure and gateway options.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS Ethernet Hotspot Gateway Product Links

Product	Range	Photo	Datasheet
GIS-R2	Ethernet		https://guest-internet.com/GIS-R2_product_page.php
GIS-R4	Ethernet		https://guest-internet.com/GIS-R4_product_page.php
GIS-R6	Ethernet		https://guest-internet.com/GIS-R6_product_page.php

GIS High Performance Enterprise (PRO) Ethernet Hotspot Gateway Product Links

Product	Range	Photo	Datasheet
GIS-R10	Pro		https://guest-internet.com/GIS-R10_product_page.php
GIS-R20	Pro		https://guest-internet.com/GIS-R20_product_page.php
GIS-R40	Pro		https://guest-internet.com/GIS-R40_product_page.php

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS Wireless Range Core functionality:	Plug and Play Wizard Custom Login Page Authentication Internet por Ficha Disclaimer Editor Access Code Generation Content Filtering Bandwidth Control Basic Firewall Usage and Billing Reports URL Filter MAC Filter Access Code API Ethernet port(s) 10/100 Wireless access point, 11n 300Mb/s

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-K1 Wireless Hotspot Gateway

The GIS-K1 is a powerful long-range wireless access point for indoor installations and has a omni-directional antennas for 2x2 MIMO with 300Mb/s capacity.

The GIS-K1 Hotspot Gateway WAN Port plugs into your ISP router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-K1 can have additional wireless access points and wired computers connected to the four LAN ports.

The GIS-K1 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits per user from any device connected to your network.

The GIS-K1 has the voucher design and printing feature that is very popular with customers in Latin America who install Internet-por-ficha sites.

The GIS-K1 Hotspot Gateway is a simple plug and play installation, requiring no specialist technical knowledge.

The login page will allow your guests access to the Internet using one of the following methods:

- Open Access: no login page but firewall rules applied
- Agree to terms and conditions
- Login with a pre-generated login code
- Provide email address and other information
- Purchase access using a credit card
- 2-tier access: free slow speed + purchase high speed

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-K3 Wireless Hotspot Gateway

The GIS-K3 is a powerful long-range wireless access point for outdoor installations and has a directional antenna for 2x2 MIMO with 300Mb/s capacity.

The GIS-K3 Hotspot Gateway WAN Port plugs into your ISP router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-K3 can have additional wireless access points connected to the LAN port.

The GIS-K3 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits per user from any device connected to your network.

The GIS-K3 has the voucher design and printing feature that is very popular with customers in Latin America who install Internet-por-ficha sites.

The GIS-K3 Hotspot Gateway is a simple plug and play installation, requiring no specialist technical knowledge.

The login page will allow your guests access to the Internet using one of the following methods:

- Open Access: no login page but firewall rules applied
- Agree to terms and conditions
- Login with a pre-generated login code
- Provide email address and other information
- Purchase access using a credit card
- 2-tier access: free slow speed + purchase high speed

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-K5 Wireless Hotspot Gateway

The GIS-K5 is a powerful long-range wireless access point for indoor installations and has an omni-directional antenna for 2x2 MIMO with 300Mb/s capacity.

The GIS-K5 Hotspot Gateway WAN Port plugs into your ISP router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-K5 can have additional wireless access points connected to the LAN port.

The GIS-K5 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits per user from any device connected to your network.

The GIS-K5 has the voucher design and printing feature that is very popular with customers in Latin America who install Internet-por-ficha sites.

The GIS-K5 Hotspot Gateway is a simple plug and play installation, requiring no specialist technical knowledge.

The login page will allow your guests access to the Internet using one of the following methods:

- Open Access: no login page but firewall rules applied
- Agree to terms and conditions
- Login with a pre-generated login code
- Provide email address and other information
- Purchase access using a credit card
- 2-tier access: free slow speed + purchase high speed

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-K7 Wireless Hotspot Gateway

The GIS-K7 is a powerful long-range wireless access point for outdoor installations and has an omni-directional antenna for 2x2 MIMO with 300Mb/s capacity.

The GIS-K7 Hotspot Gateway WAN Port plugs into your ISP router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-K7 can have additional wireless access points and wired computers connected to the four LAN ports.

The GIS-K7 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits per user from any device connected to your network.

The GIS-K7 has the voucher design and printing feature that is very popular with customers in Latin America who install Internet-por-ficha sites.

The GIS-K7 Hotspot Gateway is a simple plug and play installation, requiring no specialist technical knowledge.

The login page will allow your guests access to the Internet using one of the following methods:

- Open Access: no login page but firewall rules applied
- Agree to terms and conditions
- Login with a pre-generated login code
- Provide email address and other information
- Purchase access using a credit card
- 2-tier access: free slow speed + purchase high speed

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS Ethernet Range Core functionality:	Plug and Play Wizard Custom Login Page Authentication Internet por Ficha Disclaimer Editor Access Code Generation Content Filtering Bandwidth Control Firewall Usage and Billing Reports PayPal® and Credit Card Billing (except GIS-R2) URL Filter MAC Filter Configuration Backup/Restore Access Code API

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-R2 Ethernet Hotspot Gateway

The GIS-R2 is a high performance dual-processor gateway with a throughput of 100Mb/s

The GIS-R2 Hotspot Gateway plugs into your current router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-R2 works with all types of Internet connected devices, including wireless access points and wired computers.

The GIS-R2 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Main features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits per user from any device connected to your network.

The GIS-R2 Hotspot Gateway is a simple plug and play installation, requiring no specialist knowledge.

The login page will allow your guests access to the Internet using the following methods:

Providing email address and other information

Login with a pre-generated login code

Agree to terms and conditions ... or Open Access

Documentation

Datasheet

Quickstart

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-R4 Hotspot Gateway

The GIS-R2 is a high performance dual-processor gateway with a throughput of 150Mb/s

The GIS-R4 Hotspot Gateway plugs into your current router and provides controlled access to the Internet for up an unlimited number of guests.

The GIS-R4 works with all types of Internet connected devices, including wireless access points and wired computers.

The GIS-R4 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Main features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits **per user** from any device connected to your network.

The GIS-R4 Hotspot Gateway is a simple plug and play installation, requiring no specialist knowledge.

The login page will allow your guests access to the Internet using the following methods:

Providing email address and other information

Login with a pre-generated login code

Automatic billing for Internet access

Agree to terms and conditions

or Open Access

Documentation

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-R6 Hotspot Gateway

The GIS-R6 is a high performance dual-processor gateway with a throughput of 200Mb/s

The GIS-R6 Hotspot Gateway plugs into your current router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-R6 works with all types of Internet connected devices, including wireless access points and wired computers.

The GIS-R6 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Main features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits **per user** from any device connected to your network.

The GIS-R6 Hotspot Gateway is a simple plug and play installation, requiring no specialist knowledge.

The login page will allow your guests access to the Internet using the following methods:

Providing email address and other information

Login with a pre-generated login code

Automatic billing for Internet access

Agree to terms and conditions

or Open Access

Documentation

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS Pro Range Core functionality:	Very high performance, high throughput Plug and Play Wizard Custom Login Page Authentication Disclaimer Editor Access Code Generation Content Filtering Bandwidth Control Advanced Firewall Usage and Billing Reports PayPal® and Credit Card Billing URL Filter MAC Filter Configuration Backup/Restore Access Code API

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-R10 Hotspot Gateway

The GIS-R10 is a very high performance gateway that has an Intel 64-bit dual-core processor with a throughput of 300Mb/s and dual-WAN

The GIS-R10 Hotspot Gateway plugs into your current router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-R10 works with all types of Internet connected devices, including wireless access points and wired computers.

The GIS-R10 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Main features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits **per user** from any device connected to your network.

The GIS-R10 Hotspot Gateway is a simple plug and play installation, requiring no specialist knowledge.

The login page will allow your guests access to the Internet using the following methods:

Providing email address and other information

Login with a pre-generated login code

Automatic billing for Internet access

Agree to terms and conditions

or Open Access

Documentation

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-R20 Hotspot Gateway

The GIS-R20 is a very high performance gateway that has an Intel 64-bit dual-core high performance processor with a throughput of 500Mb/s and dual-WAN

The GIS-R20 Hotspot Gateway plugs into your current router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-R20 works with all types of Internet connected devices, including wireless access points and wired computers.

The GIS-R20 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Main features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits **per user** from any device connected to your network.

The GIS-R20 Hotspot Gateway is a simple plug and play installation, requiring no specialist knowledge.

The login page will allow your guests access to the Internet using the following methods:

Providing email address and other information

Login with a pre-generated login code

Automatic billing for Internet access

Agree to terms and conditions or Open Access

Documentation

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-R40 Hotspot Gateway

The GIS-R40 is a very high performance gateway that has an Intel 64-bit quad-core high performance processor with a throughput of 800Mb/s and quad-WAN

The GIS-R40 Hotspot Gateway plugs into your current router and provides controlled access to the Internet for an unlimited number of guests.

The GIS-R40 works with all types of Internet connected devices, including wireless access points and wired computers.

The GIS-R40 Hotspot Gateway allows you to safely and securely share your Internet connection with your guests.

Main features include displaying a custom login page, capturing user data for marketing and managing users with a range of powerful tools. You can choose how *you* want to provide Internet access.

Bandwidth controls to improve quality of service (QoS) on the unit can be enabled to limit user download and upload speed, spreading the available bandwidth evenly across users. You can also set time and data limits **per user** from any device connected to your network.

The GIS-R40 Hotspot Gateway is a simple plug and play installation, requiring no specialist knowledge.

The login page will allow your guests access to the Internet using the following methods:

Providing email address and other information

Login with a pre-generated login code

Automatic billing for Internet access

Agree to terms and conditions

or Open Access

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Peripherals

GIS-TP1: Printer

The GIS-TP1 adds access code ticket printing to any GIS hotspot gateway product.

The ticket printer has an Ethernet interface and connects to the gateway's LAN network.

A tablet computer or computer can be used to control the printer. Buttons are displayed on the tablet screen or monitor for up to 10 different access code durations. Touching any button causes the ticket to be generated and printed.

The ticket printer is plug and play, simply enter the business information that should be printed on the ticket and the printer is ready to use.

The printer uses low cost 58mm (2 ¼") thermal paper that is available for point of sale printers from any office supply store.

You can learn how to setup your printer by clicking

https://www.guest-internet.com/docs/en/admininterface/advanced/printersetup

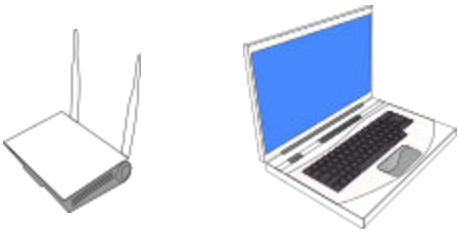
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Setup

The setup section will walk you through the basics of installing and using a GIS unit.

Requirements

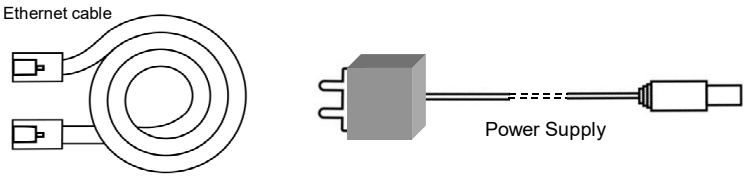
To setup your GIS unit you need:



A computer

A router or modem

A GIS unit



A Power Supply

Ethernet/Internet cables

Once you have everything from the list above (the power supply and one Ethernet cable comes with the unit), proceed to the QuickStart Guide.

Quickstart Guide

Each Quickstart Guide will guide you through the setup and basic configuration of your GIS unit.

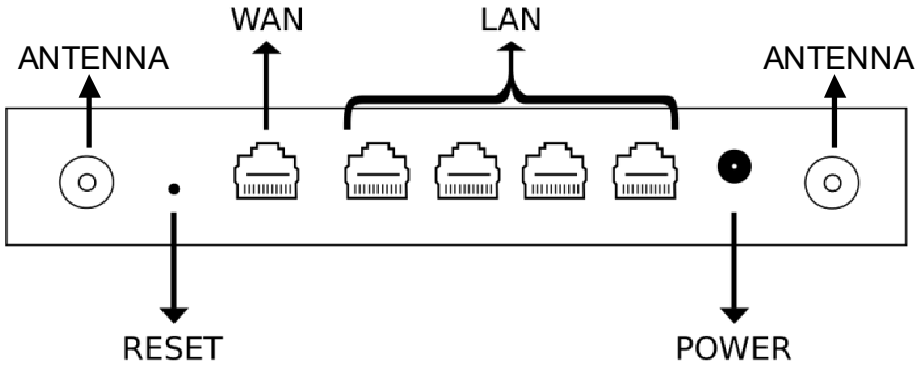
- GIS-K1 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-k1
- GIS-K3 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-k3
- GIS-K5 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-k5
- GIS-K7 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-k7
- GIS-R2 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-r2
- GIS-R4 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-r4
- GIS-R6 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-r6
- GIS-R10 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-r10
- GIS-R20 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-r20
- GIS-R40 : https://www.guest-internet.com/docs/en/setup/quickstart/gis-r40

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

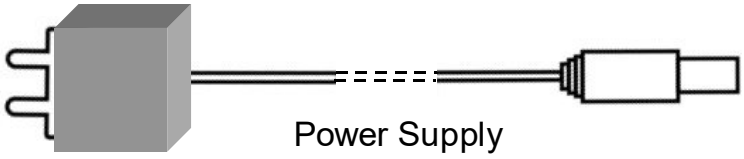
GIS-K1 Quickstart Guide

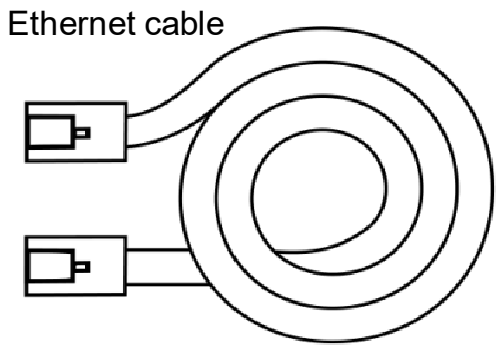
This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-K1 includes an external power supply of 12v, 1A

The back of your GIS-K1 unit:



The necessary cables to setup your unit:

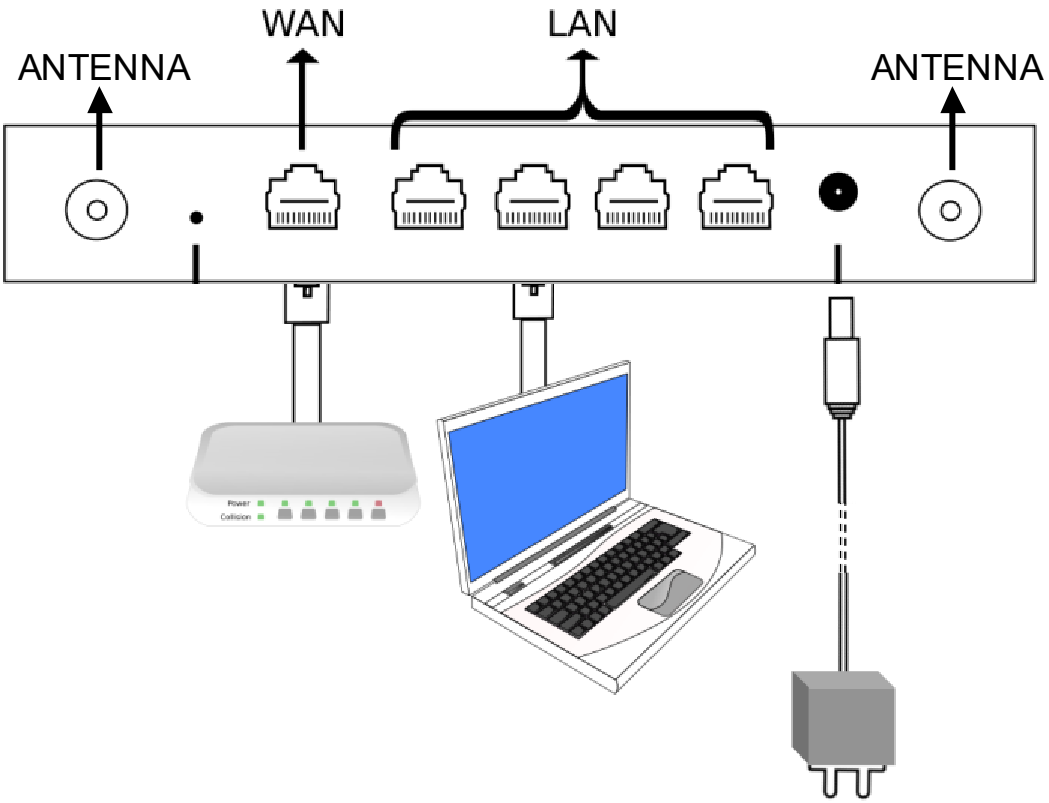




Connection Steps

1. Power on the GIS-K1 by connecting the power supply provided
2. Wait 30 seconds for the GIS unit to complete the boot process
3. Connect an Ethernet cable on the WAN port to your router
4. Connect an Ethernet cable on the LAN port and connect the other end to your computer

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

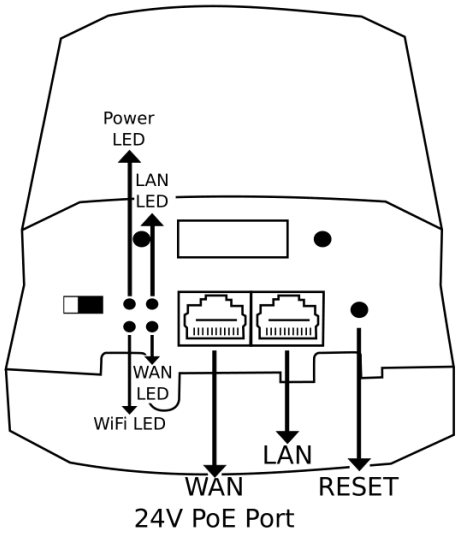
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

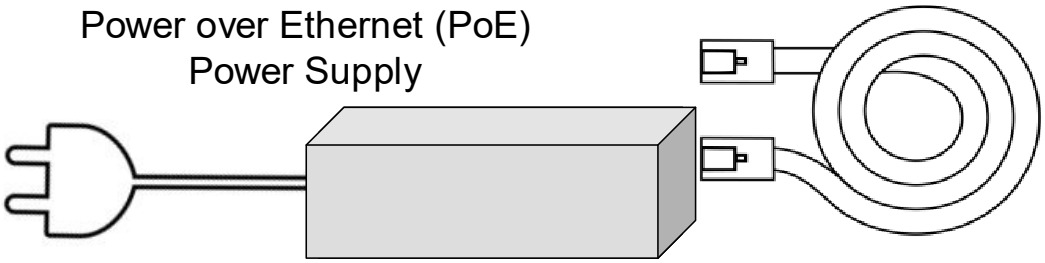
GIS-K3 Quickstart Guide

This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-K3 includes a power-over-Internet (PoE) power supply of 24v, 0.5A.

The back of your GIS-K1 unit:



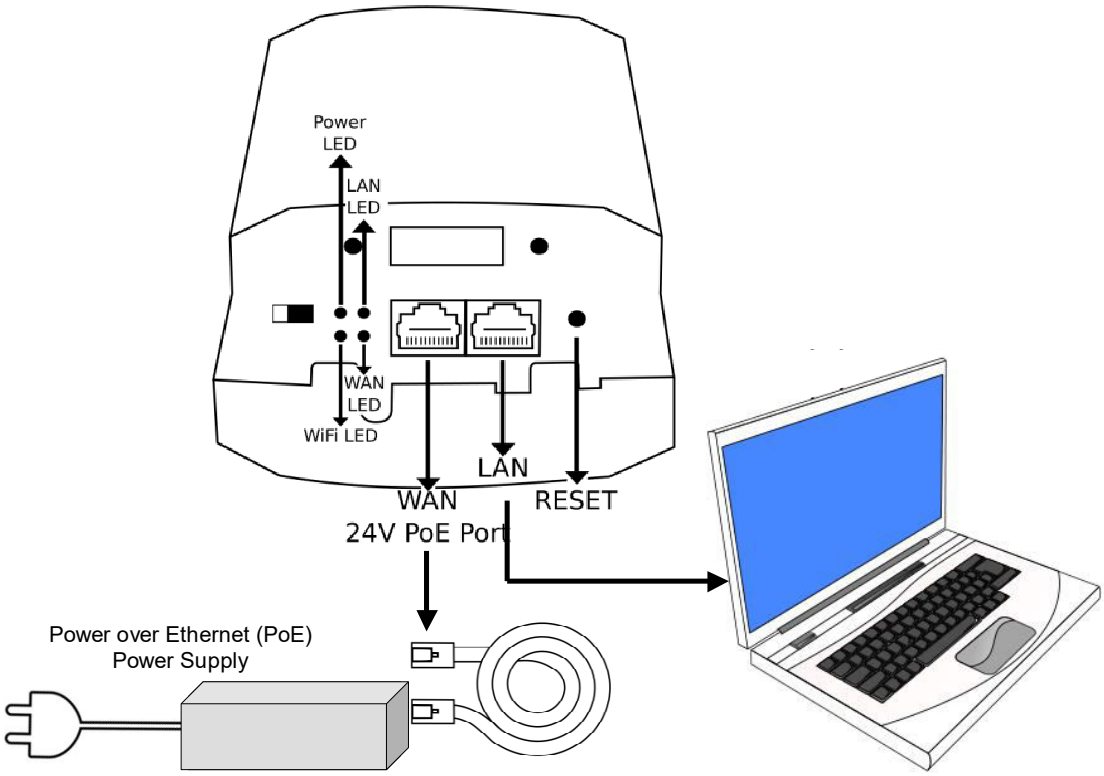
The necessary cables to setup your unit:



Connection Steps

5. Power on the GIS-K1 by connecting the power supply provided
6. Wait 30 seconds for the GIS unit to complete the boot process
7. Connect an Ethernet cable on the WAN port to your router
8. Connect an Ethernet cable on the LAN port and connect the other end to your computer

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

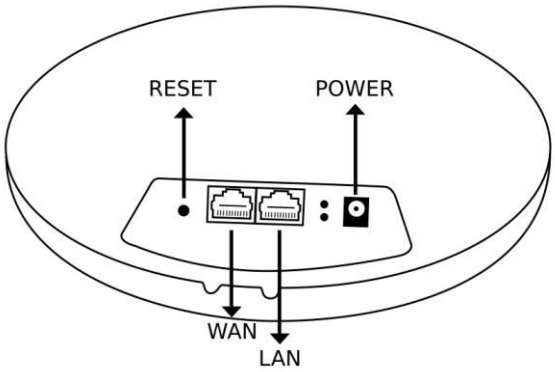
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

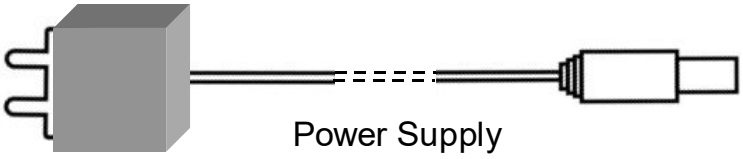
GIS-K5 Quickstart Guide

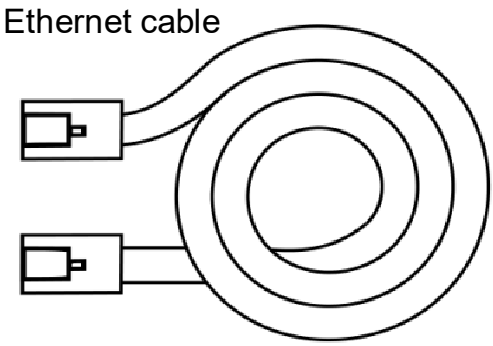
This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-K5 includes an external power supply of 12v, 1A. The GIS-K5 WAN port can also be powered by a 48v PoE switch.

The back of your GIS-K1 unit:



The necessary cables to setup your unit:

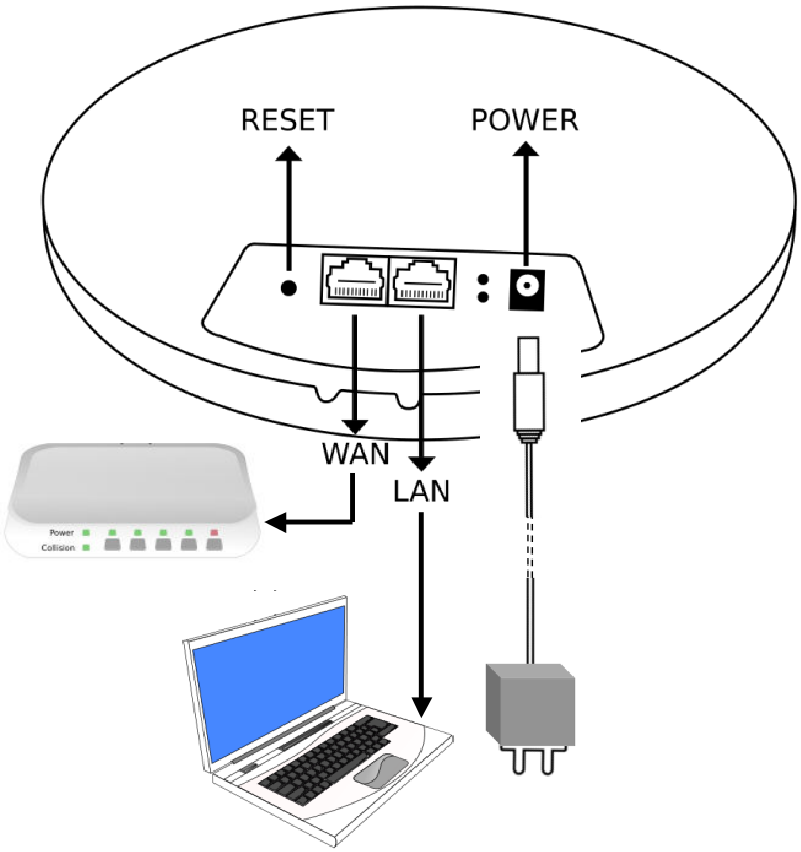




Connection Steps

9. Power on the GIS-K1 by connecting the power supply provided
10. Wait 30 seconds for the GIS unit to complete the boot process
11. Connect an Ethernet cable on the WAN port to your router
12. Connect an Ethernet cable on the LAN port and connect the other end to your computer

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

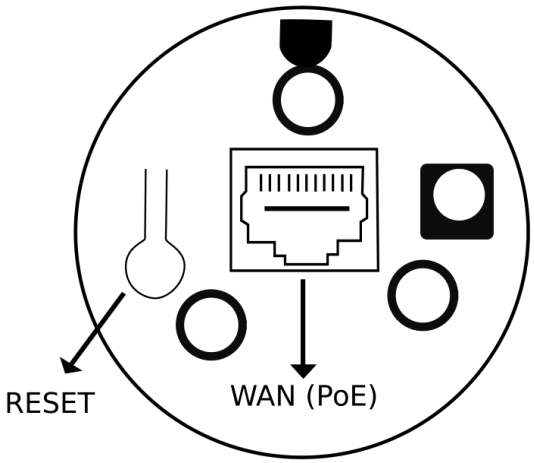
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

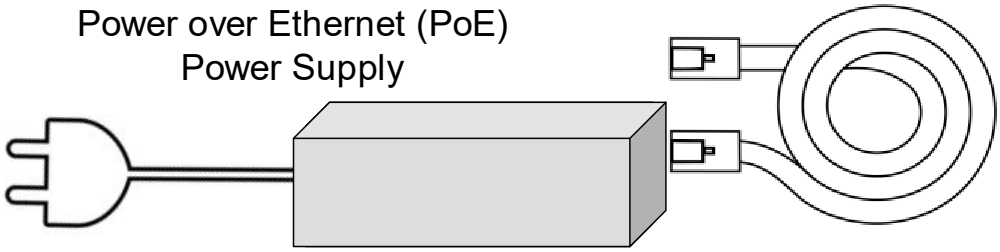
GIS-K7 Quickstart Guide

This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-K7 includes a power-over-Internet (PoE) power supply of 24v, 0.5A.

The back of your GIS-K1 unit:



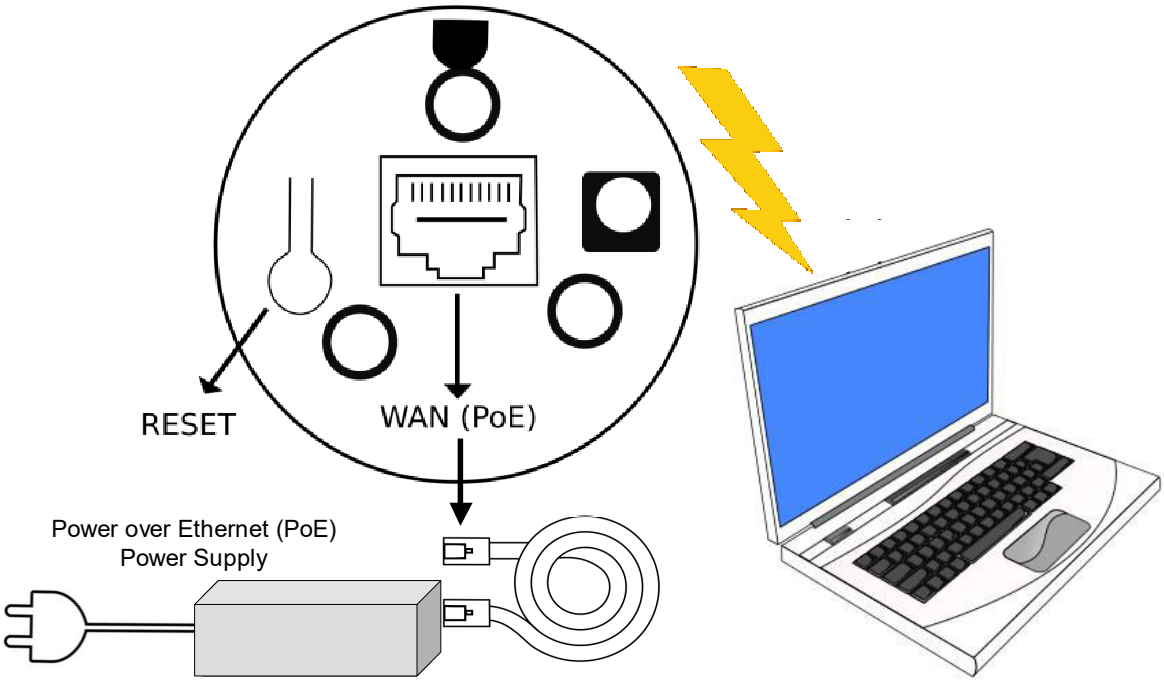
The necessary cables to setup your unit:



Connection Steps

13. Power on the GIS-K1 by connecting the power supply provided
14. Wait 30 seconds for the GIS unit to complete the boot process
15. Connect an Ethernet cable on the WAN port to your router
16. Connect an Ethernet cable on the LAN port and connect the other end to your computer

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

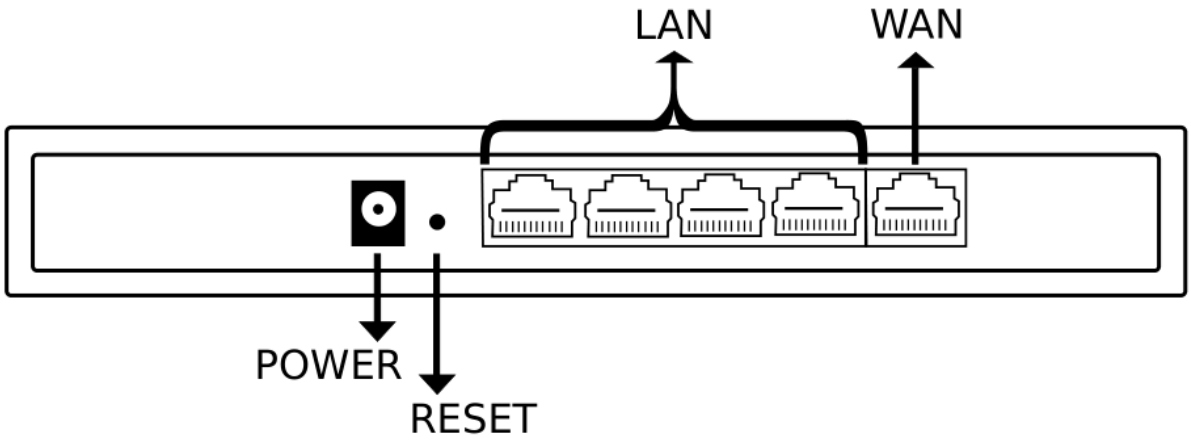
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

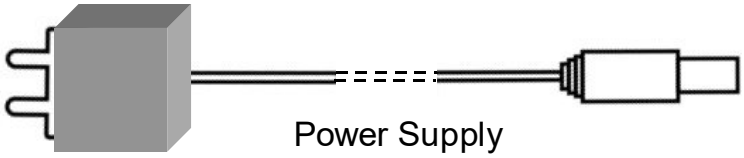
GIS-R2 Quickstart Guide

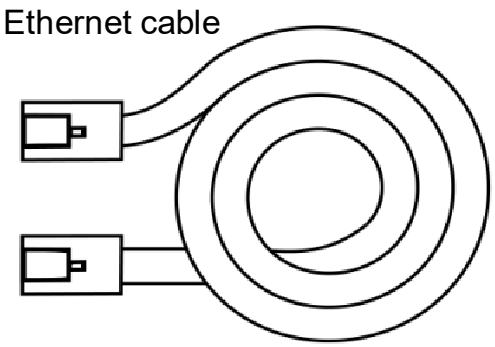
This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-R2 includes an external 12v 1A power supply.

The back of your GIS-R2 unit:



The necessary cables to setup your unit:

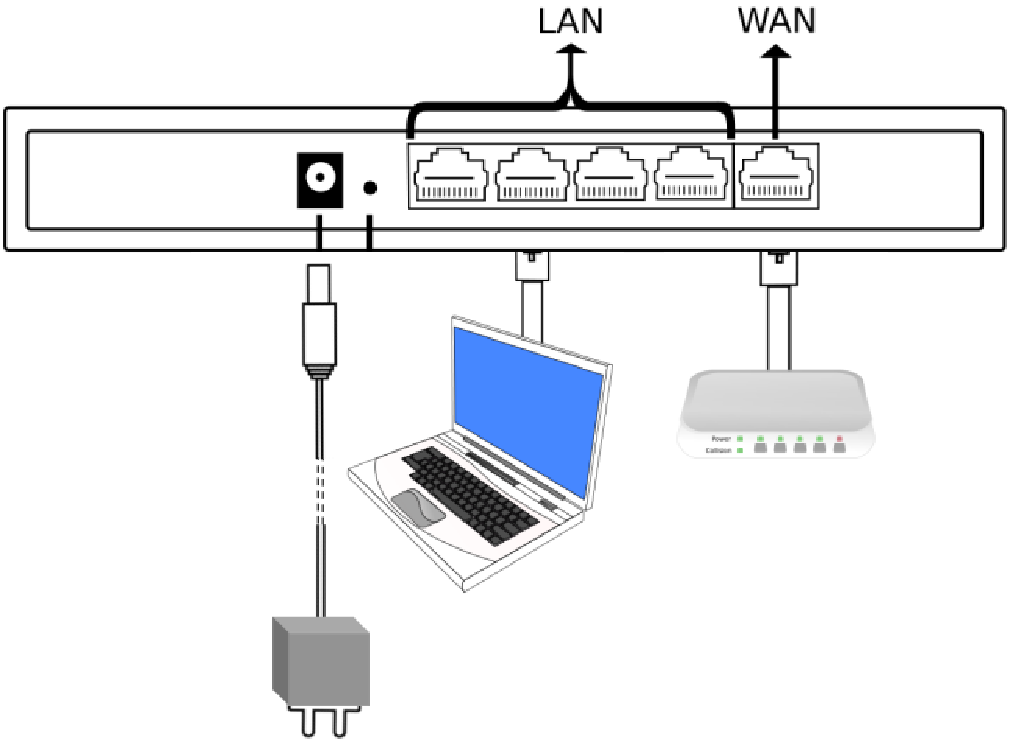




Connection Steps

1. Power on the GIS-R2 by connecting the power supply provided
2. Wait 30 seconds for the GIS unit to complete the boot process
3. Connect an Ethernet cable on the WAN port to your router
4. Connect an Ethernet cable on the LAN port and connect the other end to your computer/AP

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

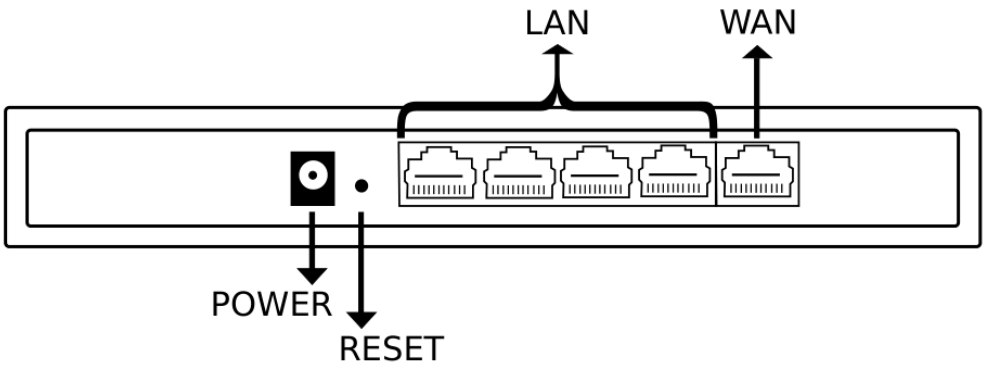
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

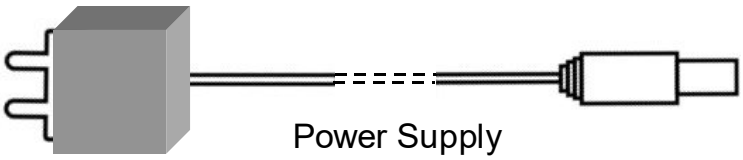
GIS-R4 Quickstart Guide

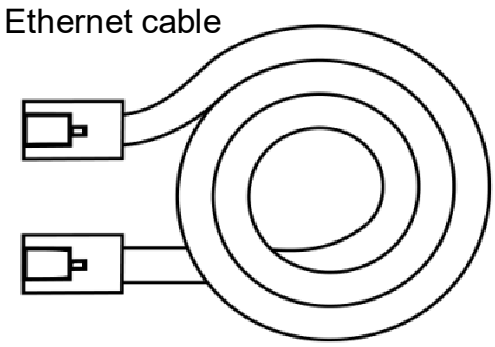
This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-R4 includes an external 12v 1A power supply.

The back of your GIS-R4 unit:



The necessary cables to setup your unit:

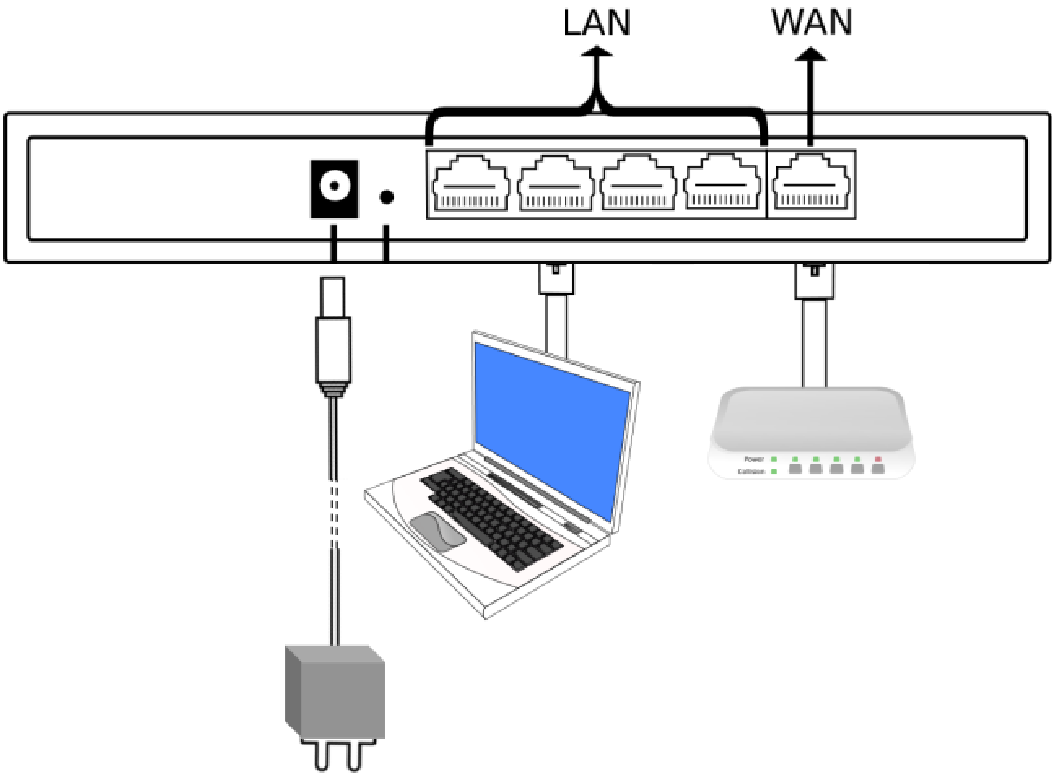




Connection Steps

1. Power up using the power supply provided
2. Connect an Internet cable on the LAN port and connect the other end to a computer/AP
3. Connect the Ethernet cable on the WAN port and the other end to a port of the router

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

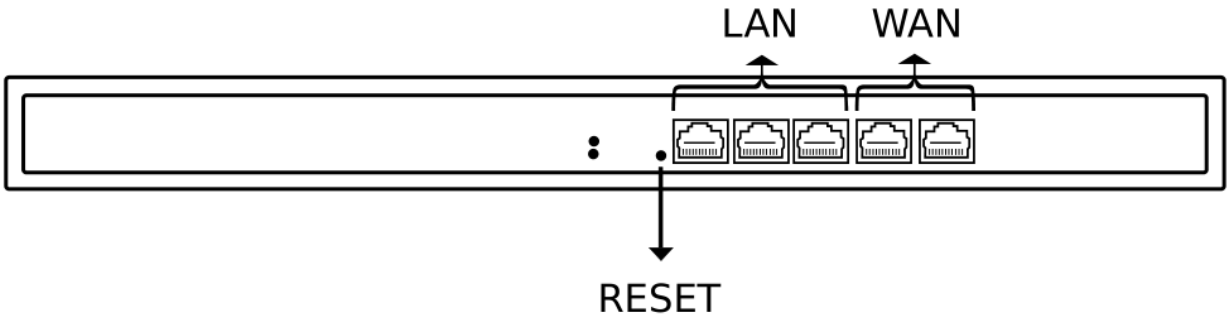
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

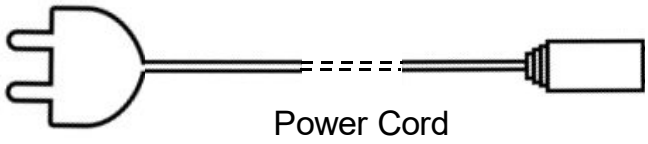
GIS-R6 Quickstart Guide

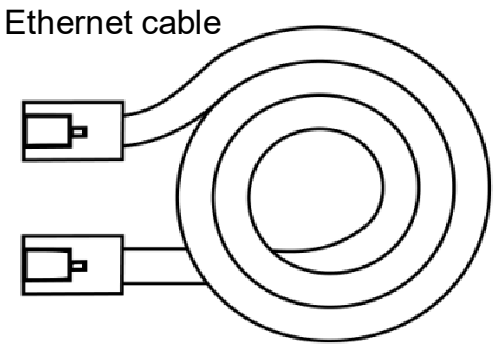
This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-R6 includes a power cord for a 110v-240v power connection.

The back of your GIS-R6 unit:



The necessary cables to setup your unit:

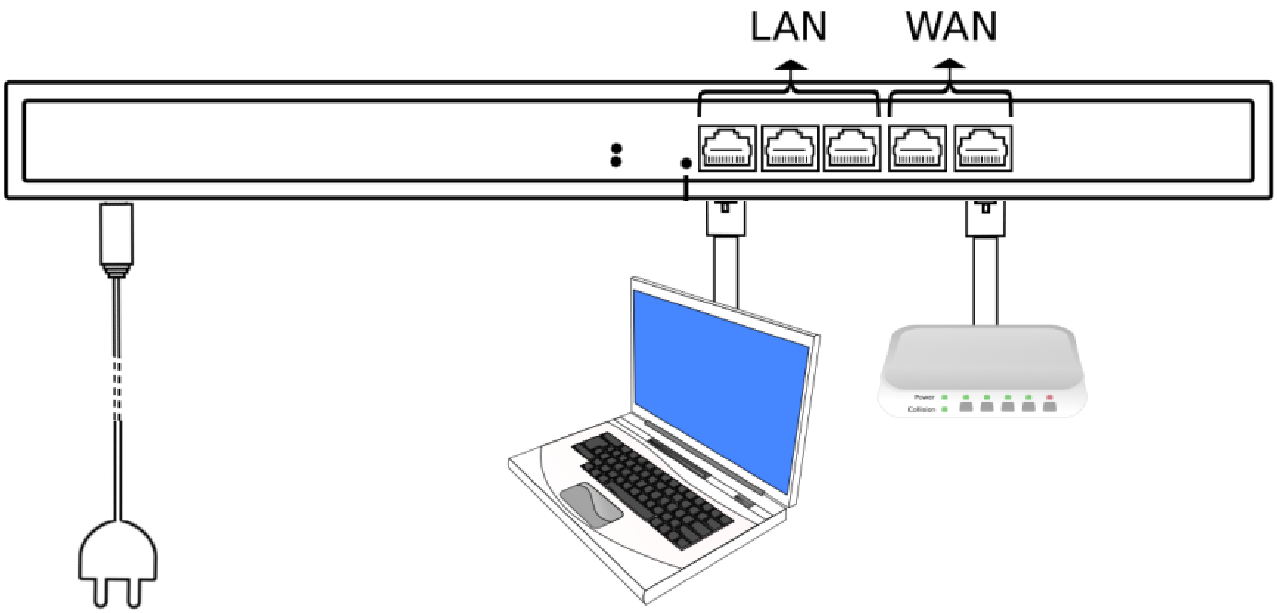




Connection Steps

1. Power up using the power supply provided
2. Connect an Internet cable on the LAN port and connect the other end to a computer/AP
3. Connect the Ethernet cable on the WAN port and the other end to a port of the router

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

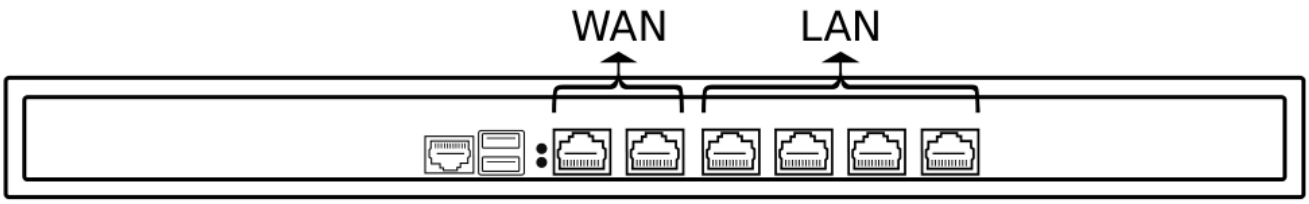
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

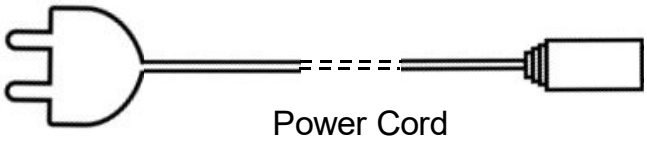
GIS-R10 Quickstart Guide

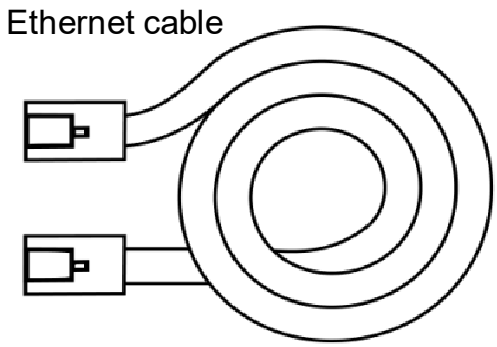
This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-R10 includes a power cord for a 110v-240v power connection.

The back of your GIS-R10 unit:



The necessary cables to setup your unit:

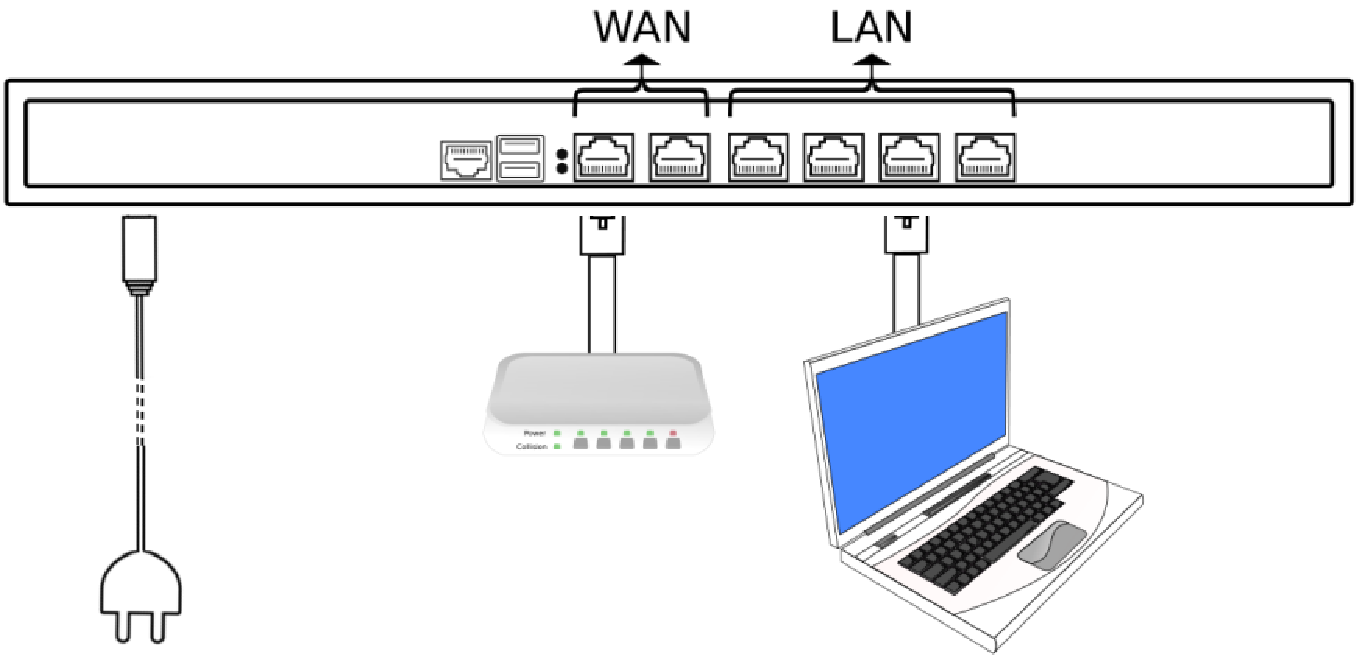




Connection Steps

1. Power up using the power supply provided
2. Connect an Internet cable on the LAN port and connect the other end to a computer/AP
3. Connect the Ethernet cable on the WAN port and the other end to a port of the router

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

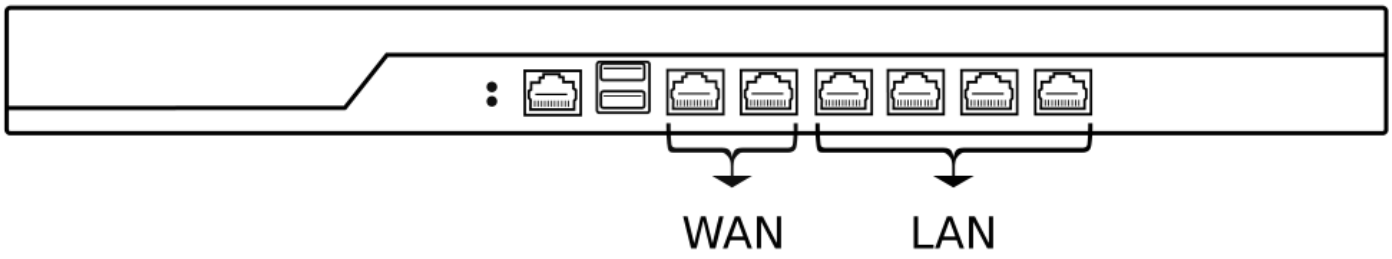
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

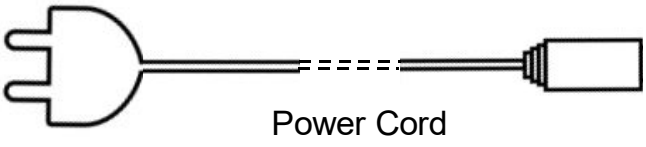
GIS-R20 Quickstart Guide

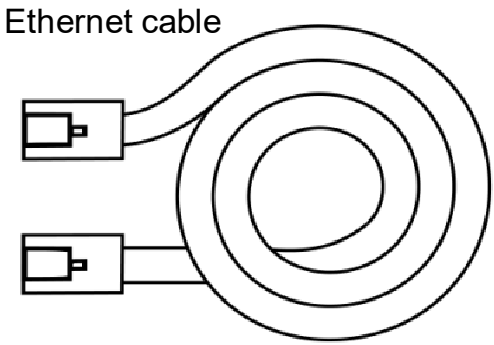
This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-R20 includes a power cord for a 110v-240v power connection.

The back of your GIS-R20 unit:



The necessary cables to setup your unit:

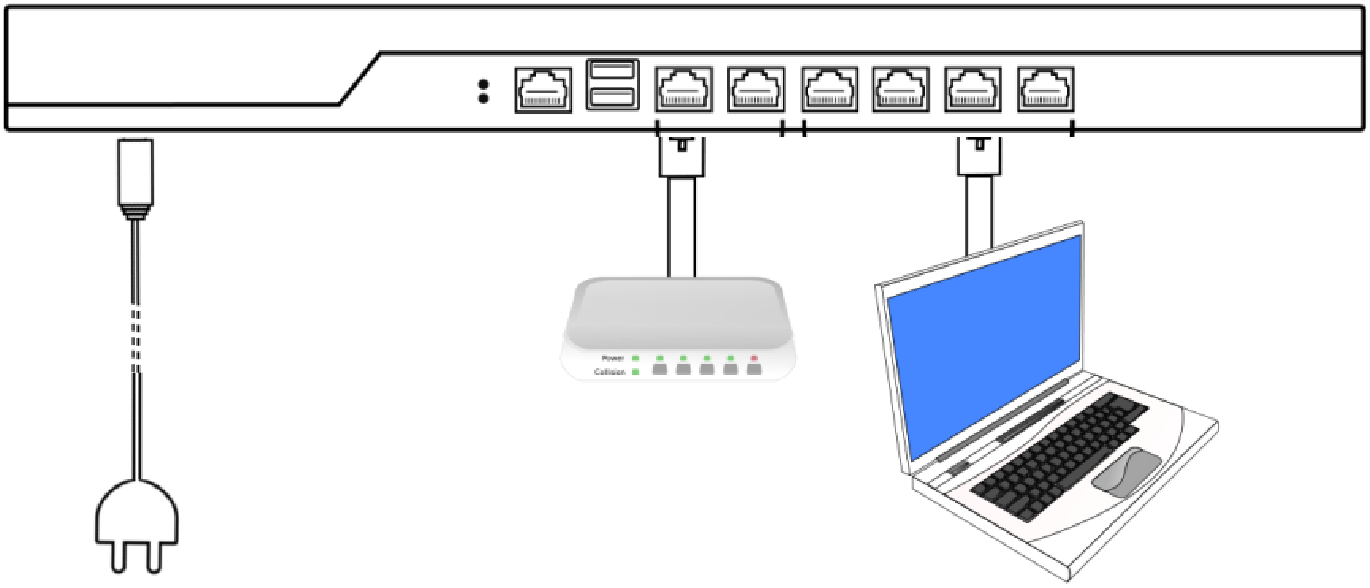




Connection Steps

1. Power up using the power supply provided
2. Connect an Internet cable on the LAN port and connect the other end to a computer/AP
3. Connect the Ethernet cable on the WAN port and the other end to a port of the router

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

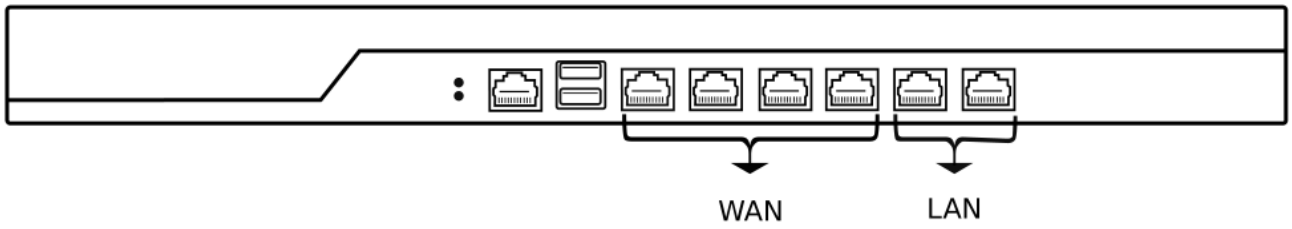
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

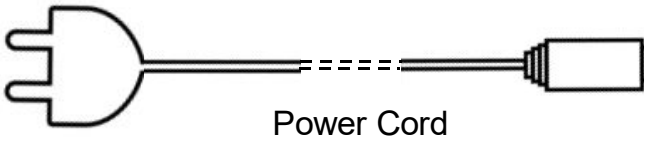
GIS-R40 Quickstart Guide

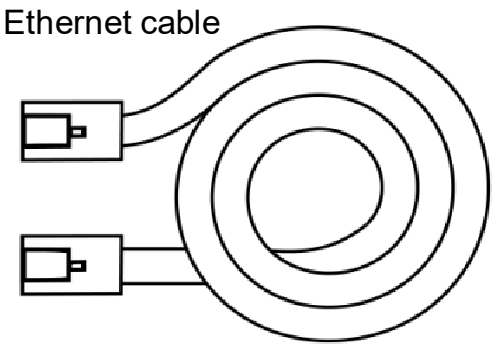
This guide will walk you through the initial installation and connection to your Guest Internet unit so that you can connect to the admin interface. The GIS-R40 includes a power cord for a 110v-240v power connection.

The back of your GIS-R40 unit:



The necessary cables to setup your unit:

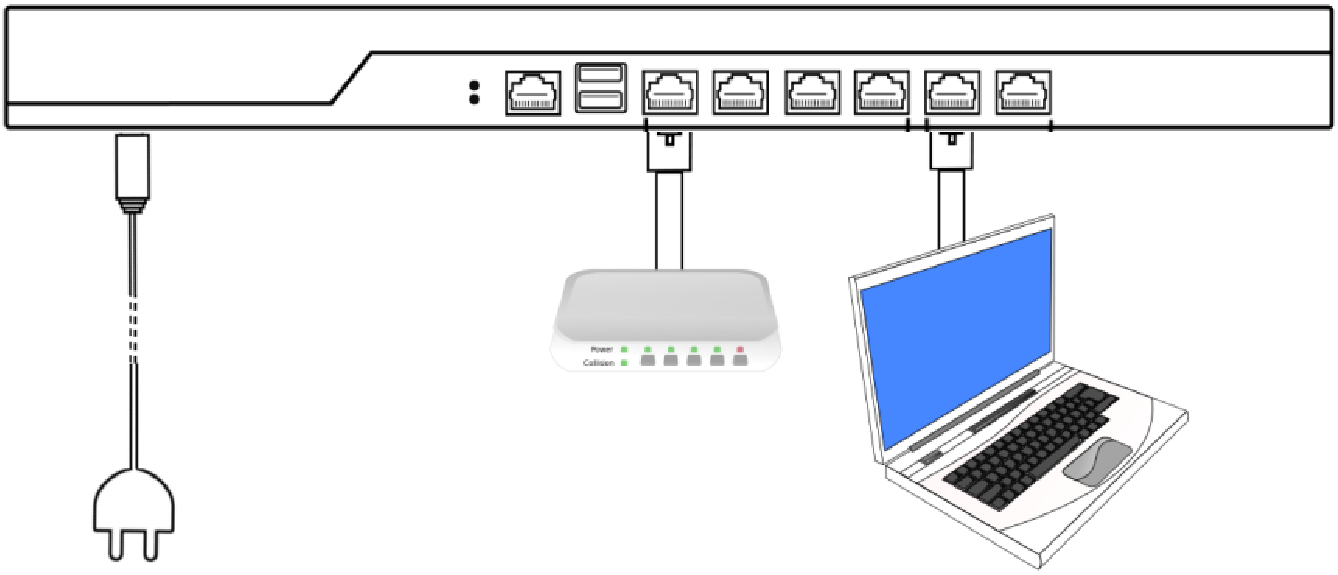




Connection Steps

1. Power up using the power supply provided
2. Connect an Internet cable on the LAN port and connect the other end to a computer/AP
3. Connect the Ethernet cable on the WAN port and the other end to a port of the router

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



- Open your browser at https://aplogin.com/admin
    - The next step to configure your GIS unit is to follow the wizards available here

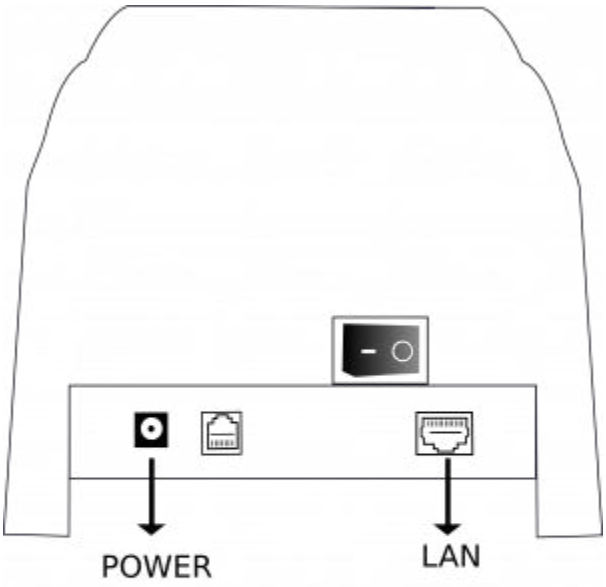
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

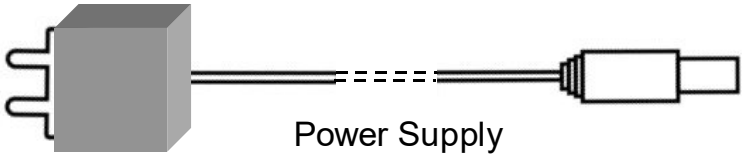
GIS-TP1 Quickstart Guide

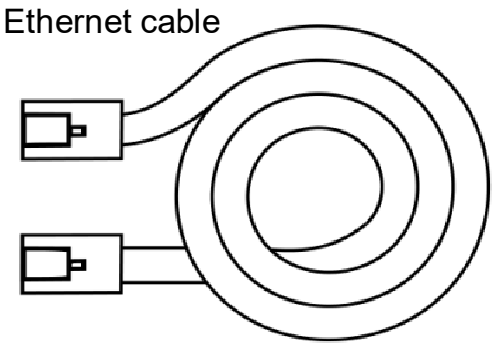
This guide will walk you through the initial installation and connection to your Guest Internet printer. The GIS-Tp1 includes an external power supply of 12v, 3A.

The back of your GIS-TP1 unit:



The necessary cables to setup your unit:

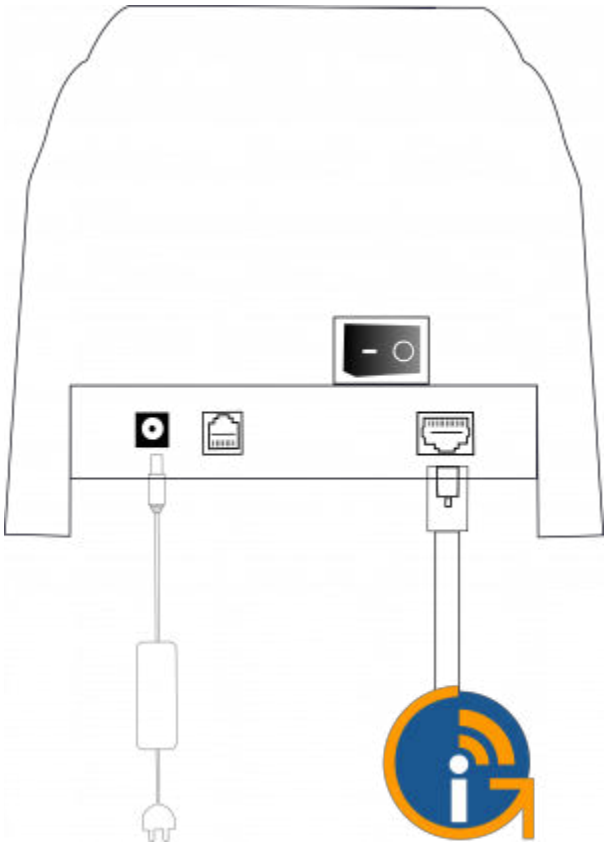




Connection Steps

1. Power up using the power supply provided
2. Connect an Internet cable on the LAN port and connect the other end to your GIS unit

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



Connect to GIS gateway LAN port

- Open your browser at https://aplogin.com/admin/printersetup.cgi
  - You can read more about printer setup here
  - You can read more about generating codes here

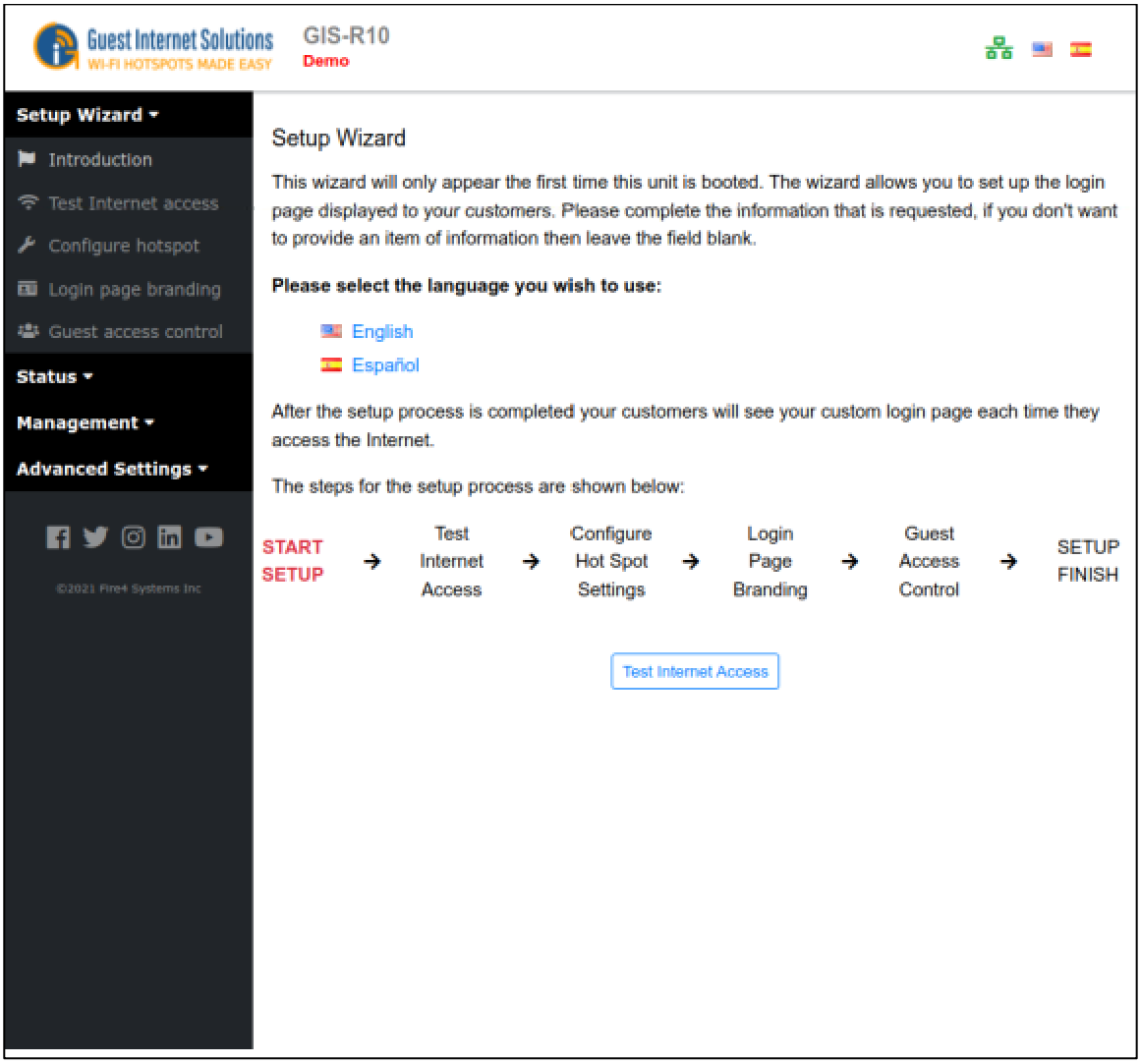
If you run into any issue with the installation of your unit please contact us.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Wizard

When your computer is connected to the GIS unit for the first time, you need to start the setup process.

To complete the setup process you will need to open your web browser, you may be automatically redirected to the GIS unit wizard if not please go to http://aplogin.com



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The setup process has four steps:

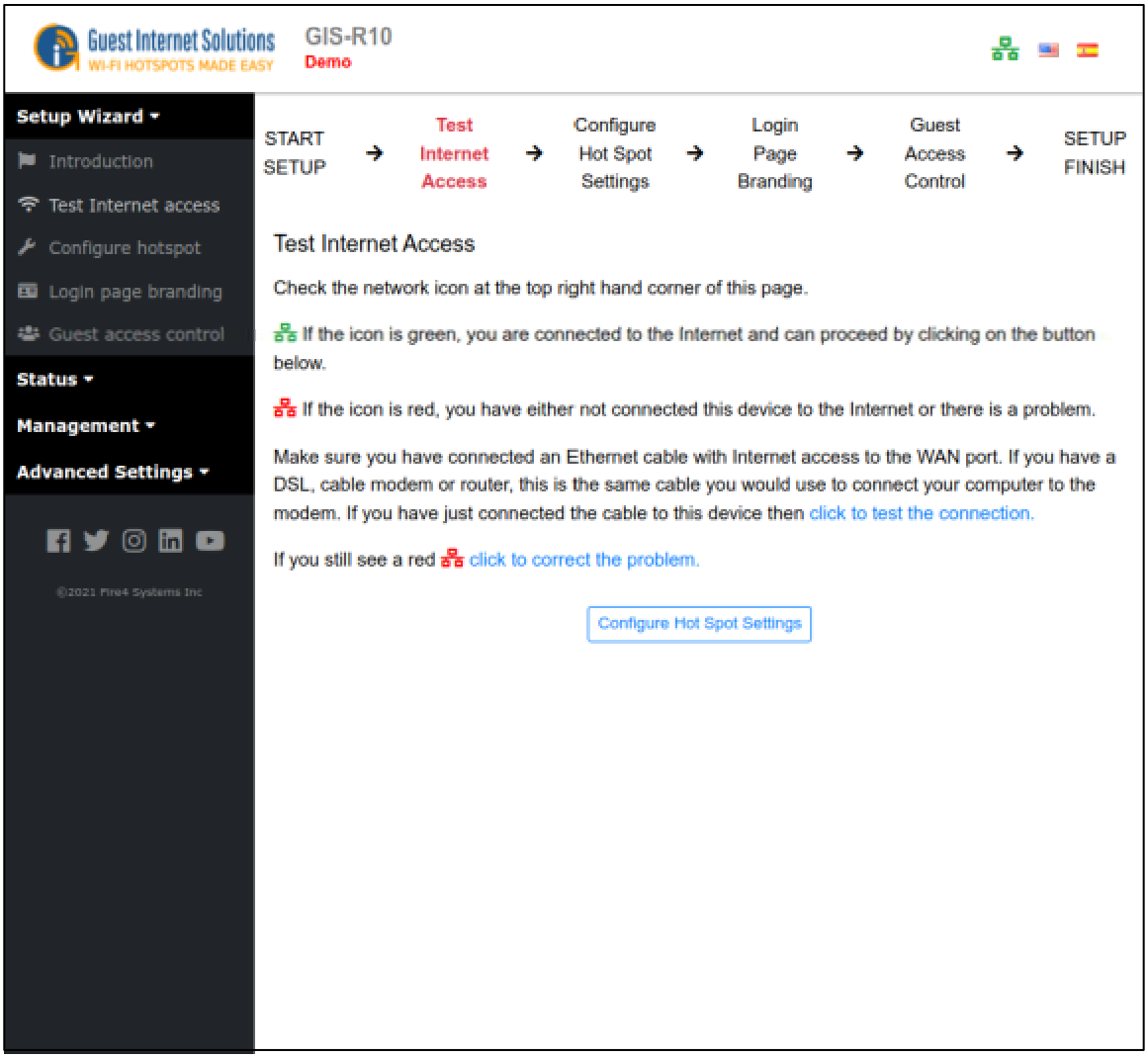
Step 1

The TEST INTERNET ACCESS setup page verifies that your Guest Internet gateway product is connected to the Internet. The setup process cannot be completed without an Internet connection.

To check if you have an internet connection look on the top right hand corner of the browser window:

You will see a green **YES** or a red **NO**.

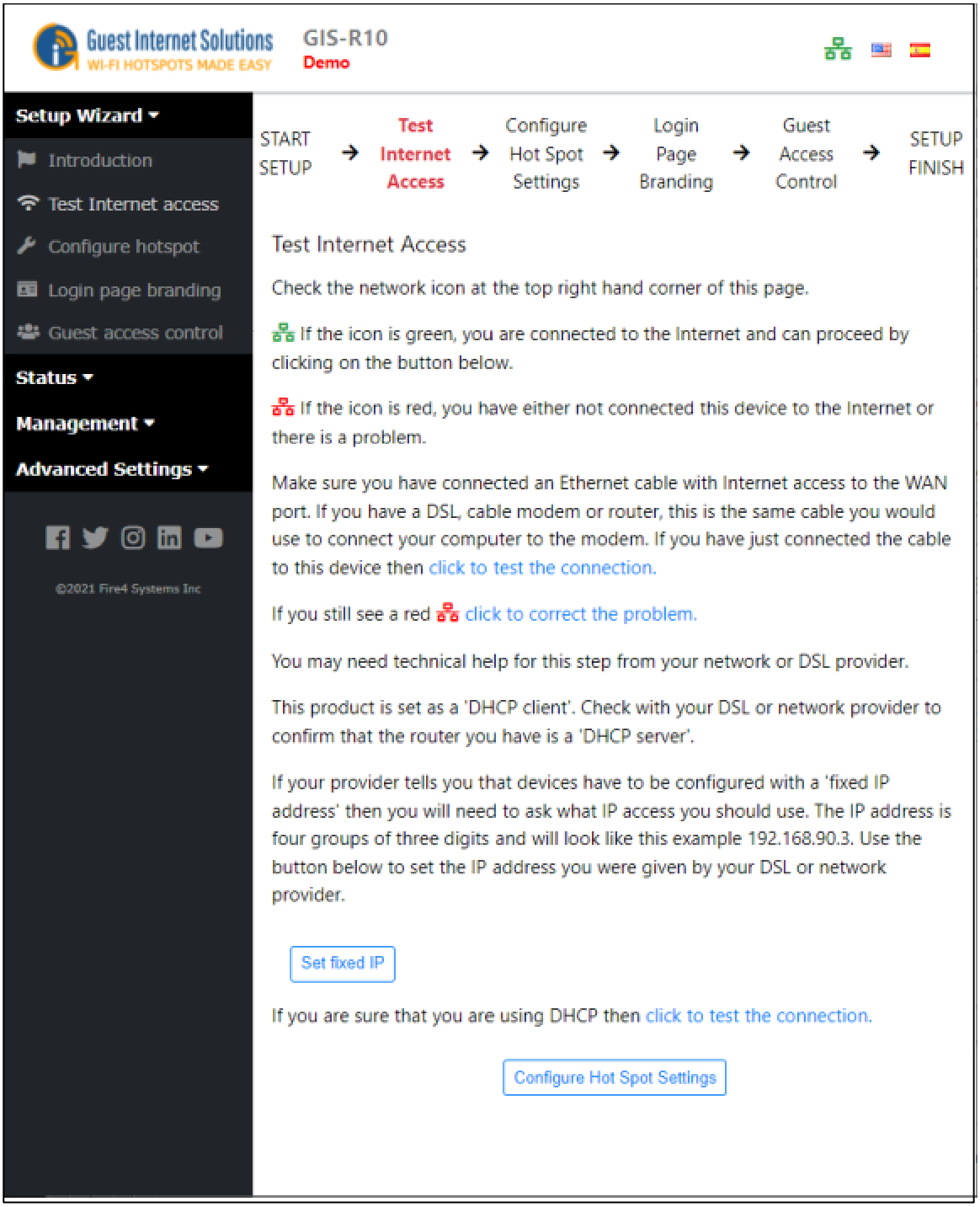
If you have a green **YES** then your product is connected to the Internet and you can proceed to the next page by clicking on the button ‘Continue to Step 2’.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

If you see a red **NO** then you have a connection problem. To resolve try the following steps:

- First verify that your modem/router provides a good Internet connection by connecting a computer directly to the modem/router using an Ethernet cable.
- Next verify that the Guest Internet product is connected to modem/router and then click on ‘click to test the Internet connection’.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

- If the Internet status still shows a red **NO** then click on ‘click to correct this problem’.
- Verify that your router is a ‘DHCP server’. Click on the link ‘click to attempt an IP address’. If you require a static IP address for your Internet connection you can do this by clicking 'click to correct the problem'.
- If you still have a red NO after trying the steps described please contact Guest Internet support.

Step 2

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.

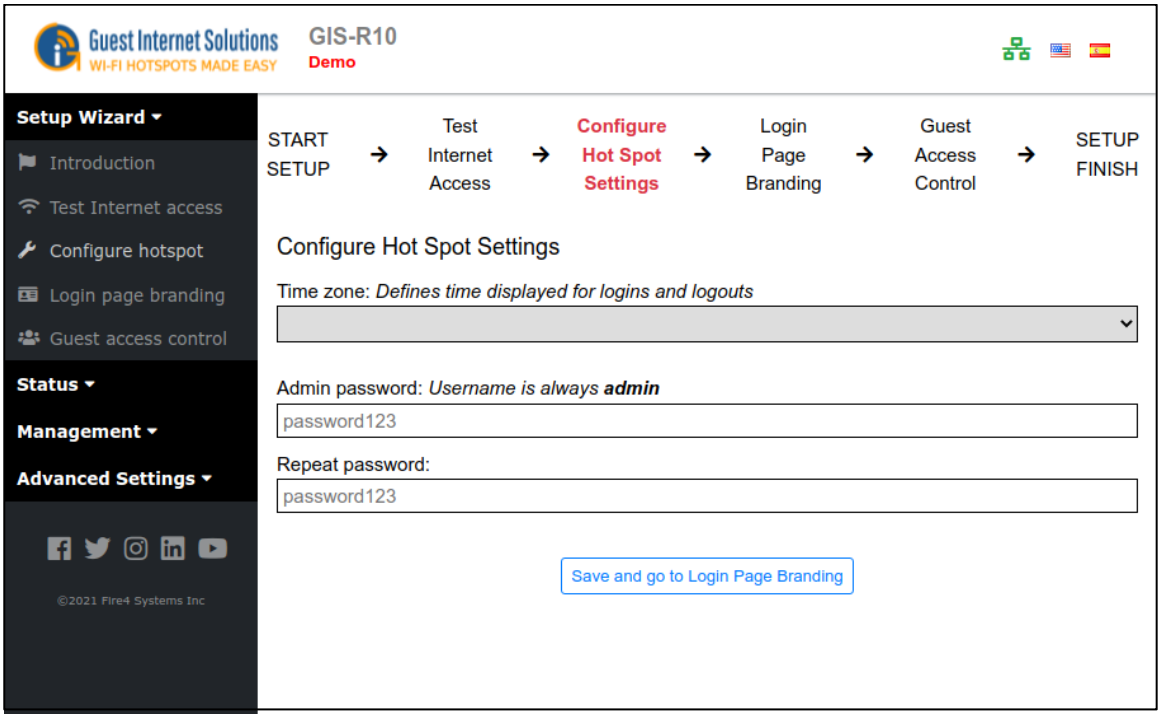
The GIS-gateway has no default administrator password. The administrator access password must be entered in the box.

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.

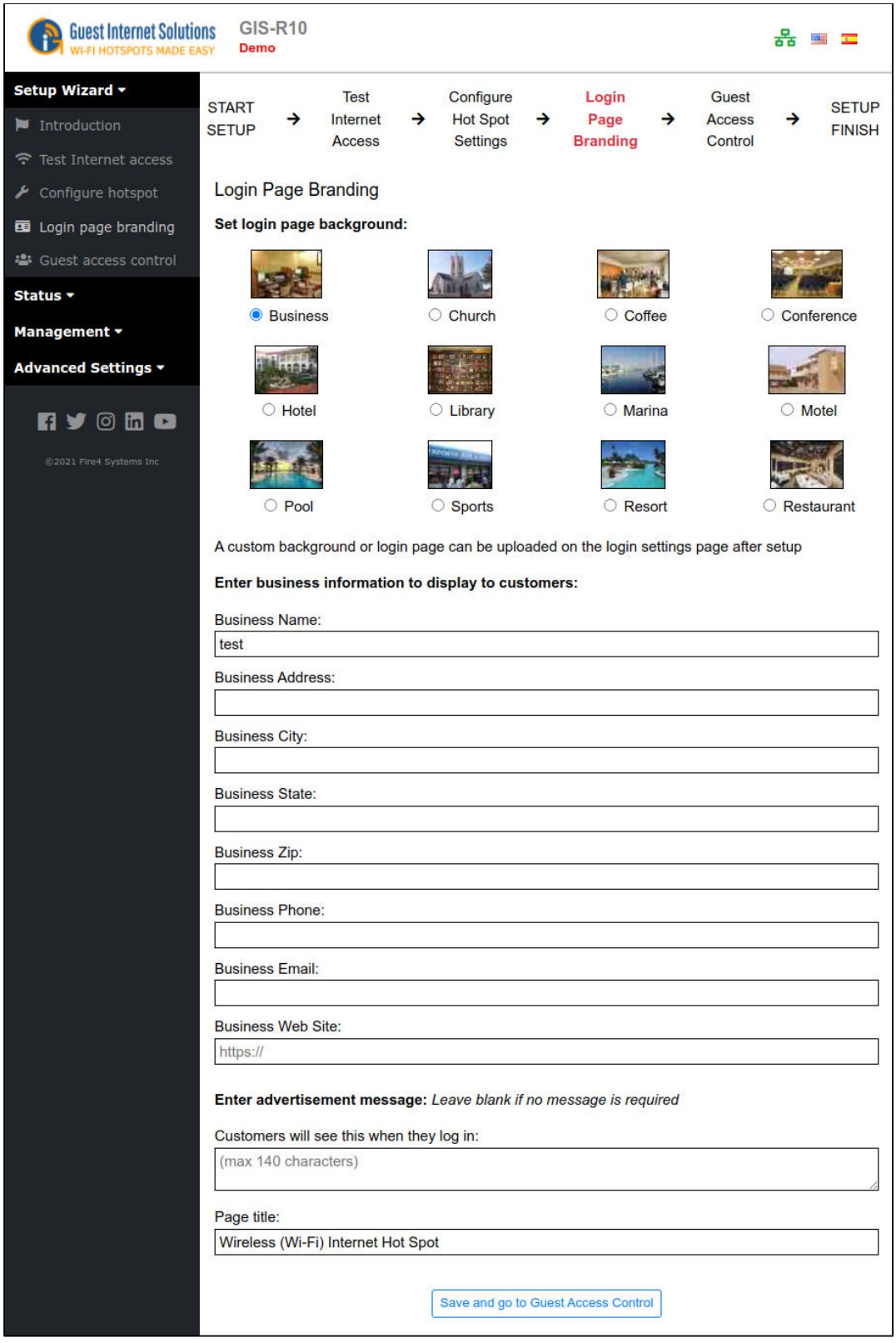
When you have completed this step click on the button to proceed to step 3.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Step 3

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.



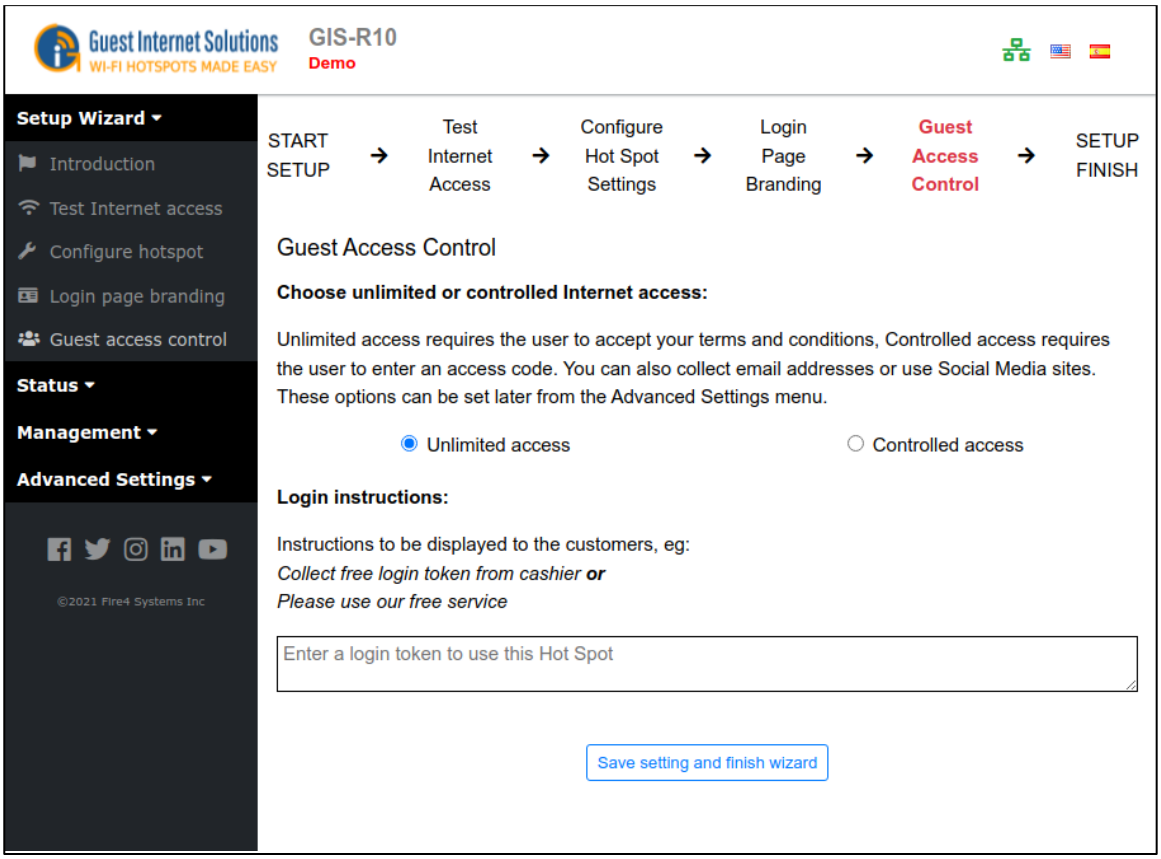
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

You can use one of our twelve Login pages, upload an image with your branding for the background or create a new Login page with HTML, CSS and JavaScript.

The types of Login Page are explained in details in the Custom Login Pages section.

Step 4

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.

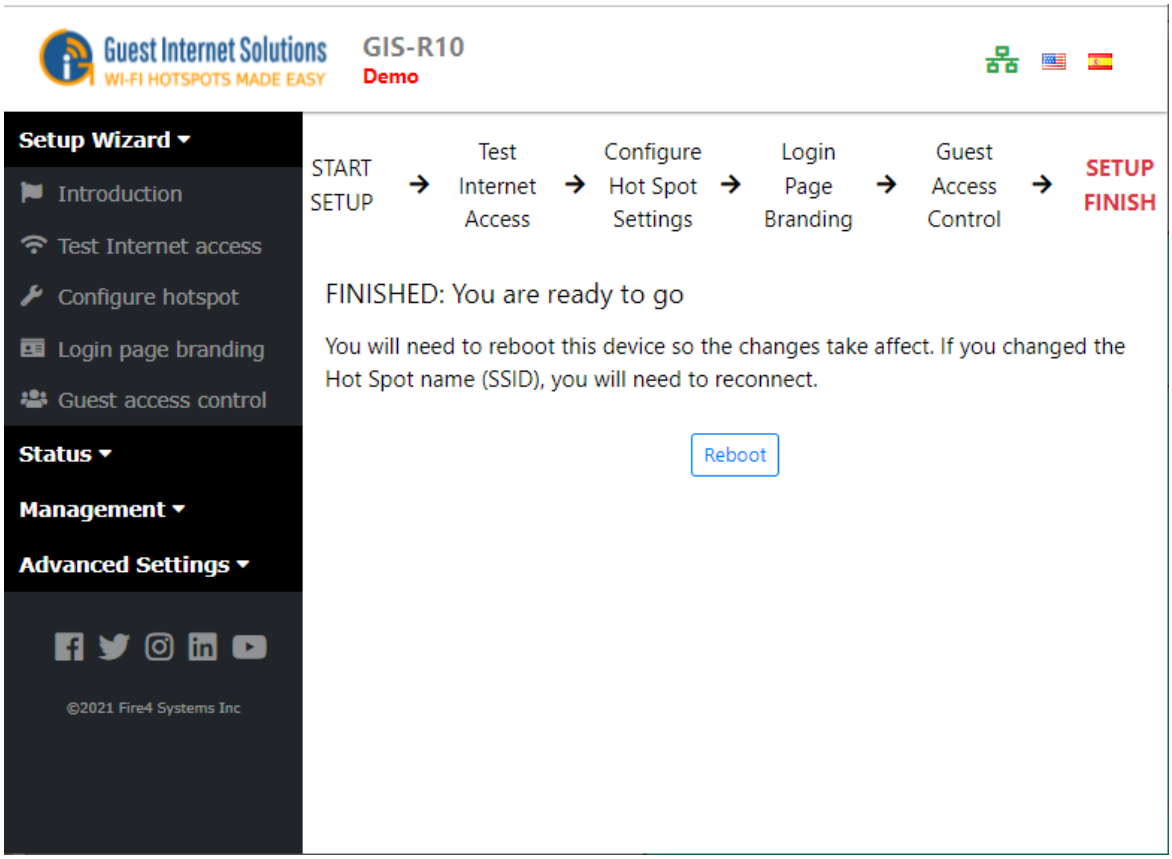
The choice you make here is determined by the way that you want to offer your Internet service for your guests. You can read more about Login Page Type by clicking here.

It is also necessary to type a message that tells your customer how to proceed to get Internet access. Explained in Login Messages.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

When completed click on the *save settings and finish wizard* button, you then need to *reboot* the Guest Internet gateway unit.

This will restart the gateway unit with all the parameters that were entered during the setup process.



When the setup process is completed your personalized wireless Internet service will be ready for your guests to start using.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Admin Interface

This section will guide you through all of the setup options and various configurations supported within the Guest Internet Products Admin console.

The Admin console on the GIS unit is broken up into 3 main sections:

- Status
- Management
- Advanced

Within the Status section you are able to view the current activity of the unit and the users connected.

Within the management section you can modify the core settings of the GIS unit as well as create access codes for guest users.

The advanced section consists of the remaining configuration options of the GIS unit; these options give a lot of control to the GIS unit but are unlikly to be changed very often and are more technically complex.

Status

The Status section shows information on the status of the product:

System Information

Connected Users

Usage Reports

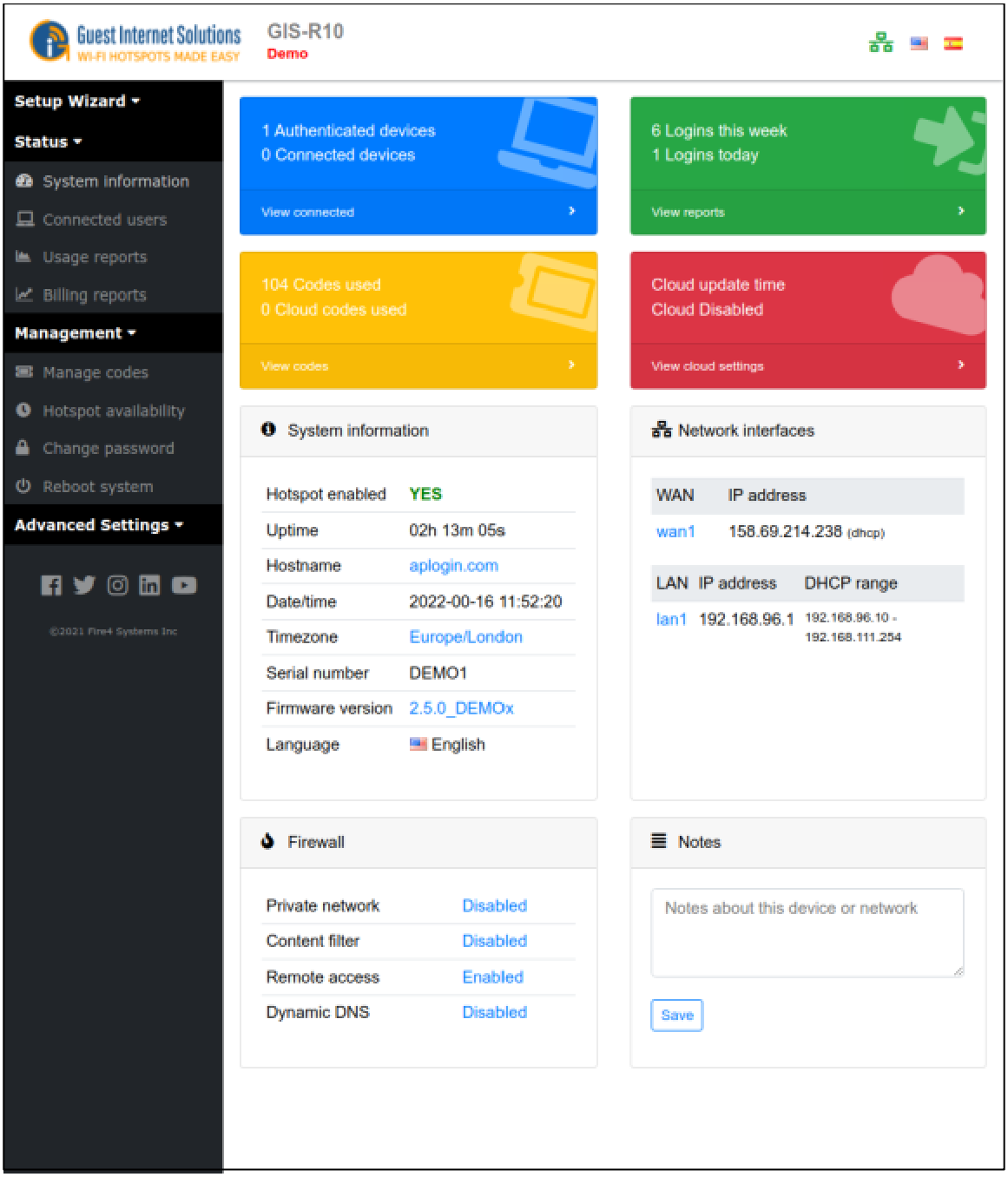
Billing Reports

System Information

The System Information section displays:

- Uptime - The time since the unit was rebooted
- Hostname
- Current date and time and timezone
- Firmware version (required for Firmware Upgrades)
- Serial number (required for Firmware Upgrades and Cloud Management)
- Verification that the device is connected to the Internet
- 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

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

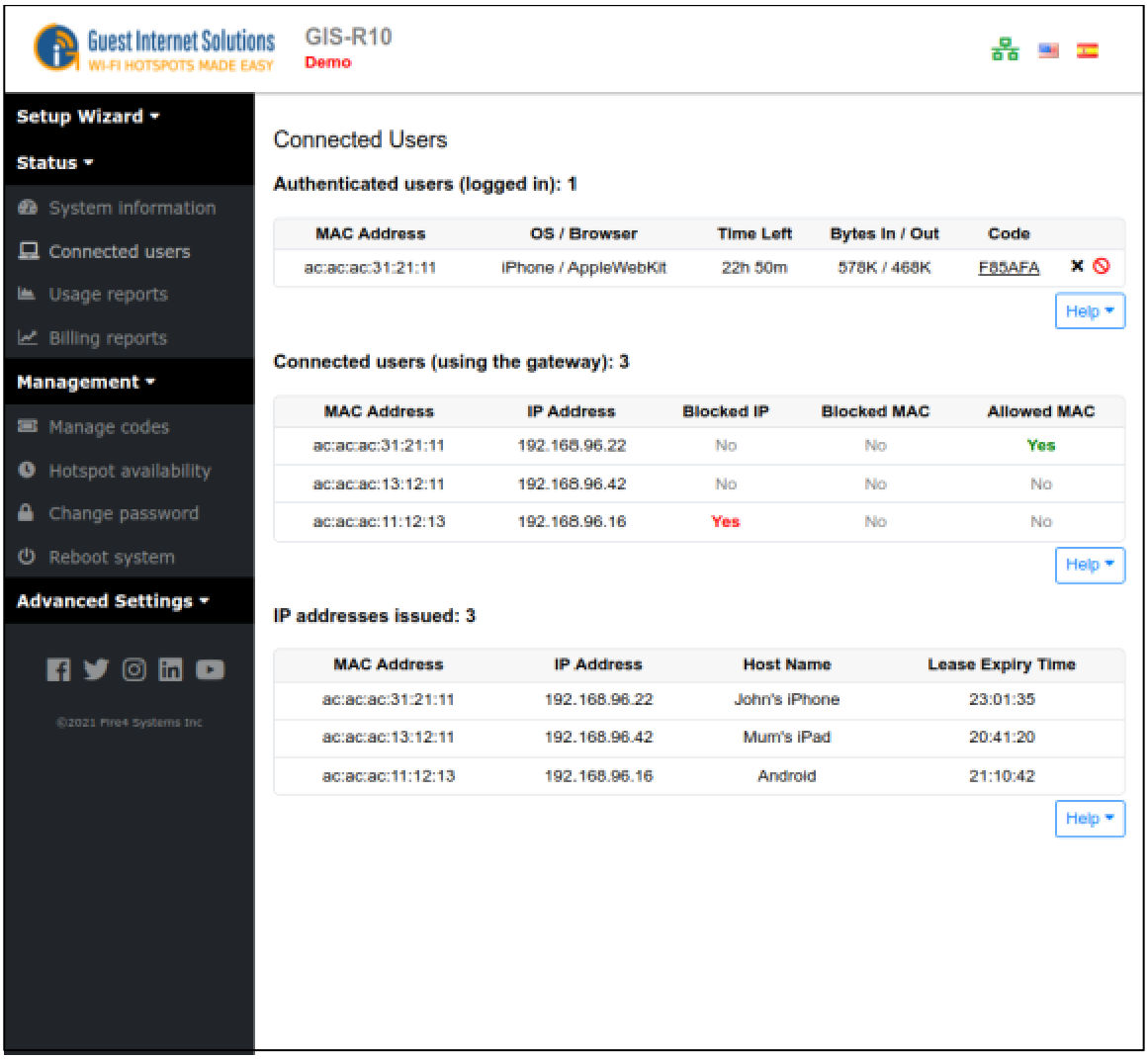


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Connected Users

There are three "boxes" on the Connected Users section.

1. Authenticated users (logged in): shows all the guests that have provided a valid access code (controlled access mode) or clicked on the disclaimer agreement button (unlimited access mode).
2. Connected users (using the gateway): lists all the computers that are connected to the gateway unit: they have requested and obtained an IP address.
3. IP addresses issued: this list is provided to show network usage not logins or Internet usage. Devices may connect and get an IP address but not attempt to use the Internet.



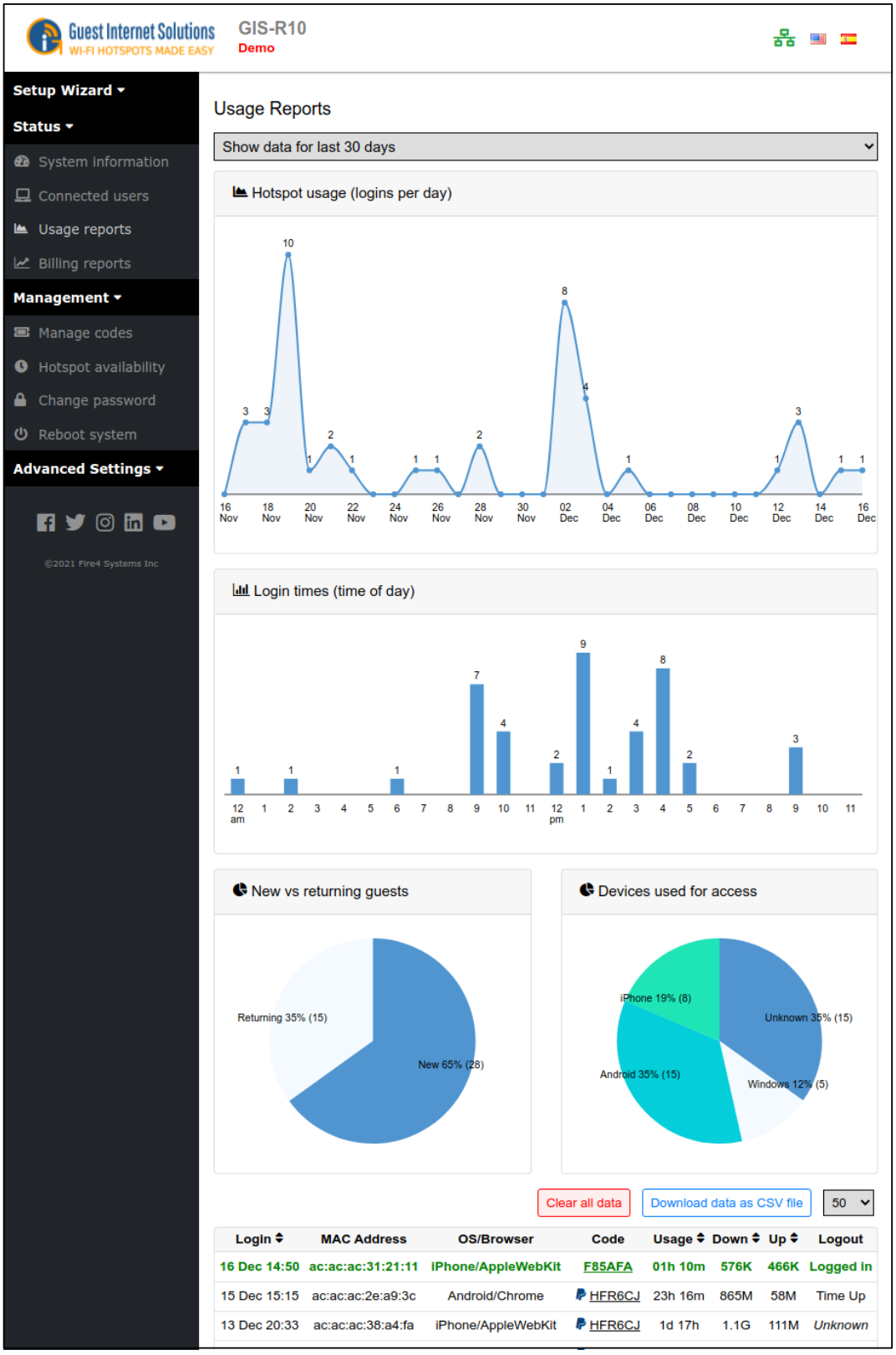
In the authenticated users box, if you click on the blue ‘X’ in the right hand column will disconnect that authenticated user.

If you click 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.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Usage Reports

Usage reports displays and stores the last 10,000 entries. The number of users per day is shown on the top graph that can extend up to 28 days in duration.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The data table has seven parameters for each entry: Login time;

- MAC address;
- Access code used;
- Time connected;
- Downloaded data volume;
- Uploaded data volume;
- Logout reasons.

The usage data can be downloaded in a CSV format and loaded into a spreadsheet program for further analysis.

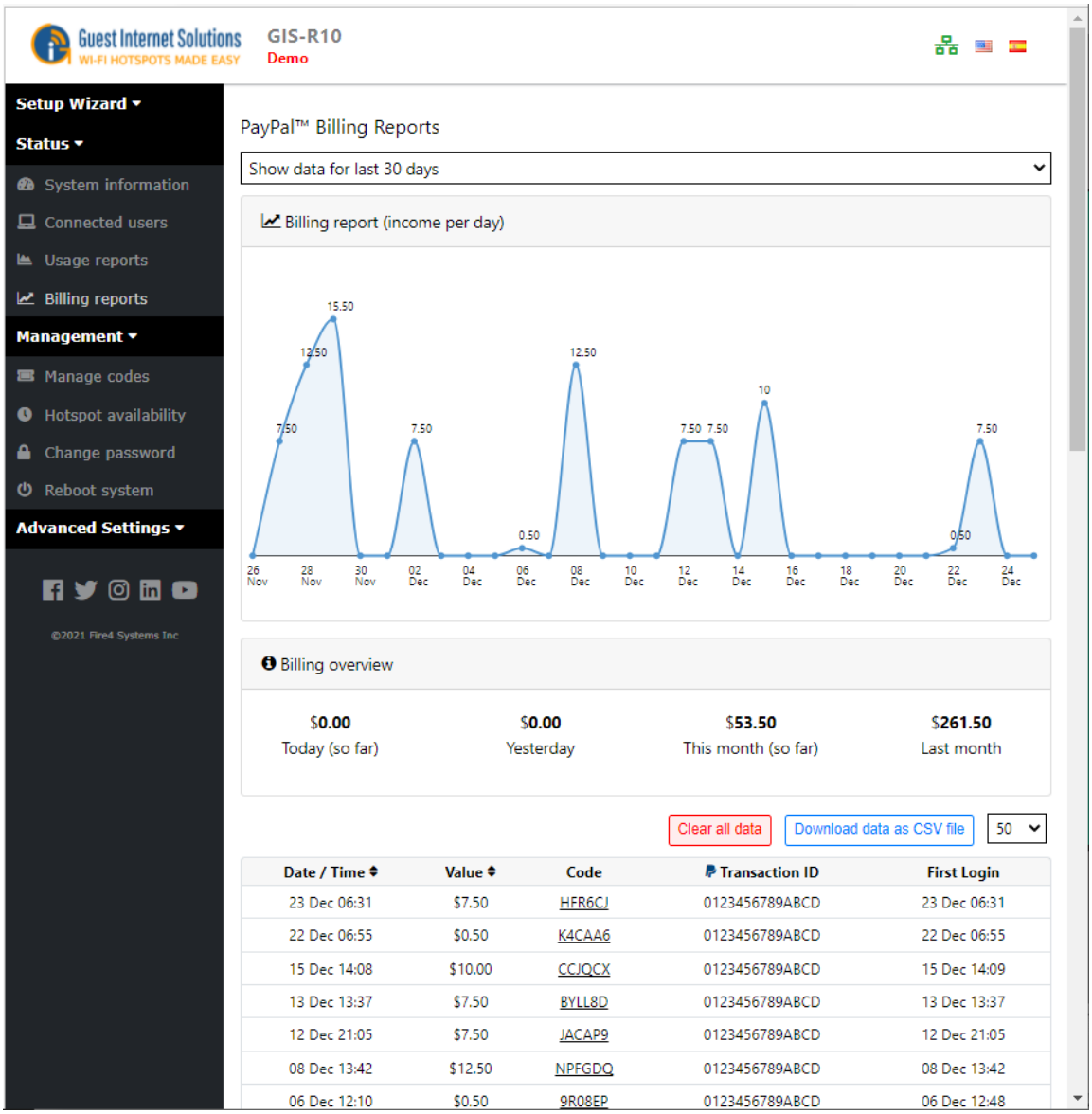
Logout Reasons

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

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Billing Reports

The GIS gateway stores a transaction report summary in the section Billing Report.
This report can be downloaded in CSV format and loaded into a spreadsheet program.



Management

Management functions are used to administer your Guest Internet unit:

Access Code Management

Hotspot Availability

Change Password

Reboot

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Management

Access Code Management

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.

Access Code Management is divided in three:

Login Code Type

Code Management

Codes Page

Login Code Type

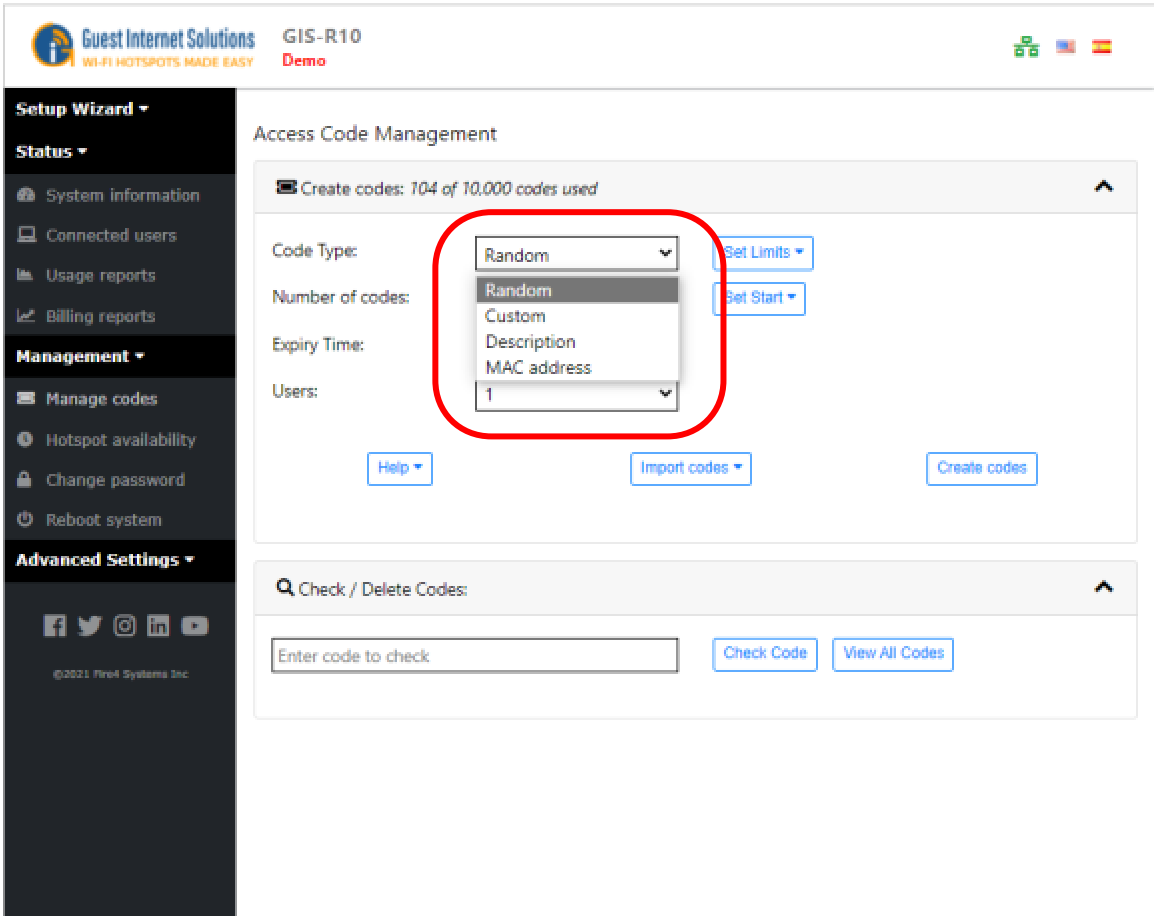
There are four Login Code Types:

Random

Custom

Description

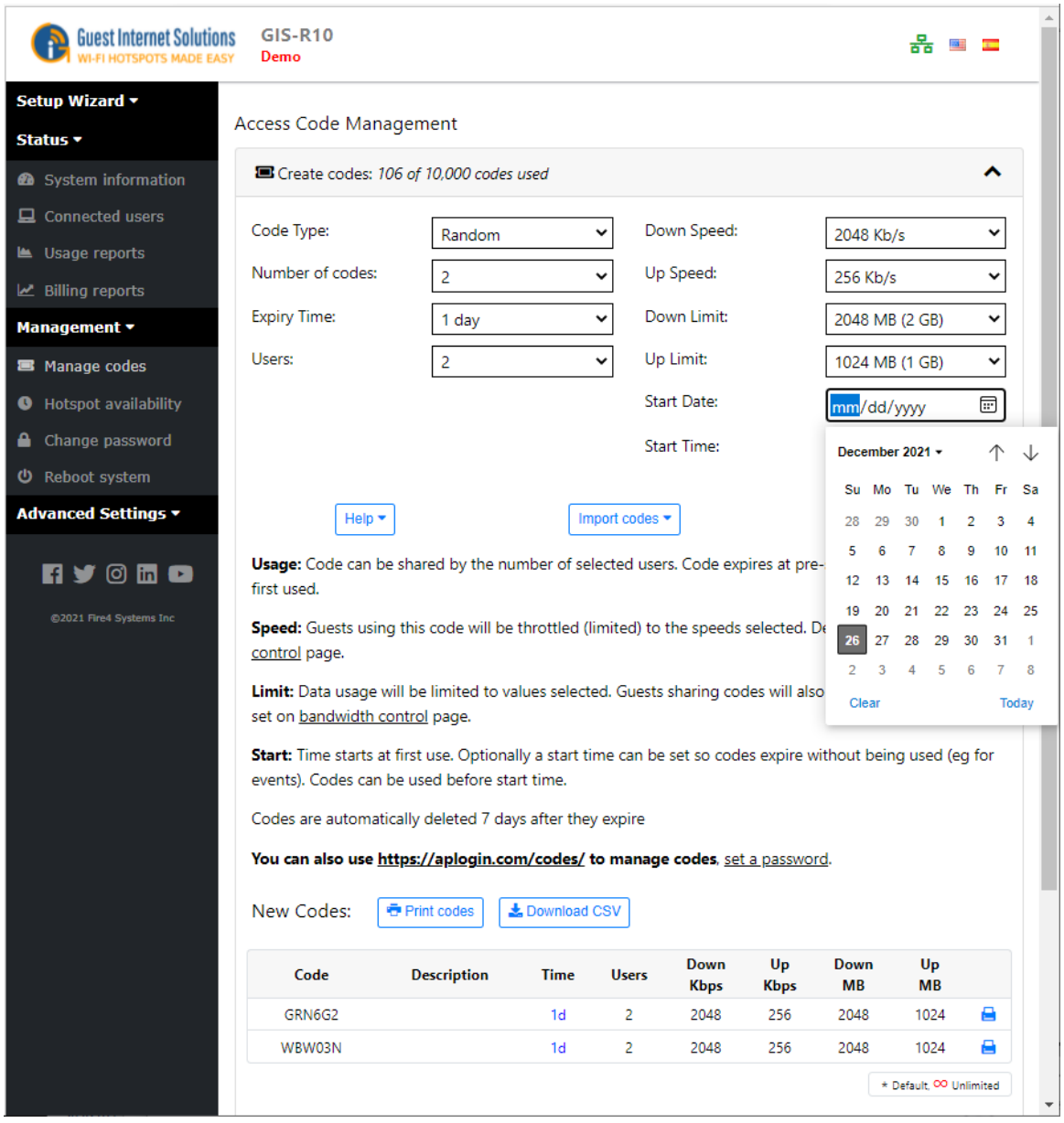
MAC Address



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Random Code

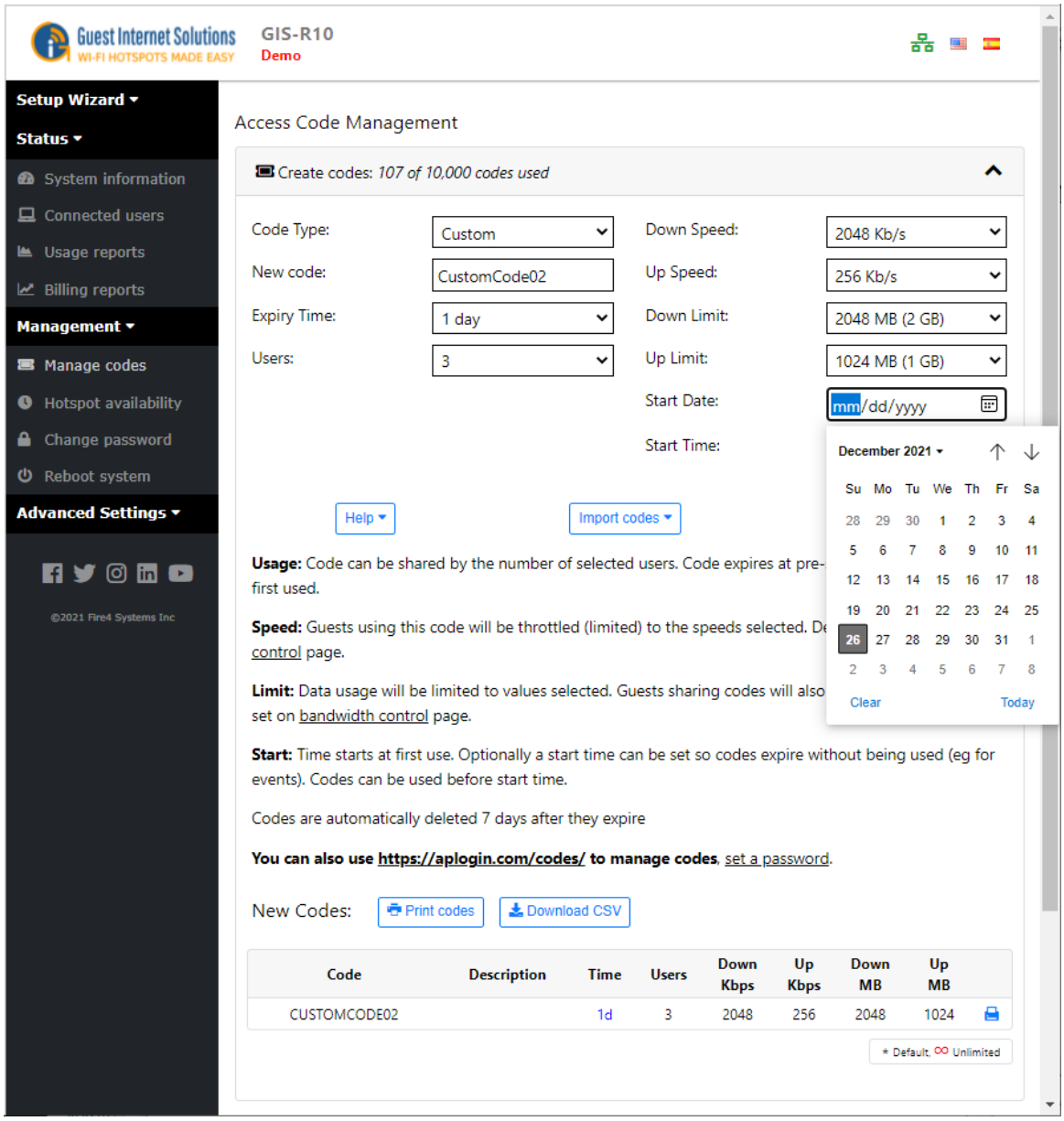
When the Random Login Code Type is selected, the unit will automatically generate a unique 6-character code. While an Access code is being created, you can set limits to each code or all of them.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Custom Code

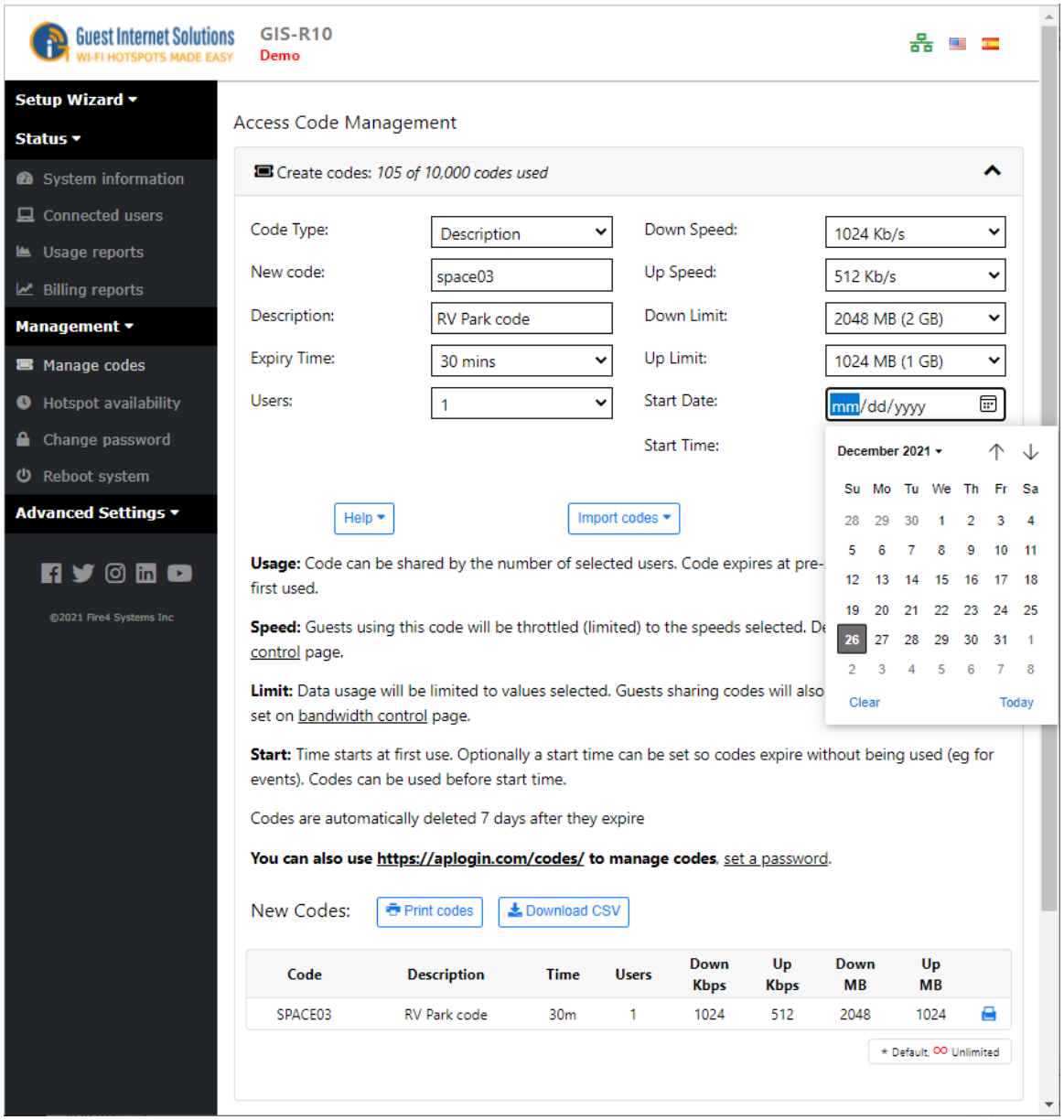
When the Custom Login Code Type is selected, you can create your code, the length limit is 10 characters with alphanumeric only characters, no space or symbol characters.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Description Code

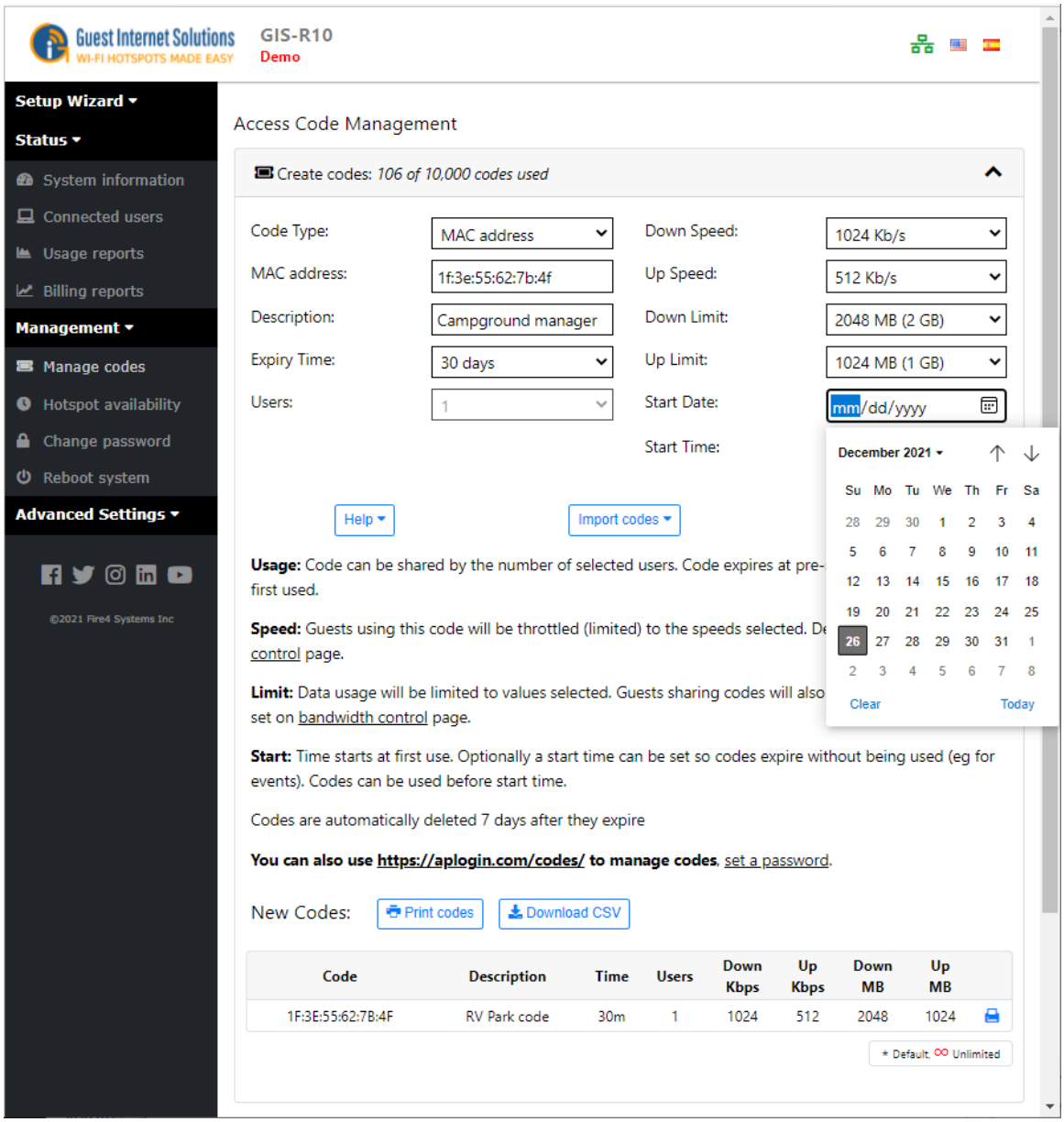
When the Description Login Code Type is selected, you can write a description for a specified code.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

MAC Code

When the MAC Login Code Type is selected, you can manually enter a devices MAC address. This device will then automatically be allowed on the Internet once connected.

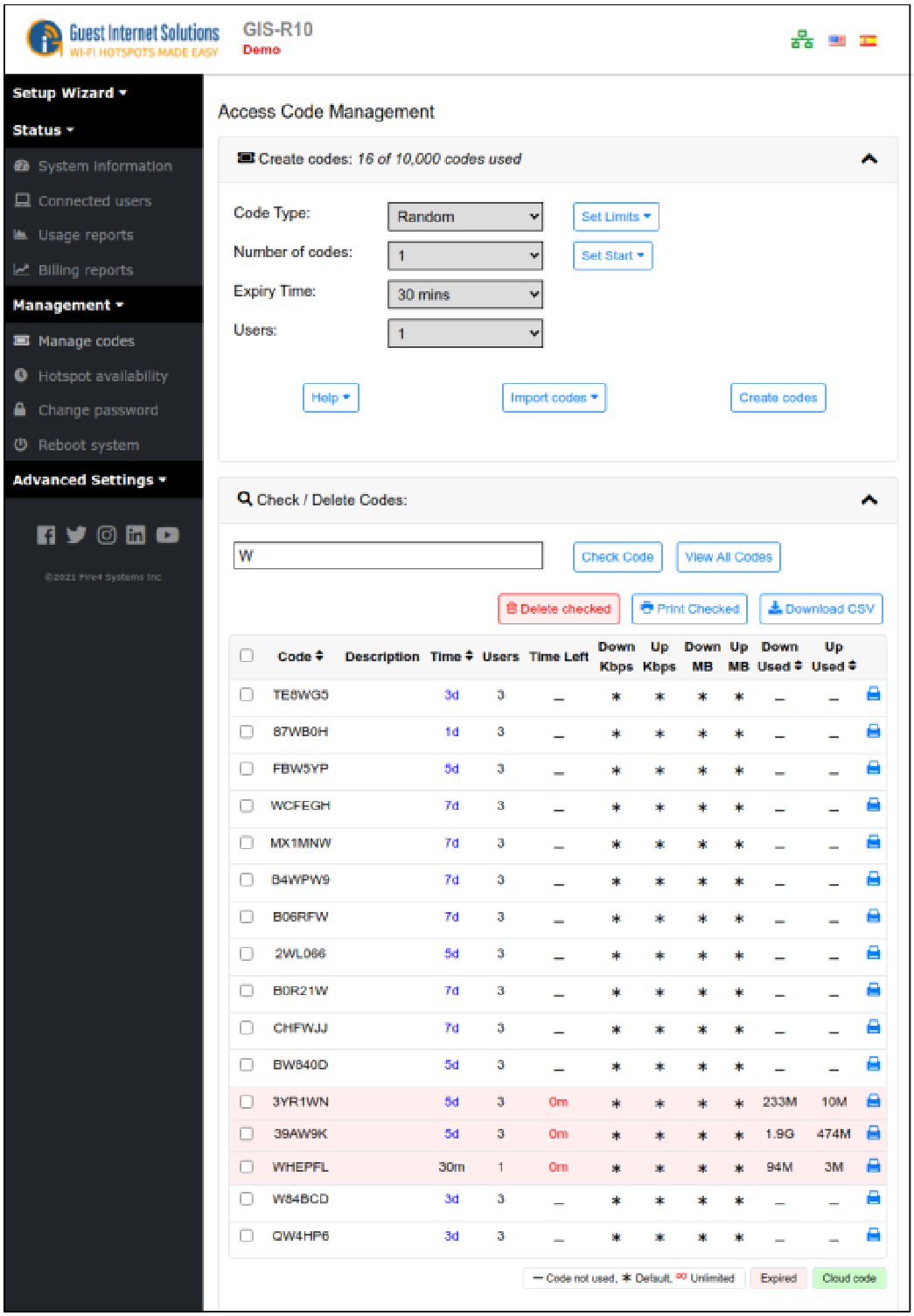


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Find/Delete Codes

After the creation of the code, you have an easy way to find and/or delete codes, you can also download/upload a list with all the codes in CSV.

You can click "View All Codes" to check all the codes being used, or type the code you want to check and click "Find Code". If you want to delete a code that is not in use any more or manage the codes being used (check the limits a user still have available), at the end of the "Manage Codes" section, there is a box "Find/Delete Codes".



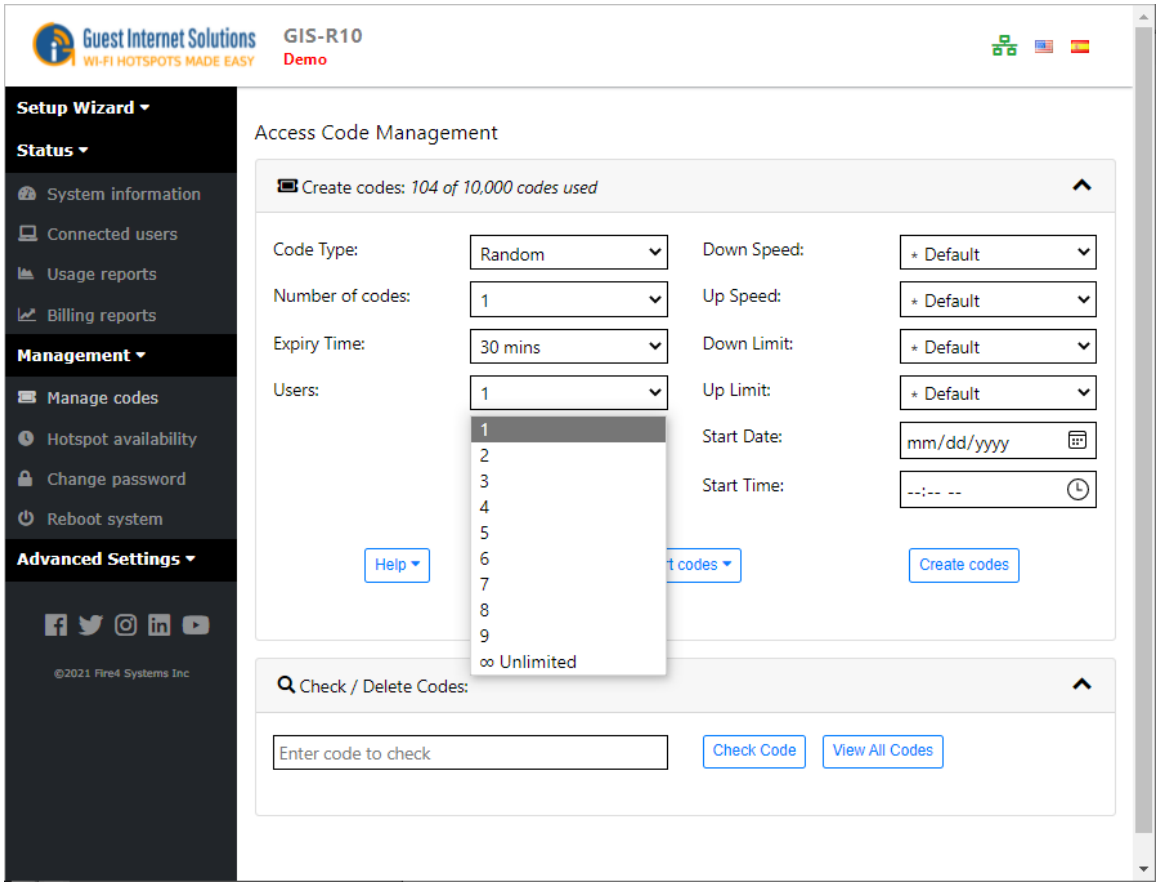
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Code Limits

There are six limits that can be established for the codes you create:

Usage

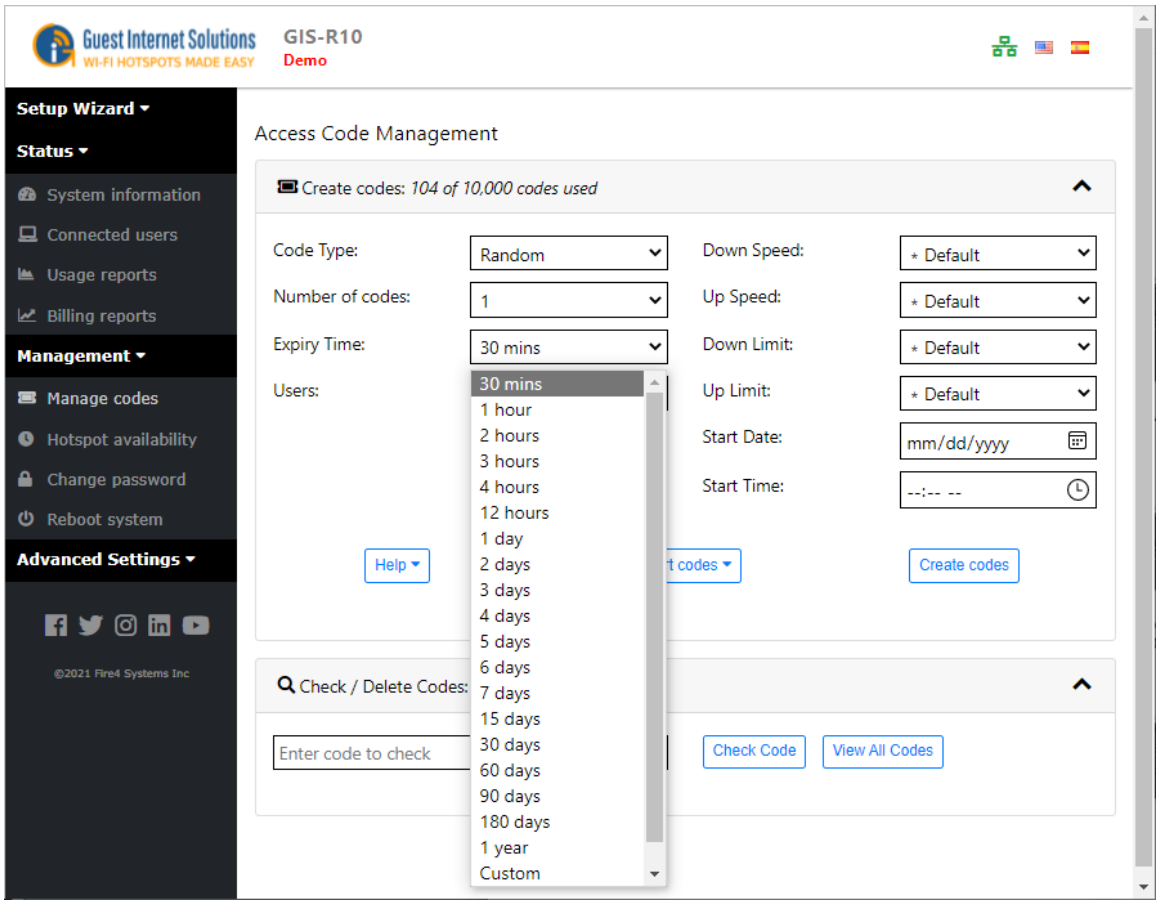
The "usage" option limits how many users can have Internet access using the same code.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Duration

The "Expire Time" option limits how the user(s) will have Internet access using a code. Different codes can have different time limit.

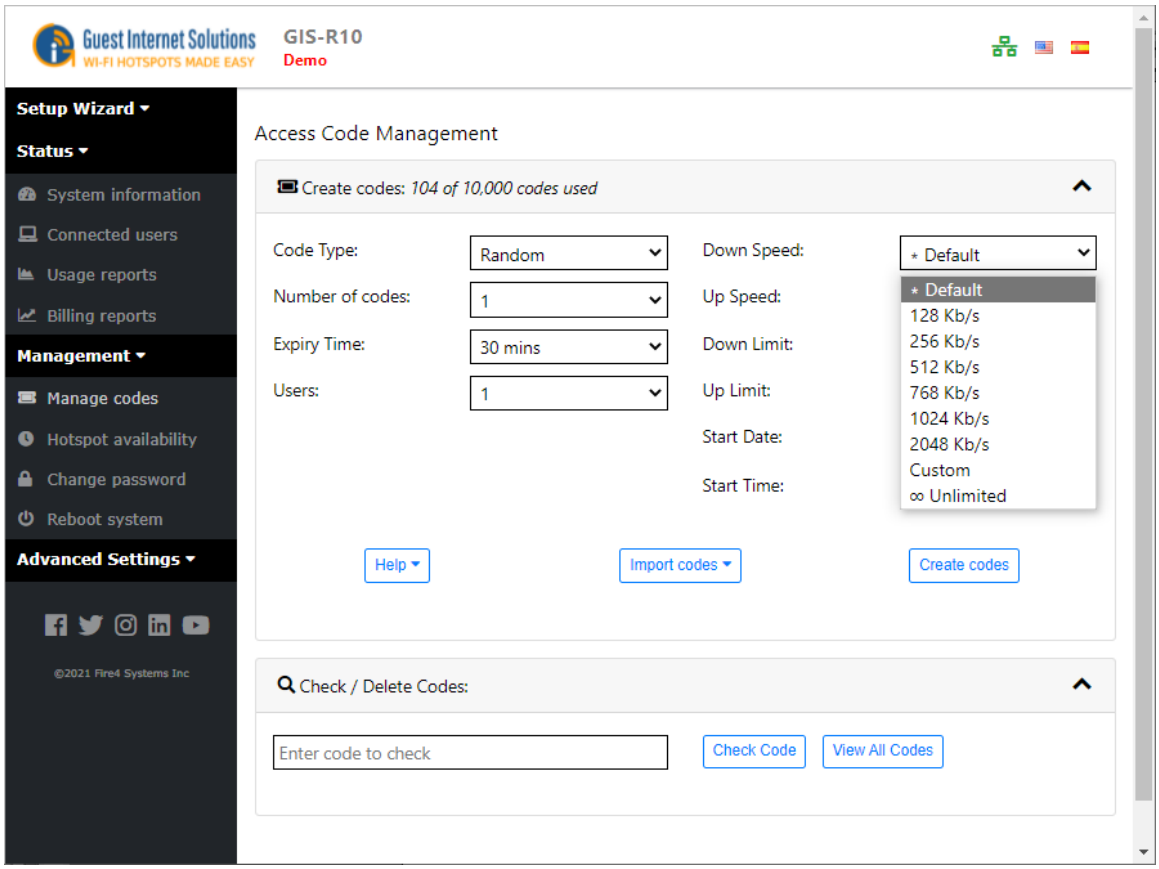


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Speed

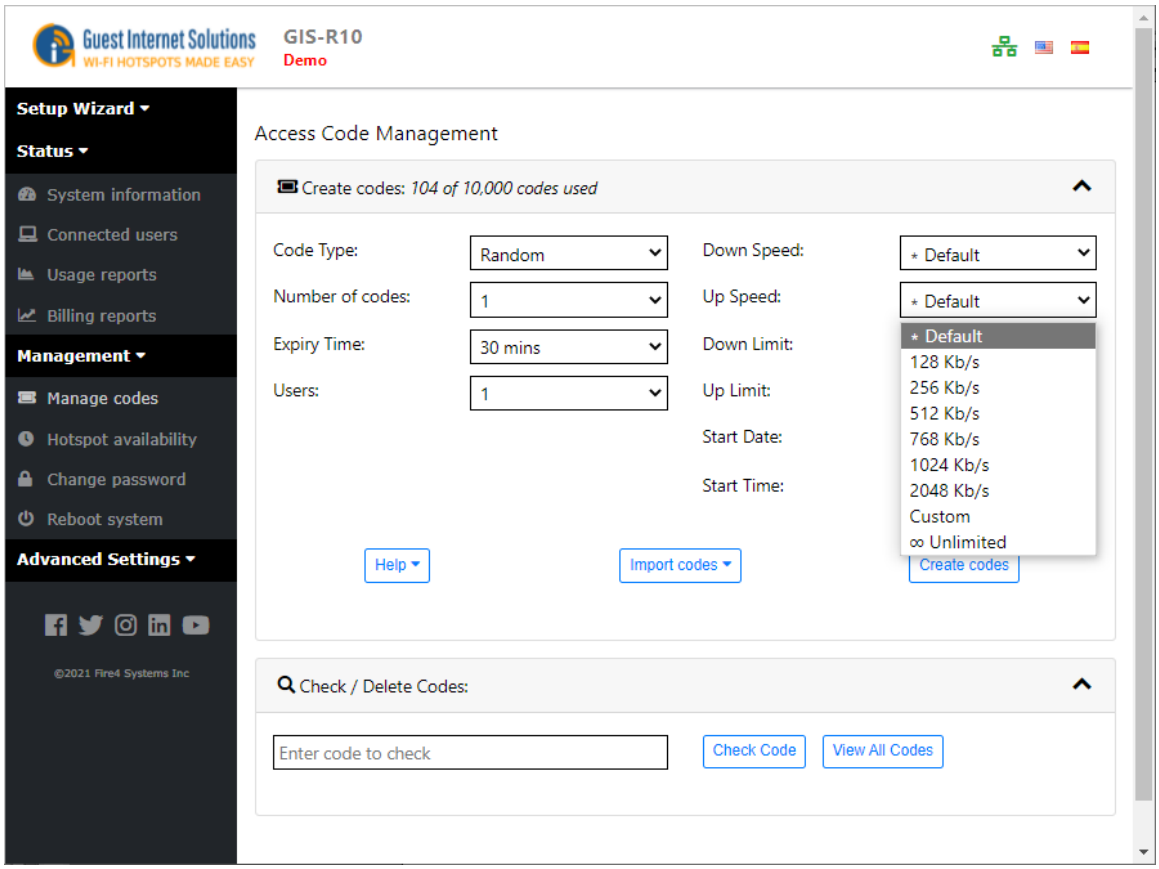
"Down Speed" and "Up Speed" options, guests using this code will be throttled (limited) to the speeds selected. Default set on bandwidth control page.

Down Speed: maximum download Internet speed



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Up Speed: maximum upload Internet speed

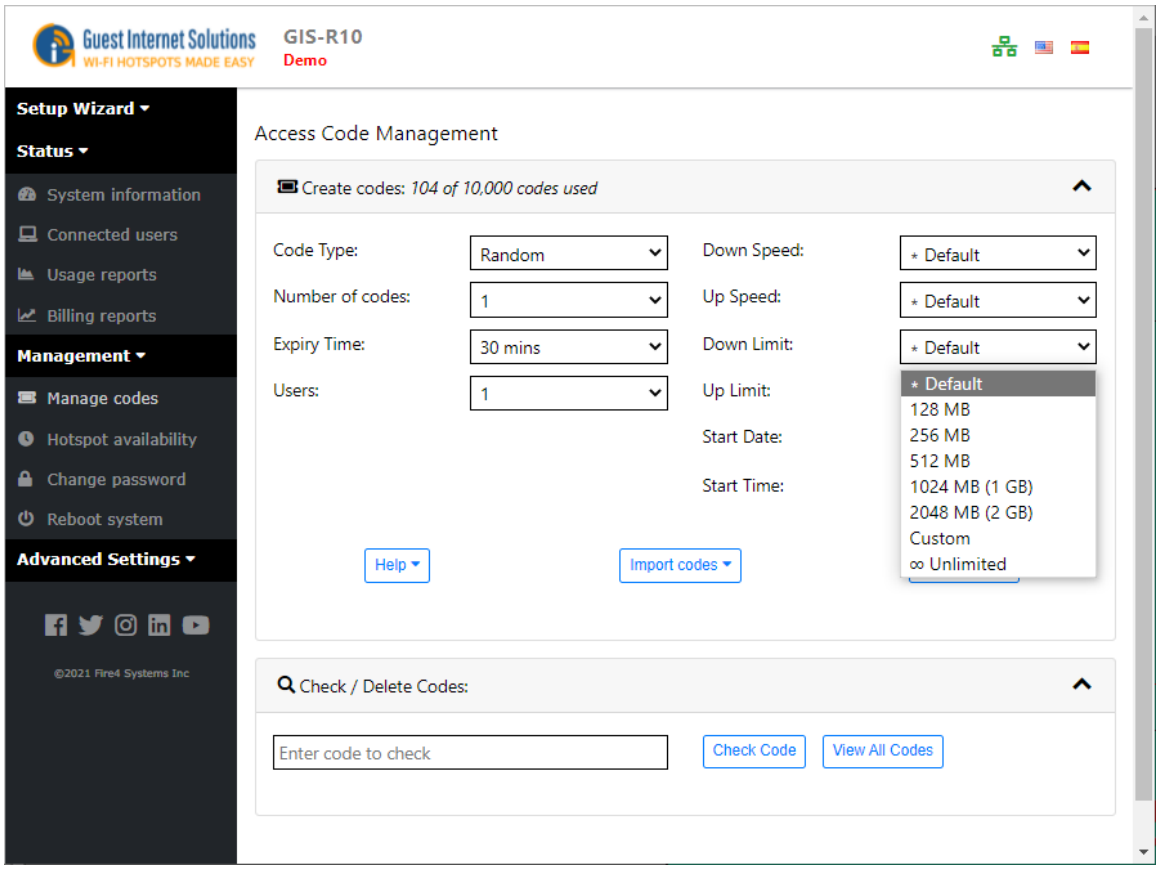


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Data

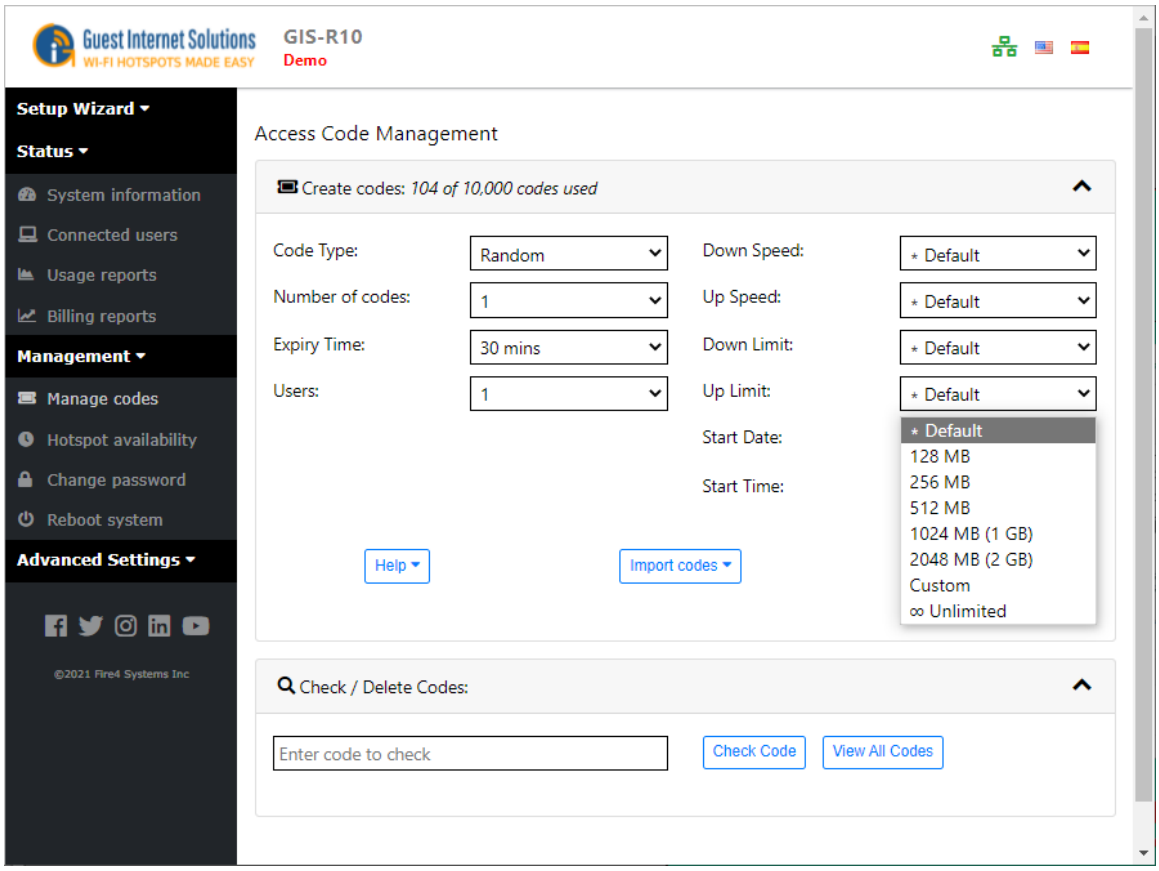
You can limit the data Download and Upload. Guests sharing codes will also share the limit. Default set on bandwidth control page.

Maximum data download bytes



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

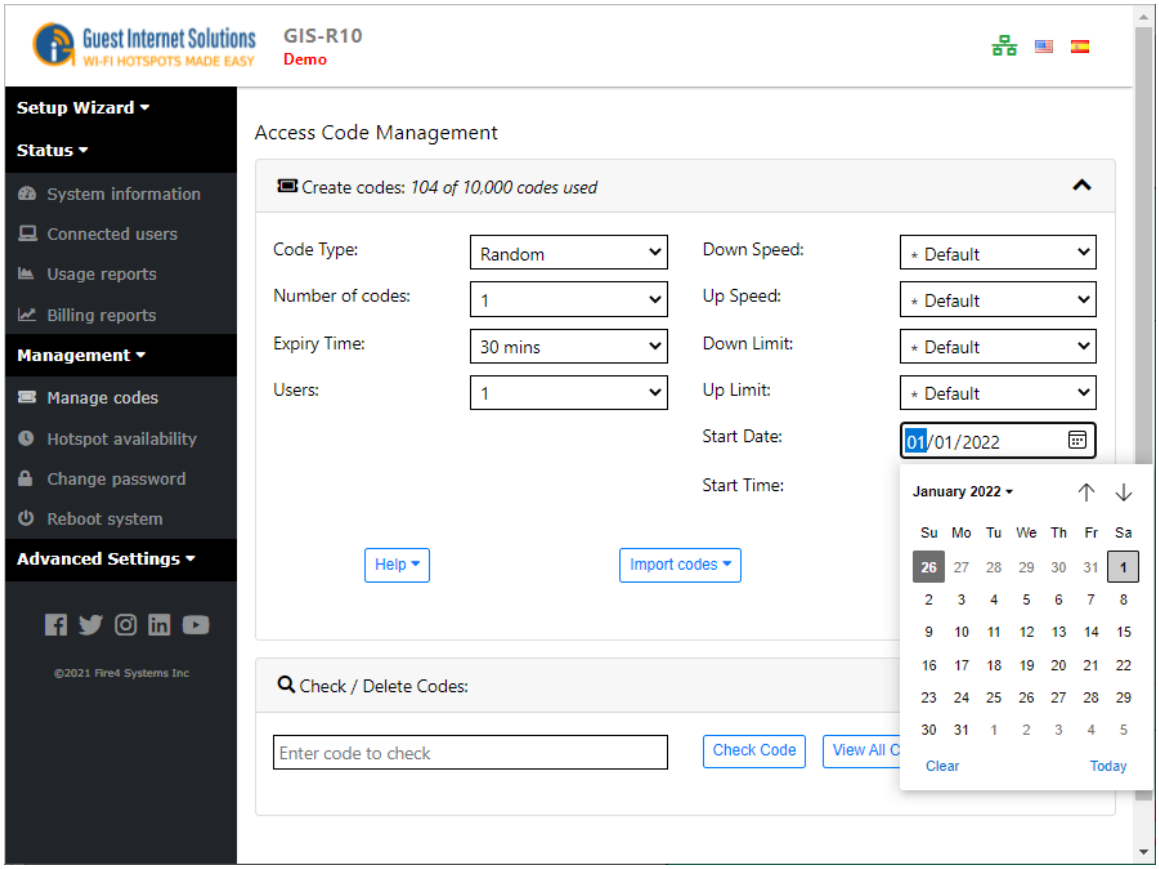
Maximum data upload bytes



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

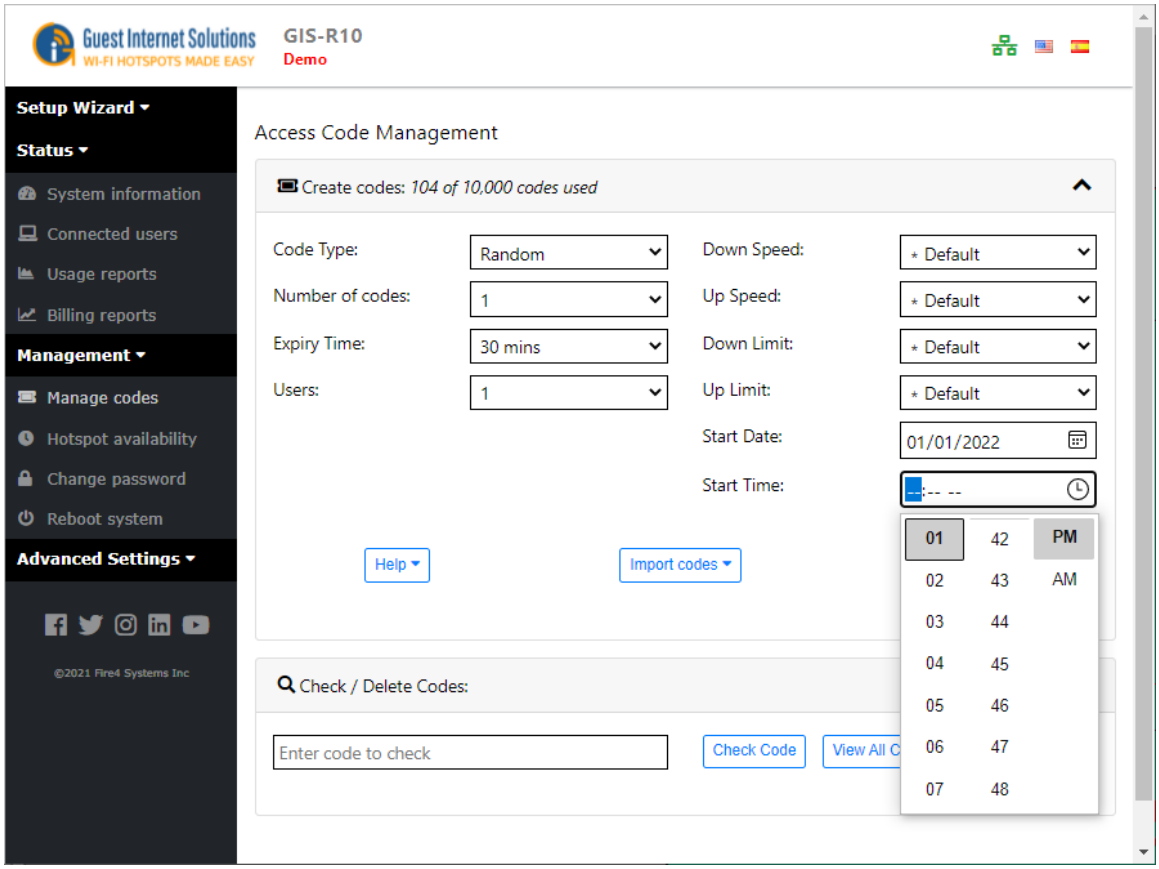
Start

Set the date when the code duration will start



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Set the time when the code duration will start



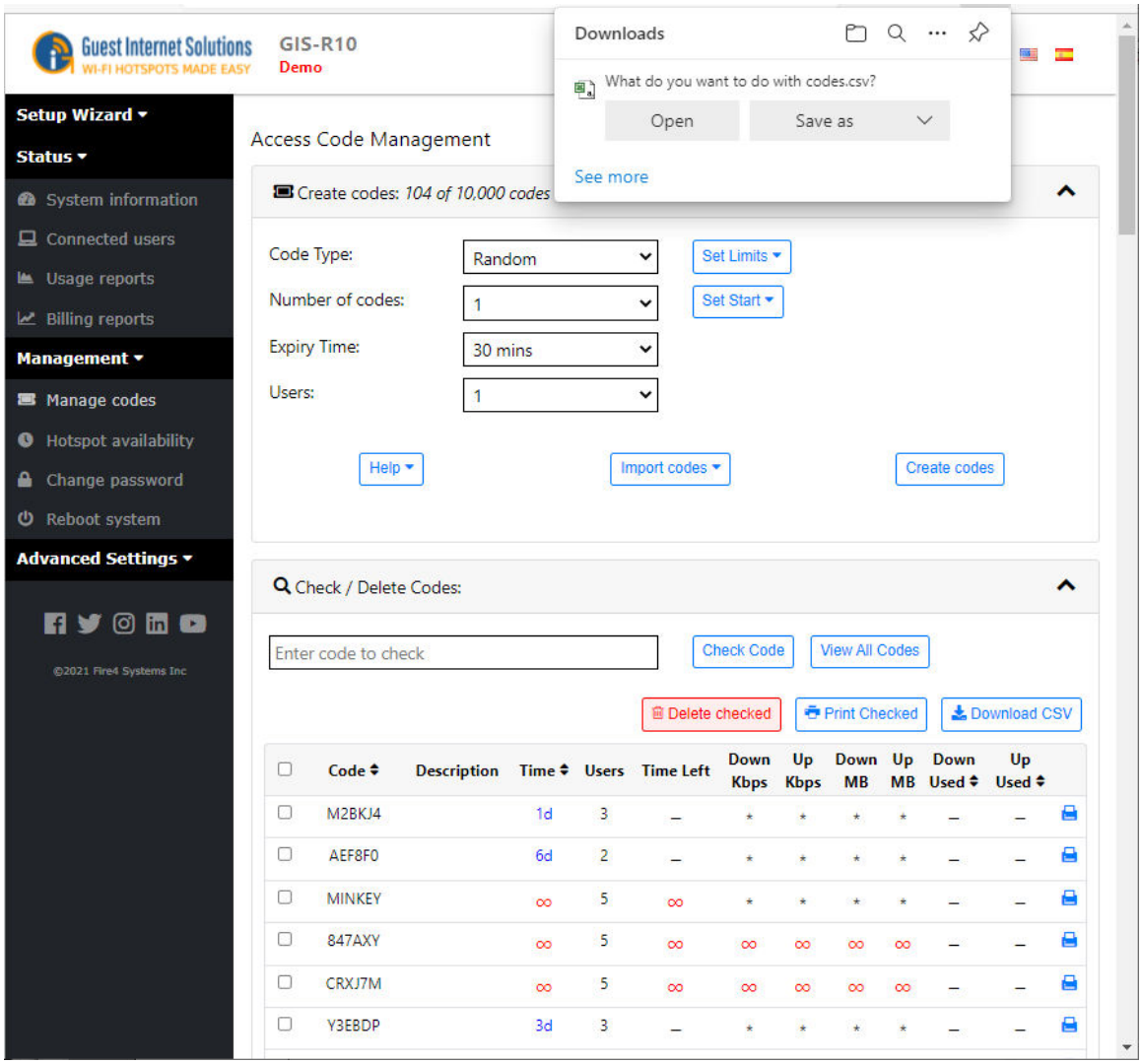
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Import and Export Codes

The system allows you to import and export a set of codes in CSV format.

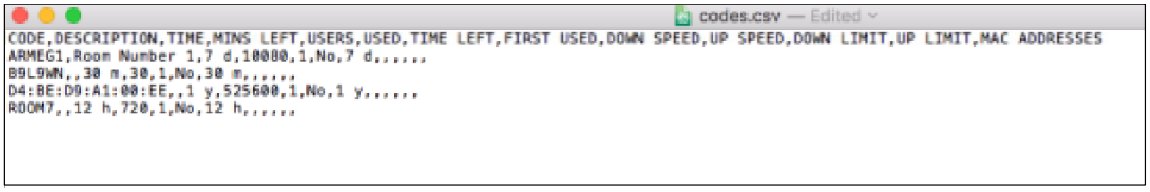
Download

Going to the "Manage Codes" option on the Admin interface, by the end of the page there is a "View All Codes" button, when clicking the button, you will see as screen like this:



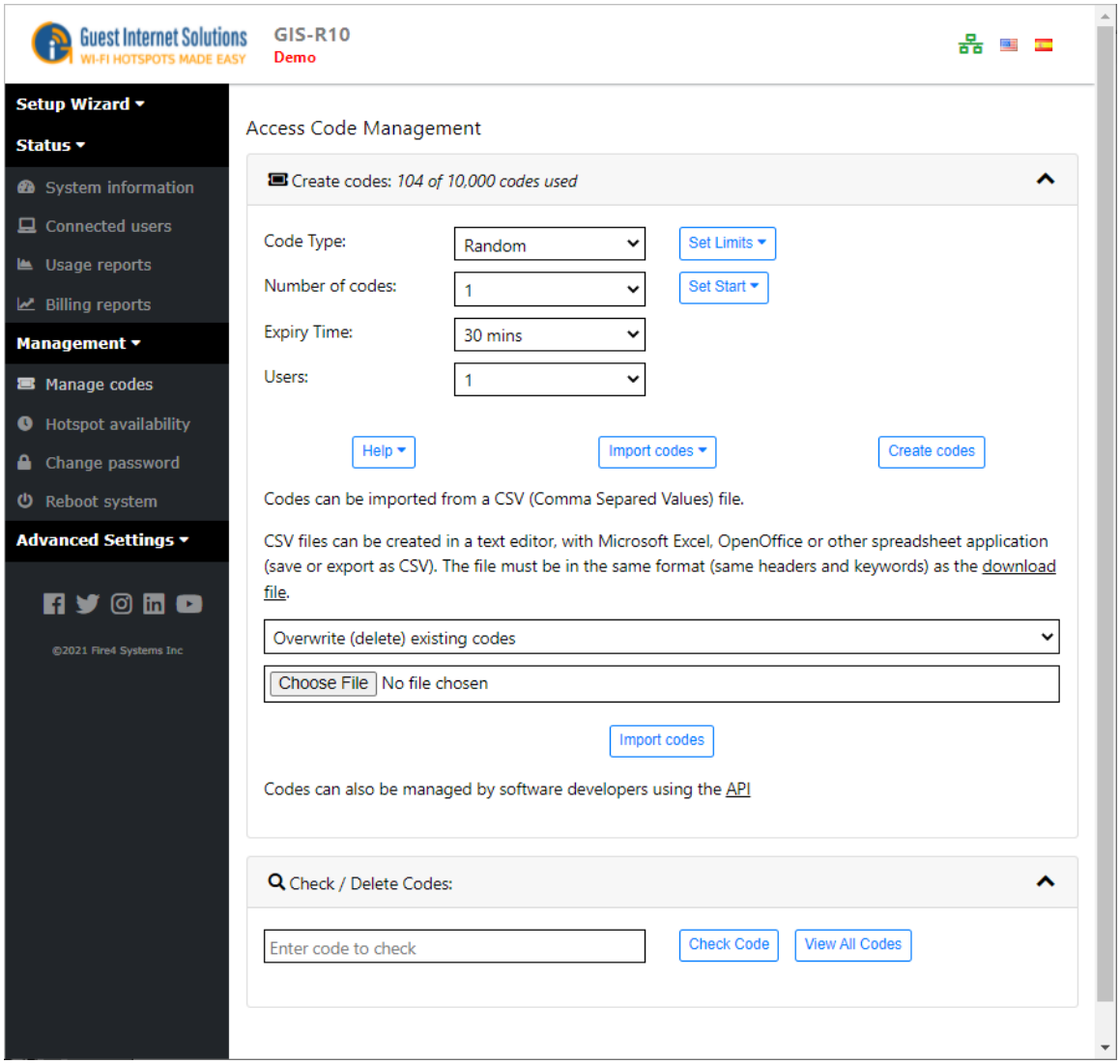
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Just click the "Download CSV file" and you will get the CSV file with all the codes you have generated.



Upload

To upload a list of Access Codes, you need to go to the "Manage Codes" option on the Admin interface, just before the Find/Delete Codes box by the end of the page, there is a link "Import Codes".



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Printing Vouchers for the voucher cash sale (Internet-por-ficha) application

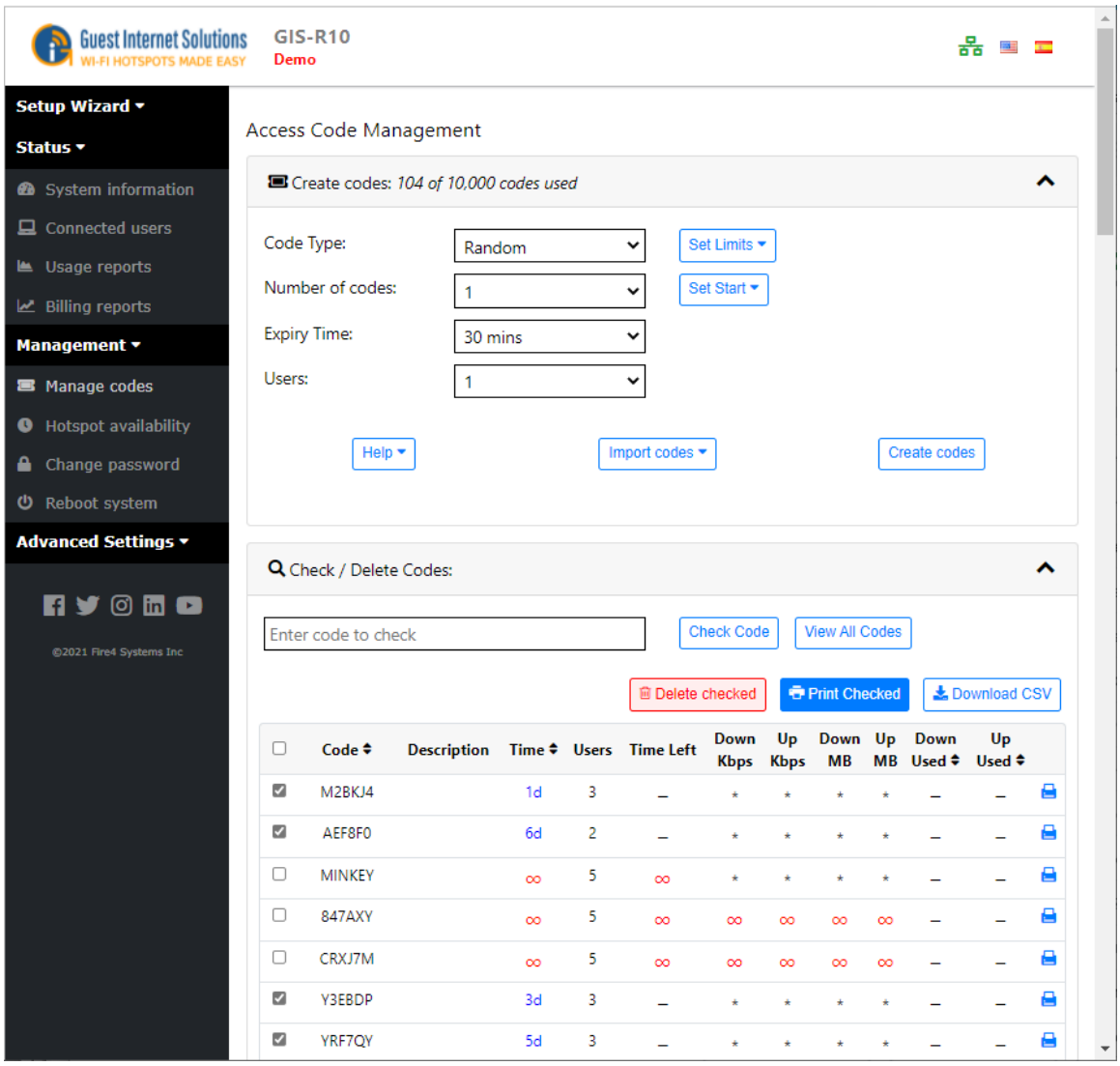
The K-series and R2/4/6 products have a feature to create and print vouchers in a 4x4 format on a letter size printer. Each voucher has a unique access code printed on it, where the access code is configured with the parameters for:

- Duration, minutes, hours, days, months
- Number of concurrent users permitted to us the code
- Download and upload speeds, download and upload byte limits

This feature supports the sale of Internet access for a cash payment (Internet-por-ficha) application that is very popular in the countries of Latin America and the Caribbean. Before the vouchers can be printed, the voucher design must be created. The voucher setup procedure is described in the 'Printer Setup' section of this manual.

Creating the codes follows the same procedure as described previously. The vouchers are printed 4x4 on a Letter size page which is 16 vouchers per page. When selecting the number of codes to create a number should be select that is a multiple of 16.

When the access code parameters have been selected click the ‘create codes' button. The voucher-printing feature includes a button ‘print codes file’ that is highlighted in the next figure.

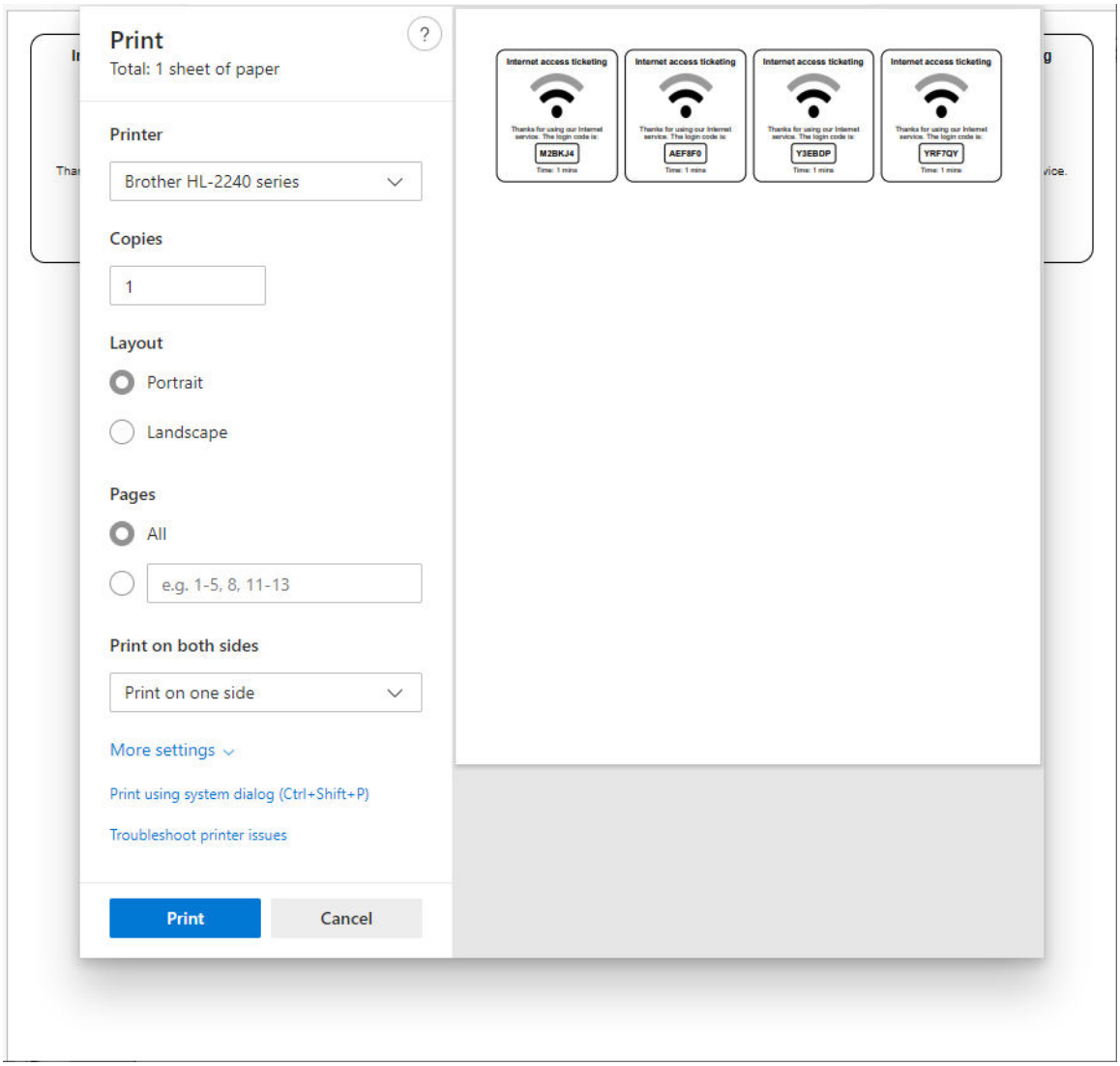


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Clicking this button opens a browser tab with the formatted vouchers, which is shown on the following figure.

The browser pages can be sent directly to a printer, or else printed to a PDF file for printing at a later date.

After printing each voucher page is chopped into individual vouchers for sale to the public.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Codes Login Page

All GIS gateway products have a special graphic user interface specifically to generate access codes that are given to guests for Internet access.

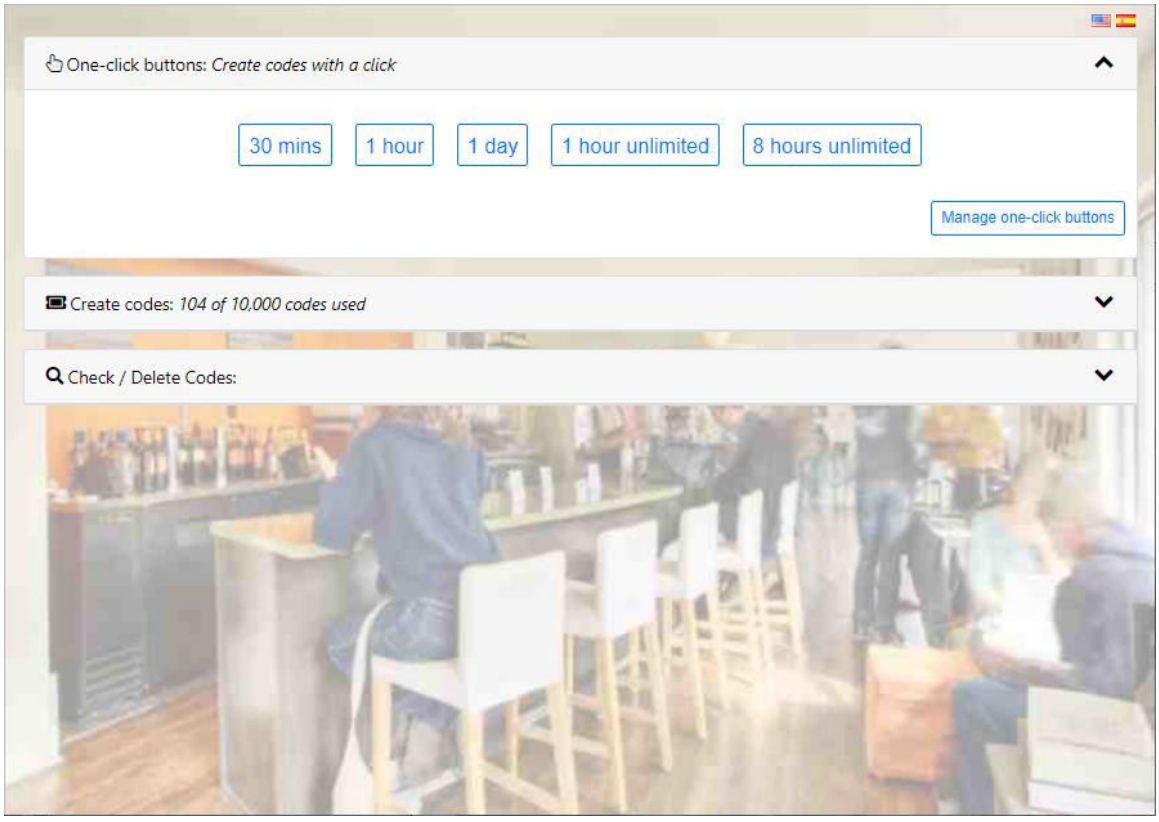
When the ticket printer is activated the display is used to print access codes onto tickets, as a self-contained PoS.

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

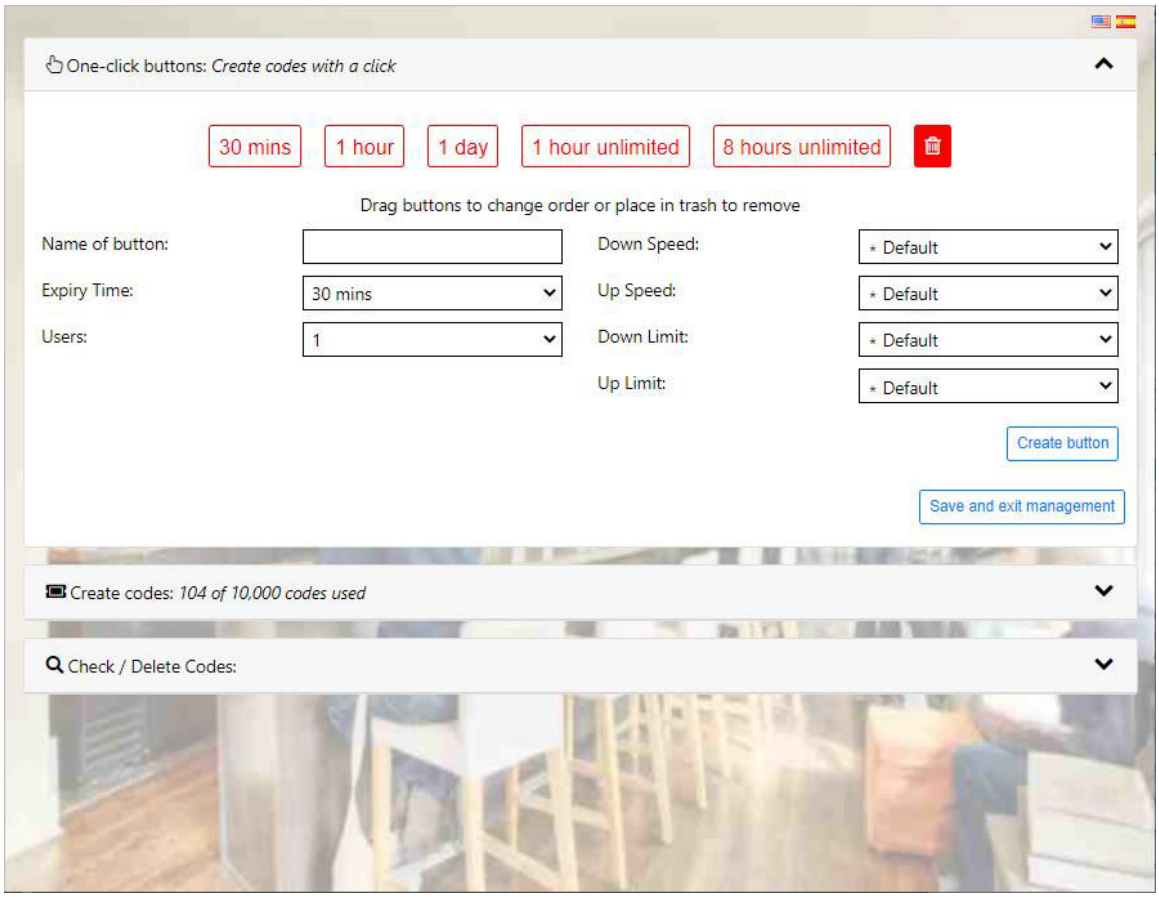
A username and password is requested when this URL is typed in and so the code administration page password must be created before this feature can be used. First login as administrator and click on the change password menu entry to create the password for the access code management page.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

It is necessary to first create buttons that are used to generate access codes.

Up to ten buttons can be added to the display. Click on the *'create button'* to add a button to the display.



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:

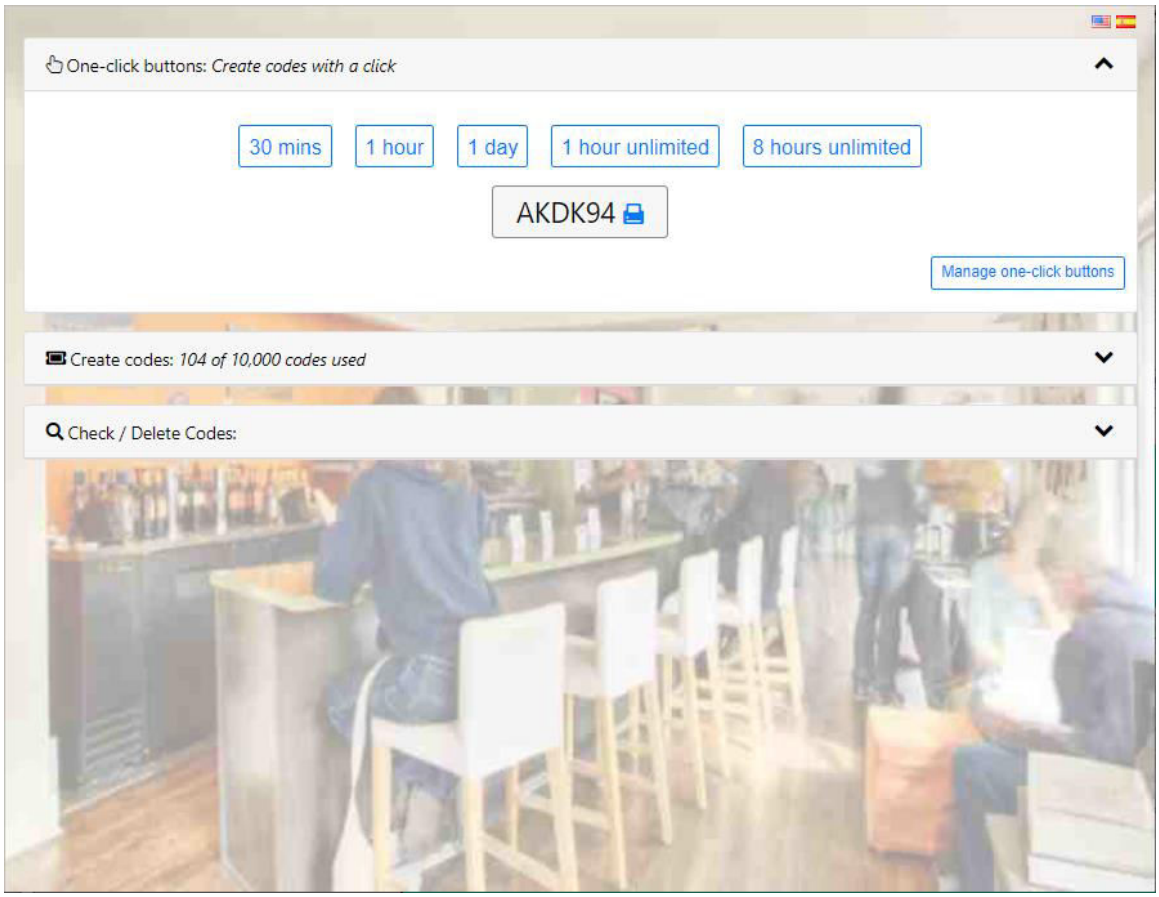
- **Single**: Only one guest can use this code. The code runs to completion after login. The duration of the code is selected by the time option.
- **Multi-User**: Many guests can use this code concurrently for Internet access. The timer starts the first time that the code is used by any user, and the code expires after the duration set for the code. Subsequent users will therefore have less time available for the code.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The download and upload speed limits can also be specified for the code using the drop down menu.

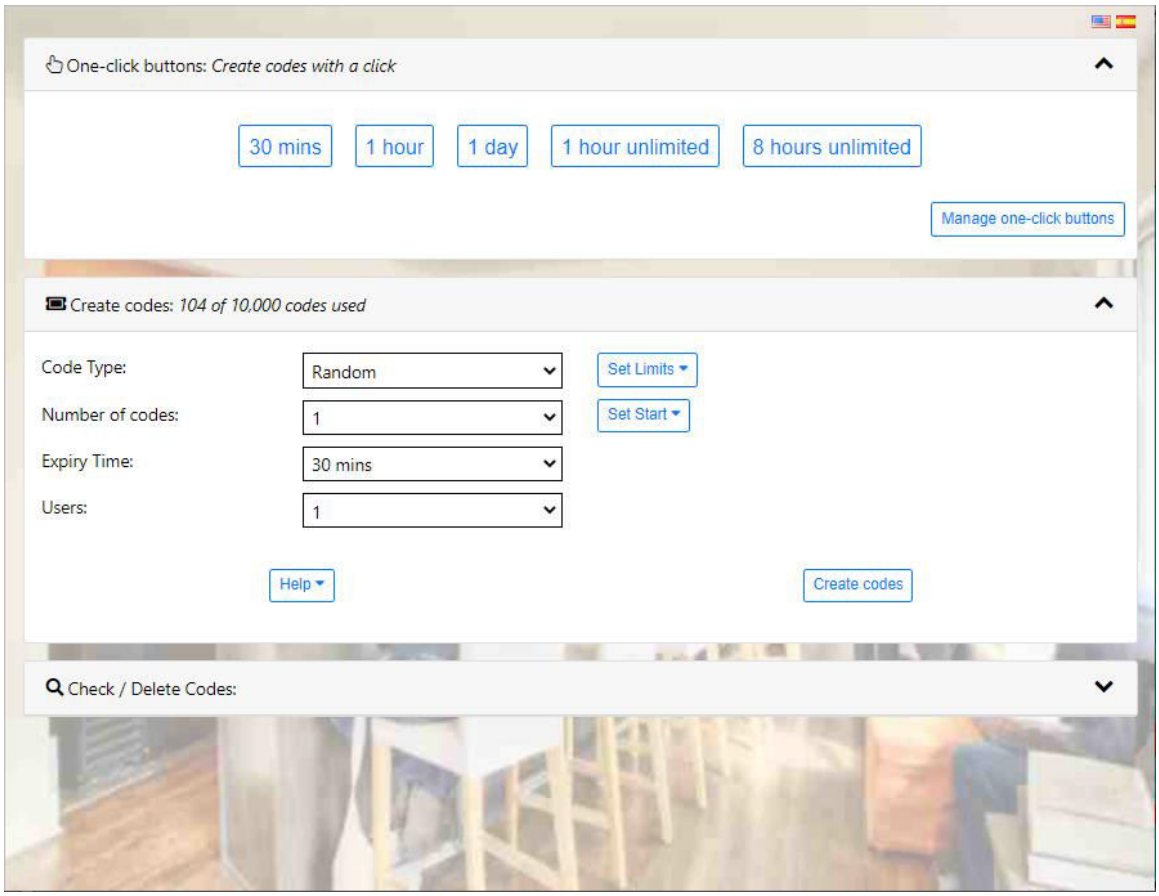
Click the *'exit management'* button to see the display with the buttons that are used to generate access codes.

When a button is clicked the access code that has been generated is shown on the display.



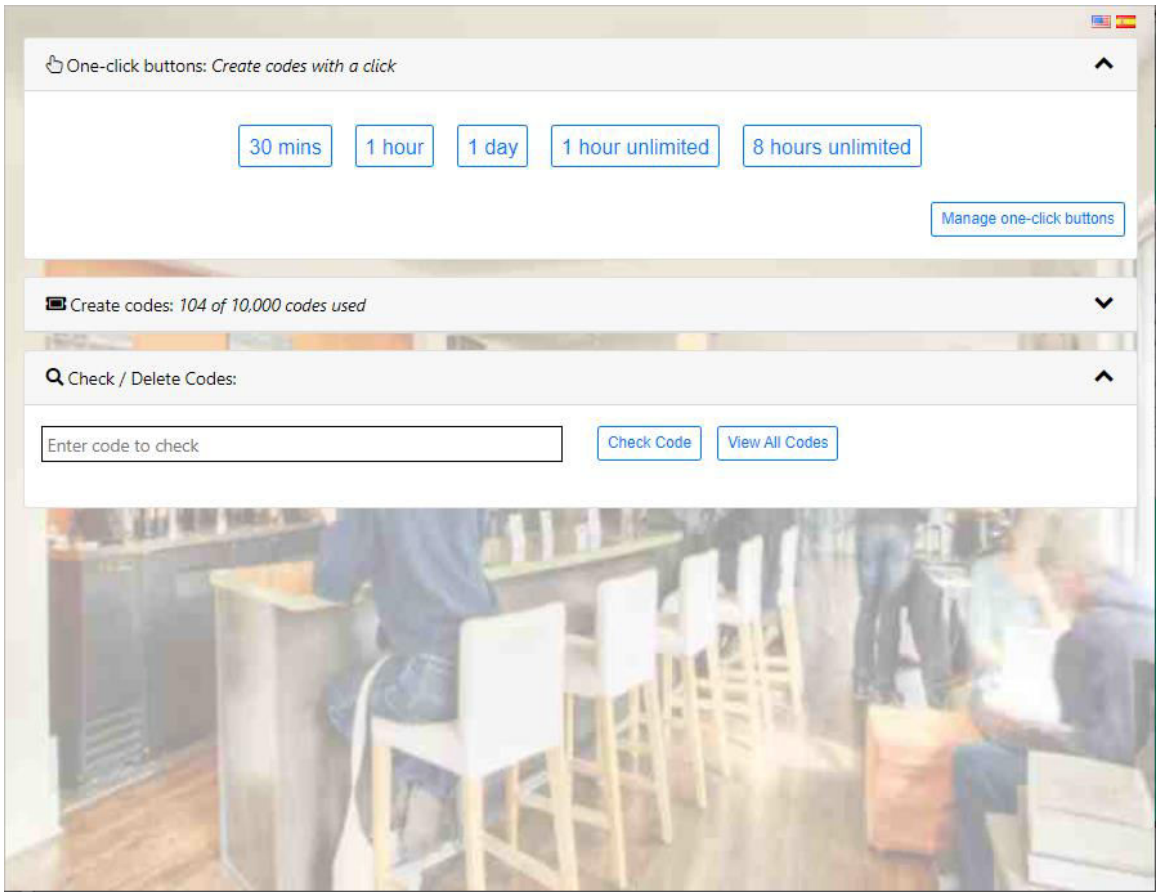
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Click the drop down menu to generate a custom code.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Click the drop down menu to check a code.

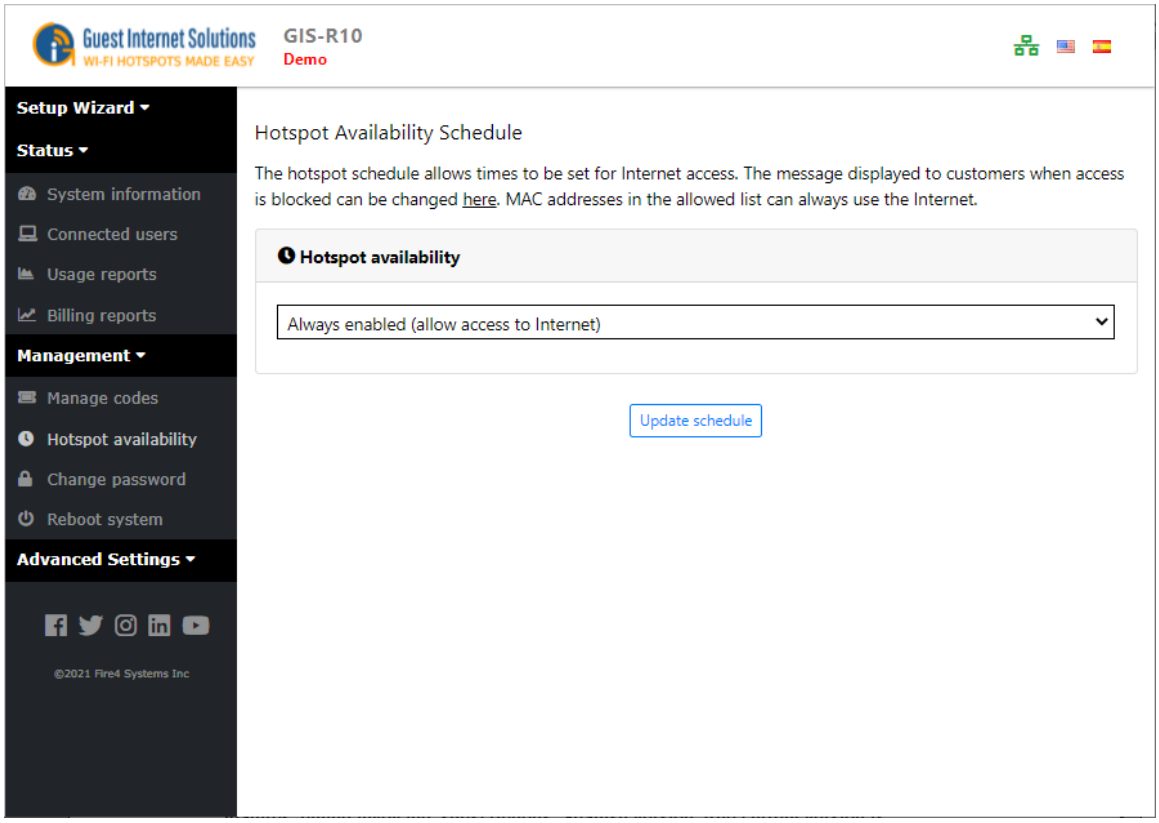


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Hotspot Availability

The GIS units allow you to control the times where the internet is available throughout the week.

Clicking on the Hotspot availability menu opens the default page, which shows always enabled.

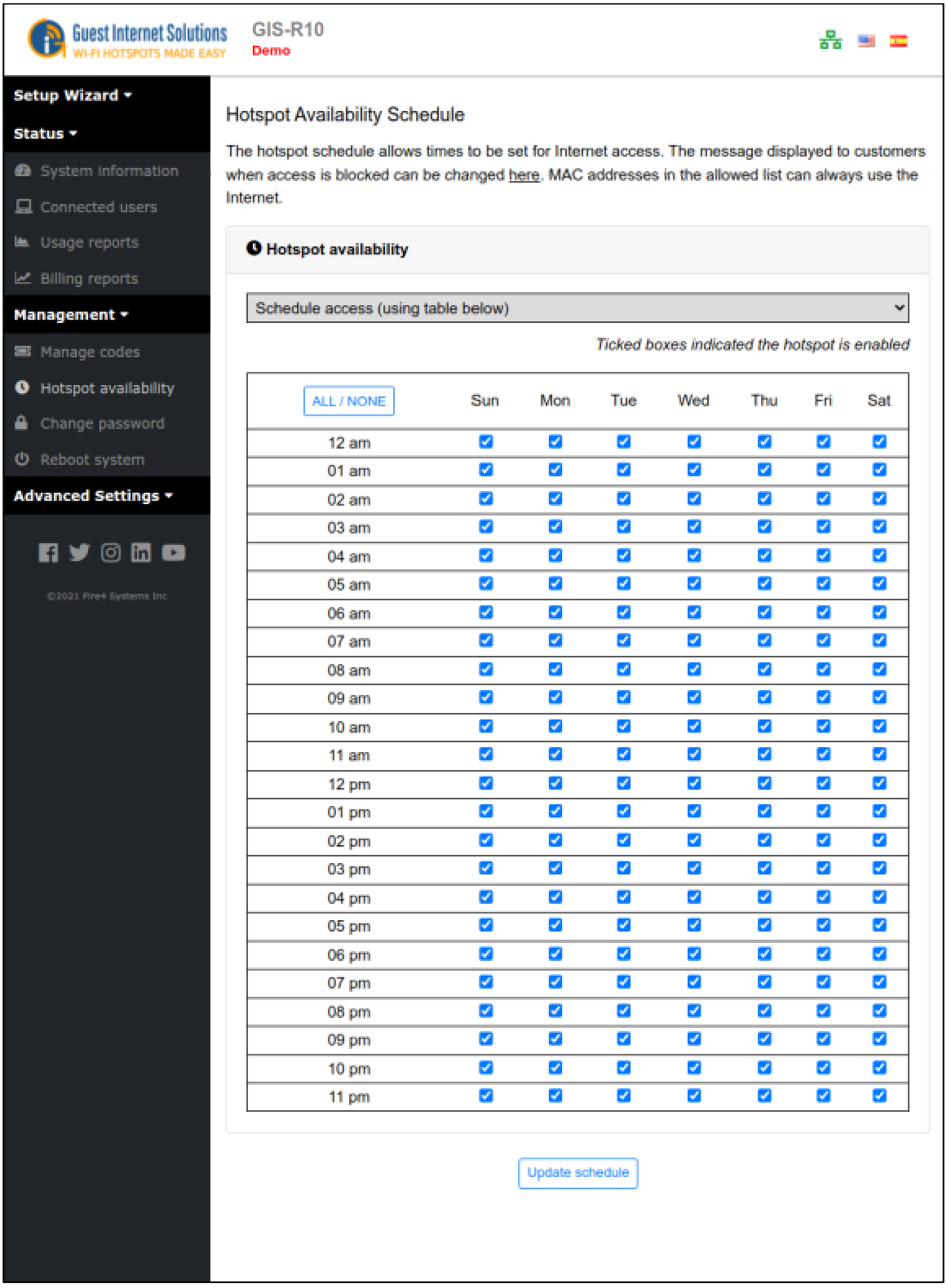


If ‘schedule access’ is selected from the drop-down menu then the selection table is displayed.

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

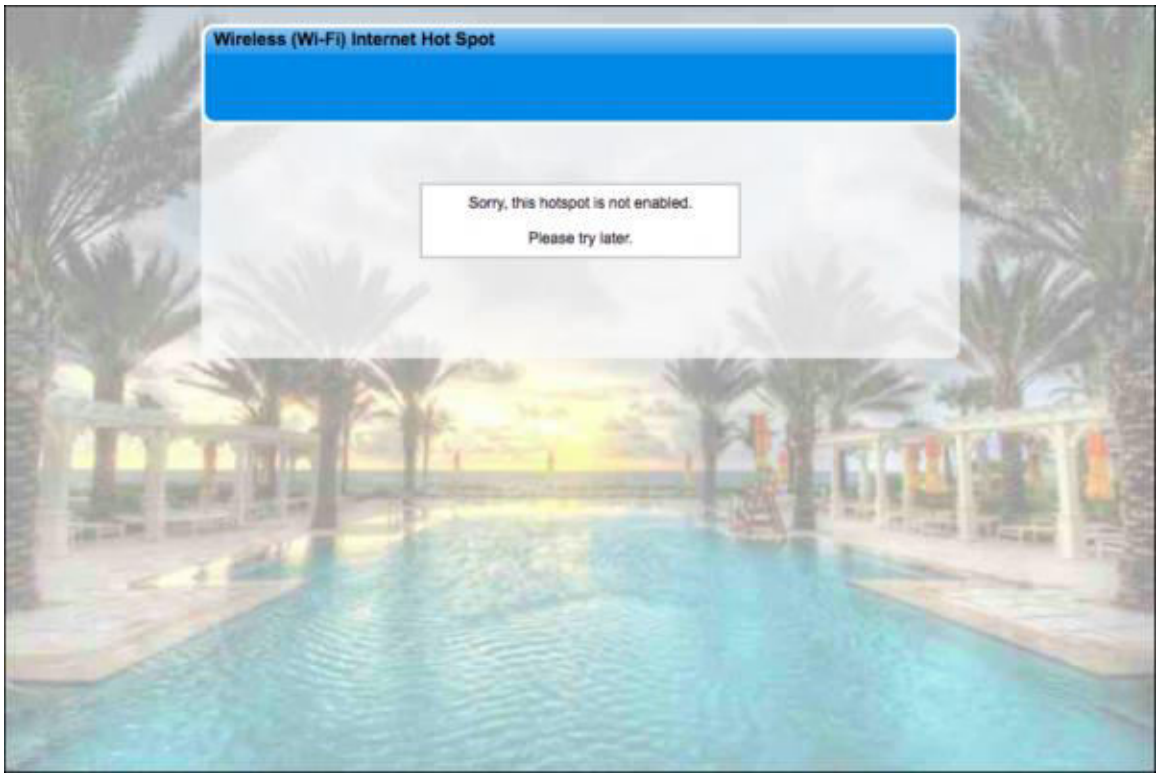
Each hourly selection box is checked for enabled when the table is first opened. Uncheck the boxes when the Hotspot service should not be provided.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

At the times when the Hotspot has been disabled, the login screen will display:

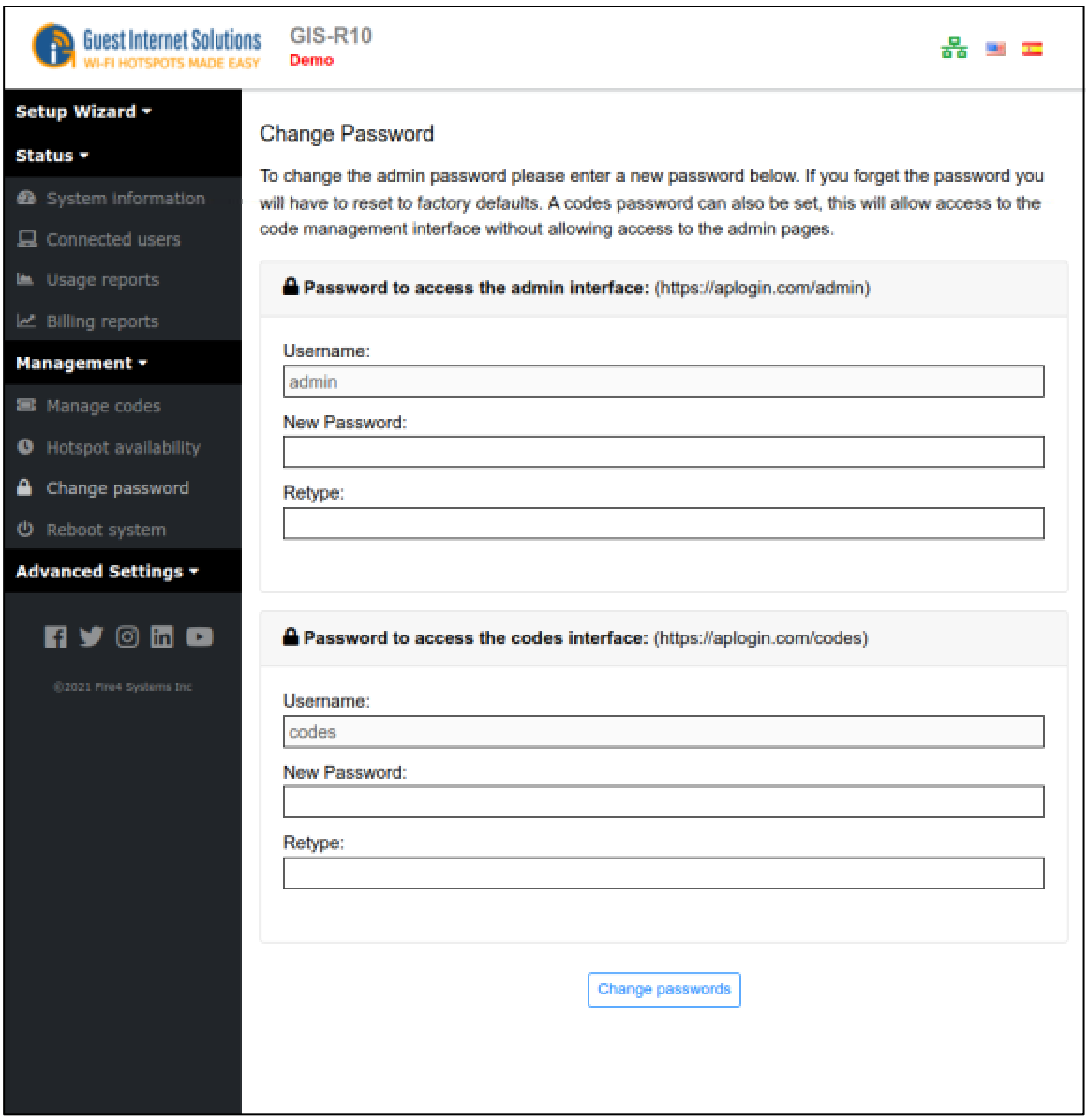


The message that is displayed can be changed, check Login Messages.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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.



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. 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.

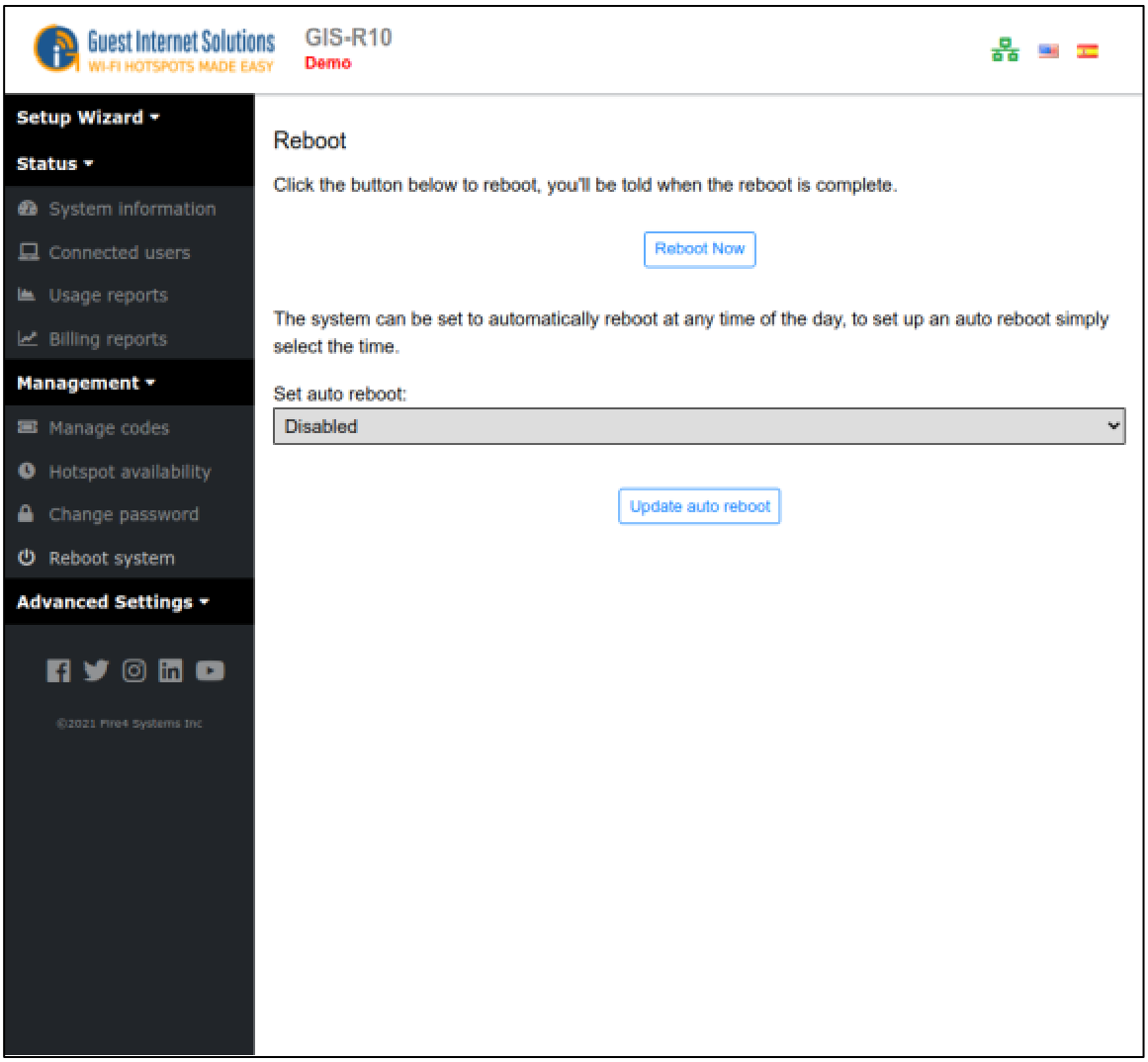
Always make a note of your passwords and keep in a safe place: if the admin password is lost then the Guest Internet gateway will have to be reset to factory defaults and you will have to configure the device again.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Reboot

The reboot system function restarts the device.

Some functions may require the device to be rebooted before the changes take effect.



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

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

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.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Advanced Settings

Advanced settings permit you to change technical parameters of your product. Changes in these parameters should not be required unless your implementation has specific network characteristics.

Advanced settings used to administer your Guest Internet unit are as follows:

Login Settings

Login Messages

Credit Car / 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

Update firmware

Backup & restore

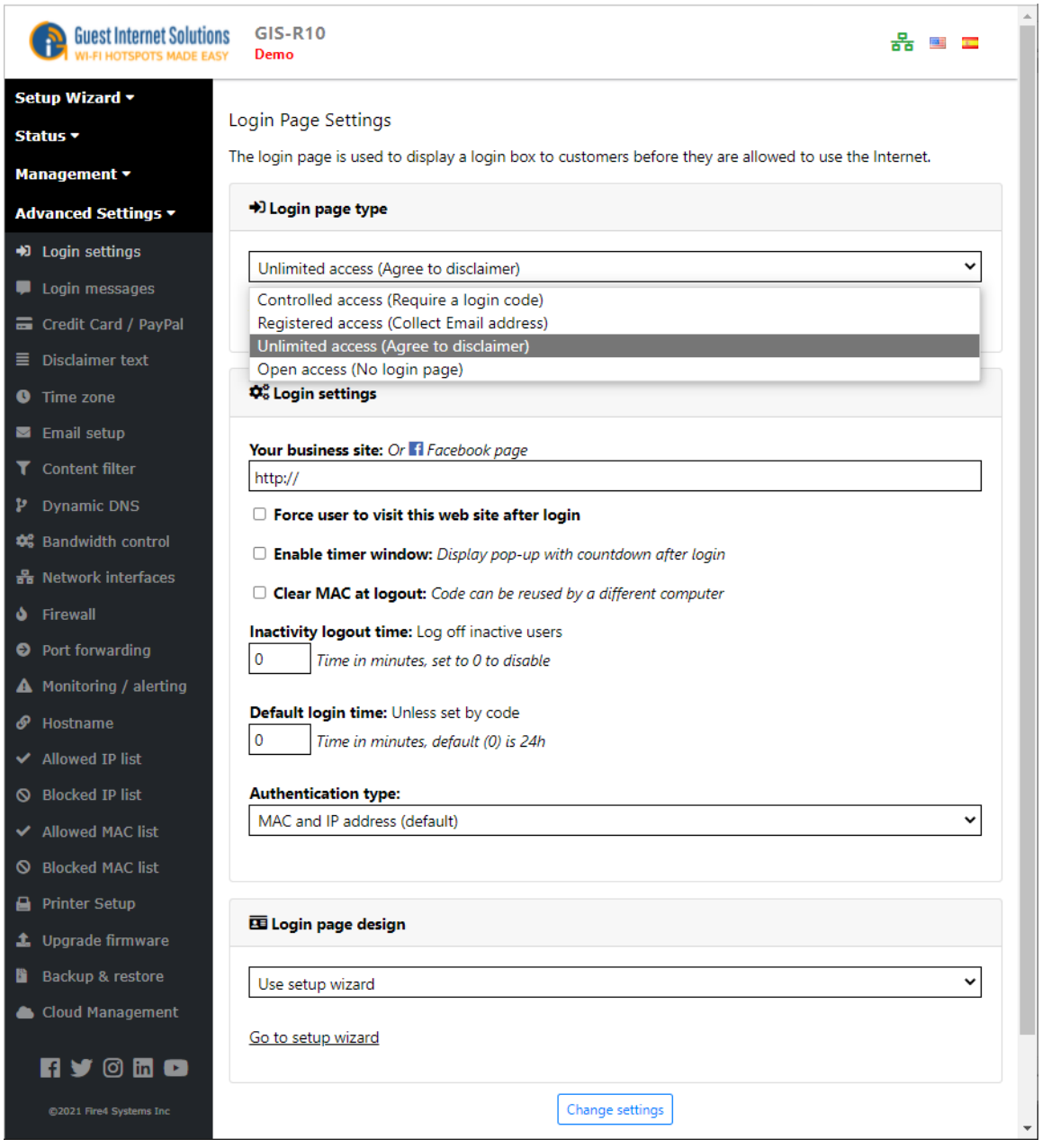
Cloud management

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Login Page Settings

The login page has four customizable configurations for the login page type.

- Unlimited access
- Controlled access
- Registered access
- Open access



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The configurable parameters common to each type of login page setting are as follows.

Login Page Type: Choose the type of login to be offered to your guests.

Business Web site: This is the Web site URL of the business providing Internet service.

Force the user to visit this website after login: By checking this box you can force the user visit to your website after logging in.

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) 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 or switched off.

Default login time: This timer (in minutes) is normally set to zero: zero means it is inactive. This timer will disconnect the user after the time specified.

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 used 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).

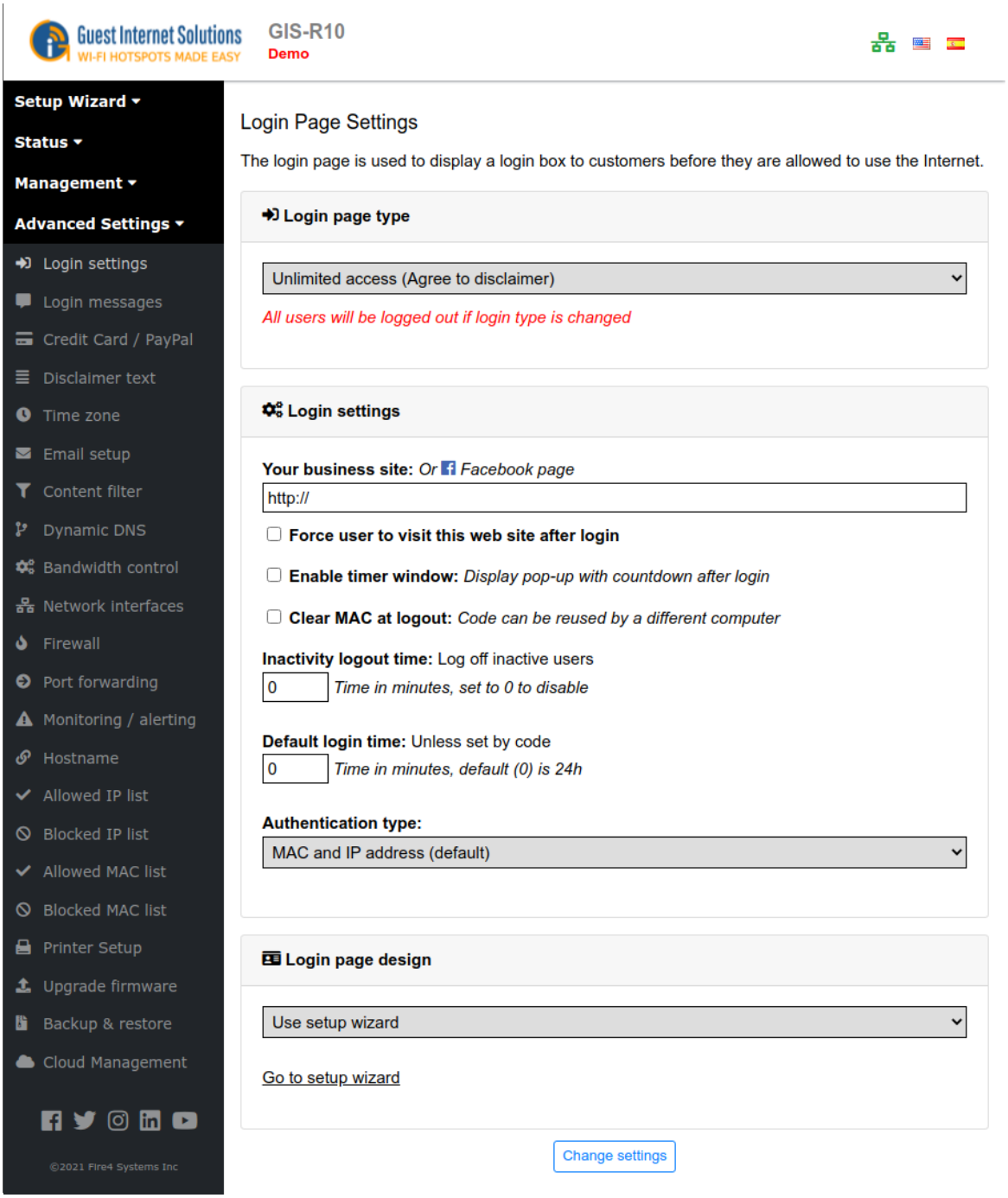
XBox auto login: Standard configuration XBox gaming products do not have a browser and therefore cannot log in to the network like a computer can. Checking this box will permit XBox products to be detected and allow them to bypass the login page and connect directly to the Internet. The firewall rules apply to the XBox however.

Custom Login Page Settings: The login page is used to display a login box to customers before they are allowed to use the internet, you can learn how to customize your login page here.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

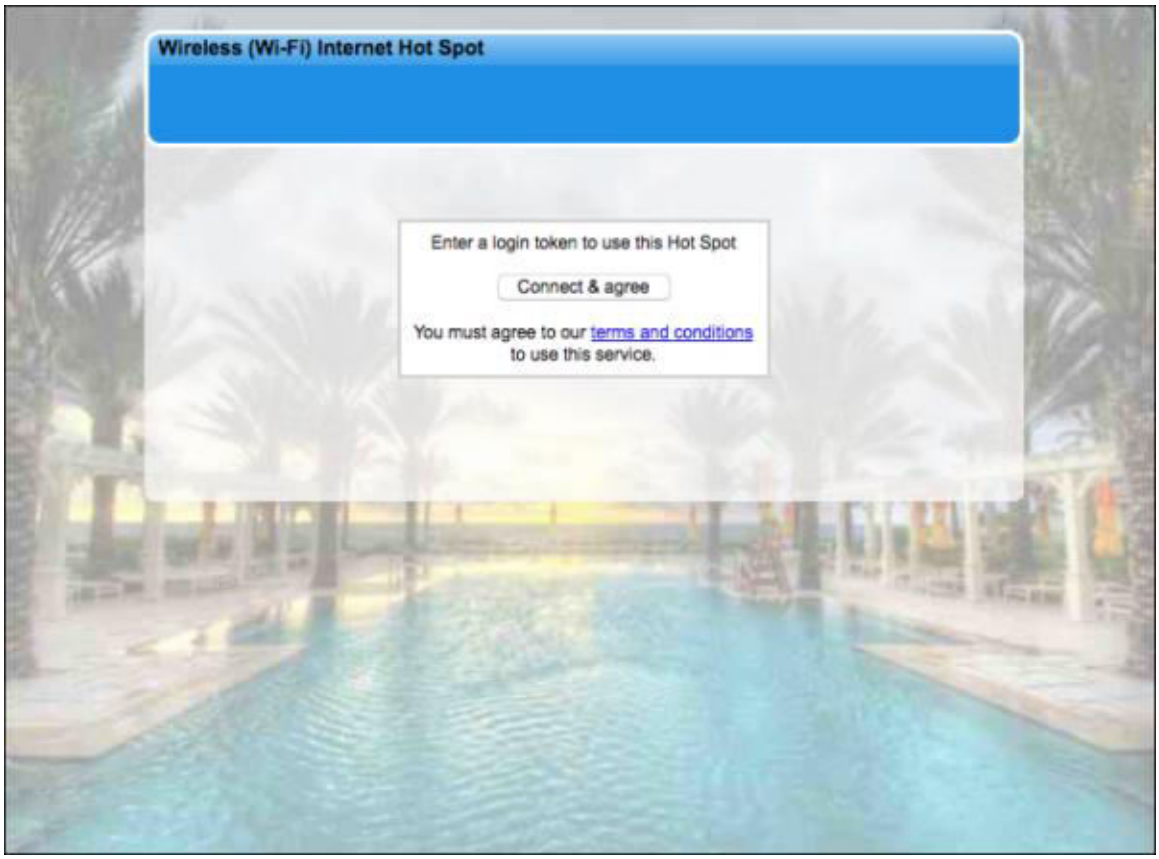
Unlimited Access

The Unlimited Access mode the user has to agree to the terms and conditions of use.
You can set a timer to determine how long users are permitted access to the Internet.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The unlimited access login page:

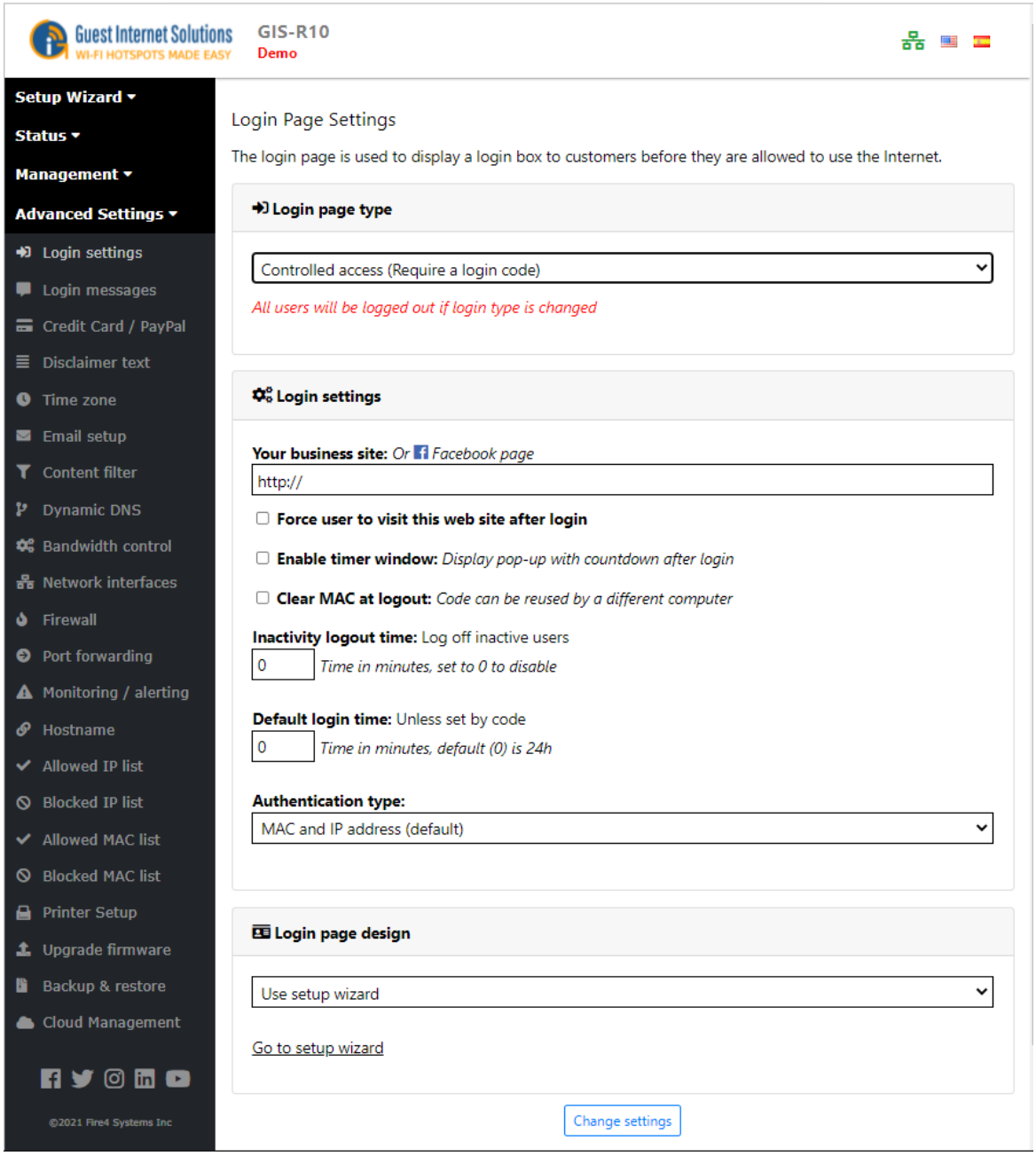


The legal disclaimer can be customized on the Admin interface.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

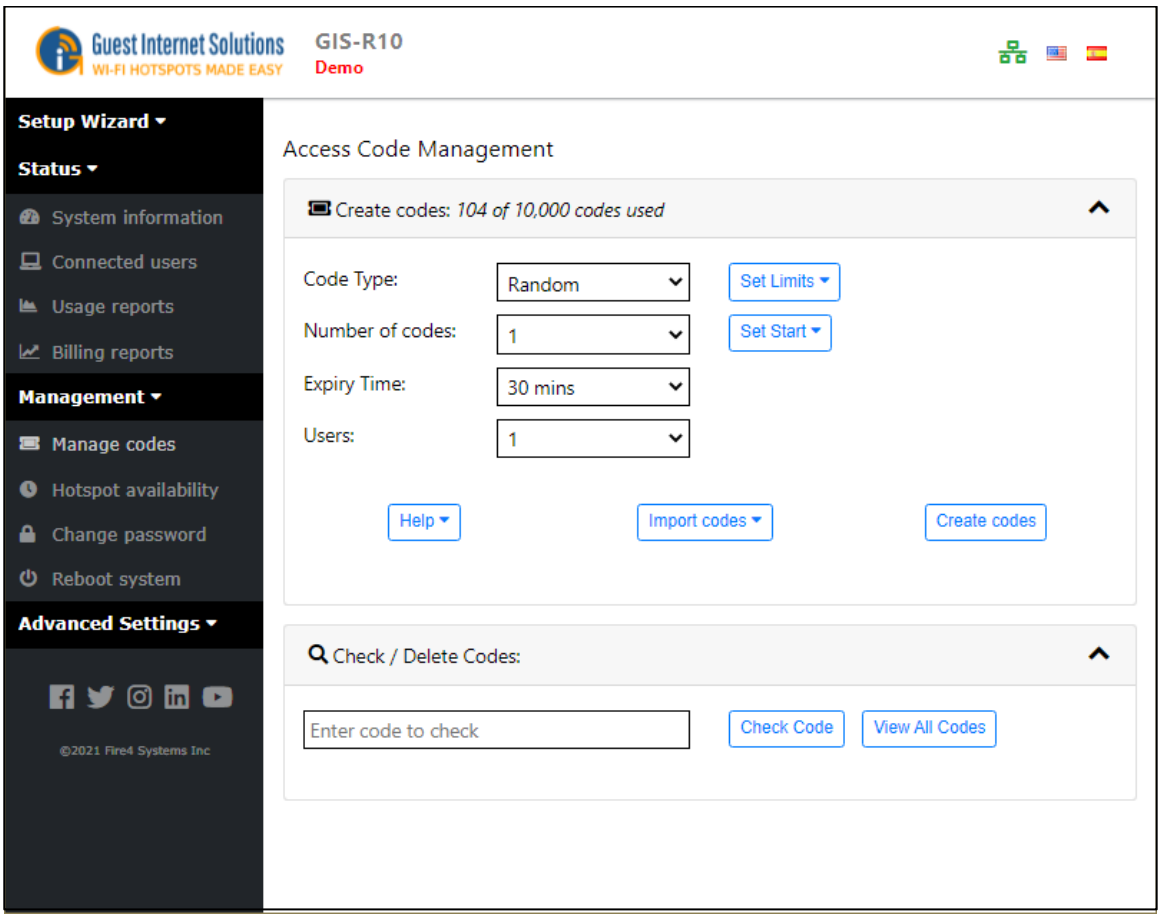
Controlled Access

If you want to control your users access to the internet using either login codes or by using Credit Card/PayPal® billing then Controlled Access should be enabled.



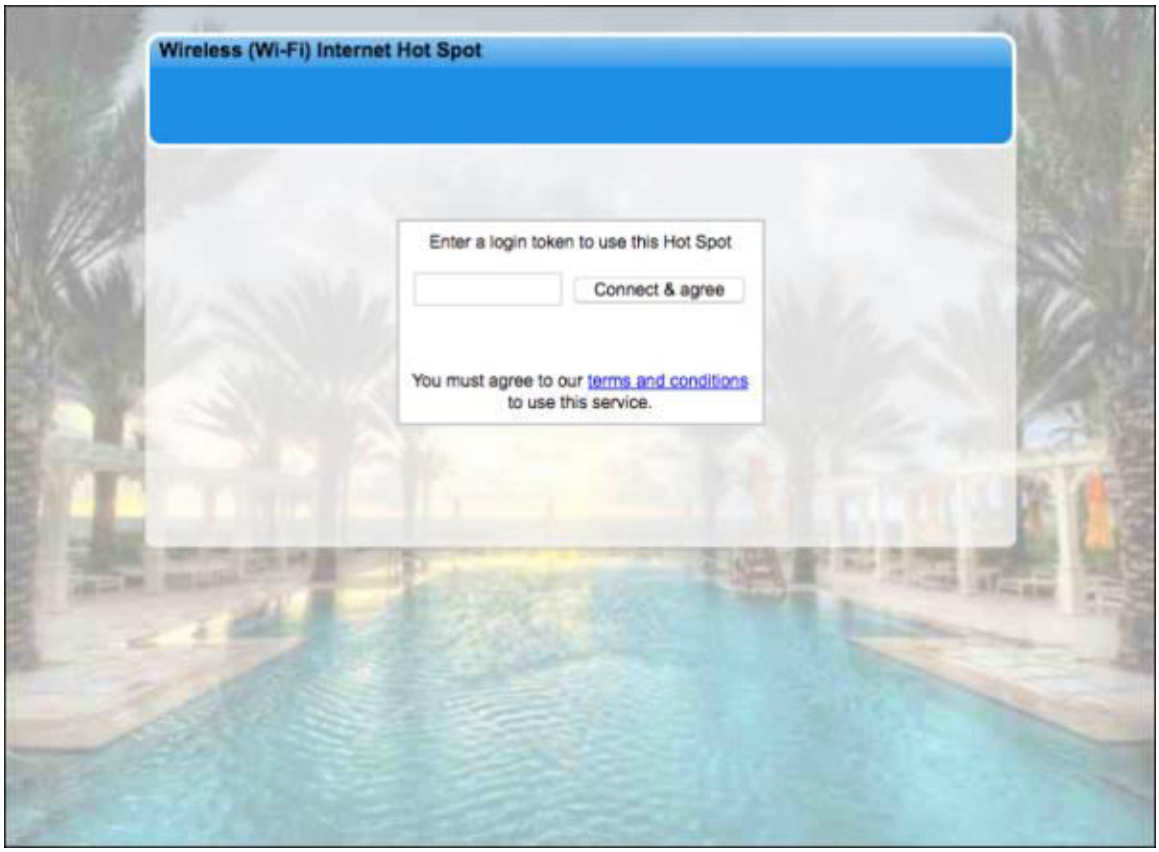
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The Controlled Access requires a login code that can be generated on "Manage Codes" based on time limit, speed limit or no limits.



It will be displayed on the user's device the "Custom Login Page" you have created; the page will display a space where the user needs to type the code and therefore connecting to the Internet.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



When clicking in "terms and conditions" the user will be redirected to a page with the disclaimer information. You can see how to edit the disclaimer here.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Controlled access with free limited login and with alternative website blocking

(PRO products only)

Controlled access has an optional free login for a preset limited period of time, and with a preset time that prevents the user to login again after the completion of the free period. The maximum download and upload data speeds and the maximum data bytes can be set for the free login. The free login also has an independent IP/domain blocking table to permit the free login to have up to 100 websites blocked. The configuration is suitable for any application where free access is provided with website blocking, and a paid service is offered with or without website blocking. Selected website blocking for a free Internet service alleviates the data burden on high volume public Internet services where the predominant data traffic is video streaming, from websites such as Youtube, Hulu and Netflix.

This feature is available only on the following products with firmware 2.5.6.1x or later.

- GIS-R10
- GIS-R20
- GIS-R40

The login procedure is a 2-tier login access method where free access is presented as an option to entering an access code, or purchasing access using a credit card.

- Free access does not require the entry of a generic access code because an additional button is added to the login page for temporary free access.
- The blocked domain/IP table is a dual table, one set of blocked domains/IP's applies to the free login and a second set of blocked domains/IP's applies to all logins.

A login button is configured for the login page with free limited Internet access and in addition the login can be made using an access code provided to the user is also available.

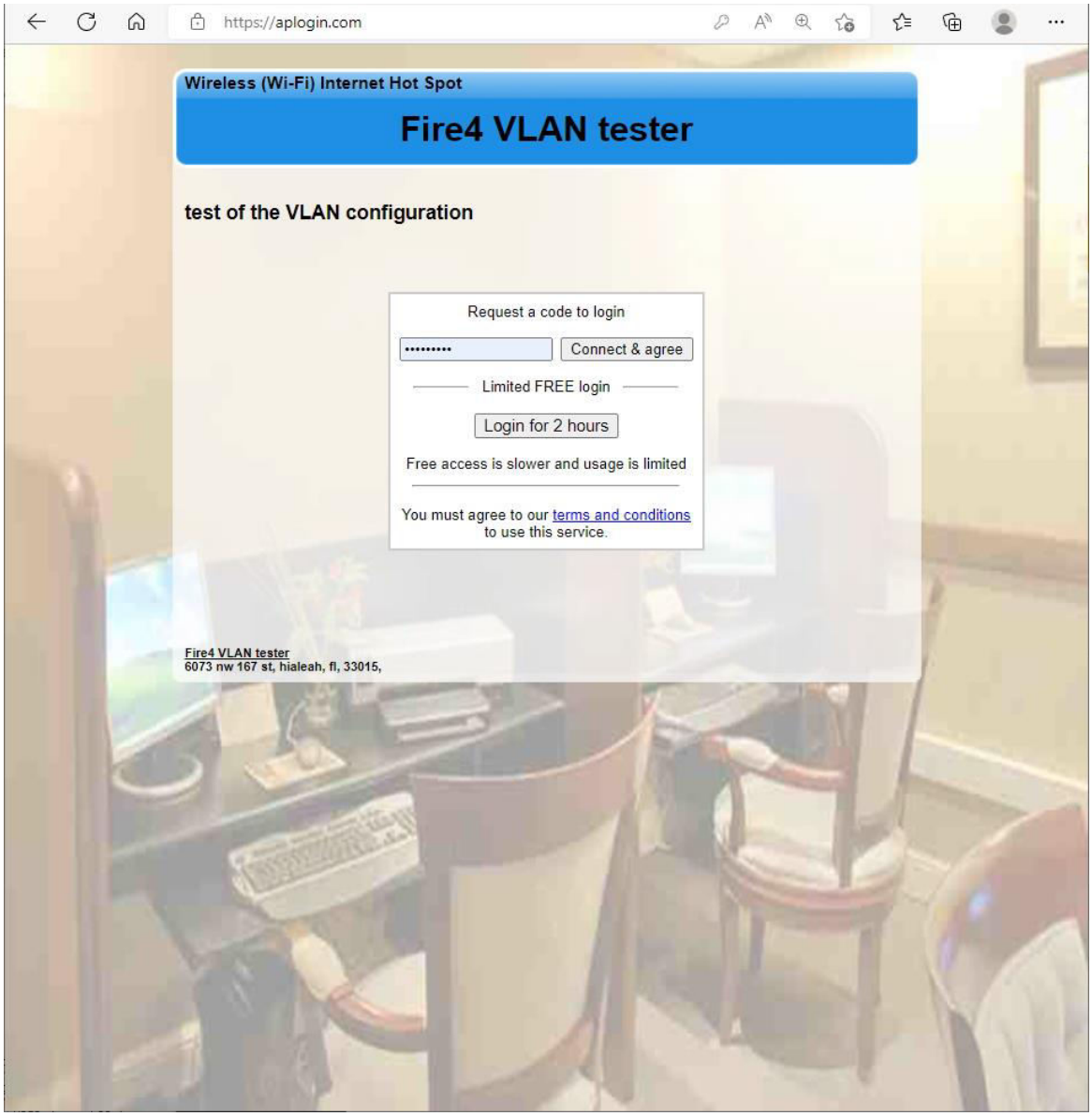
Each login mode has independent configuration for duration, speed and data volume. In addition, each login mode has independent website blocking. The free login button has the following pre-configured parameters;

- Duration that the free access is permitted.
- Duration after the free access is completed that the same user is not permitted to login.
- Maximum download and upload speeds
- Maximum download and upload byte count.
- The login is valid for 1 MAC address only
- Website blocking table that applies only to the free login

A default login screen configuration is shown on the following page.

The identification of an attempt to access a blocked website is detected through packet inspection of DNS requests, and the method functions for both encrypted and non-encrypted DNS requests.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



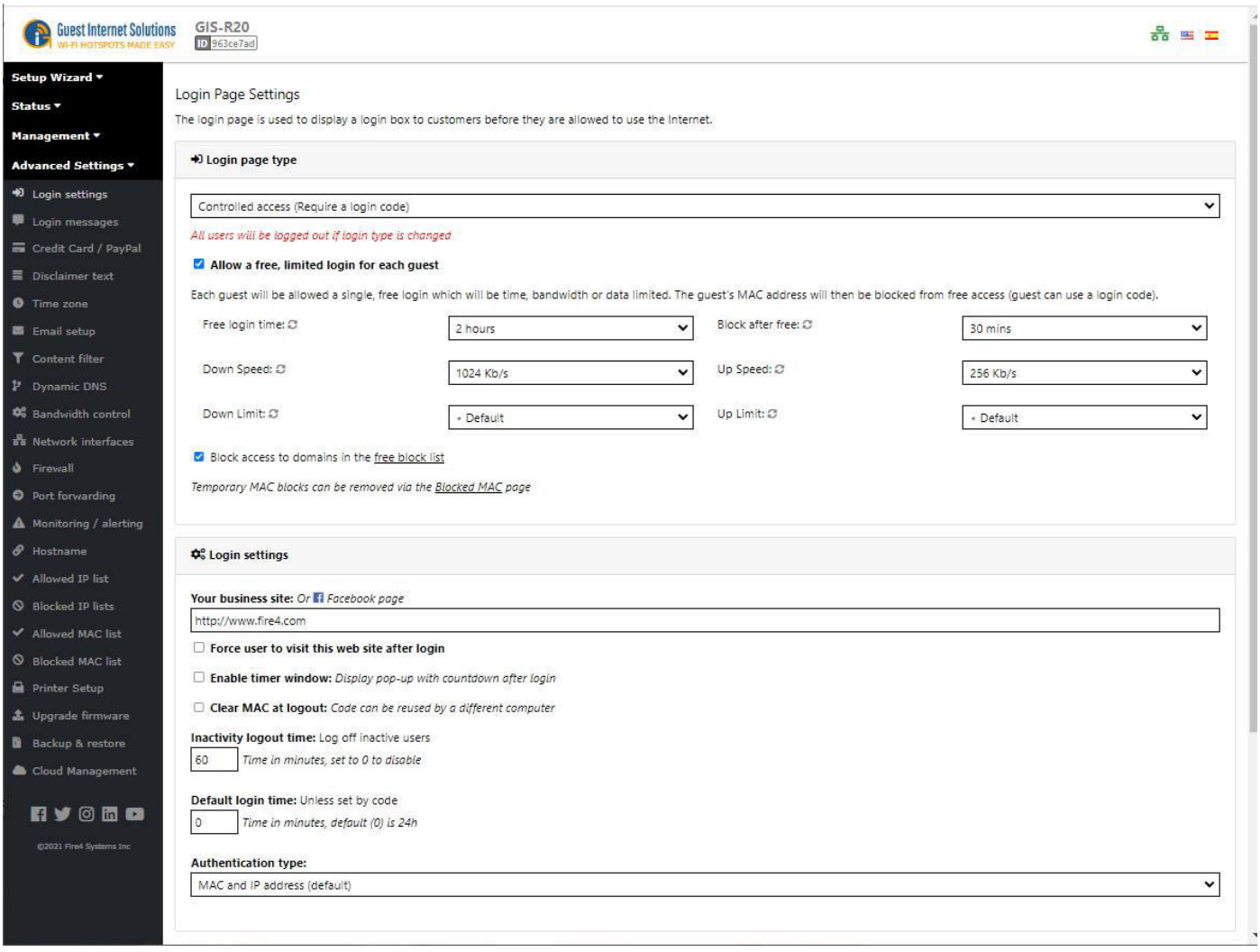
A 2-tier login page example. Access code entry is shown together with a free limited time login button. Credit card billing can also be added to this login method.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The login settings option listed in the advanced settings menu is used to configure the login page buttons.

For the login page configuration shown previously.

- Select controlled access, this will show the login code entry on the login page.
- Check the box: allow a free limited login for each guest, then select the parameters for the free login.
    - Duration of the free access.
    - Duration blocked after the free access.
    - Maximum download and upload data speeds.
    - Maximum download and upload data quantity.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

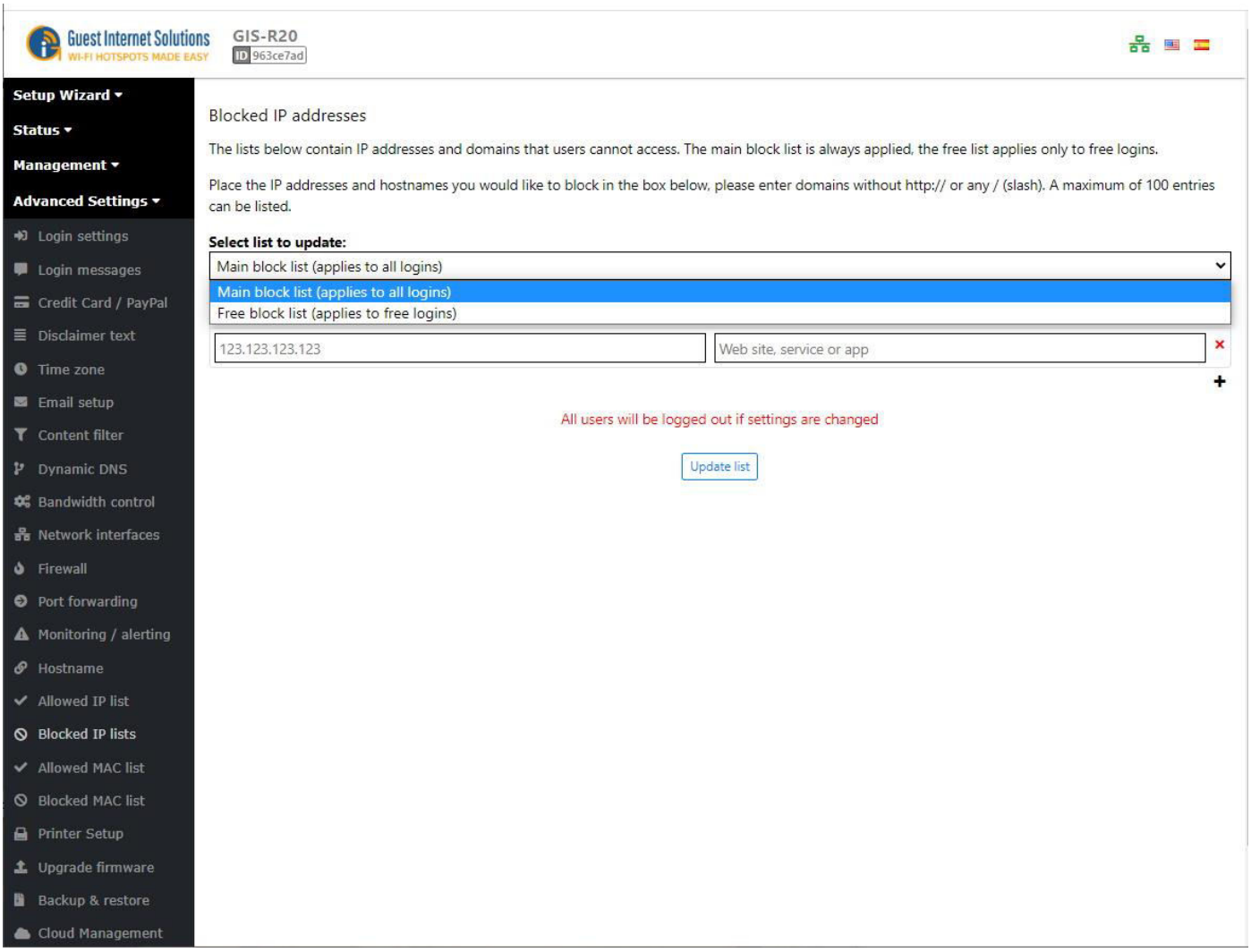
If the website blocking for the free access is required then check the box: block access to domains in the FREE blocked list.

Now open the blocked IP lists settings in the advanced settings menu. The drop down menu shows two lists, the MAIN blocked list, and the FREE blocked list.

Domain names or IP's installed in the MAIN block list are applied to ALL logins, both free and from code access.

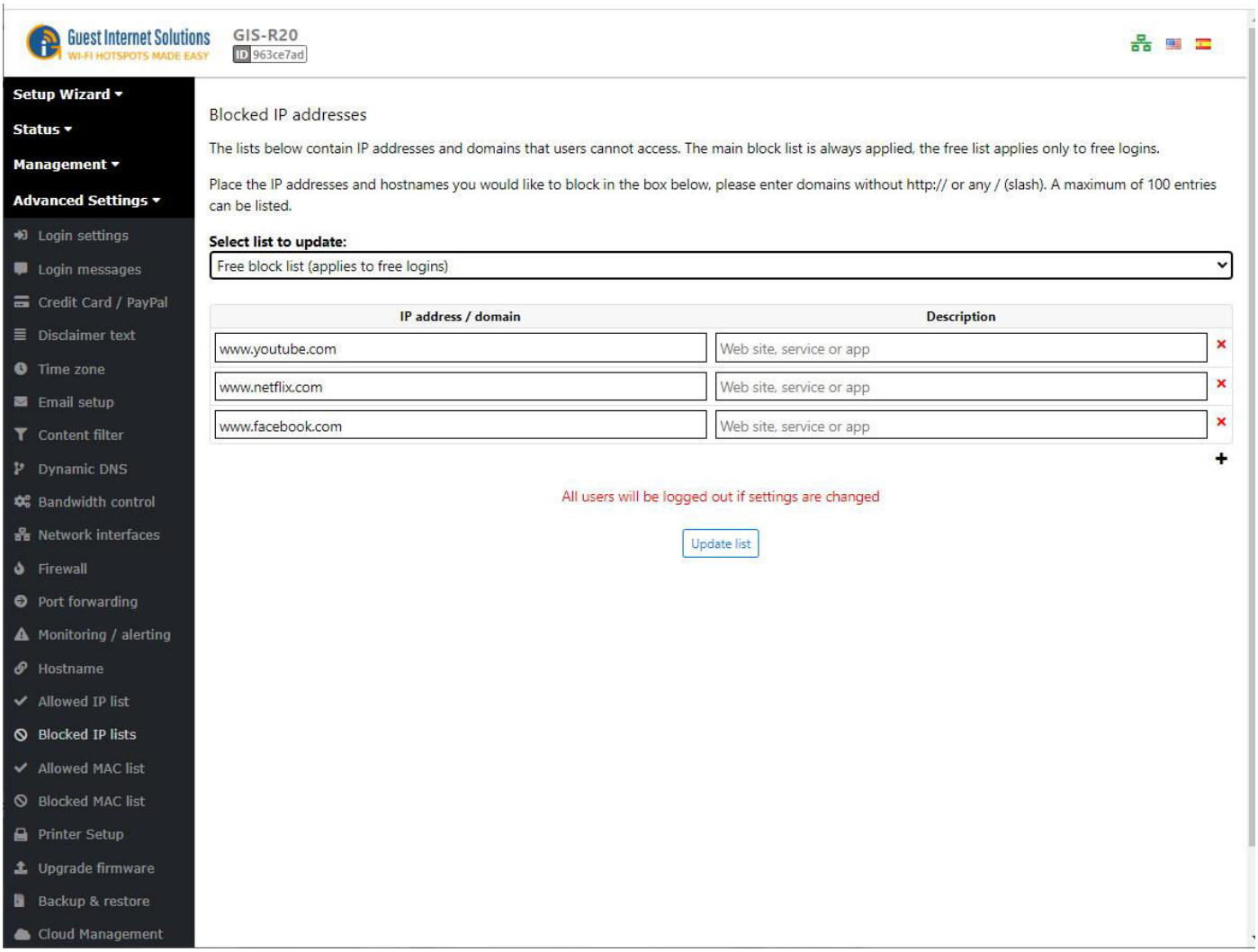
Domain names or IP's installed in the FREE blocked list are applied ONLY to the free login.

Select the table that is required for the installers application, and add the domain names or IP's required. Note that domain name such as Facebook and Youtube can resolve to one of many thousands of IP's and so the domain name should always be used.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

If domains are to be blocked for the FREE login then select FREE login from the drop down menu and enter the domain name that will be blocked. This is shown in the figure below for three domain names.



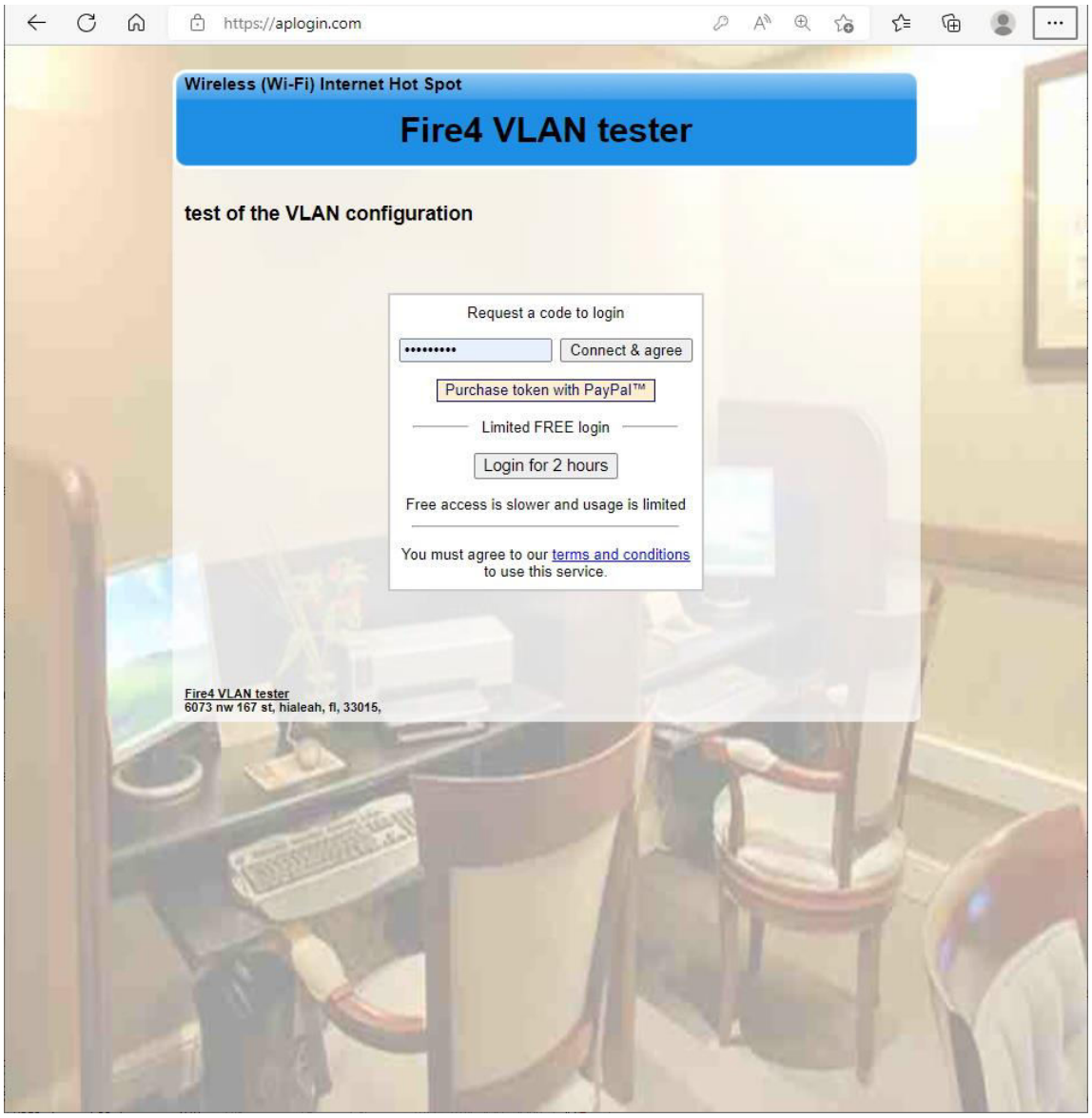
Note that when a user attempts to access one of the domains on the list there will be one of two possible outcomes;

- http:// access (non-encrypted): The user is re-directed to a login page which has a message that the website is blocked.
- https:// access (encrypted): it is not possible to redirect a SSL connection and so the browser will display an SSL_CERTIFICATE_ERROR message for the user.

This result should be documented on the users instructions for use, and indicating which websites are blocked.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

When the credit card purchase of an access code is enabled, a button is displayed for the purchase of access using a credit card as shown in the figure below.



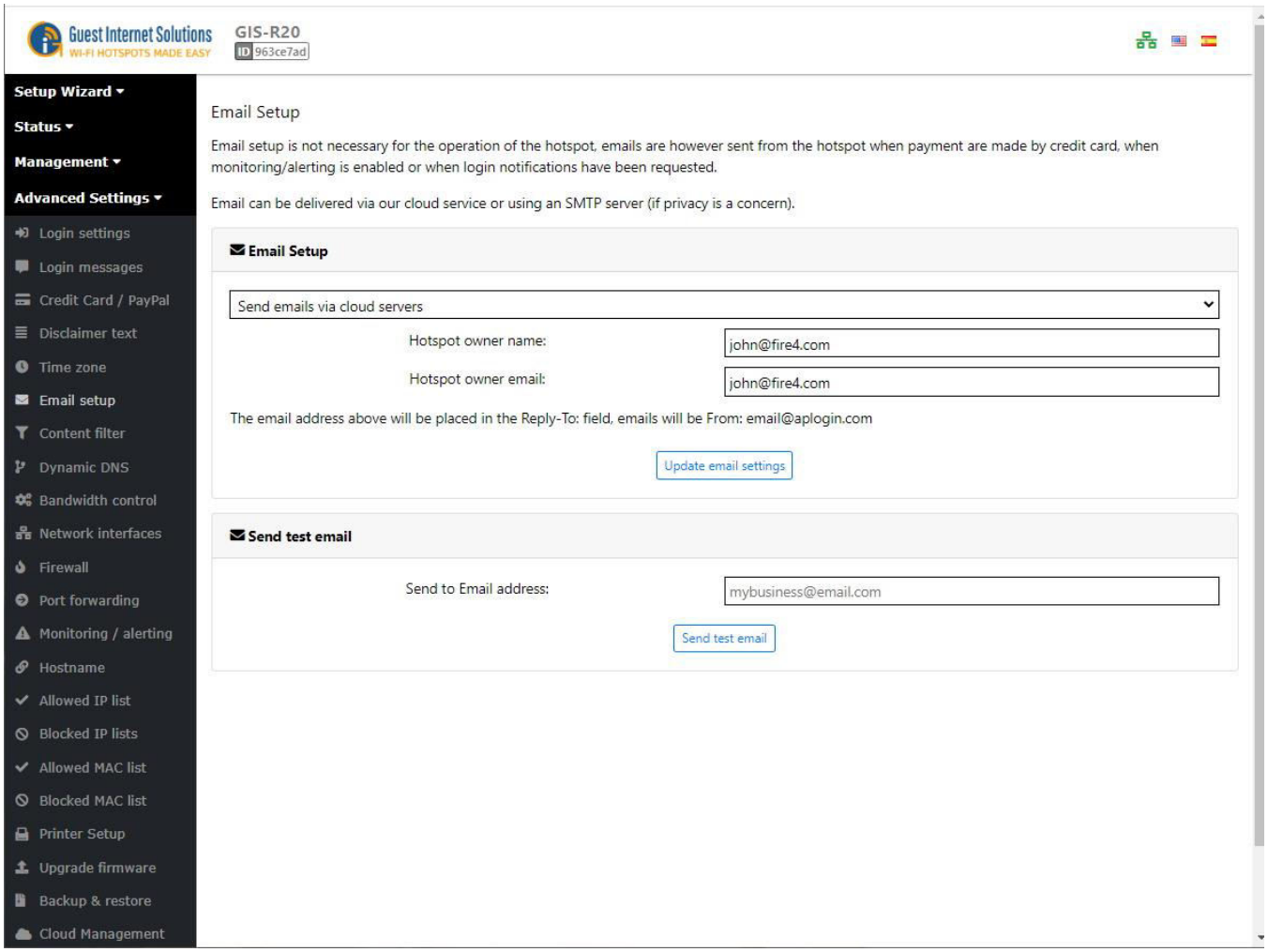
The login page shown includes the limited FREE login button.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Enabling credit card login activates the credit card payment button. Before this can be done however the email configuration must be enabled as the credit card feature posts all messages via email.

Firmware version 2.5.x now offers the option to post messages via the Cloud service. This replaces previous methods that used email services such as gmail, etc.

Open the email tab in the advanced settings section of the menu. The email configuration page is shown below.



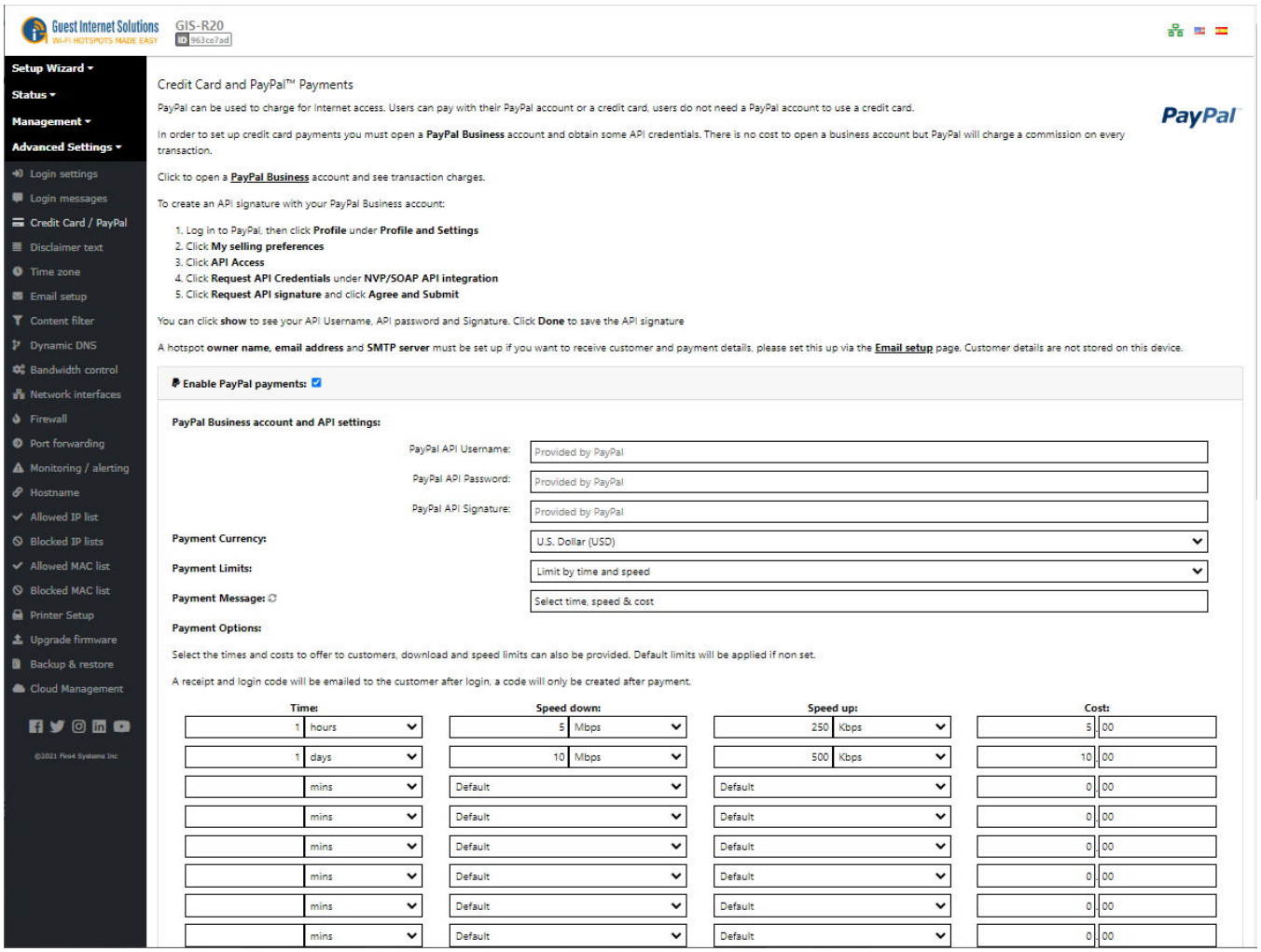
When the email settings have been configured proceed to the credit card configuration.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Open the credit card tab in the advanced settings section of the menu.

Check the box to enable credit card billing via a Paypal business account. See the product manual for more information regarding credit card billing and the procedure that the user must follow.

- Enter the three parameters provided with the Paypal business account.
- Configure the access options and restrictions.
- Configure up to 10 payment options that will be offered to users via the login page drop down menu.



Finally make a test payment to verify that a login code is returned and verify that an email message is sent to the designated email with the transaction information.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

When the free button option has been selected there are several recommendations regarding instructions that should be given to users.

We recommend that the installer should prepare a custom login page that explains to the user the free and paid login procedures selected by the installer. This method is essential for airport installations where there is no other method of providing information for the customer.

- Typically the airport user will have 30 minutes of free Internet with limited speed and possibly website blocking, then the user will be logged out for a preset period, usually 24 hours. The user can then open the login page and purchase Internet access for a period of time, with a higher preset speed limit using a credit card.

The instructions for use should describe the credit card payment process so that the user is familiar with the payment method. Obtain the information for this process from the product manual.

The instructions for use should advise the user that after purchase of access the user must KEEP A RECORD of the access code that is returned after payment, as this will be used for all subsequent accesses until the duration of the code expires.

If any websites are being blocked for the free access (such as streaming video) then the user should be advised about this on the login page.

Hotel guests should be provided with written instructions in each room describing how to use the Internet.

- The typical procedure for hotel guests is to provide a free low speed service that is not time limited. There is usually no website blocking however the speed is set low so that streaming of video data is poor quality. If the guest wishes to have high speed Internet then that is purchased via the login page using a credit card.

Document what the user will see when the website is blocked. In the case of an attempted https:// website access (encrypted) the browser will display an SSL_CERTIFICATE_ERROR message for the user.

The instruction information should also advise the user that if the users is logged in to the free service and wished to switch to the paid service the procedure to follow is;

- Open the login page, aplogin.com, the remaining time and logout button is shown.
- Click the logout button.
- Open the login page, aplogin.com, select the credit card payment option.

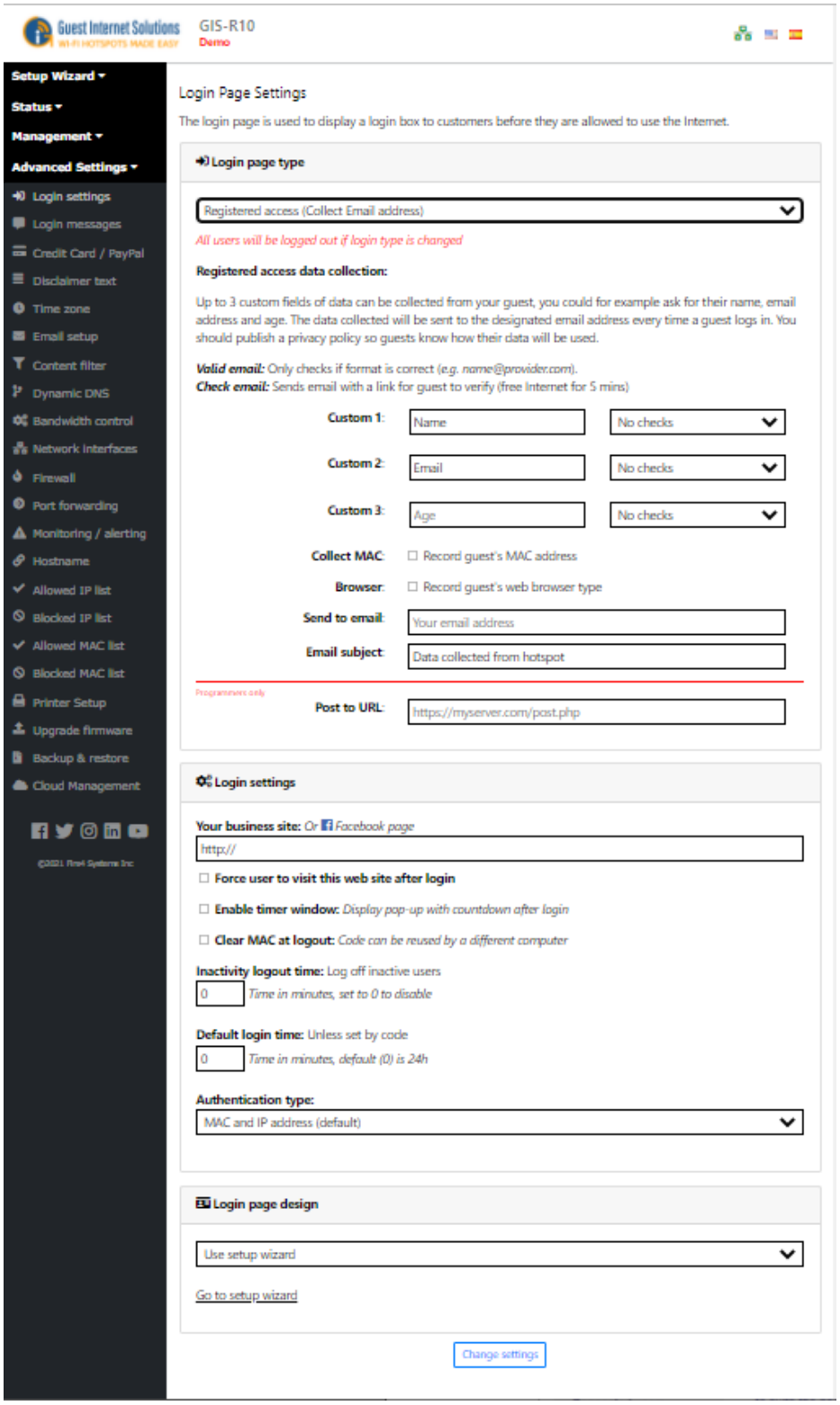
Other types of businesses such as trade shows, campgrounds and sports events can print and distribute flyers that explain the rules of Internet use.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Registered Access

By enabling the Register Access the user has to provide the data requested (i.e email address) before proceeding to the login page.

Before setting the Login Page to Registered Access you need to configure the Email Setup page.



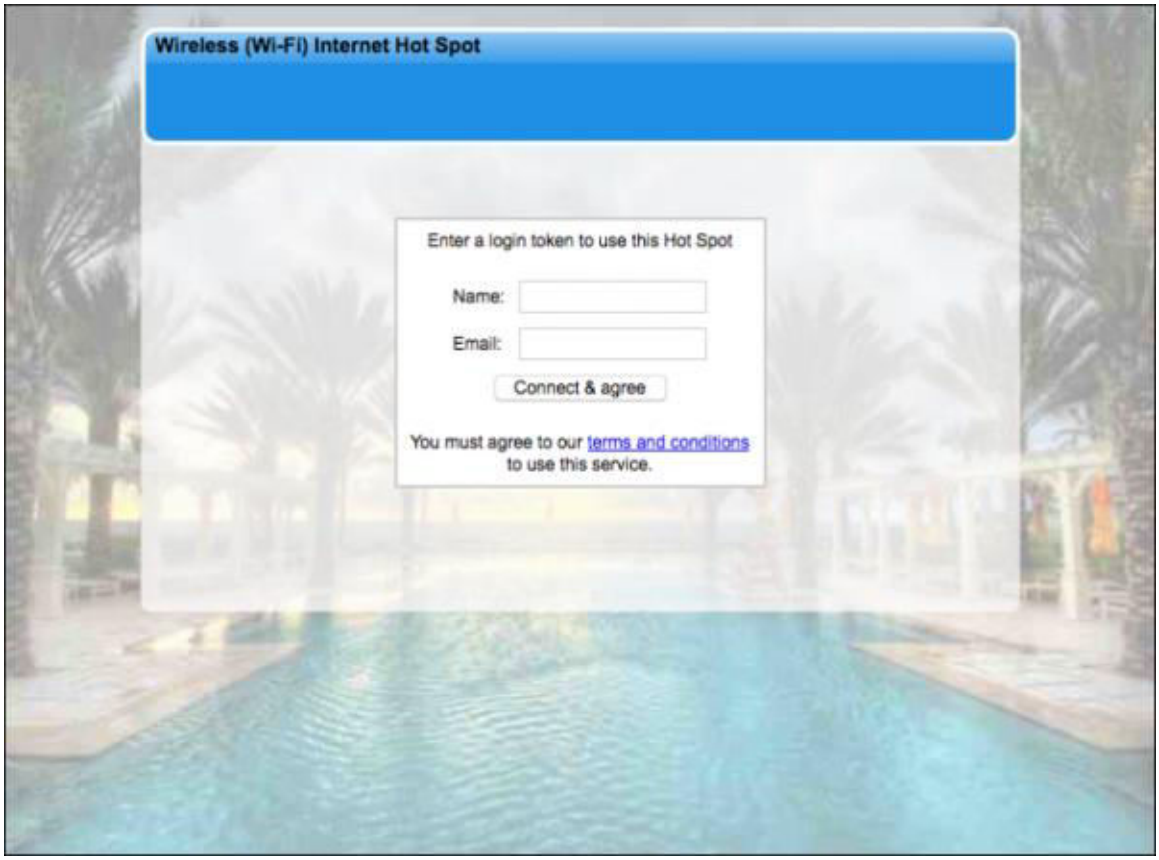
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Registered access data collection permits three data fields to be specified, and has the option to check the format of the data entered.

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 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.

No personal information is stored on the gateway.

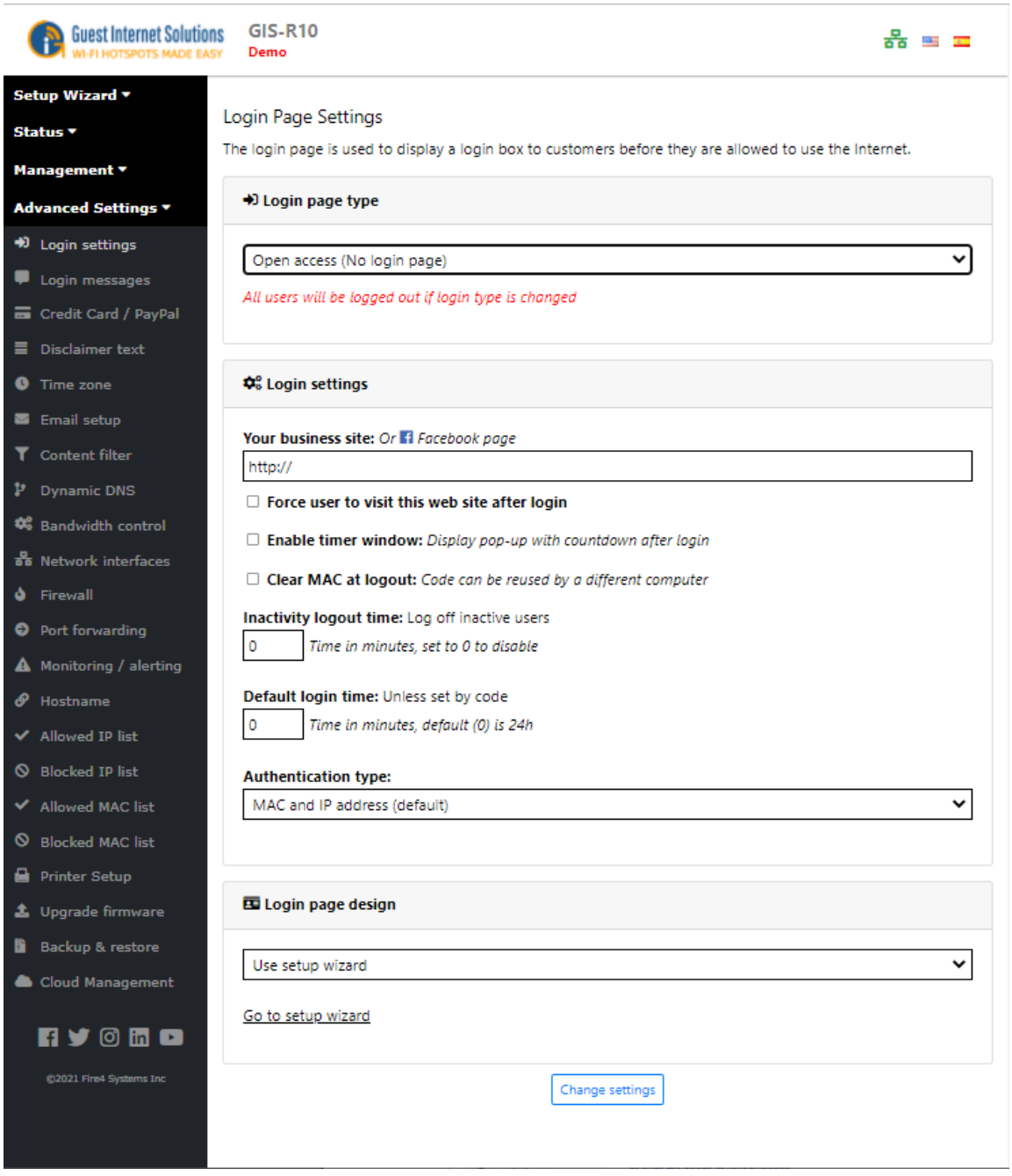


When clicking in "terms and conditions" the user will be redirected to a page with the disclaimer information. You can see how to edit the disclaimer in the section that describes the disclaimer text.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Open Access

In the Open Access mode there is no login page, however all controls will still be applied to the each user. The Open Access mode is used by condos that provide a free Internet service to residents, however each resident has download and upload data speed limits and the firewall controls are also applied to prevent misuse of the free service.

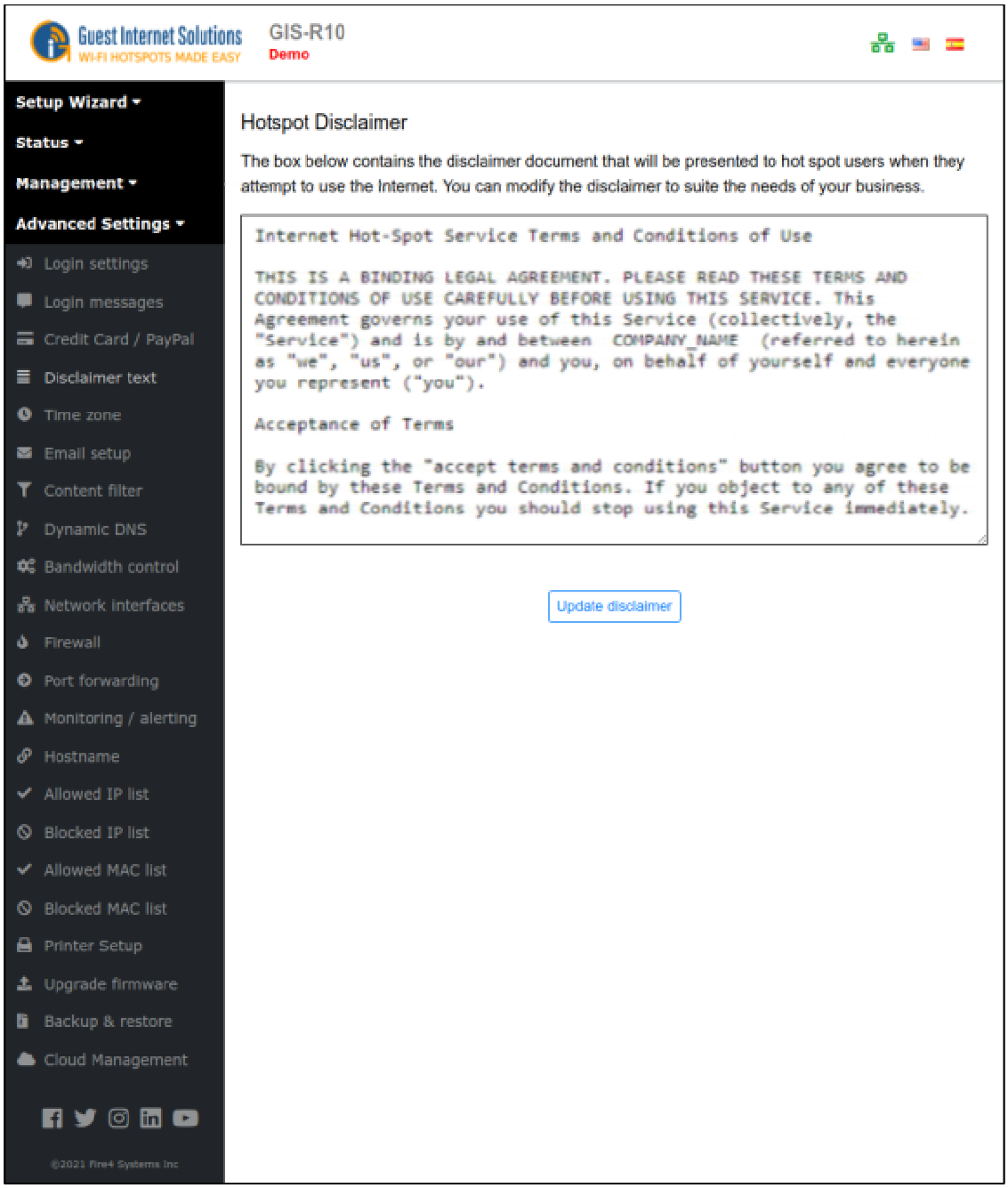


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Edit Disclaimer

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 me 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.

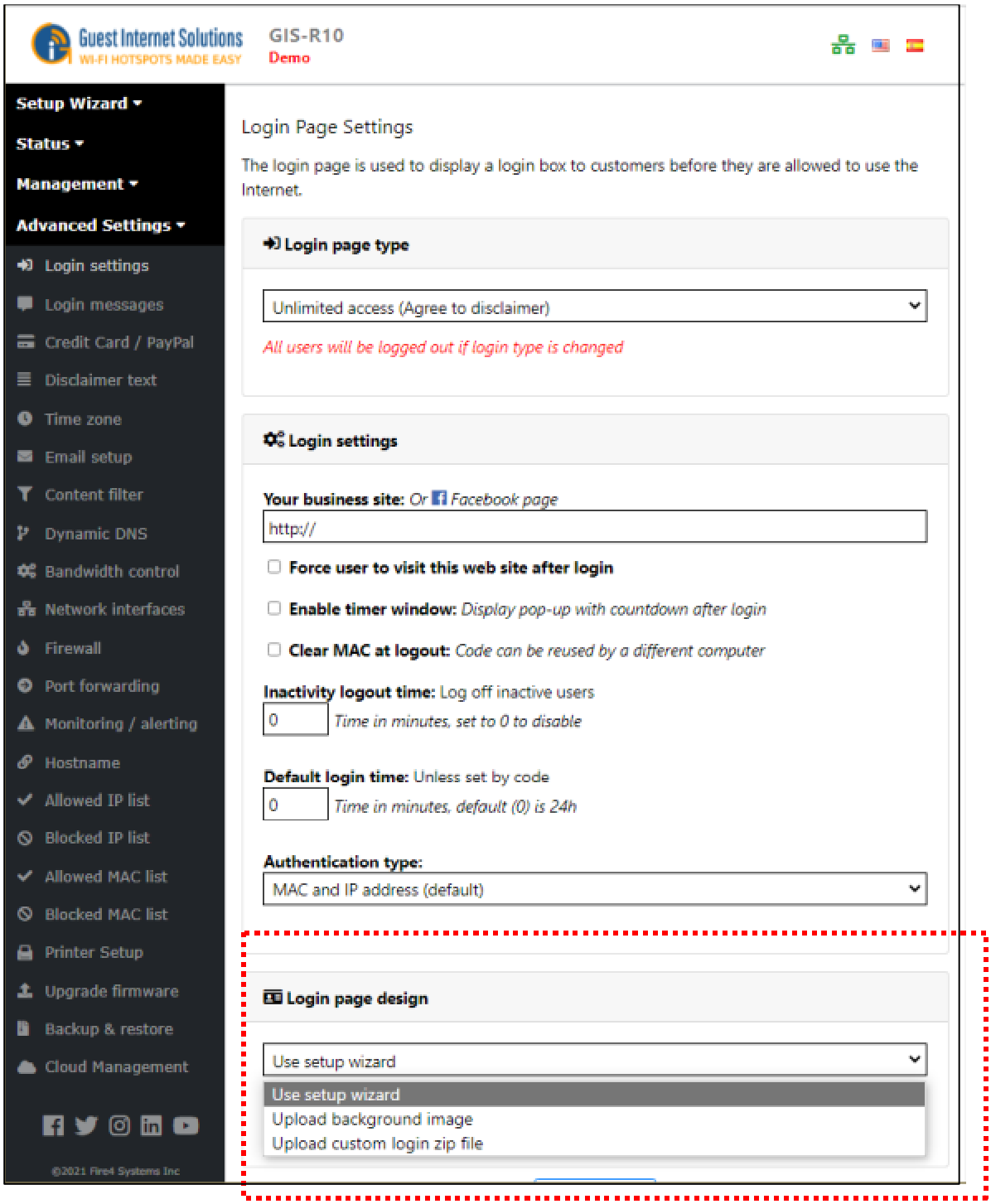


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Custom Login Pages

The login page can be changed at any time by logging in to the unit as admin and then clicking on the 'login settings' option. The GIS units offer three custom login page options:

- Wizard: select 1 of 12 backgrounds during the setup process
- Custom background: upload a JPG image
- Custom login page: login page using customized web page using HTML, JavaScript and CSS

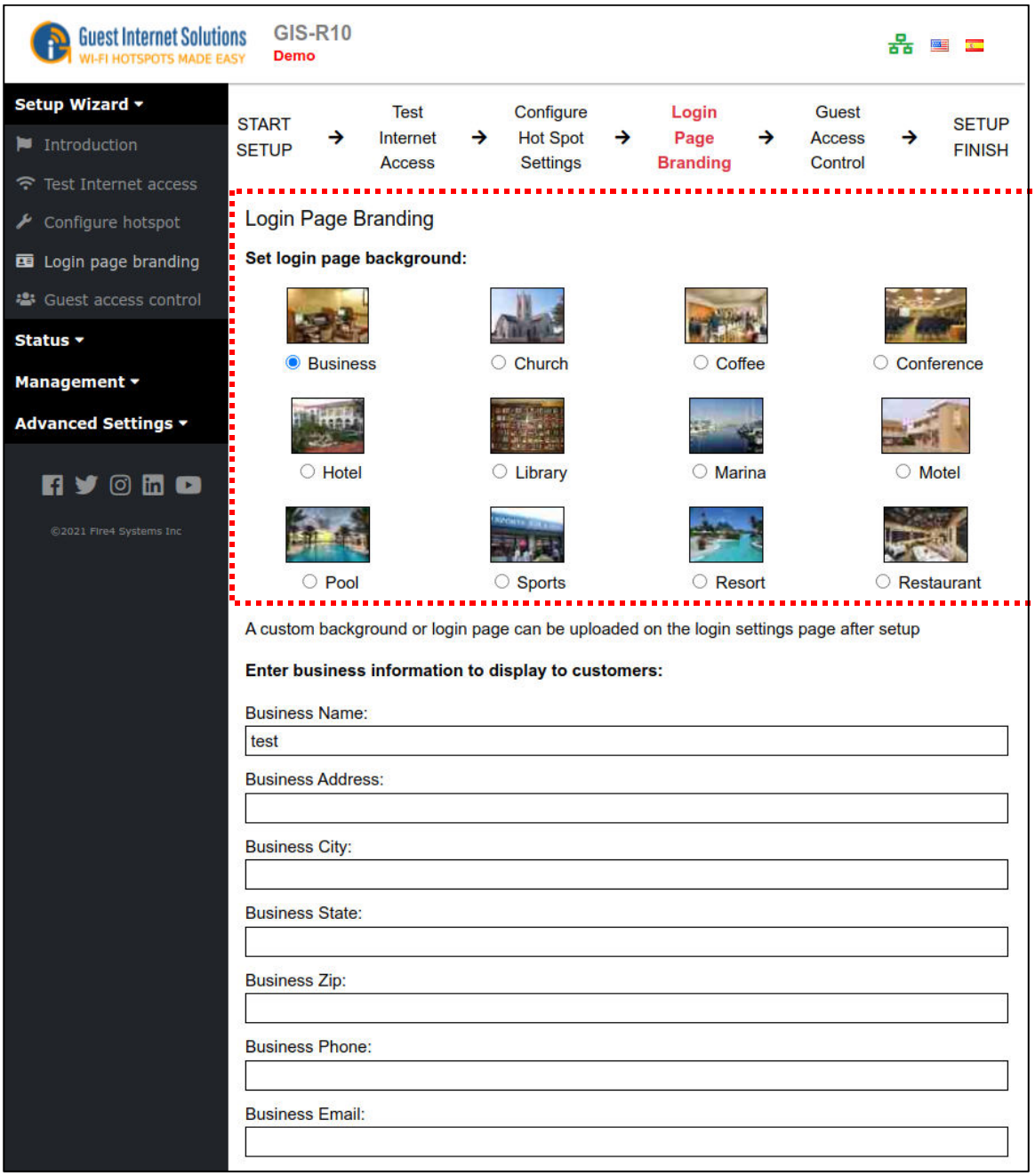


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Wizard

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.

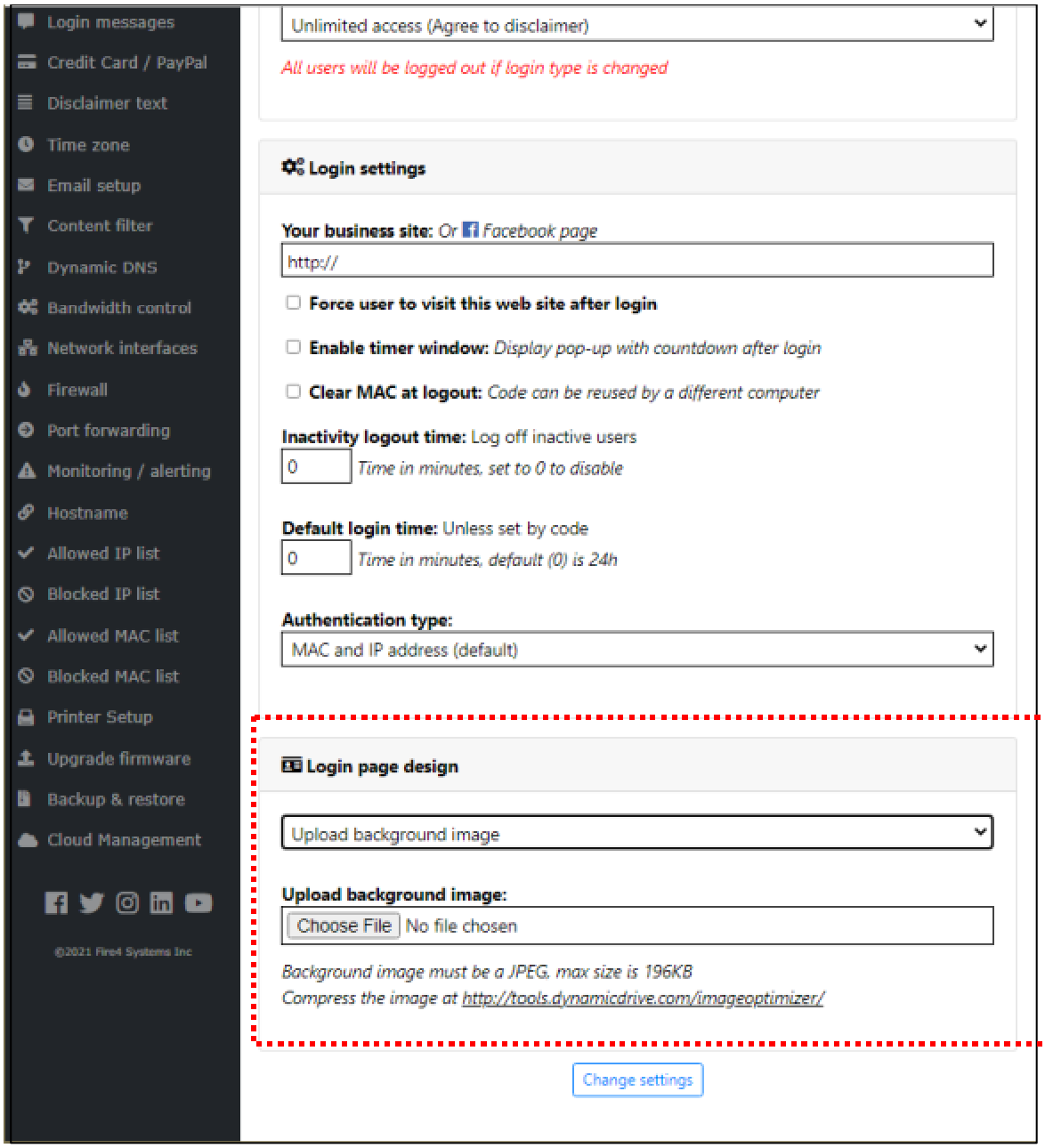
Business Center	Church	Coffee Bar	Conference Room
Hotel	Library	Marina	Motel
Pool Area	Sports Bar	Resort	Restaurant



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Custom Background

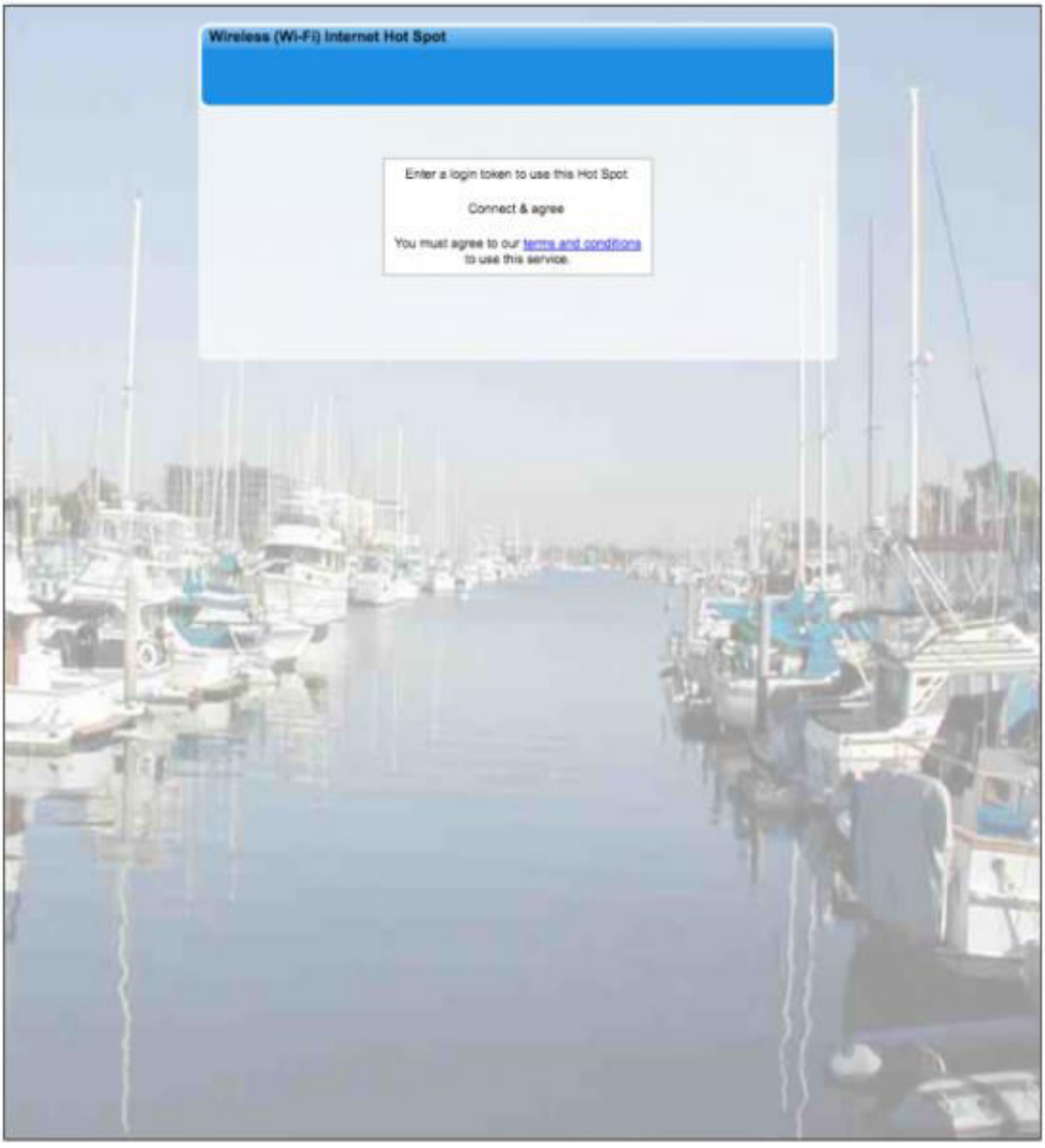
A login page custom background can be created in JPG format and uploaded using this feature. The image size should not exceed 196KB, however it should be made as small as possible so that the login page loads quickly for the user.



The background image will be placed behind the login information box and the image contrast will be reduced to highlight the information box.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The image can be a composite photo plus logo prepared using an image editor.

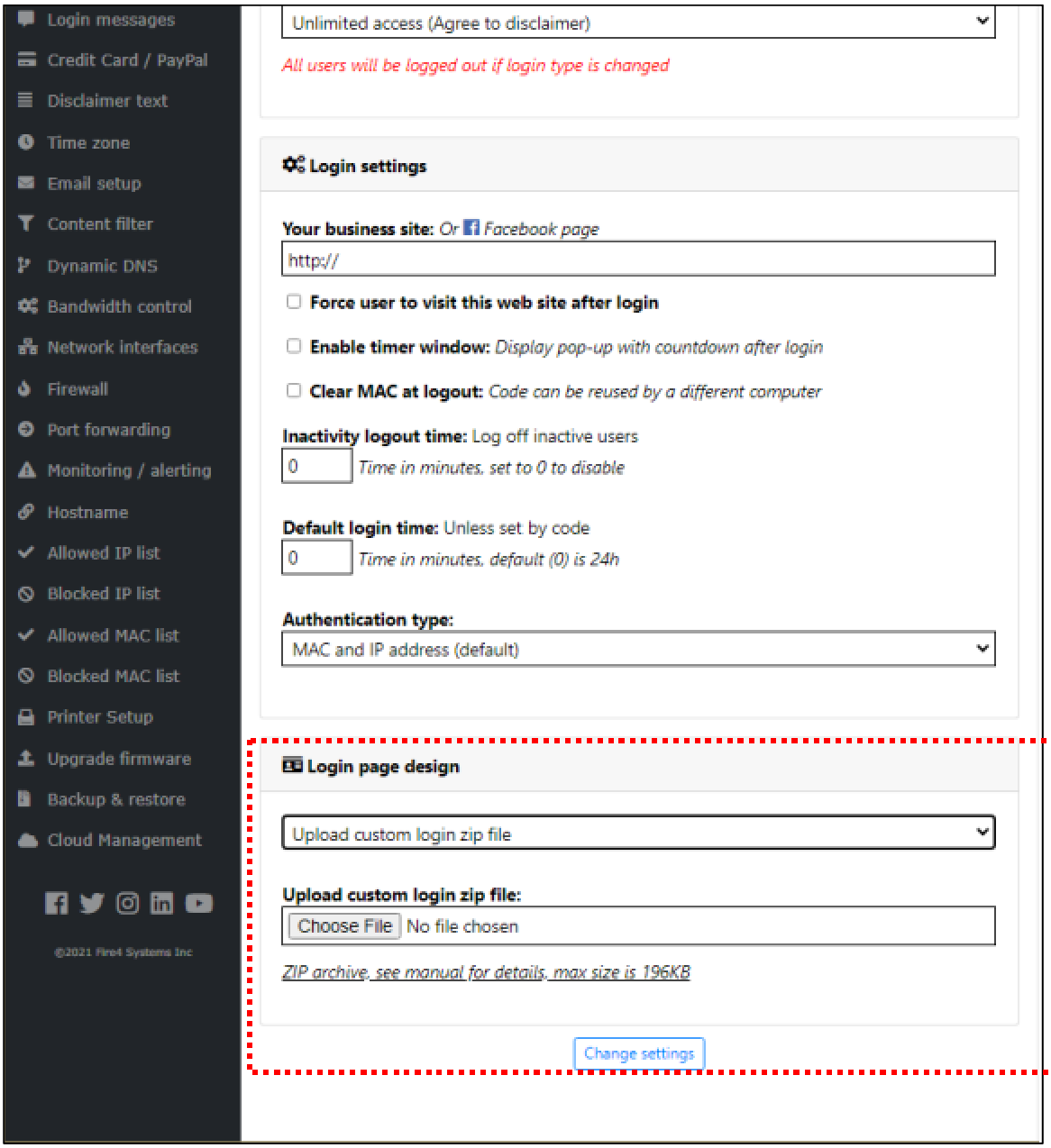


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Custom Login Page

A custom login page can be created using HTML.

The only requirement to create a login page is knowledge of programming using HTML, CSS and Javascript. Any web developer can create a login page, you can also contact us for an estimate value.



The GIS units log in page can be completely customized including: logo, corporate identity, information about the hotspot or public Internet service and advertising banners.
The login page is uploaded to the gateway as a single zip file, no more than 196KB when compressed.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The zip file needs to contain a file called **'login.html'** (all lower case, be careful not to call the file Login.html), it can also contain any other files including: images, HTML, CSS, JavaScript etc.

The login.html file must include the text shown below to locate the login box on the page.
<!--LOGIN-->
Login page sample designs can be downloaded from the Login Page Templates page.

CSS IDs

To customize the login box, there are a few CSS IDs that you need to use:

outer_table is the gray line around the login box.

inner_table is the background of the login box.

main is the most important, as all the login box codes are held within this, so can be used to select login box elements with CSS for example:

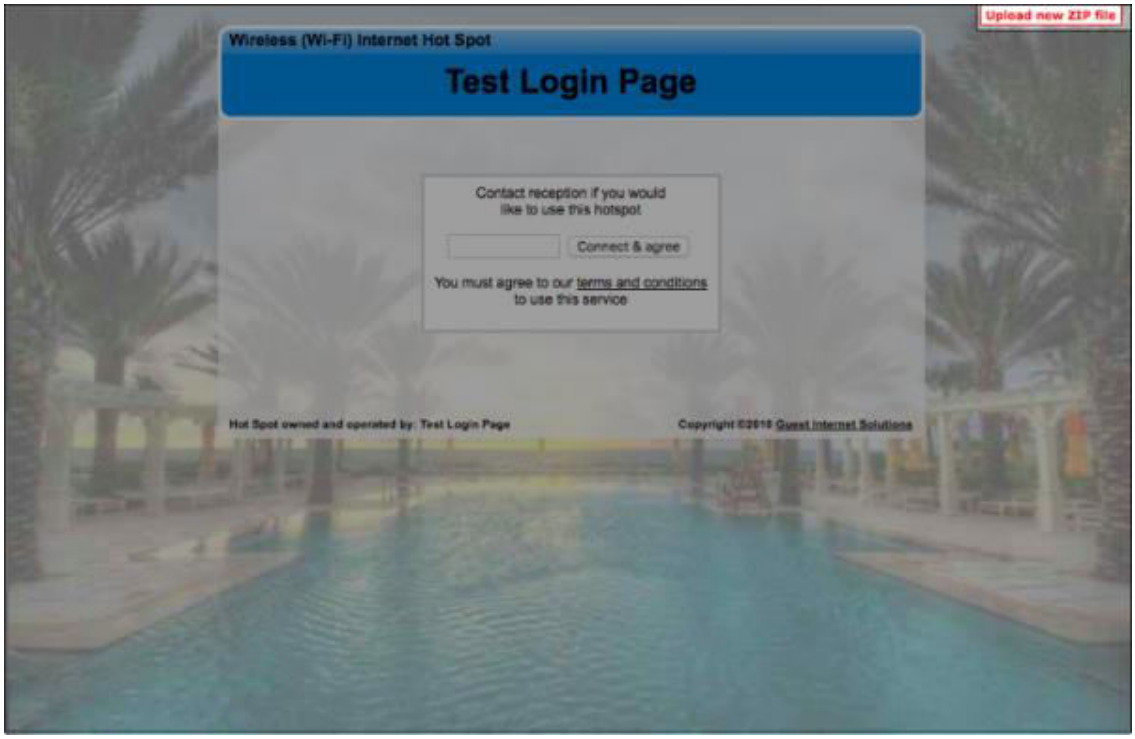
```
#main input[name="data1"]{}
```

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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 click here

User: test Password: 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.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Login Page Templates

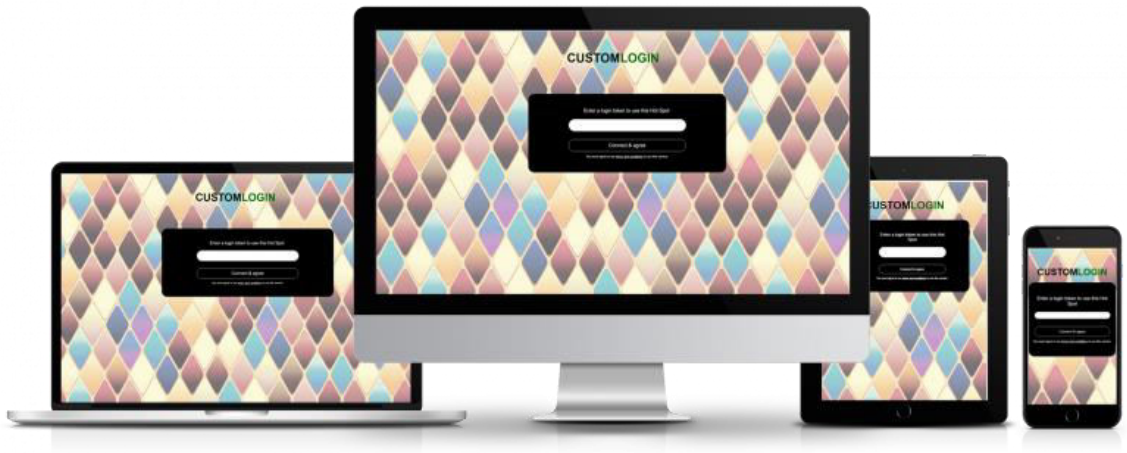
We offer a range of free templates that can be uploaded to your GIS unit and be used in any Login Page Type.

https://www.guest-internet.com/docs/en/admininterface/advanced/loginsettings/loginpagetype

Choose below the layout that best suits your business, download it and edit the information needed with basic HTML and CSS:

Download template here

https://www.guest-internet.com/docs/en/admininterface/advanced/loginsettings/customloginpages/customloginpage/templates/basic.zip



Download template here

https://www.guest-internet.com/docs/en/admininterface/advanced/loginsettings/customloginpages/customloginpage/templates/pattern.zip

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Download template here

https://www.guest-internet.com/docs/en/admininterface/advanced/loginsettings/customloginpages/customloginpage/templates/pink_spa.zip

Download template here

https://www.guest-internet.com/docs/en/admininterface/advanced/loginsettings/customloginpages/customloginpage/templates/relax.zip

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Download template here

https://www.guest-internet.com/docs/en/admininterface/advanced/loginsettings/customloginpages/customloginpage/templates/science.zip

Download template here

https://www.guest-internet.com/docs/en/admininterface/advanced/loginsettings/customloginpages/customloginpage/templates/water.zip

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

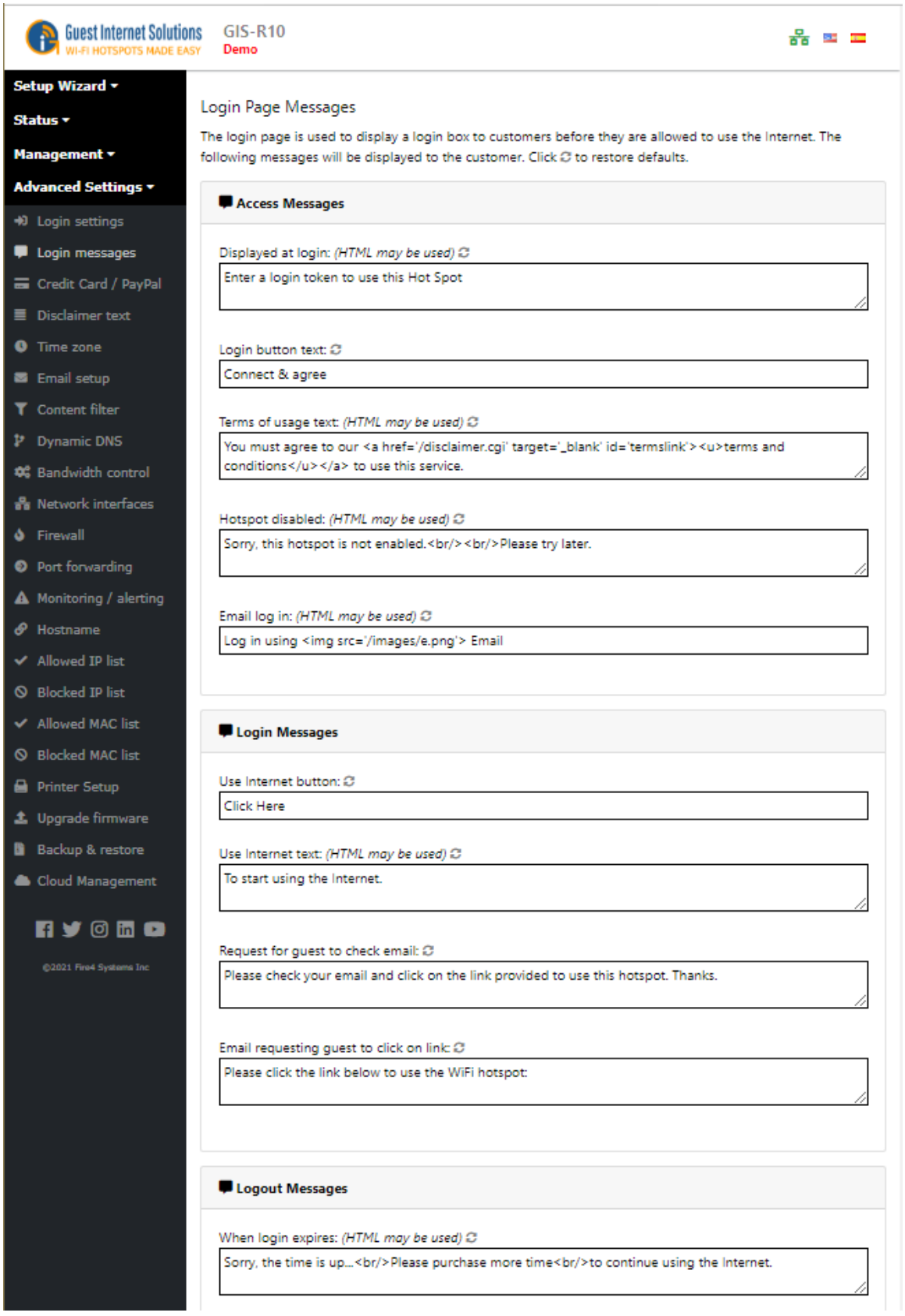
Download multilingual template here

https://www.guest-internet.com/docs/en/admininterface/advanced/loginsettings/customloginpages/customloginpage/templates/multilanguage.zip

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Login Page Messages

All messages displayed on the login pages can be modified.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Translate the login page messages if the hotspot is being setup in a non-English speaking country, permitting interaction with the users to be in the native language.

Access Message 1: When the Controlled Access mode is selected this message is displayed in the login box shown on the login page.

Access Message 2: This message appears on the button in the login box.

Access Message 3: When the Unlimited Access mode is selected this message is displayed in the login box shown on the login page.

Access Message 4: When the Hotspot Availability mode is enabled this message is displayed in the login box shown on the login page when the hotspot is inactive.

Access Message 5: When the Registered Access mode is selected this message is displayed in the login box shown on the login page.

Login Message 1: This message is displayed on the button after the Access Code has been successfully entered.

Login Message 2: This message is displayed below the button with the Login Message 1.

Logout Message 1: This message is displayed in the timer box when the Access Code time has expired.

Logout Message 2: This message is located inside the button of the timer box.

Timer Message 1: This message is shown at the top of the timer box.

Timer Message 2: This message is shown at the lower part of the timer box.

Logout Message 3: This message is shown in the timer box after logout.

Logout Message 4: This message is shown at the lower part of the timer box after logout.

MAC Message: This message is shown to users that are on the allowed MAC list.

Error Message 1: This message is displayed in the login box when there is no Internet connection.

Error Message 2: This message is displayed in the login box when the user has been blocked due to violation.

Error Message 3: This message is displayed in the login box when the web site the user is trying to access has been blocked.

Error Message 4: This message is displayed in the login box when the user has been blocked due to the use of file sharing software.

Error Message 5: This message is displayed in the login box when an operational error has been detected.

Error Message 6: This message is displayed in the login box when the access code is not valid.

Error Message 7: This message is displayed in the login box when the access code is in used.

Error Message 8: This message is displayed in the login box when the access code has exceeded its limit.

Error Message 9: This message is displayed in the login box when the access code expired.

Error Message 10: This message is displayed in the login box when the login text box is empty.

Error Message 11: This message is displayed in the login box when the email address provided by the user is invalid.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Credit Card / PayPal™

The credit card billing feature allows you to sell Internet access by charging your customers' credit card.

The feature requires you to have a valid business account with PayPal™, a personal account cannot be used to charge credit cards.
Your customers **do not** need to have a PayPal™ account, they can pay with credit card.

Before continuing with the billing setup you need to configure the Email Setup.

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.

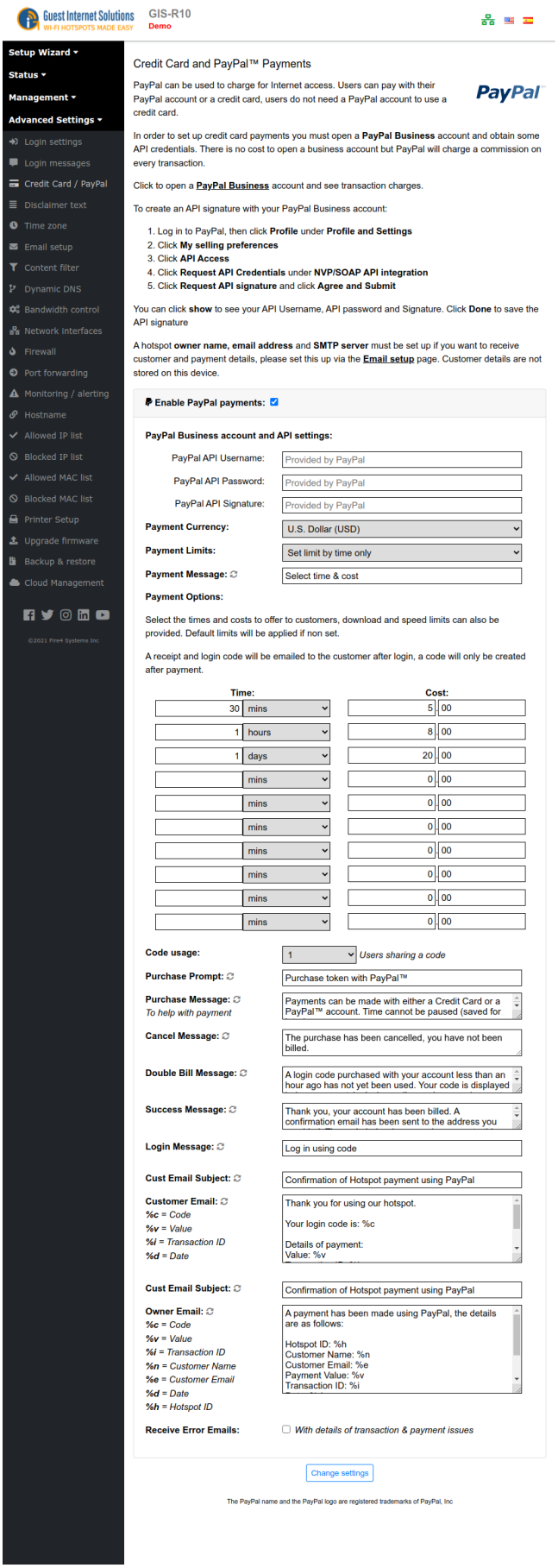
A log is maintained that has a transaction ID. If you need additional information it is necessary to log into your PayPal™ business account and use the transaction ID to obtain additional information about the transaction.

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.

Currently this feature is available in all of our product models, except GIS-R2.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

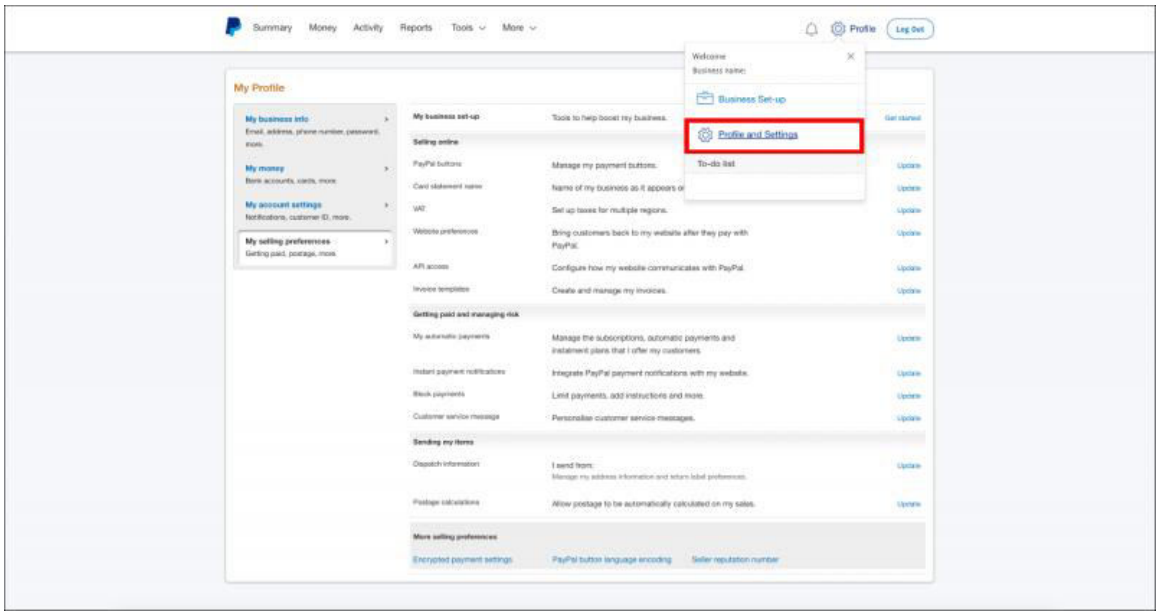


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

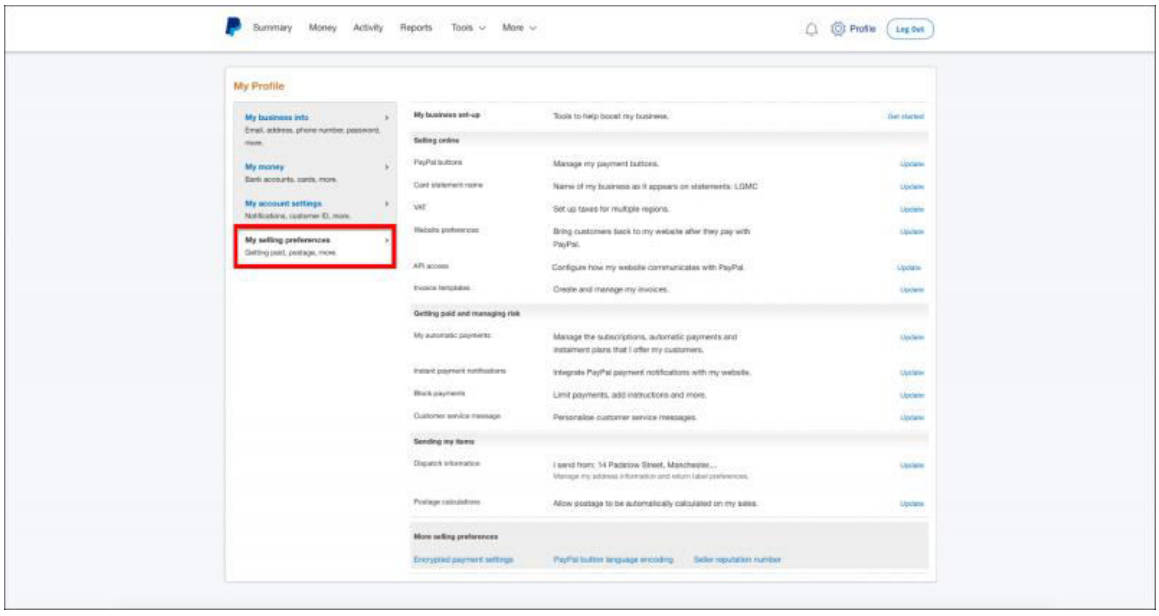
PayPal™ Setup: Step 1:

Creating an API signature with your PayPal™ Business account:

1. Log in to your PayPal™ account, then click **Profile and Settings**

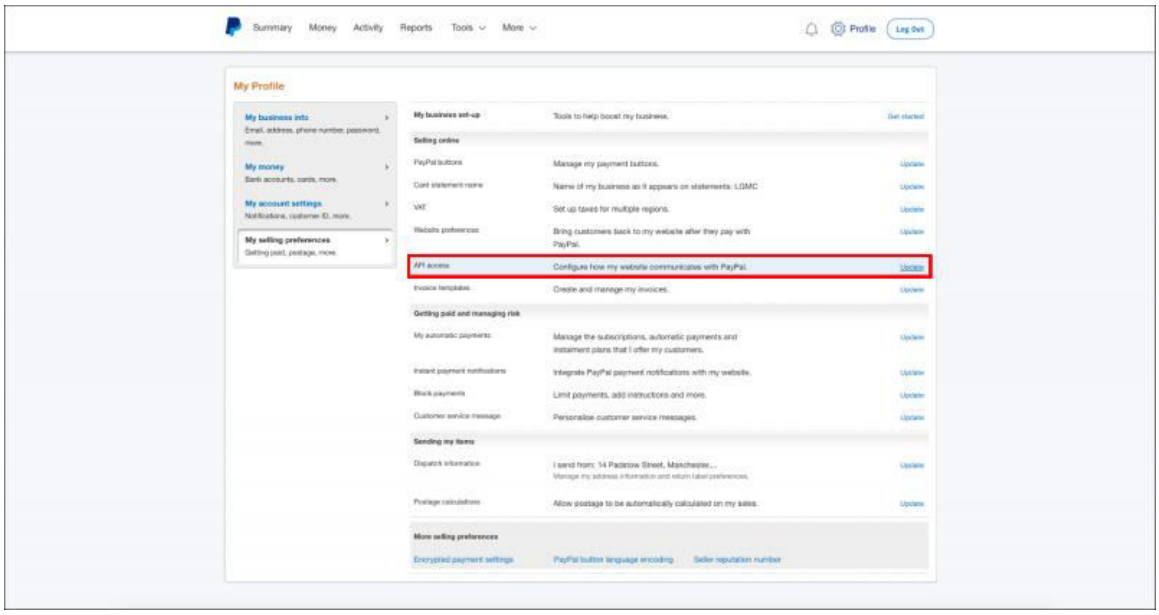


2. Click **My selling preferences**

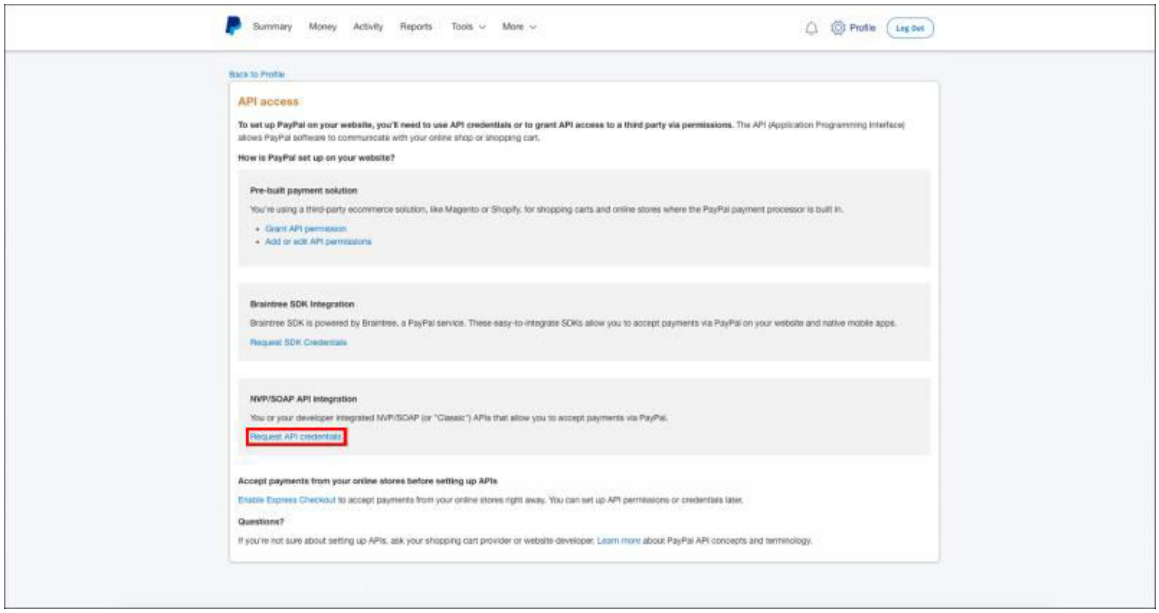


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

3. Click **API access**

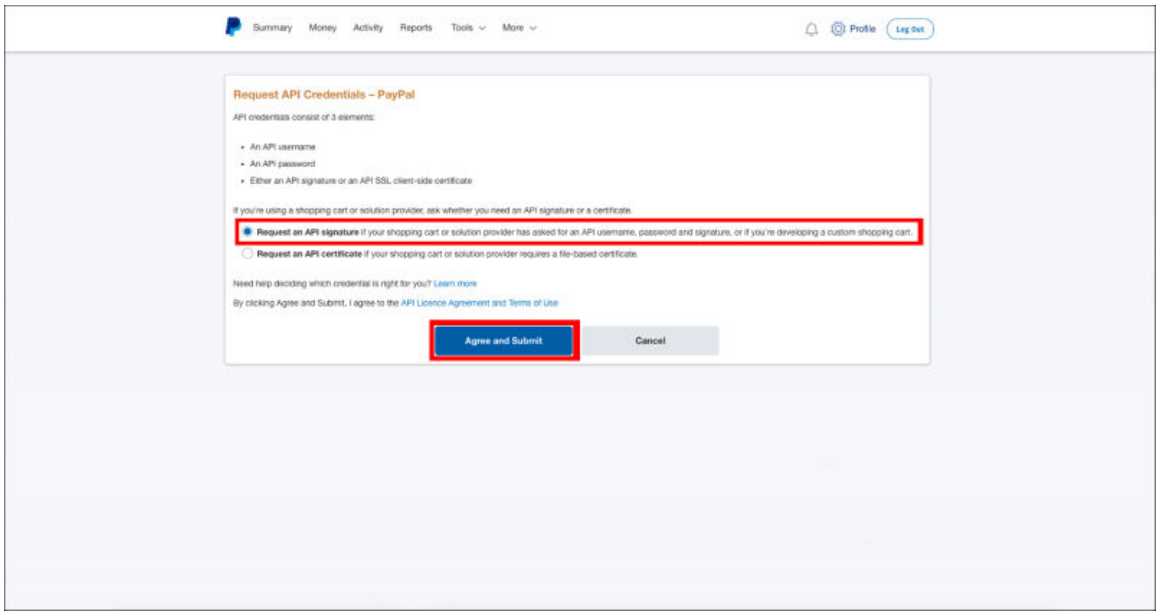


4. Under **NVP/SOAP API integration** click **Request API credentials**

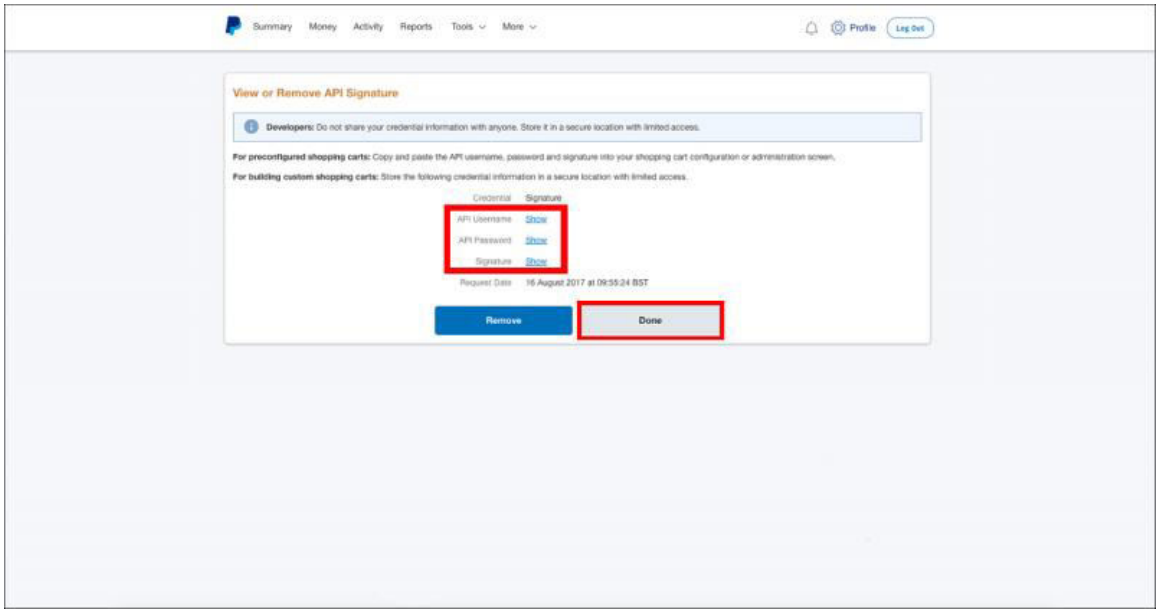


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

5. Select **Request API signature** and click **Agree and Submit**



6. You can click **Show** to see your API Username, API Password and Signature. Click **Done** to save the API signature



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.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

PayPal™ Setup: Step 2:

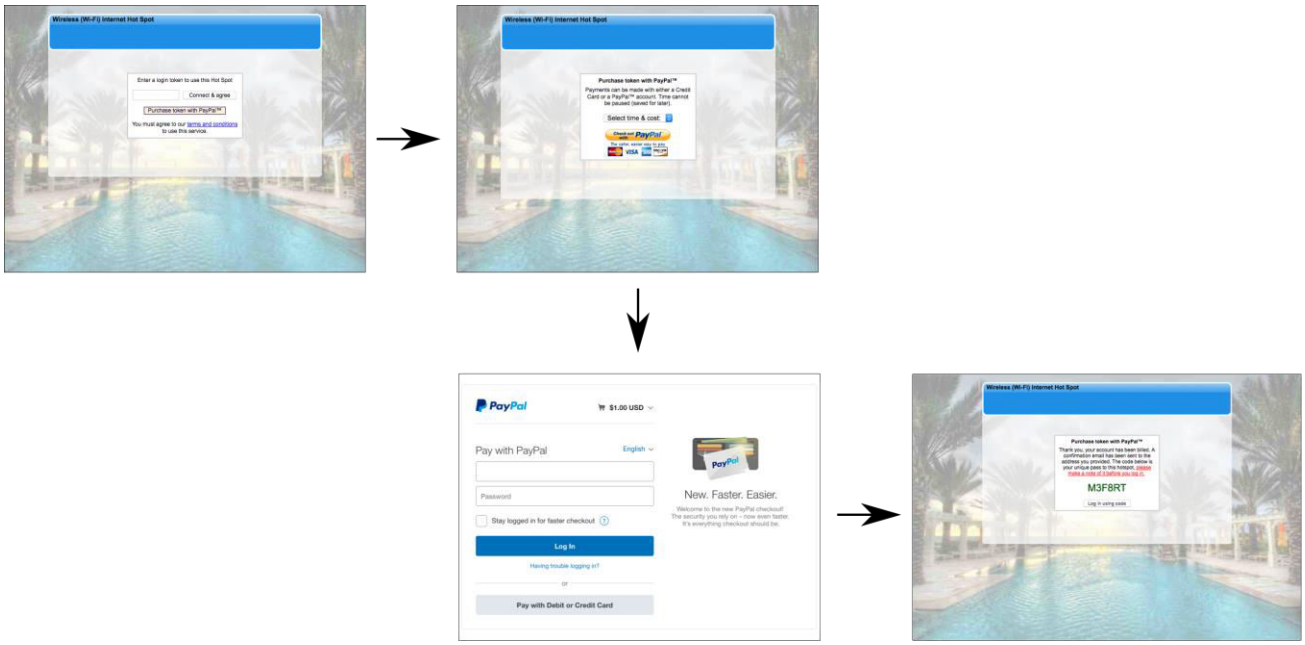
Go to the Credit Card/PayPal section of your admin interface:

- Check the **Enable PayPal payments** checkbox.
- The **PayPal Business account and API settings** section must be filled with the information acquired on **Step 1**
- Select the currency you want to use on the **Payment Currency** drop down menu
- Select how you want to set limits (time, data or speed) on the **Payment Limits** drop down menu
- **Payment Message** is the message the guest is going to see on the login page, before selecting a option
- **Payment Options**: enter up to ten (time,data or speed and cost) parameters using the drop down menu. These are the Internet access packages that will be offered to users.
- The **Code usage** option allows you to select how many users or devices are permitted to use the code.

The boxes below the payment settings are the messages shown on the user's computer screen to indicate success or failure of the purchase.
Two message boxes at the bottom of the page show the format of the messages sent to the hotspot user and to you. Take care if changing these messages.

There is a final check box **Receive Error Emails**:
When a transaction does **not** complete then it is not necessary to receive a message about this in most cases. However you 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.

A complete transaction record is provided by the PayPal™ business account, and the information can be downloaded and imported into popular accounting programs.
The GIS gateway also stores a report summary in the section Billing Reports.



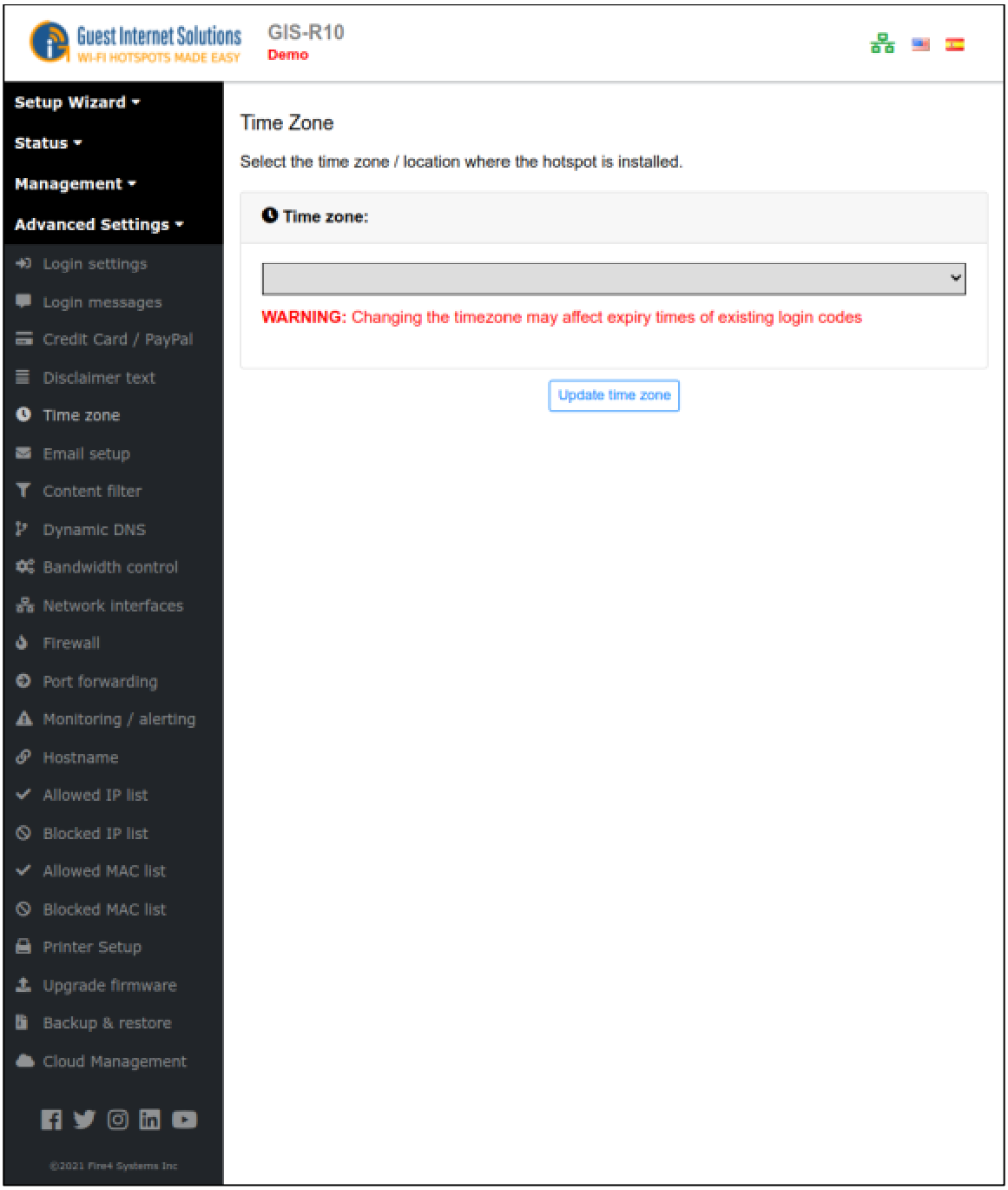
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Timezone

The timezone is set initially during the setup wizard process.

If the product is moved to a different timezone at a later date then the new timezone can be selected using this page.

Before changing the time zone all codes should be deleted as a change of timezone will invalidate the codes.

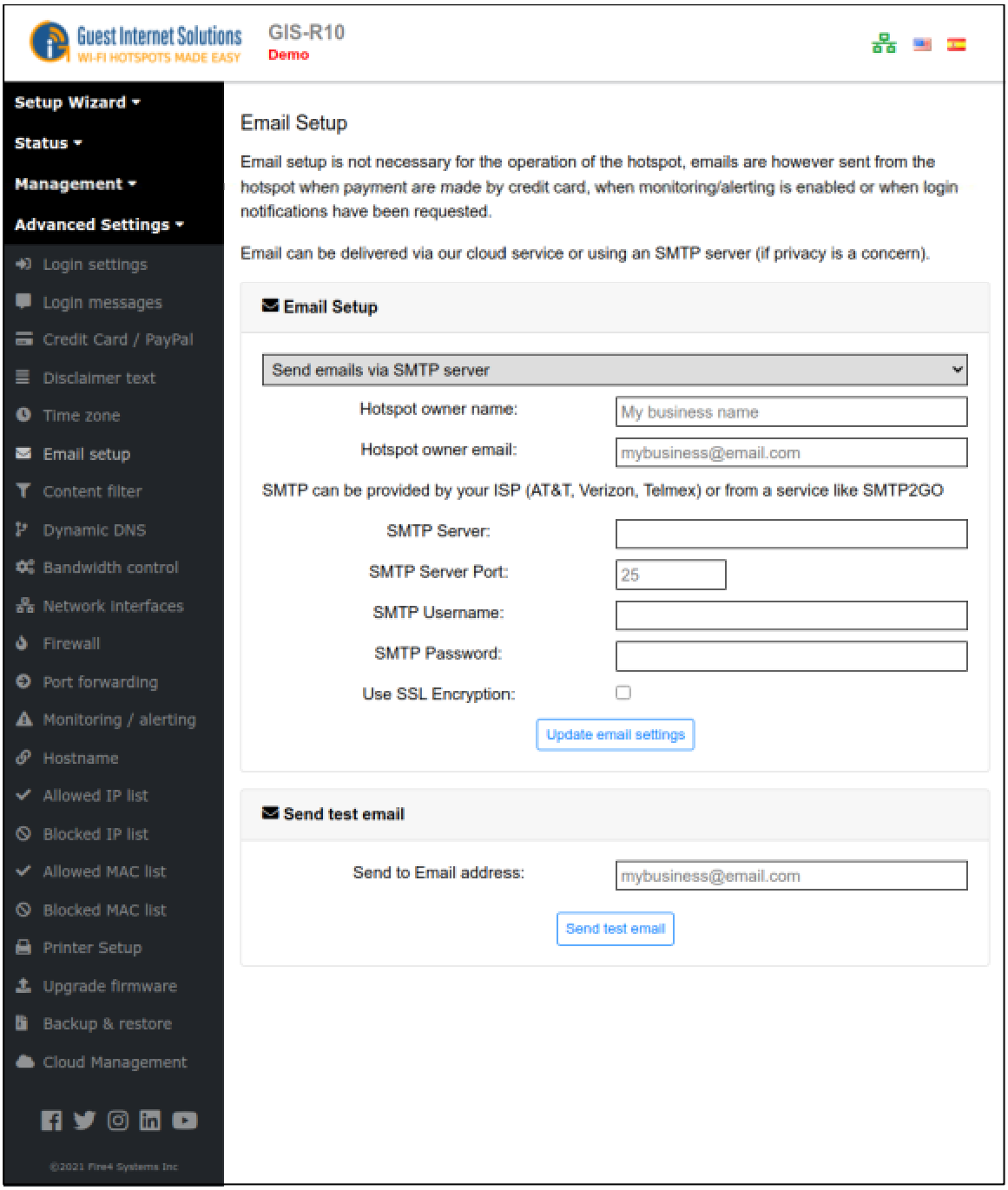


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Email Setup

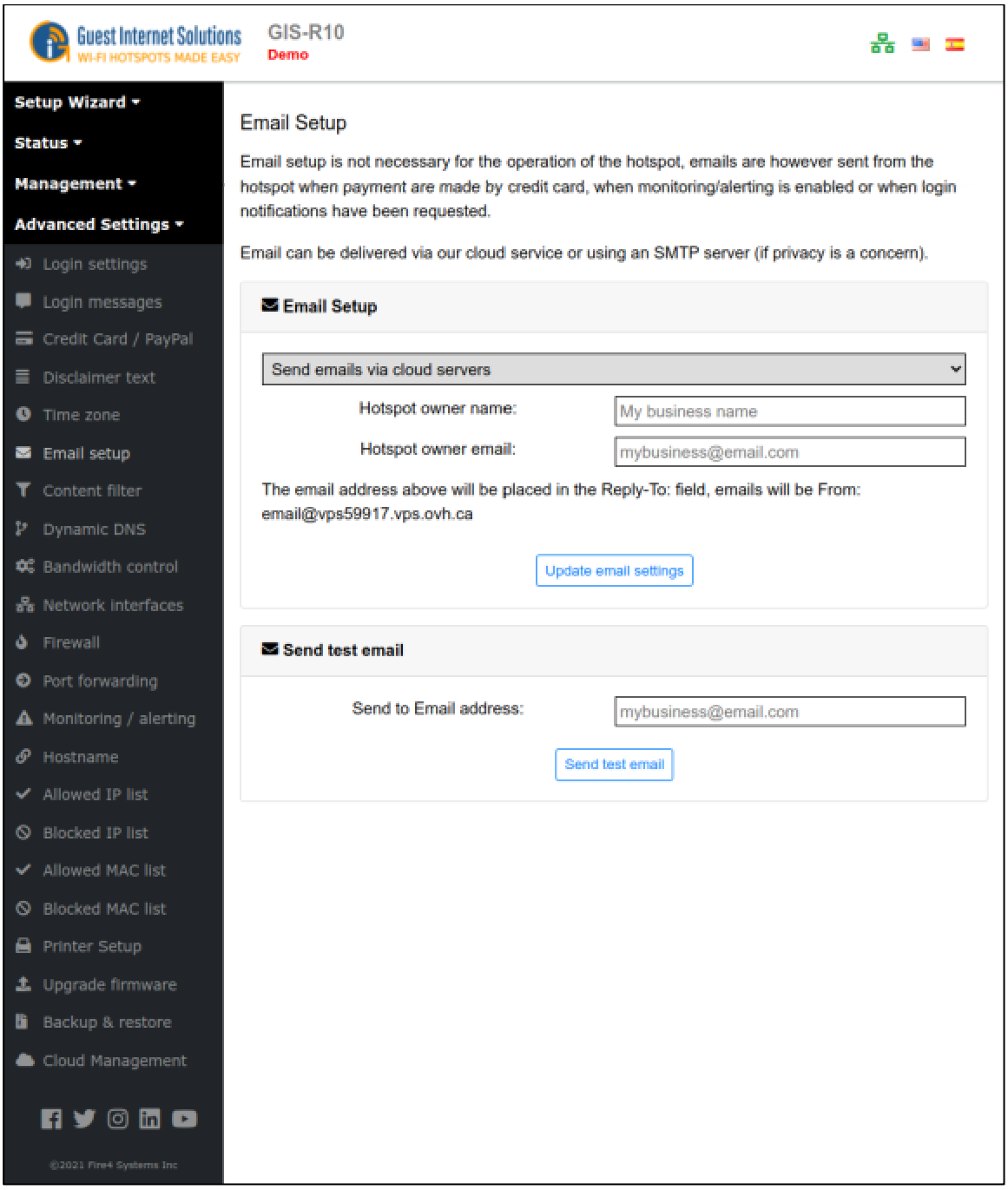
The Email server permits sending messages to the Hotspot owner. The Monitoring and alerting feature can send a failure message to the Hotspot owner and the PayPal credit card billing will send a transaction report via email. Some login options can send user information to the Hotspot owner.

The Email server can be configured to use the SMTP server that is provided by the ISP.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Alternatively the Email server can use the Guest Internet cloud service.



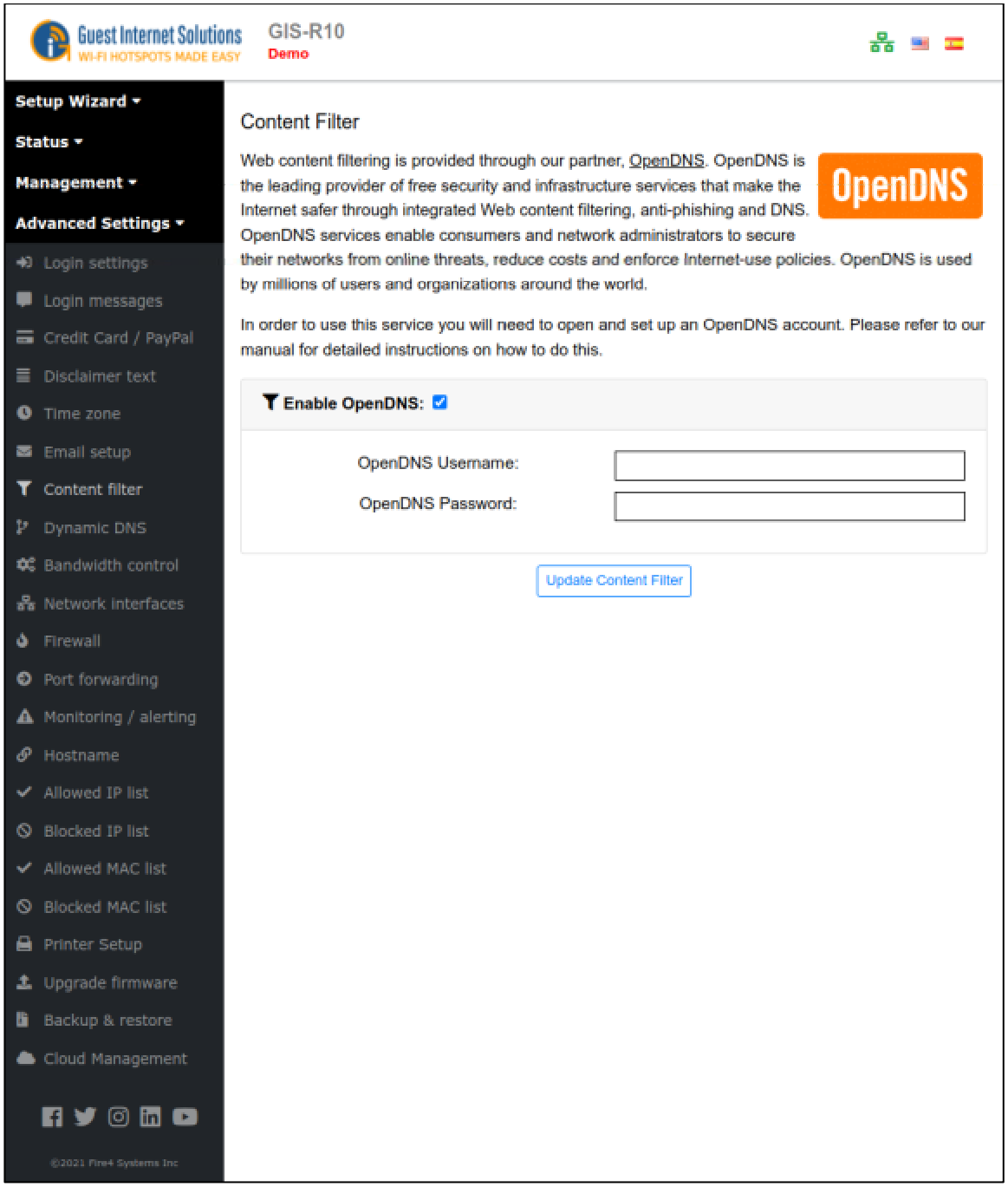
Email transmission via the services of Outlook, Gmail, AOL, and Hotmail has been removed due to increased security, which made the use of these services difficult.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Content Filter

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 3rd party content filtering service, OpenDNS, who maintains a current list of web sites to block.

Before the GIS content filtering service can be used an account must be created with OpenDNS. For more information please go to the OpenDNS Website:
http://www.opendns.com/



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

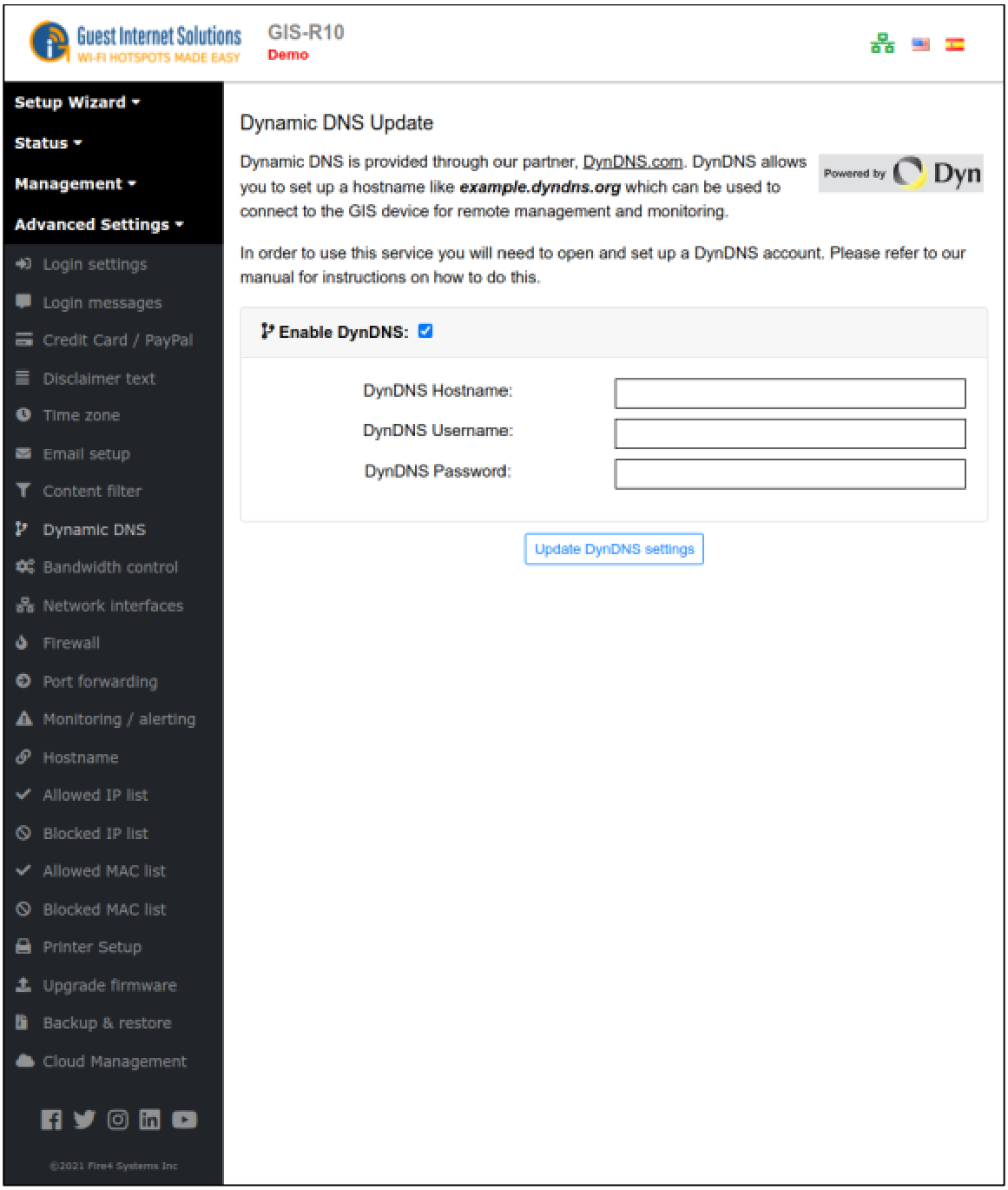
Dynamic DNS

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 an account with DynDNS. When the box is checked to enable the DynDNS 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.

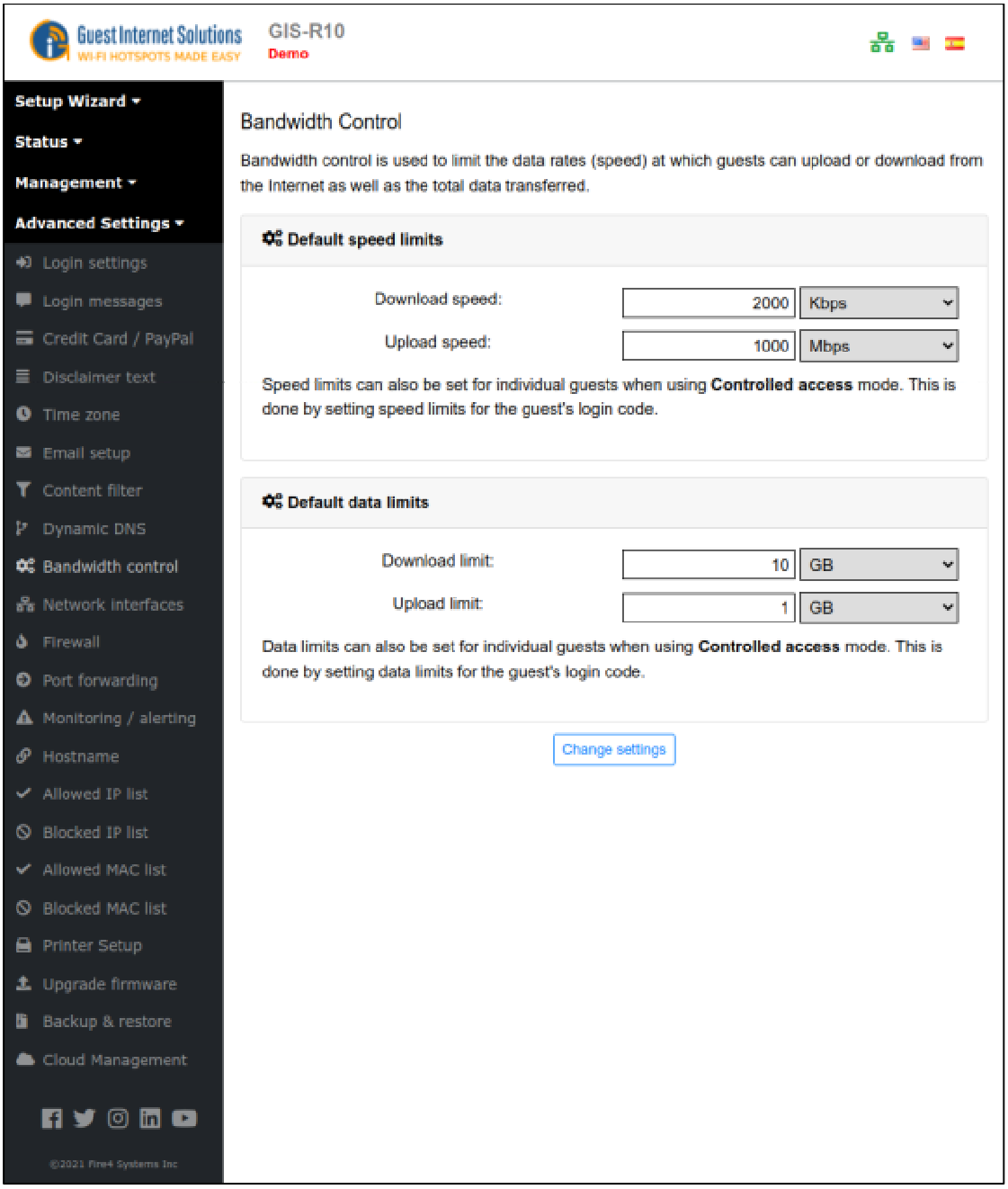


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Bandwidth Control

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 Internet connection speeds vary with the download bandwidth available usually a higher than the upload bandwidth. 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.

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.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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.

Your Internet connection may require that all computers and network devices be configured with ‘fixed or static 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.

Wireless product Interface

Products with a wireless interface (**GIS-K1/GIS-K3/GIS-K5/GIS-K7**) 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

The screen 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, it 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.

Products that have a wireless interface also have an additional menu page for **wireless settings**.

There are two configuration options: Name (SSID) and Channel.

The Name (SSID) (Service Set IDentifier) is the name that is broadcast by the wireless transmission and users will see this name on their computers. Any laptop computer within range of the transmission will detect and show the SSID.

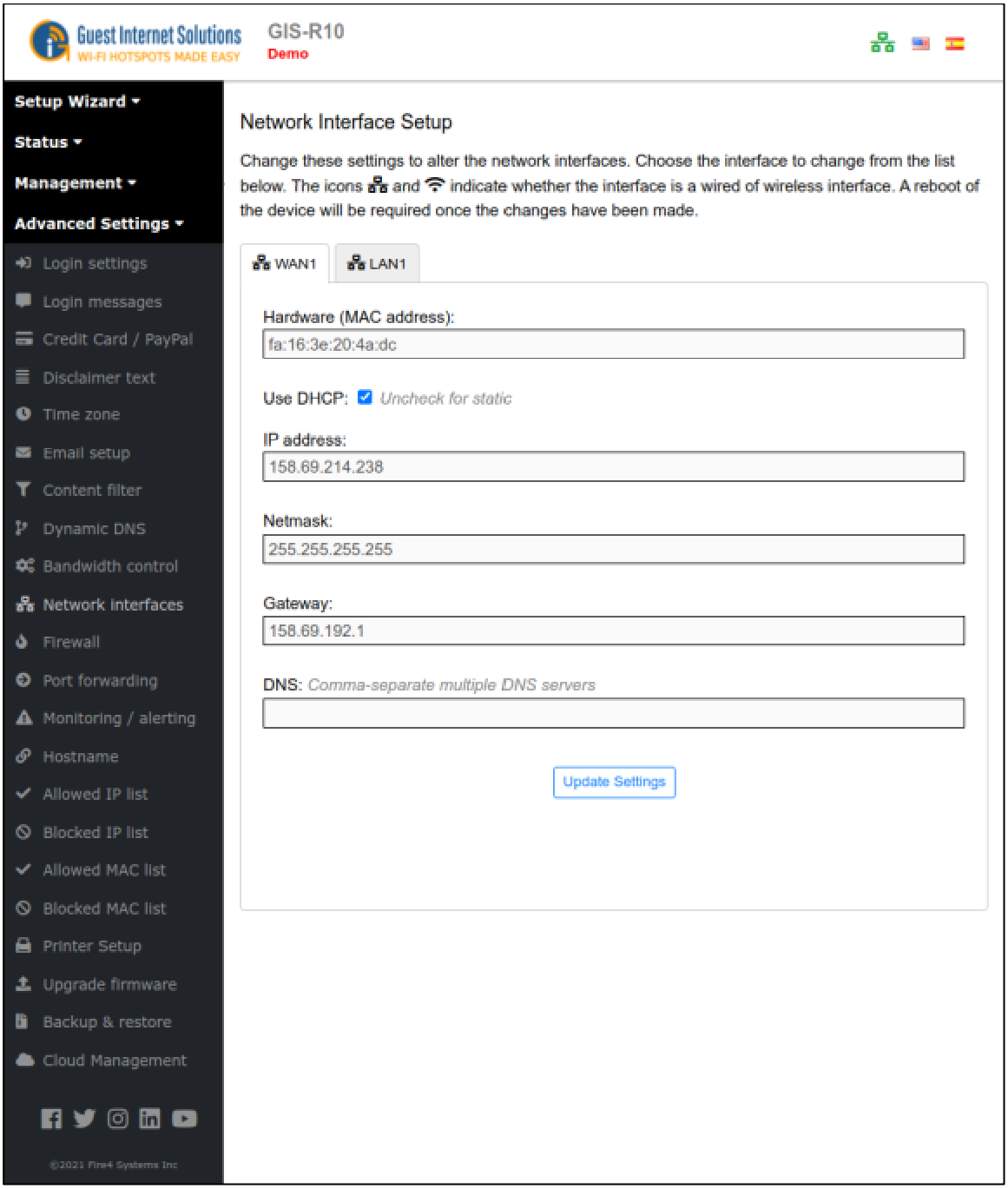
The Channel is the frequency that the wireless uses for communications. Wireless data transfer may seem slow when many wireless access points use the same channel. The channel can be selected to avoid conflict with adjacent transmitters if there is more than one hotspot at a location. Change the channel number to improve wireless performance. It will be necessary to use laptop identification software, to identify the channel number of adjacent transmissions.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

WAN Connection

The WAN tab (Wide Area Network) settings is for the gateway unit Internet port. Depending on the Guest Internet product, there can be up to four WAN ports. When there are two or more WAN ports each port can be connected to a different ISP to increase performance and reliability. When all ISP circuits are working then the data load from the users is spread over the WAN circuits. If one WAN circuit fails then the users are switched to the functional WAN circuits. This is called redundancy.

The DHCP box checked for the default DHCP client configuration where the DSL router provides the IP address for the gateway. Your Internet connection 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.



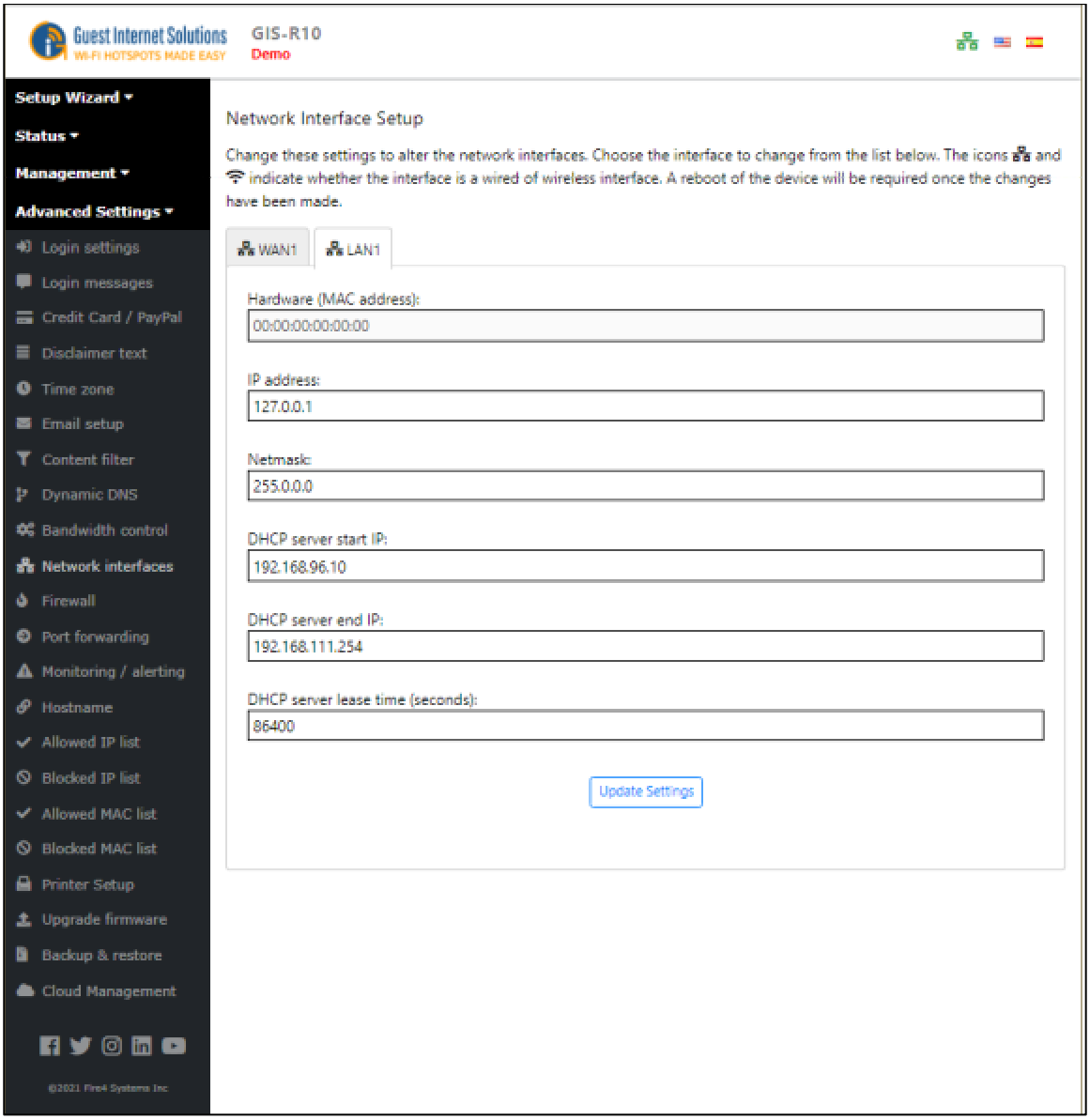
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

LAN Connection

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.

Guest Internet products have different numbers of LAN ports. When a product has more then one LAN port, each LAN is an isolated subnet and the DHCP IP ranges do not overlap

The LAN Network Interfaces configuration permits you to set parameters that will improve the service for your guests. However take care not to overlap DHCP ranges.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS Default IP Ranges

The LAN ports are always a DHCP server and provide IP addresses for devices connected to the LAN ports. The table below displays the range for each LAN port on the GIS unit:

LAN1 Start 192.168.96.10	**LAN2 Start** 192.168.112.10
LAN1 End 192.168.111.254	**LAN2 End** 192.168.127.250
LAN3 Start192.168.128.10	**LAN4 Start** 192.168.144.10
LAN3 End192.168.143.250	**LAN4 End** 192.168.159.250
LAN5 Start192.168.160.10	**LAN6 Start** 192.168.176.10
LAN5 End192.168.175.250	**LAN6 End** 192.168.191.250
LAN7 Start192.168.192.10	**WLAN Start** 192.168.112.10
LAN7 End192.168.207.250	**WLAN End** 192.168.127.250

If you are setting an static IP, please use an IP address outside the DHCP pool, but within the same subnet:

This should be used when setting up an access point in bridge mode.

LAN1 Start 192.168.96.2	**LAN2 Start** 192.168.112.2
LAN1 End 192.168.96.9	**LAN2 End** 192.168.112.9
LAN3 Start192.168.128.2	**LAN4 Start** 192.168.144.2
LAN3 End192.168.128.9	**LAN4 End** 192.168.144.9
LAN5 Start192.168.160.2	**LAN6 Start** 192.168.176.2
LAN5 End192.168.160.9	**LAN6 End** 192.168.176.9
LAN7 Start192.168.192.2	**WLAN Start** 192.168.112.2
LAN7 End192.168.192.9	**WLAN End** 192.168.112.9

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

VLAN configuration for segmented LAN networks

LAN network VLAN configuration is included with the PRO series of gateway products. VLAN configuration requires the installation of firmware equal to or higher than 2.5.6.4x.

The PRO series includes the following products;

- GIS-R10
- GIS-R20
- GIS-R40

Any older product that uses the Intel family of processors can be upgraded to VLAN operation by installing the firmware 2.5.6.4x or higher. Older products include the GIS-R80, GIS-R16 and older versions of the GIS-R10 and GIS-R20.

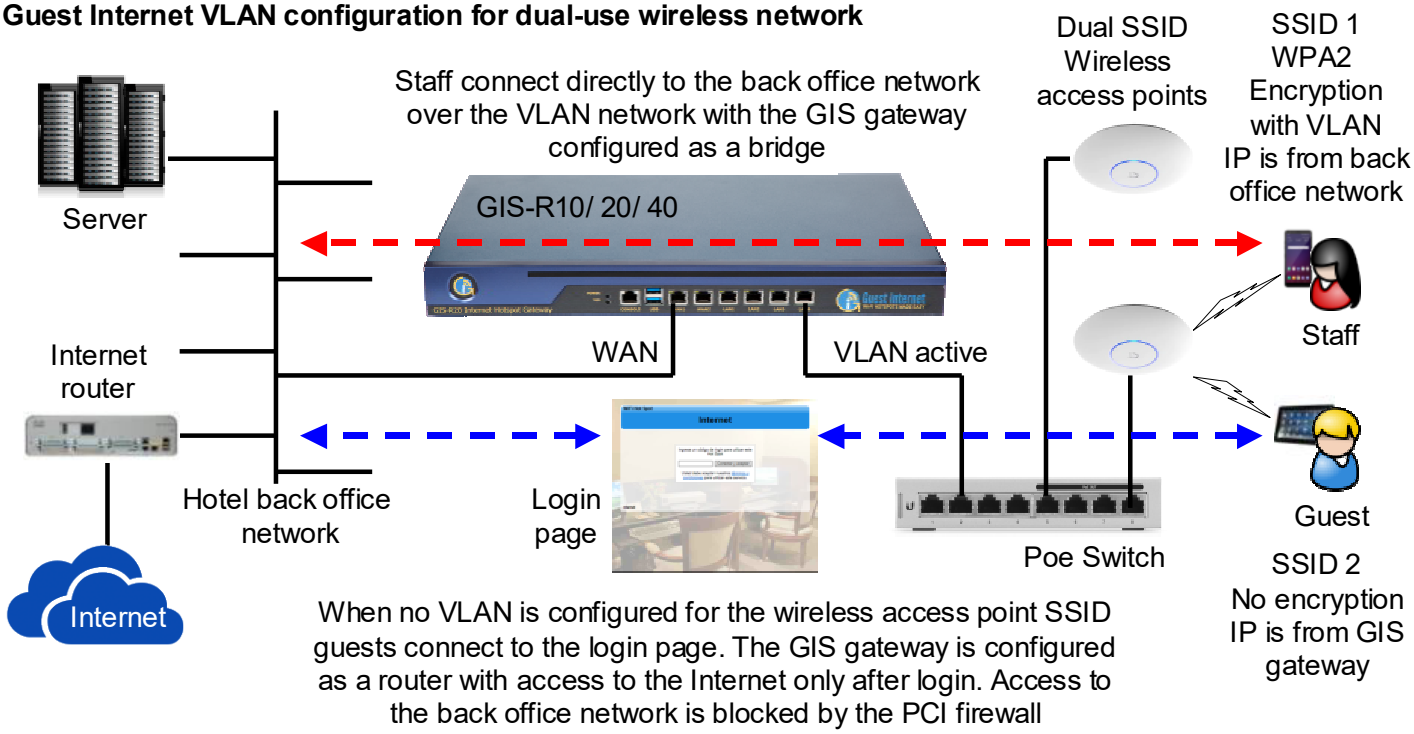
The VLAN configuration permits segmentation of the LAN network. For example, a hotel can install one wireless network infrastructure with two or more SSID's that provide isolated access for guests and staff. The cost of the wireless infrastructure installation is therefore halved.

The VLAN configuration requires the use of wireless access points that van be configured with multiple SSID's where each SSID can be configured optionally with a VLAN ID, and can be configured with or without encryption.

The wireless access point configuration process depends on the manufacturer. Popular wireless products such as Ubiquiti Unifi permit up to 4 SSID's to be configured where each SSID can be configured with or without encryption and can be configured with or without a VLAN ID.

The Guest Internet unit is installed in the network as shown in the diagram below.

Guest Internet VLAN configuration for dual-use wireless network



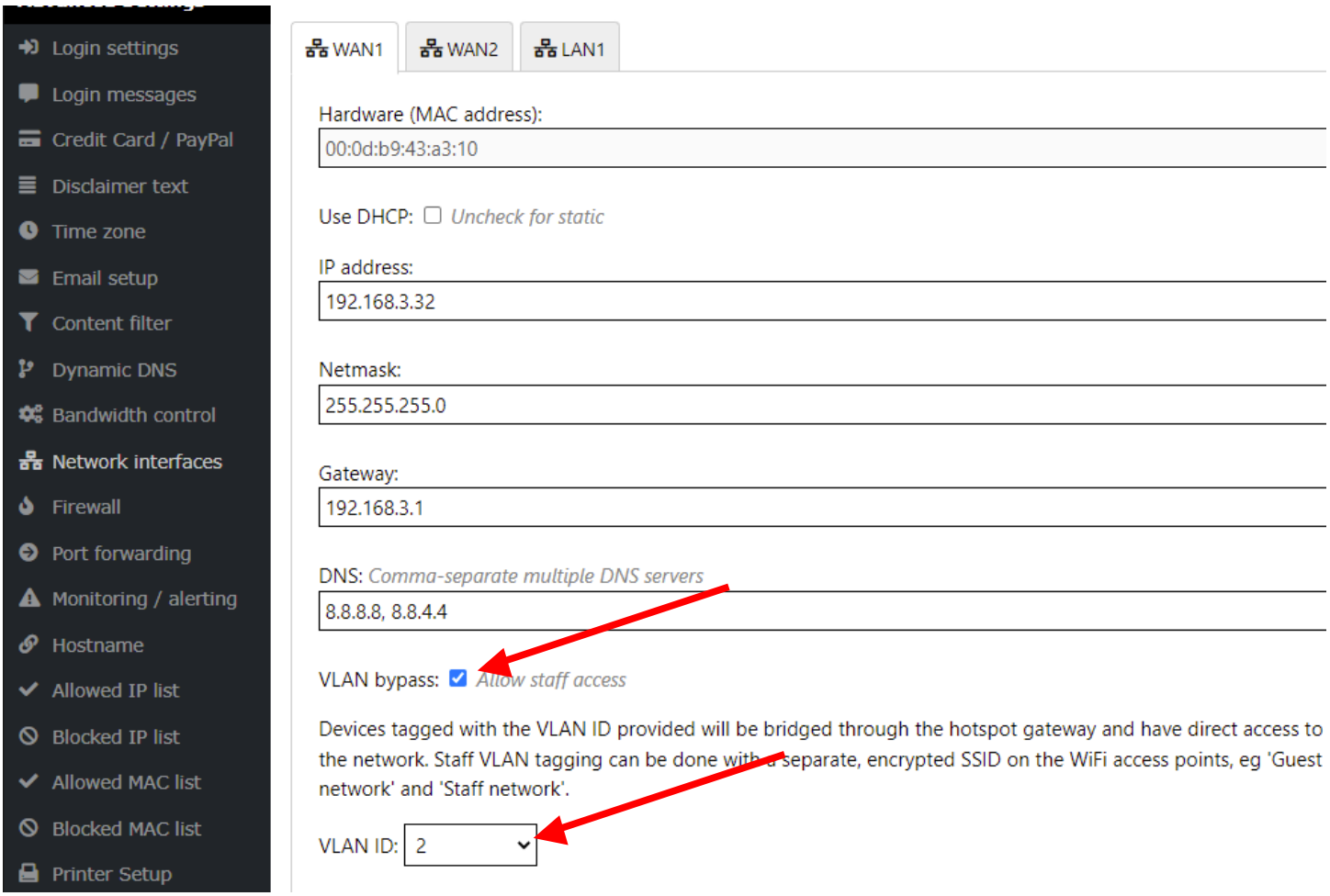
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

A hotel configuration might require the following:

- Guest WiFi: the wireless is not encrypted, when a guest connects then the guest computer receives an IP address from the GIS DHCP server, and the guest browser opens the login page. The guest is isolated from the back office network by the PCI DSS compliant firewall.
- Staff WiFi: the wireless is encrypted and each staff device is configured with an encryption key. The staff connection is bridged through the GIS unit and receives an IP address from the back office DHCP server. The staff device communicates with back office applications.

The GIS VLAN is configured for a WAN port. The VLAN ID number set for the WAN port must correspond with the VLAN ID set for the wireless SSID. The user connecting to the SSID will then be routed to the WAN port with the corresponding VLAN ID. As the GIS units have multiple WAN ports then each SSID can be routed to different WAN port.

The configuration of the WAN port VLAN ID is shown in the figure below. The box is checked to activate the VLAN bypass as shown. The VLAN ID corresponding to the SSID VLAN ID is added to the box shown. Finally the button is clicked to update the page.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Roaming configuration for cellular WiFi

Many Guest Internet customers provide a mobile broadband service for their customers. Two mobile broadband applications are listed below.

- Airports where a mobile broadband service provides an Internet service for both subscribers and for individuals who purchase Internet access.
- Municipal networks where a wireless Internet service provider is delivering an Internet service to many customers throughout the town or city.

Many large and small businesses offer a mobile broadband service. Some larger mobile broadband businesses are shown in the table below.

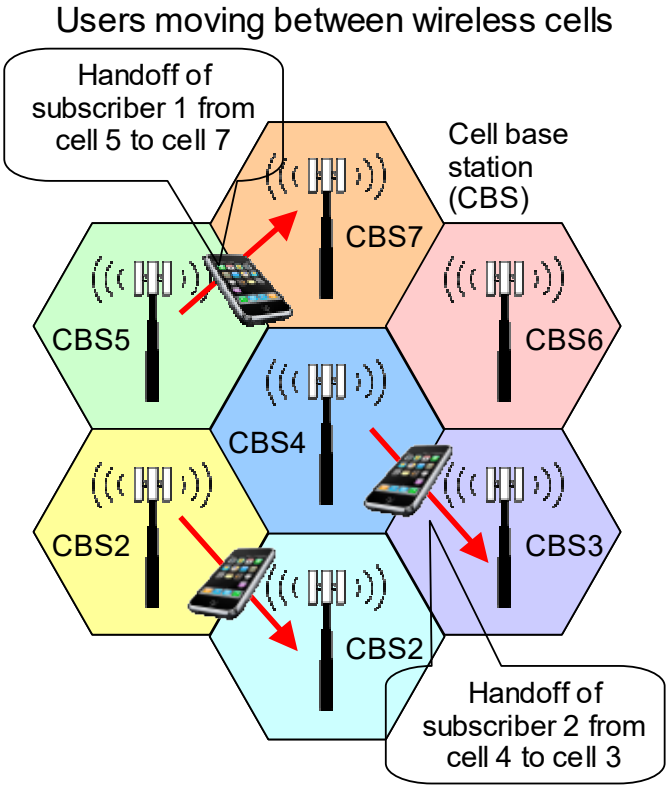
boingo wireless	iPass	pronto networks
WeFi Share Wifi. Get Money.	extenet SYSTEMS Mobile Connectivity Everywhere	bandspeed
device scape	gogo Inflight Internet	XCOMGLOBAL

The Guest Internet cloud manages the users of a wireless WiFi network of wireless access points in a similar way that a mobile phone network manages the movement of subscribers through a network of 4G towers.

A user is issued an access code, which permits the user to connect to any wireless in the network. As the user moves through the network between wireless access points a cloud handoff process moves the user from one tower to the next and so the user maintains a wireless connection.

All wireless access points in the network have identical SSID's and the users device connects to the SSID with the strongest signal.

The handoff process between wireless access point towers is illustrated in the diagram.

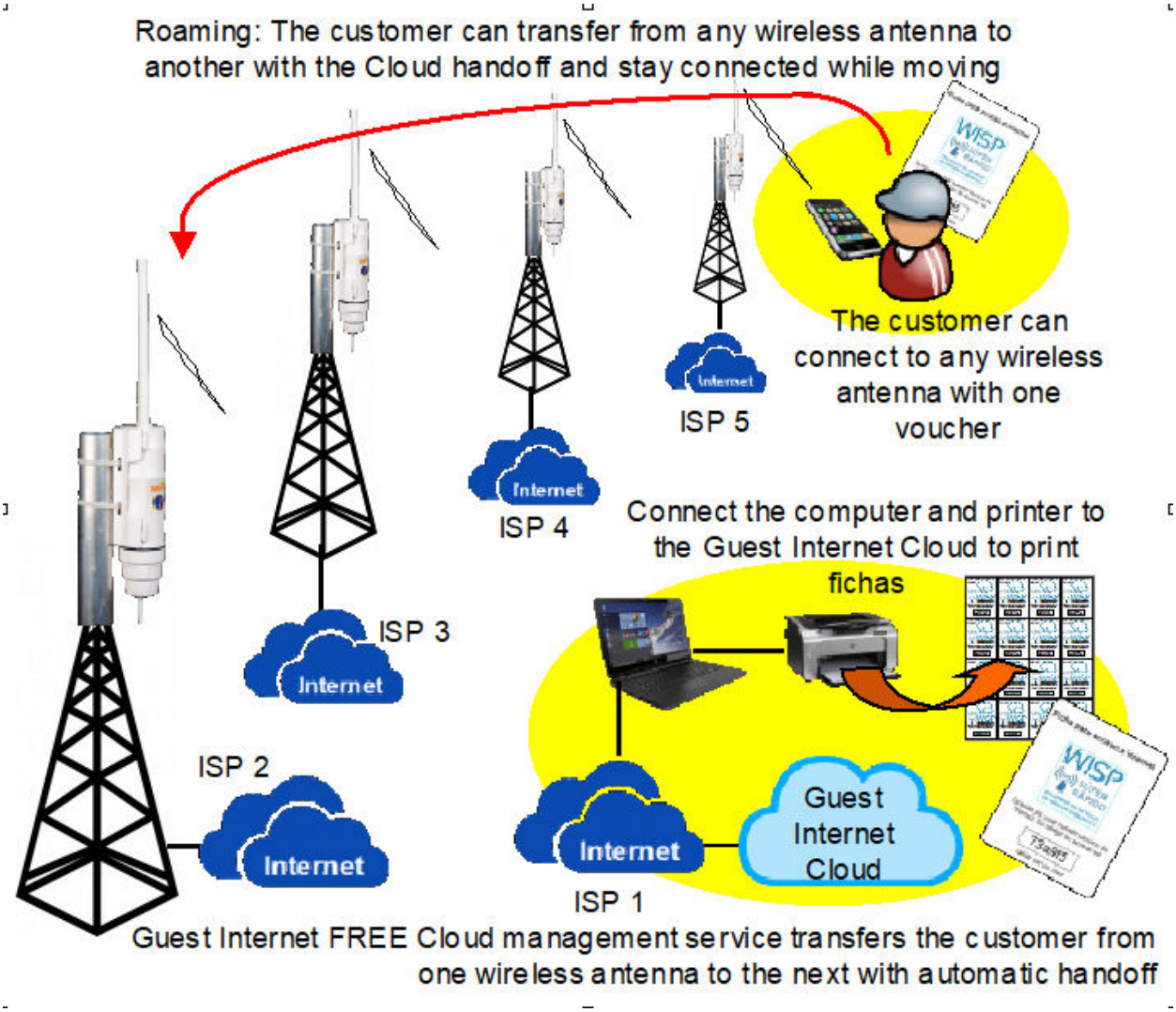


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

All wireless access points and gateways in the network are configured to be part of a cloud group and cellular WiFi roaming is configured using the cloud group. Each wireless access point and gateway can be connected to a different ISP. The cloud account group settings also include the function to generate access codes and print the access codes onto sheets of vouchers in a 4x4 format using a letter size printer. The sheets of vouchers can then be cut up so that a voucher can be given to each user. Some Spanish-speaking countries sell the vouchers to mobile broadband customer through a business called “Internet-por-fichas”.

The next diagram illustrates the simple business process that is required to sell Internet access.

- Create access codes with embedded parameters, duration of the code after first use until expiration, optional max down/up data speed, optional max down/up data byte cap, number of concurrent users allowed, sequential device change allowed, etc.
- Print vouchers in a 4x4 format using a letter size printer.
- Cut up the vouchers and distribute to points of sale.
- Customers purchase vouchers and connect to any wireless access point (WAP) in the group.
- Customers can move through the group of WAP’s and as each is communicating with the cloud the customer will be transferred from one to the next as the customers device MAC address is recognized.

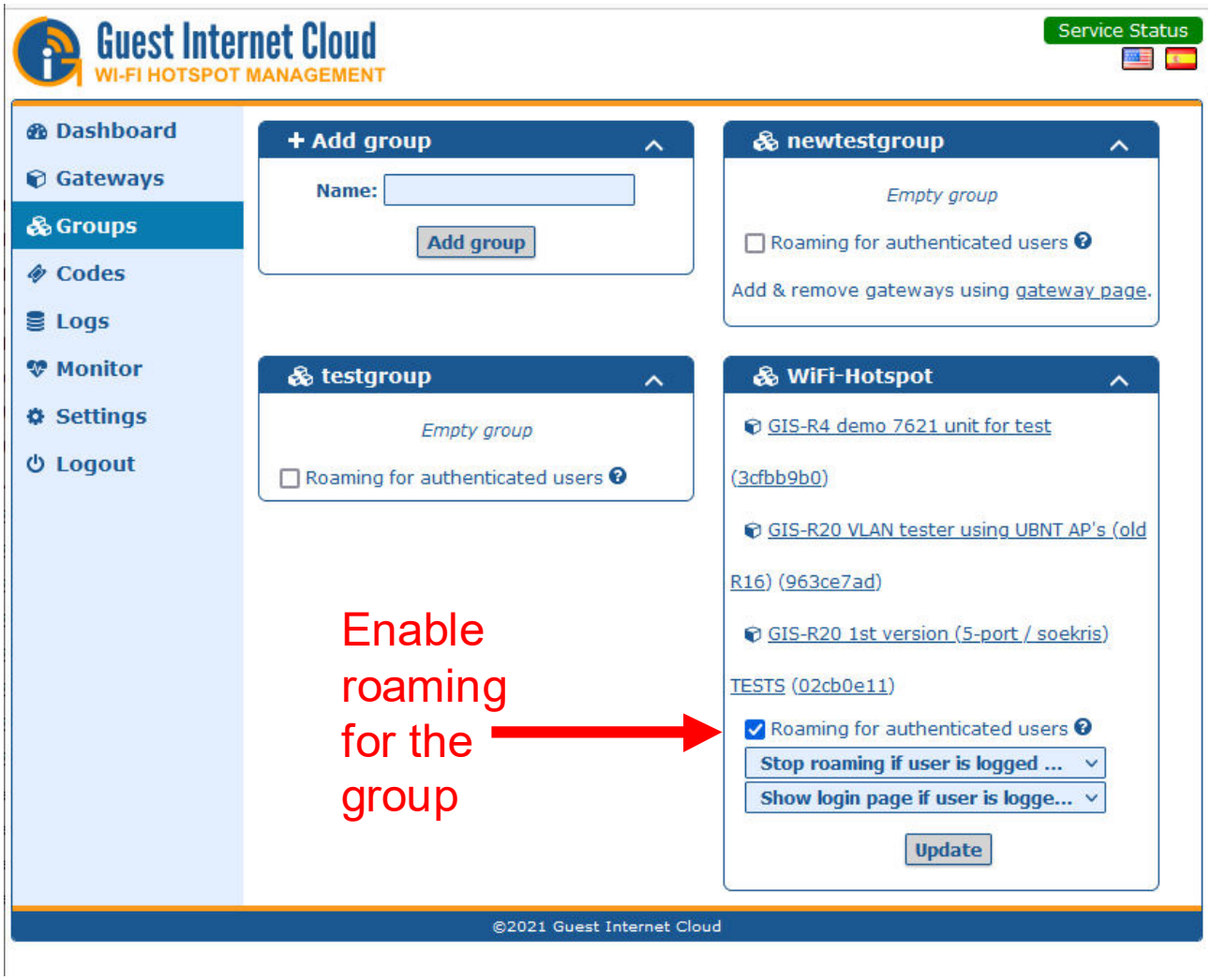


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Roaming is activated by checking the box in the cloud group settings to allow ‘Roaming for authenticated users'. This permits a device MAC address to be recognized when a user moves from on WAP to the next.

There are two parameters associated with the selection of roaming;

- Stop roaming if user is logged out / keep user roaming until code expires
- Show login page if user is logged out / auto login if user is logged out



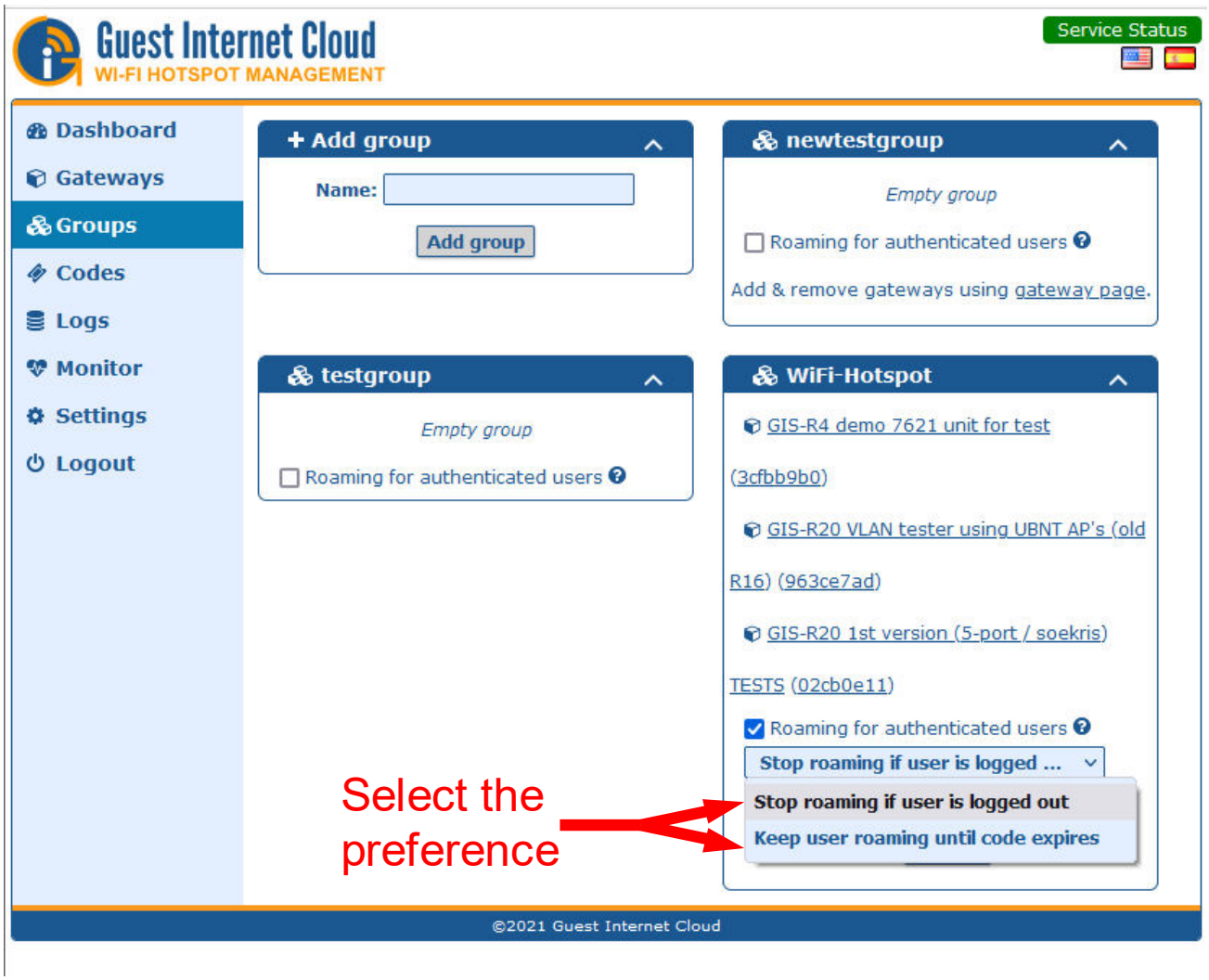
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Configuration of: Stop roaming if user is logged out / keep user roaming until code expires

Select: Stop roaming if user is logged out in the case where the user has logged out using the login page aplogin.com or else the user has been logged out for some violation of use.

Select: Keep user roaming until code expires when it is desired that the user will continue to have Internet access even after being logged out, until the expiration of the access code.

See the following screen display.



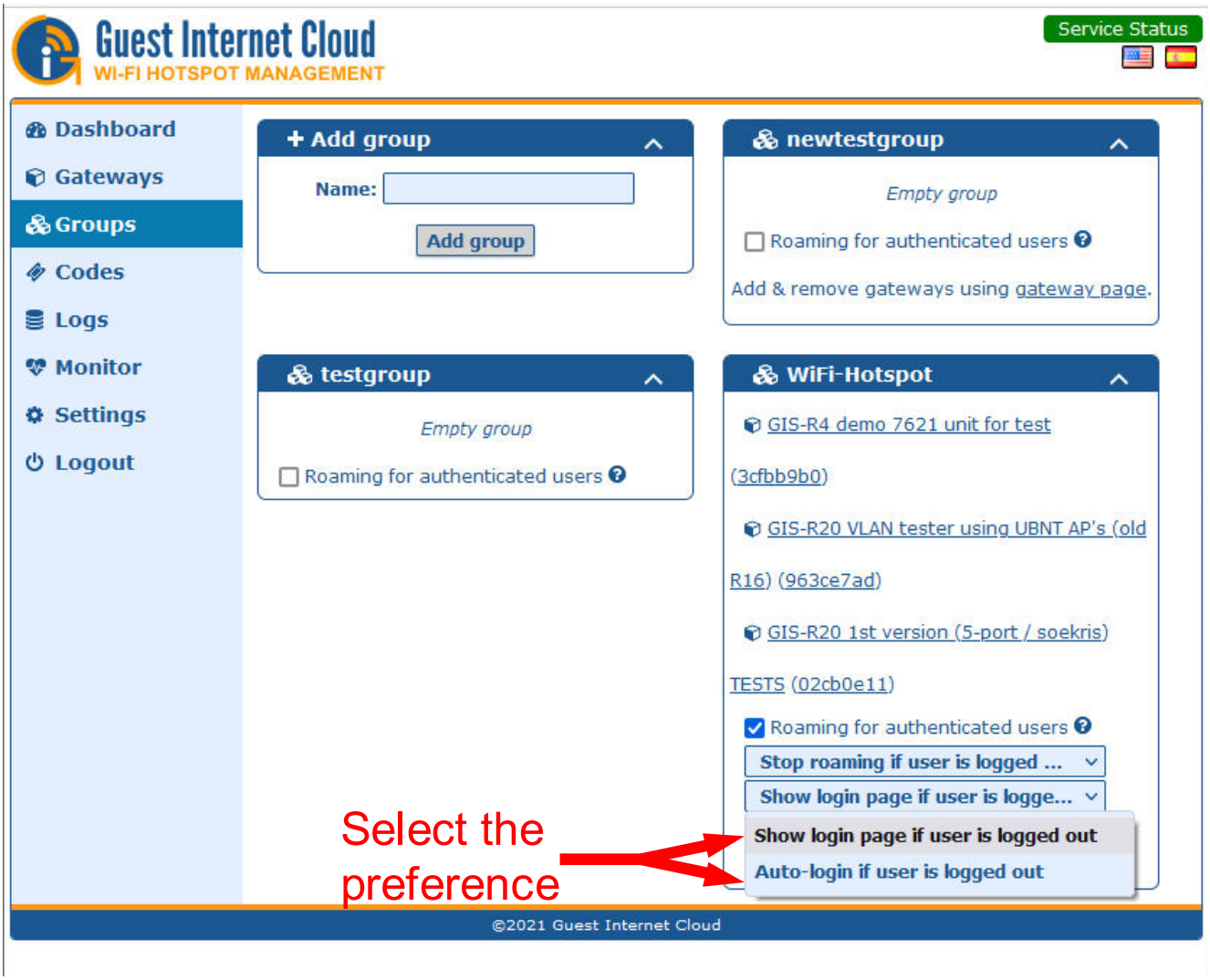
The next configuration is: Show login page if user is logged out / auto login if user is logged out

Select: Show login page if user is logged out displays the login page when the user has been logged out and the use must reenter the access code provided.

Select: Auto login if user is logged out to permit the user to maintain the Internet connection without requiring the reentry of the access code.

See the following screen display.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



As a user moves from one wireless tower to the next wireless tower eventually the next tower will have the stronger wireless signal (signal strength in –dBm) and the computer/device will switch to the next wireless tower and issue a DHCP request. When a wireless access point identifies a DHCP request from a wireless device it will advise the cloud and provide the device MAC address. If the device has been logged in to any WAP in the group the cloud will reply with the device access parameters. If the MAC address is not recognized as having connected to any WAP in the group then the login page will be displayed for the user and the user will enter the access code. Upon entry of a valid access code the WAP will inform the cloud that a new user is logged in and provide the access parameters to the cloud. Where possible the WAP DHCP server will provide the IP address previously allocated to the device if that IP is available.

This is a process called “handoff” from one tower to the next. The handoff process requires more steps than those described above, the explanation has been simplified for clarity

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Firewall

The gateway has a firewall that provides several features:

Remote Management

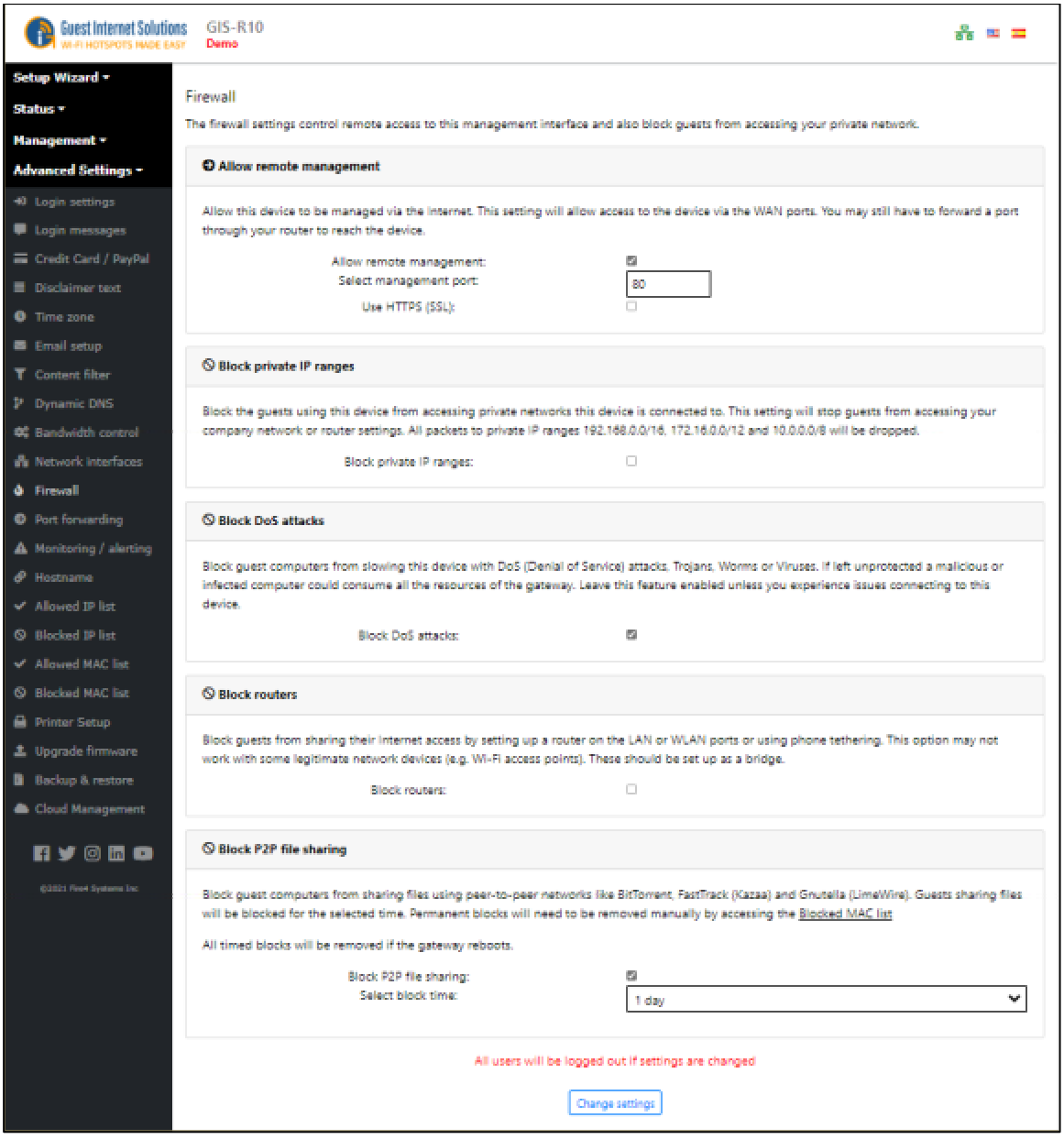
Blocking Private IP address ranges

Blocking of virus DoS attacks

Blocking of peer-2-peer file sharing

Blocking of routers

SSL



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Remote Management

The Remote Management permits administrator login access via the Internet port to allow remote management of the gateway by opening the HTTPS port. Remote access must use SSL for security reasons.

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 443 for HTTPS/SSL on the public facing device to the GIS unit.

Blocking Private IP address ranges

Blocking Private IP address ranges 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

Blocking of virus DoS attacks

Blocking of virus DoS attacks blocks any computer infected with 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.

Blocking of peer-2-peer file sharing

When "block P2P file sharing" is selected, it blocks any computer that has active torrent file sharing software.

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.

Blocking of routers

Blocking of routers prevents users from connecting a router and sharing their single use access code with multiple devices.

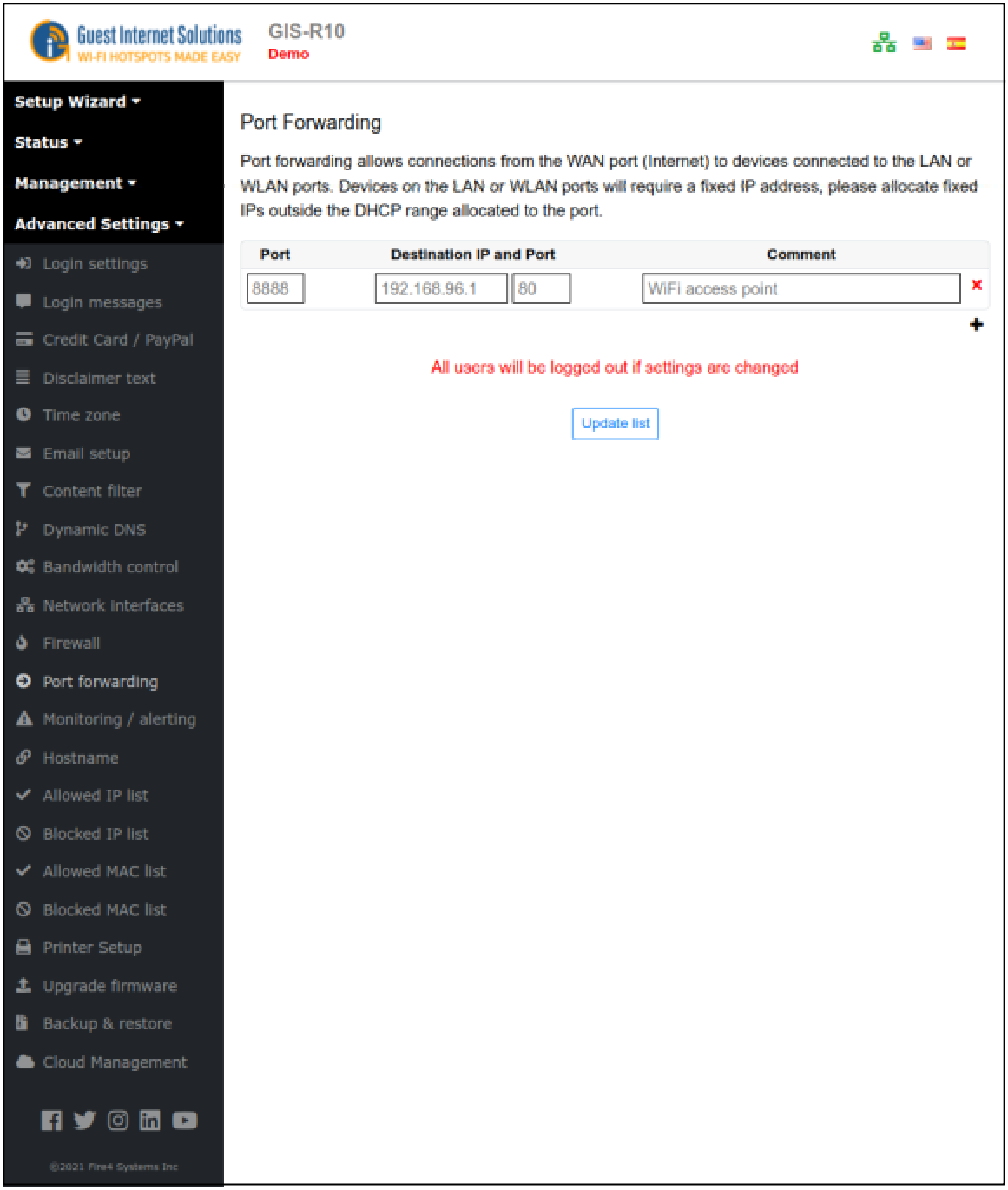
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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).



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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.

Important: 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 you 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.

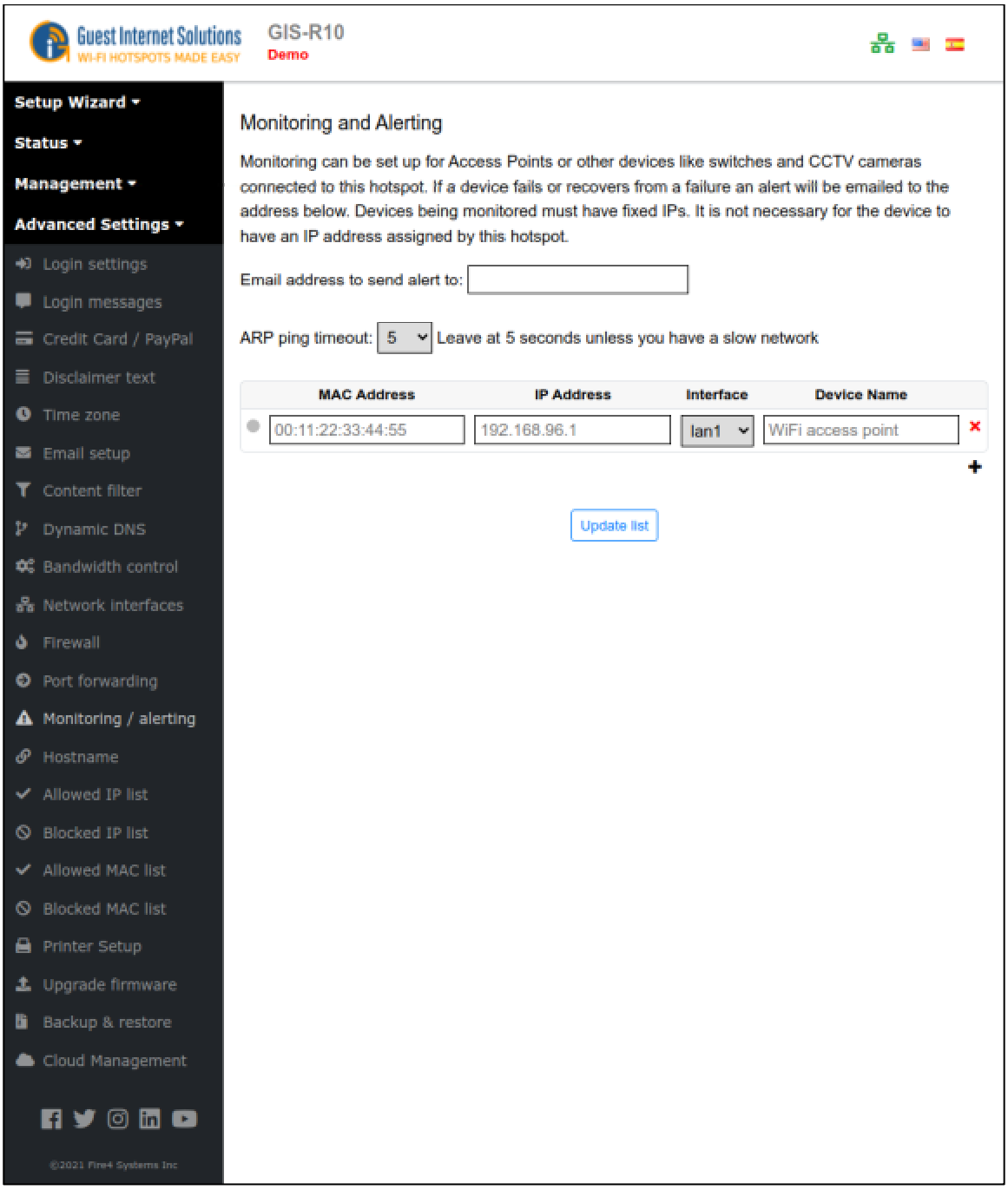
The email message has a subject line and content derived from the device name entered when configuring monitoring and alerting as follows:

> Subject: AP Lounge on the GIS-R2 is DOWN
> Device 'AP Lounge on the GIS-R2' with MAC address '00-80-48-50-93-3a'
> attached to Hotspot ID 000000000 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:

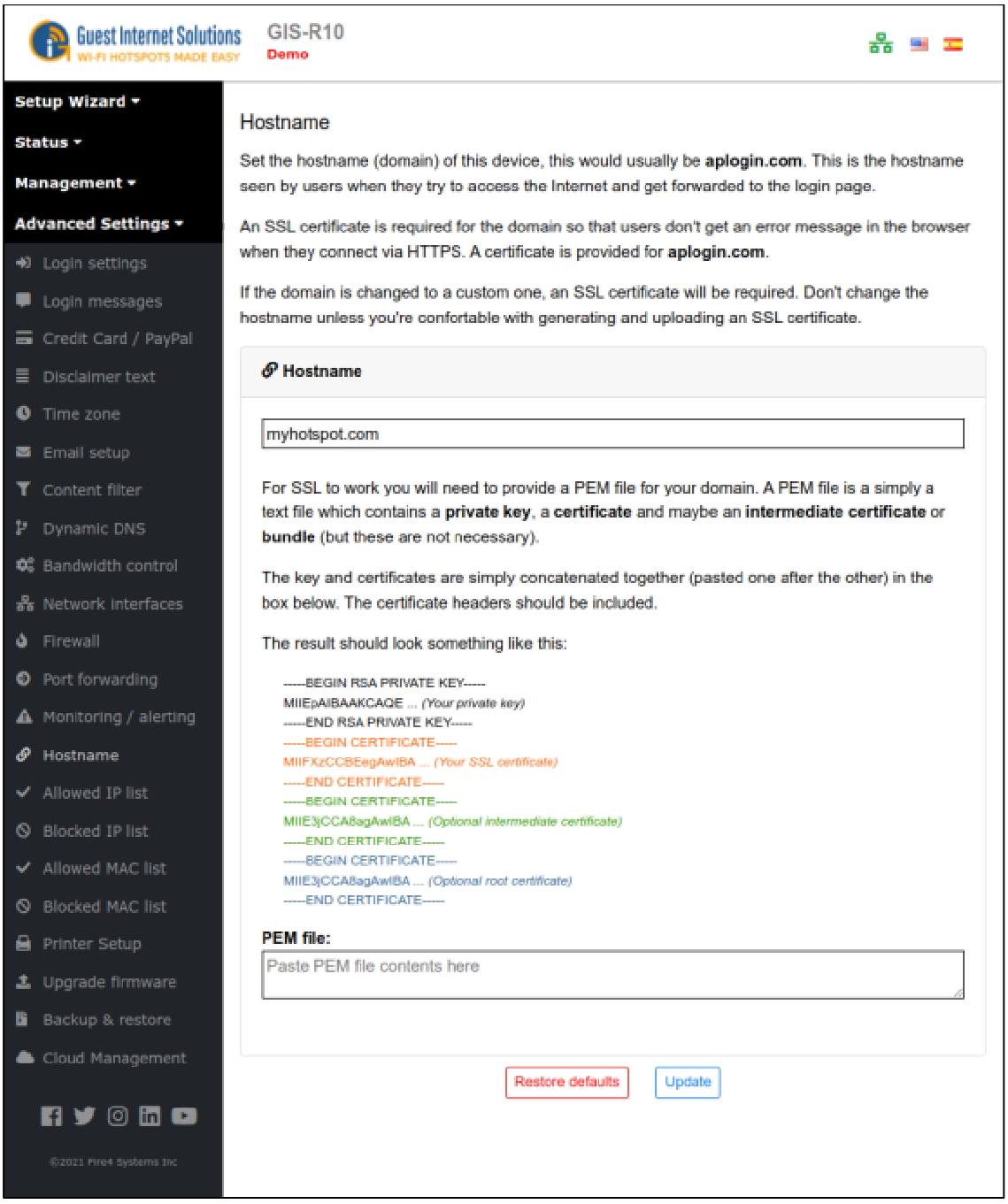
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Hostname (read the **WARNING** below before proceeding)

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.** The Hostname should only be changed to implement specific uses, such as a walled garden. When the Hostname menu entry is clicked the page shown below appears in the browser window.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The hostname can be changed, however the URL for the new name must be a valid Internet domain name and be purchased together with a valid SSL certificate. The domain name and SSL certificate can then be uploaded using the hostname menu. The hostname is changed only for very special applications. The hostname **should not be changed** for normal use.

***** WARNING *****

DO NOT CHANGE THE HOSTNAME UNTIL YOU HAVE DONE THE FOLLOWING
1. Purchased the domain you wish to use for the HOSTNAME.
2. Registered the domain name with a hosting service so that is added to the DNS system.
3. Purchased a valid SSL certificate for your domain name.
WHEN THESE STEPS ARE COMPLETE ADD YOUR DOMAIN NAME AND SSL CERTIFICATE TO HOSTNAME. FAILURE TO FOLLOW THESE STEPS WILL BLOCK ACCESS TO THE GIS PRODUCT.

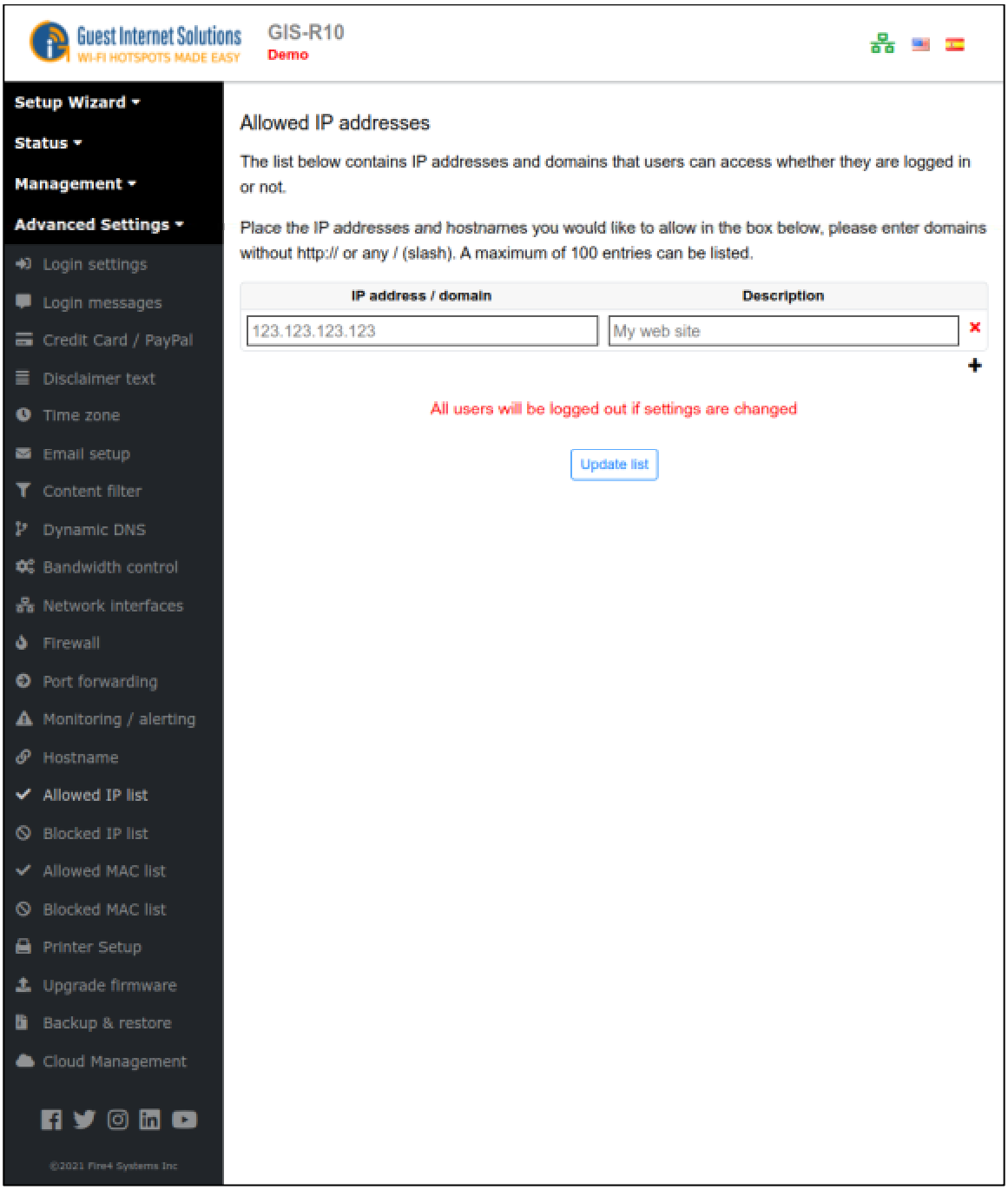
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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.

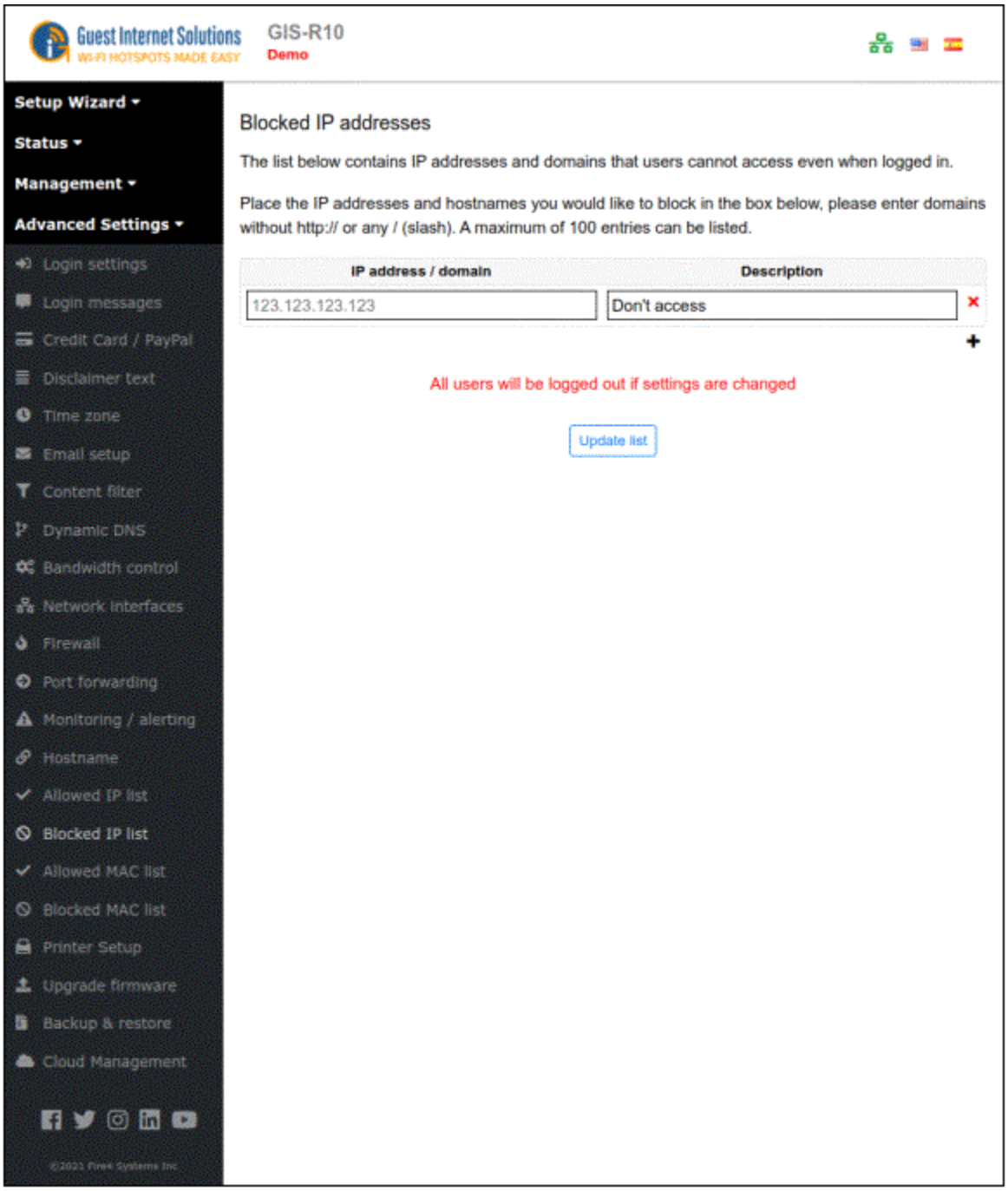


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Blocked IP List

Blocked IP addresses prevent guests having access to websites after the guest has completed the login process. The IP address of the Web site can be entered, or the domain name of the Web site can be entered in the table shown in the figure below. Note that when entering the domain name, enter only www. Do not include http:// in front of the domain name.

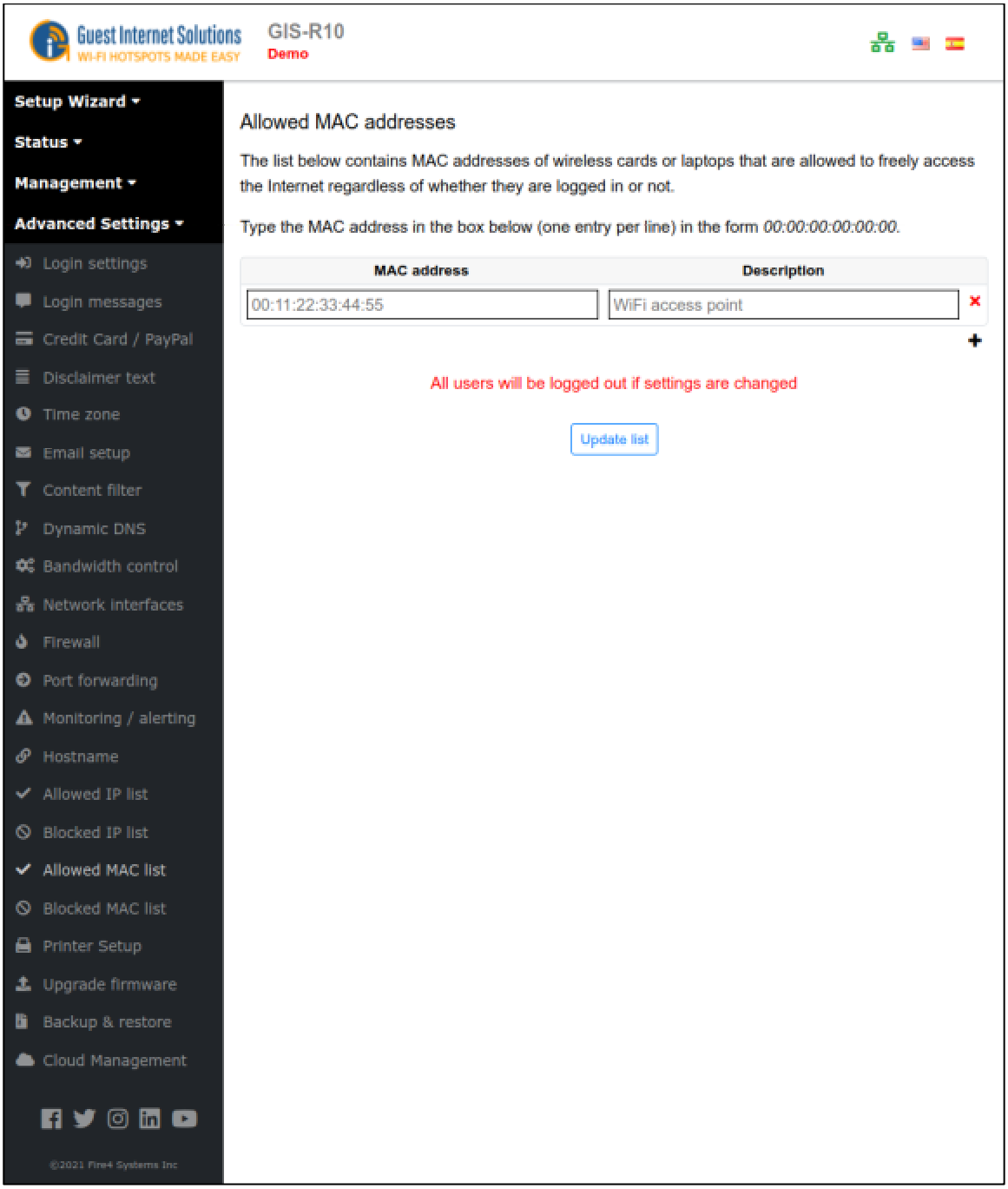
Website blocking identifies websites that the users requests through analysis of DNS requests. Each request is compared with the blocked IP /domain table to identify websites that the user cannot access. The New Generation software has a procedural change for website blocking that was introduced due to the widespread browser configuration of encrypted DNS requests, with the US distribution of Firefox now having encrypted DNS set as default.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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.

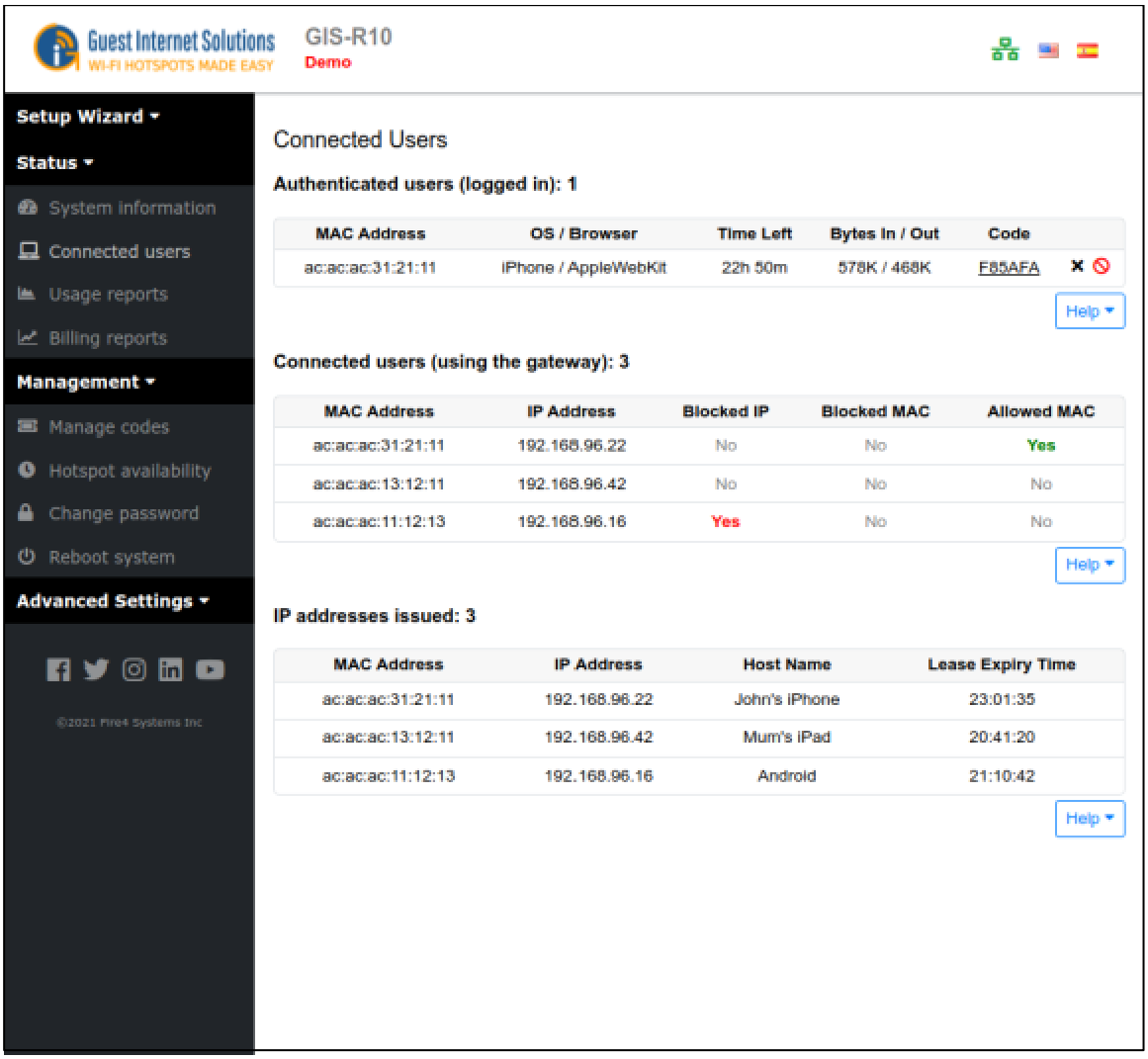
There is no limit to the number of MAC addresses that can be entered. A typical MAC address might look like this: **00:2C:0D:55:A3:1E**

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

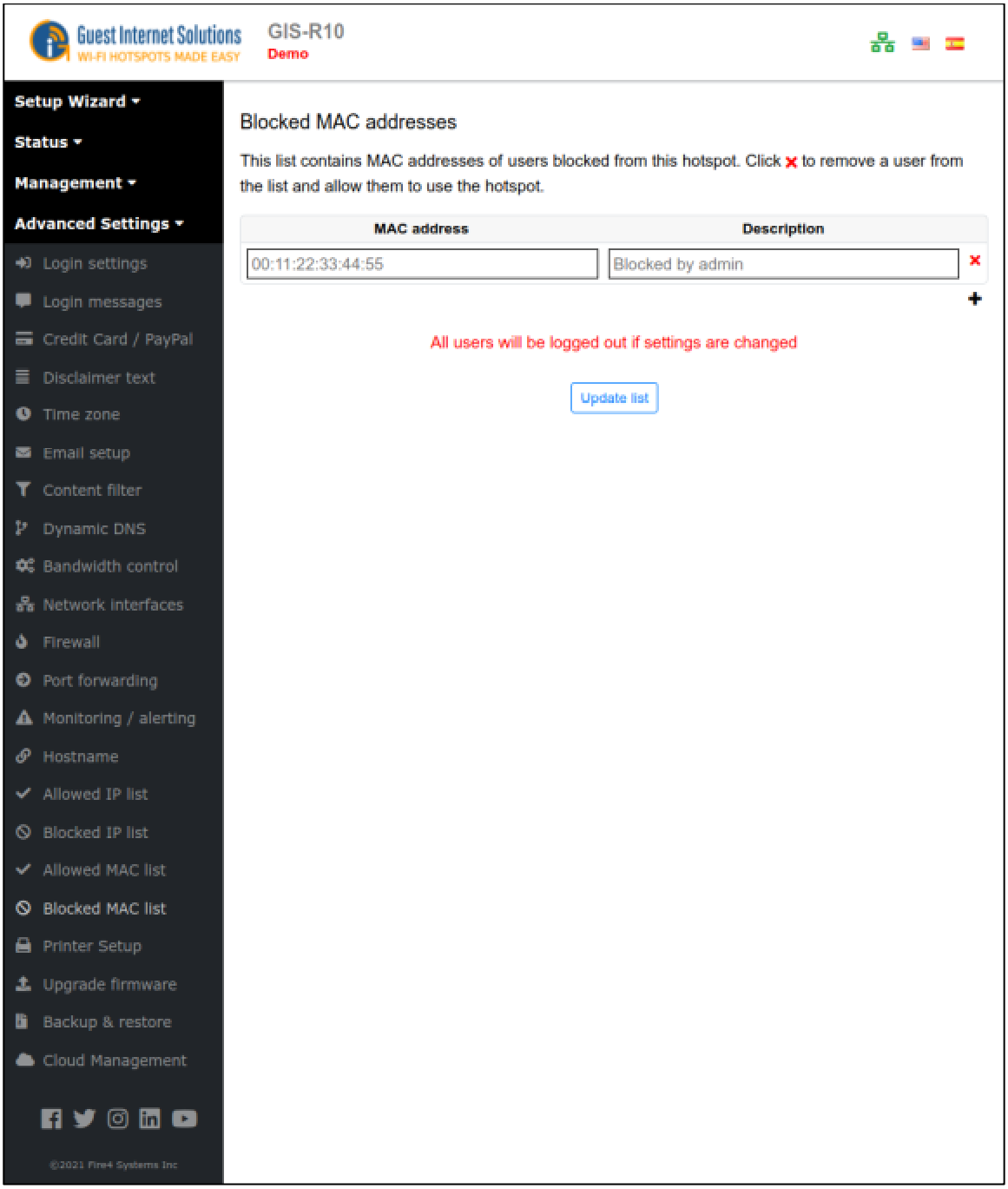
Any user currently logged in to your network can be prevented from accessing the Internet by adding the MAC address of that user on the blocked MAC address list.

To add a MAC address to the blocked list, you first need to go to the Connected users on the Admin interface and click on the red rectangle.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

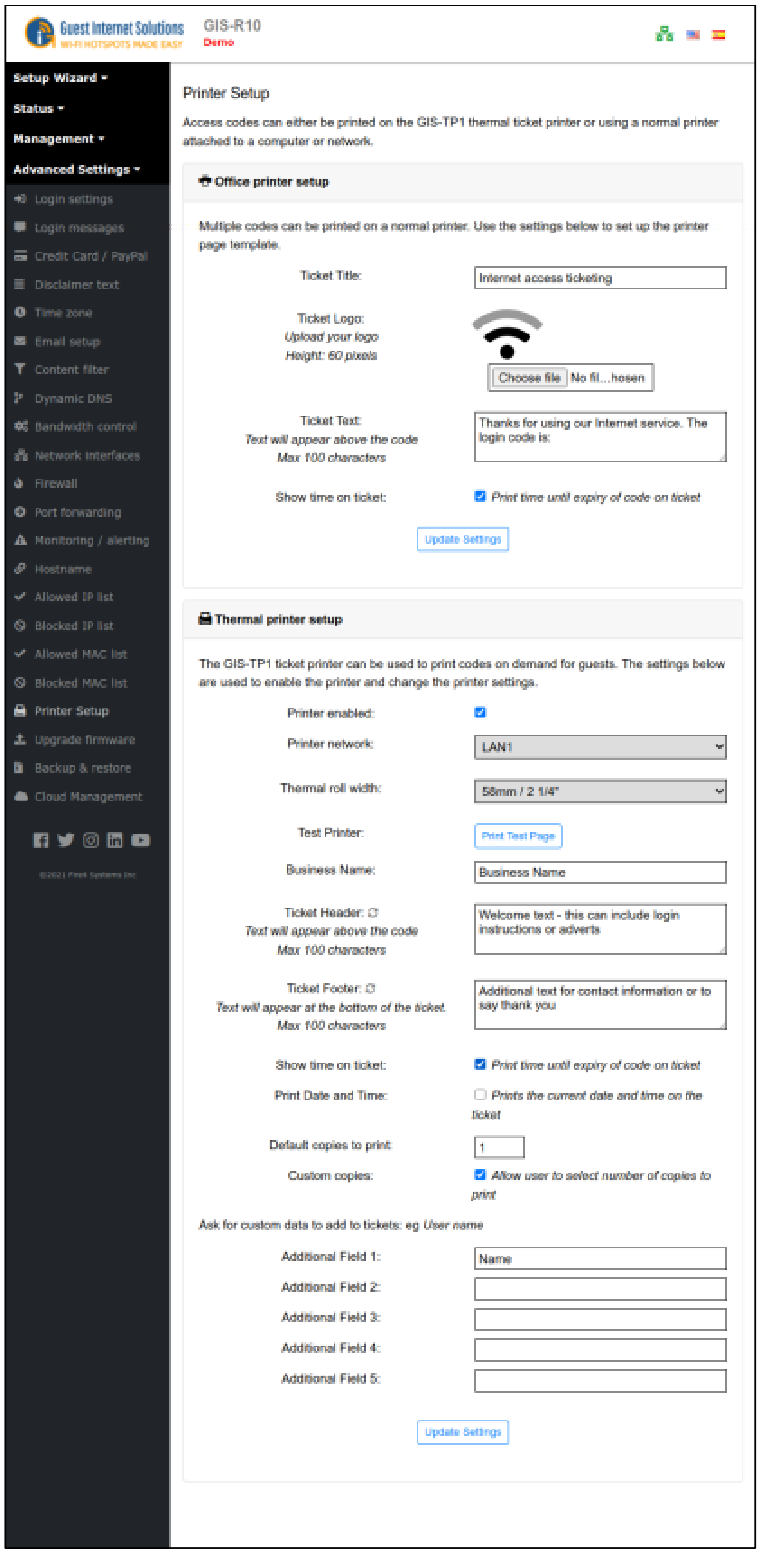
You can then check your list and unblock users.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Setup Configuration for Printers

Access codes can be printed using the GIS-TP1 thermal printer or using a letter printer to print multiple vouchers per page in a 4 x 4 format. The Printer Setup page is used to configure both the GIS-TP1 thermal printer ad the voucher printing. The application for voucher printing is called 'Internet-por-ficha', which is very popular in Latin America and the Caribbean. The Printer Setup screen is shown in the figure below.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Printer Setup for GIS-TP1 Access Code Printer

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 tablet, personal computer or laptop.

When the configuration page is first opened the printer status will be shown as disabled. You need to:

- Click on the printer status enable button to enable printing.
- Type the messages that will be displayed before the access code on the ticket:
    - the business name
    - the ticket header text
- The ticket footer text is printed below the access code.
- A check box selects the option to print the duration of the access code and below that another checkbox selects the option to print the current date and time.
- Additionally, you can either type the number of copies or select the option thar allow user to select custom number of copies at print time.
- Finally, you have 5 additional fields, where you can enter any other useful information to be printed on the ticket.

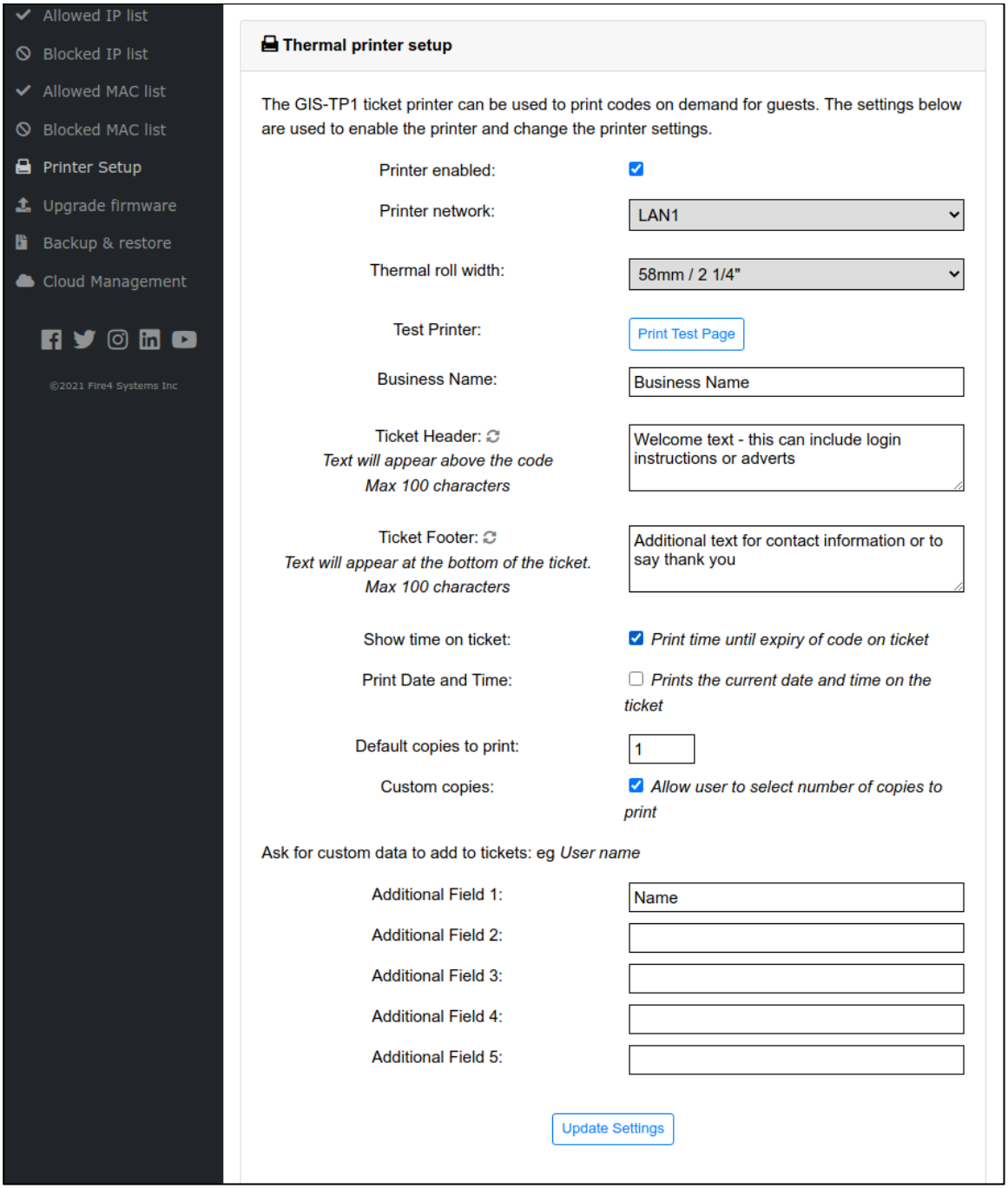
You need to ensure that a CODES password has bee set in the Change Password section.

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.

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.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



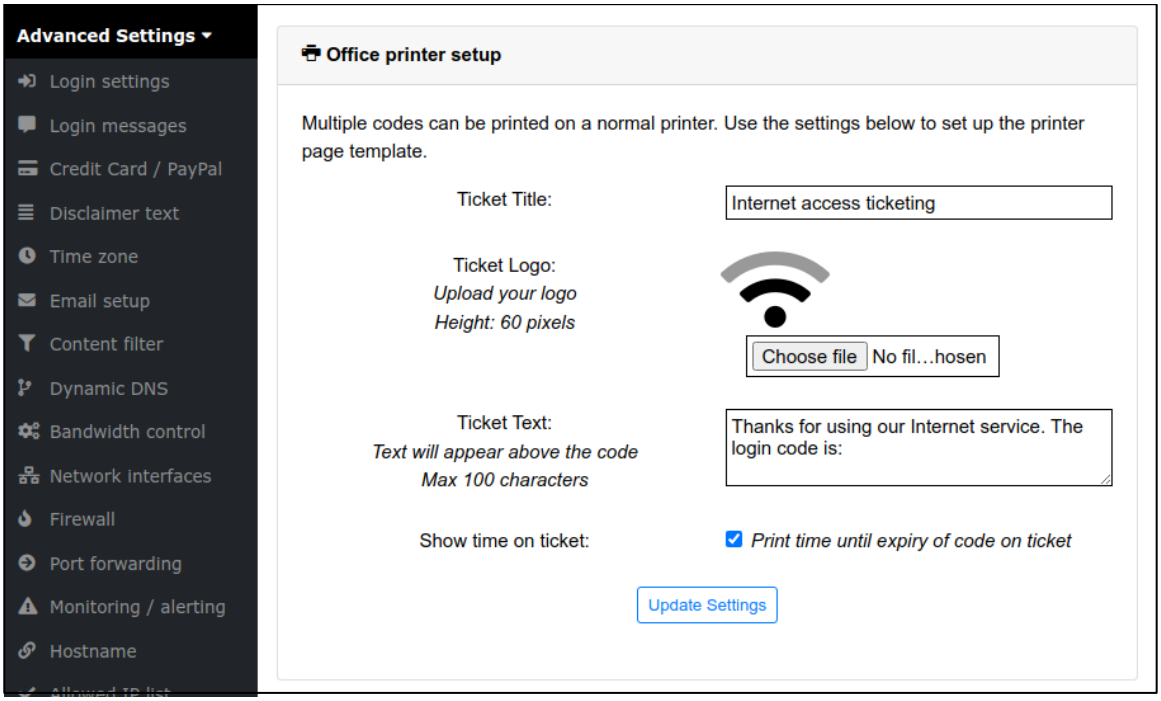
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Printer Setup for Letter Printer Access Code vouchers

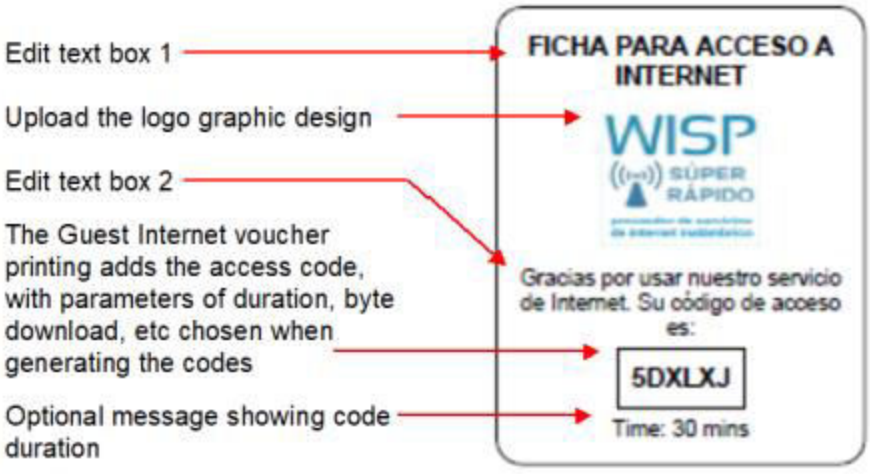
There are four configuration parameters for the voucher.

- Add text for the ticket title
- Upload the business logo
- Add text that will explain how to use the voucher
- Check a box to display the duration of the access code if required

The printer setup for the voucher is shown in the figure below



The figure below shows how the text fields and logo are printed on the voucher. The Access code is unique for each voucher.

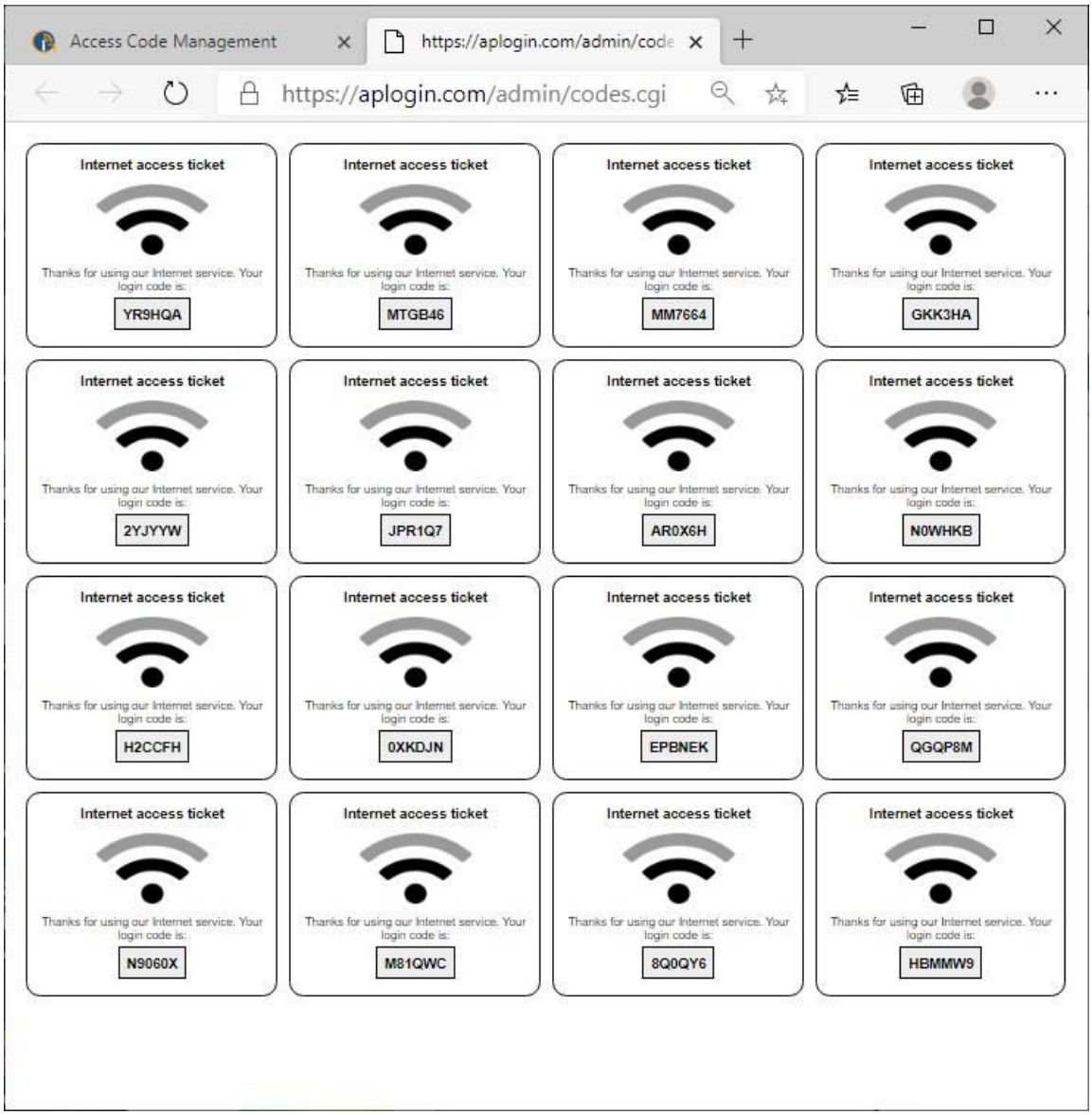


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

When the voucher design has been configured up to 10,000 vouchers can be generated and printed on sheets in a 4x4 format using any letter size printer. The access code generation page is used to initiate the generation and printing of the vouchers with access codes; see the relevant section of this manual for information about access code generation.

The print command displays the vouchers in a browser window, which can then be printed. Alternatively the vouchers can be printed as a PDF file for printing at a later date.

Each printed sheet is cut into individual vouchers for cash sales.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

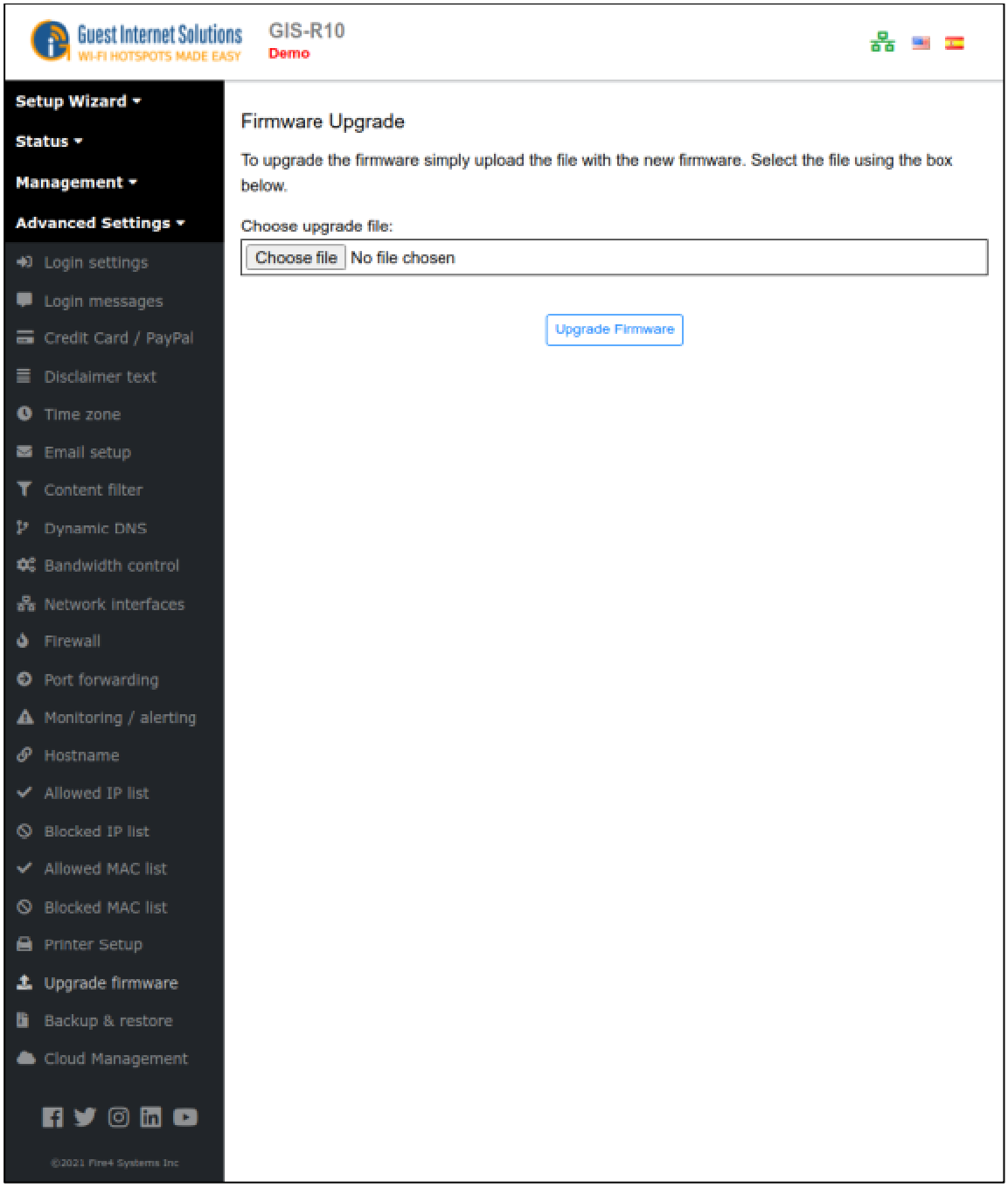
Upgrade Firmware

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.



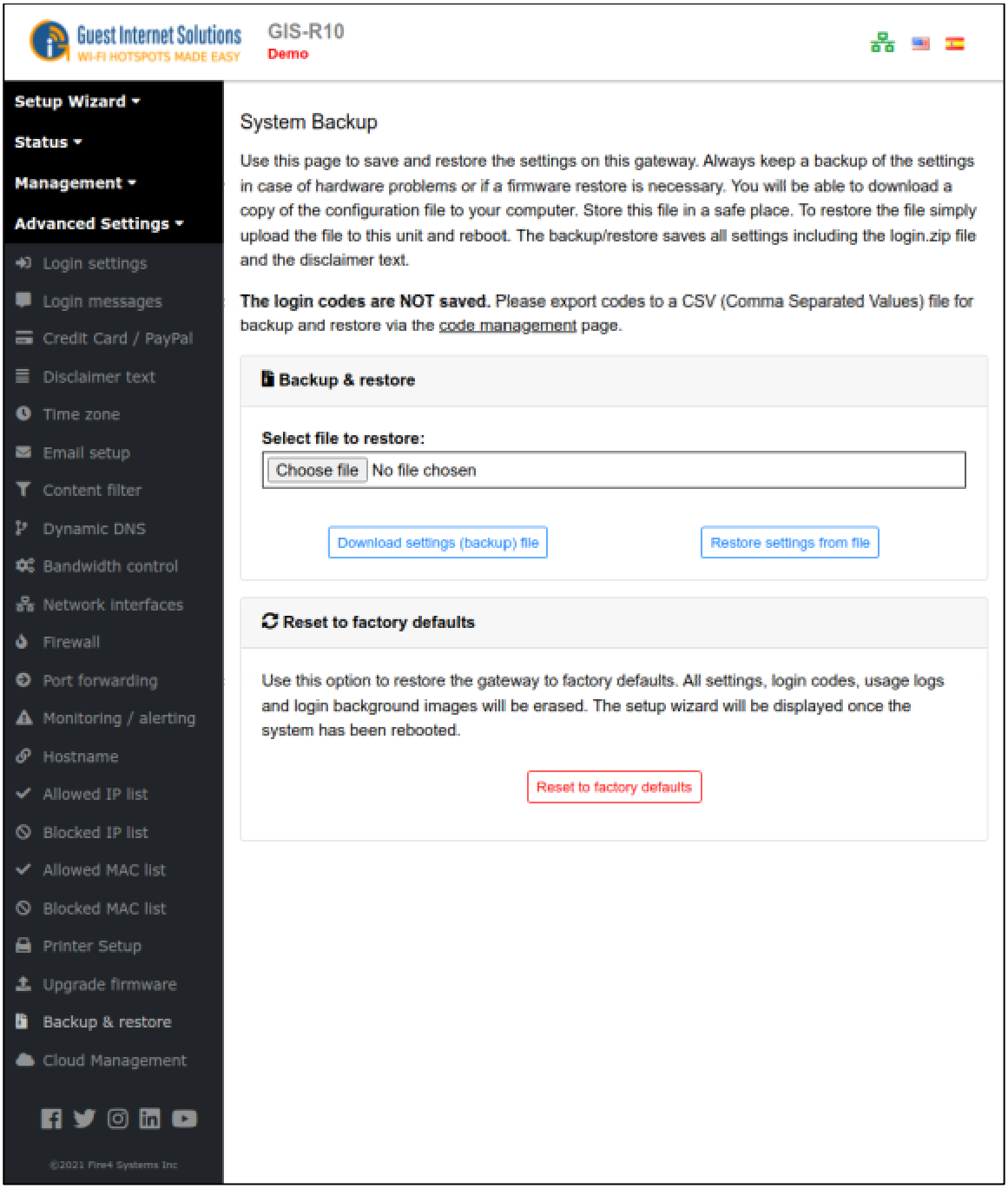
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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.

Backup & 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.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

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. One gateway is configured for the application and then the configuration file is saved, so the configuration file can be restored into all other gateways to be installed at different locations, thus speeding the installation process.

Reset to factory defaults

Use this option to restore the gateway to factory defaults. All settings, login codes, usage logs and login background images will be erased.

Activating cloud management

Guest Internet products must be activated before a cloud account can be used to manage the product.

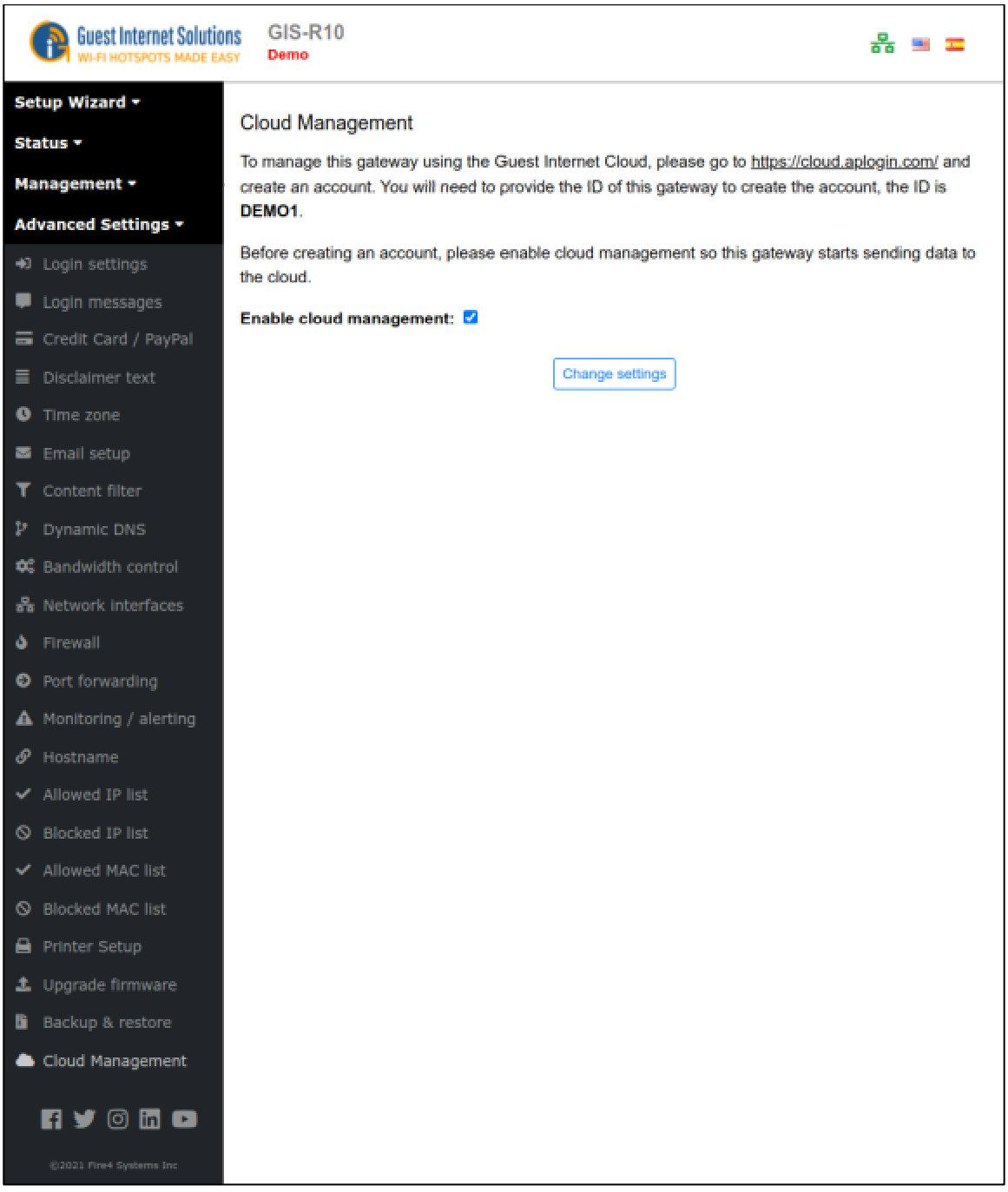
Click on the Cloud Management menu entry in the Advanced Settings section , see the following page.

Check the box: Enable Cloud Management

Add the serial number to a new or existing account.

Creating and using a cloud management account is described in the next section.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Cloud Management

You can create a free GIS cloud account that permits you to log into your portal from anywhere, then monitor and manage all of your GIS products.

To learn more about the GIS Cloud, please click here.

Setup Cloud Usage Guide

Request Cloud Enabled Firmware

Guest Internet Cloud

Sign up for a free account using your GIS unit serial number and see the benefits of using the cloud.

Unlike other cloud based systems, your GIS unit will continue to run without access to the Cloud making it more resilient to outages.

Click here to register for your account.

*Cloud functionality may not be available on older hardware

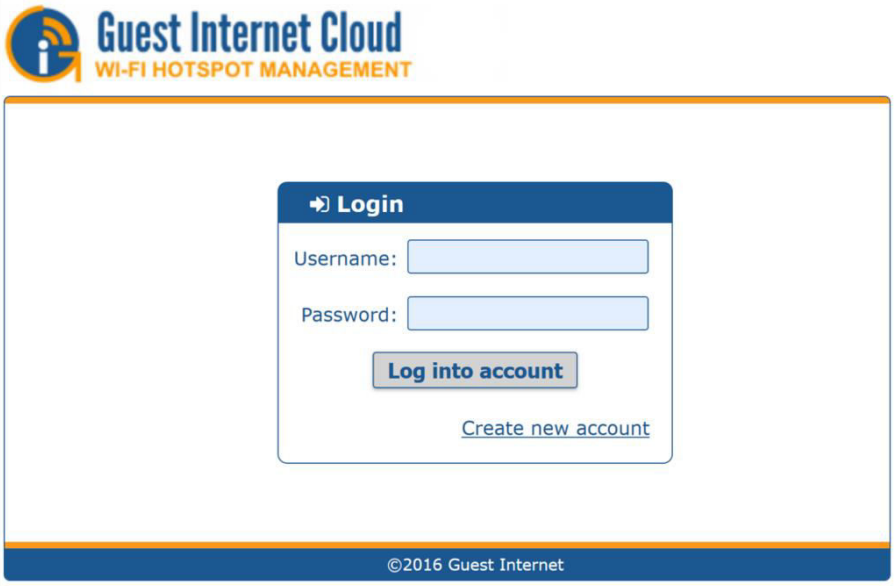
Cloud Management

The GIS Cloud permits any customer to log into their personal portal from anywhere, then monitor and manage all of their GIS products.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

A Cloud account is free

When a new GIS product is being installed it will give the option to create a new Cloud account or register the product with an existing Cloud account. Then access the Cloud portal to monitor and manage the product.



The Cloud is optional

Connect a computer to the network and open the browser to access the GIS GUI for monitoring and configuring the product. However most customers prefer to use the Cloud for product management.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Manage remotely

Access any GIS product from anywhere by logging in to the personal portal. No need to modify network settings, no need to configure port forwarding.

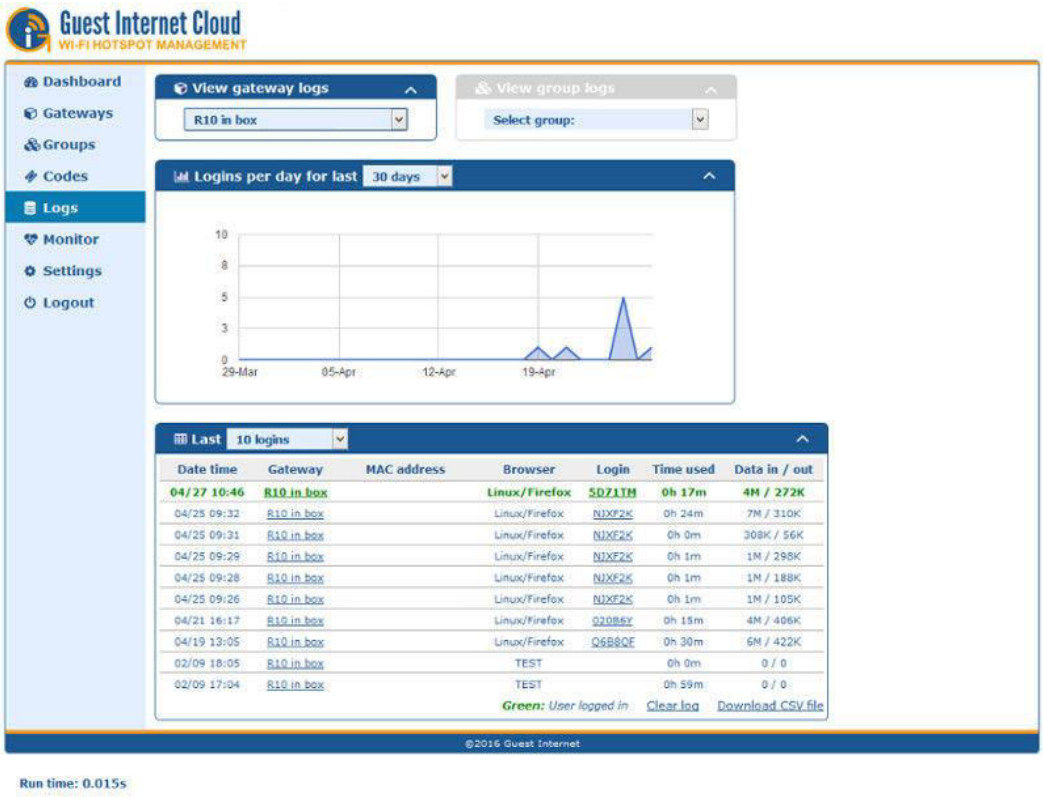
The power of the Cloud

The GIS Cloud gives access to one or to many GIS products, there is no limit to the number of products that can be monitored and managed using the Cloud portal, and no limit to network growth.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

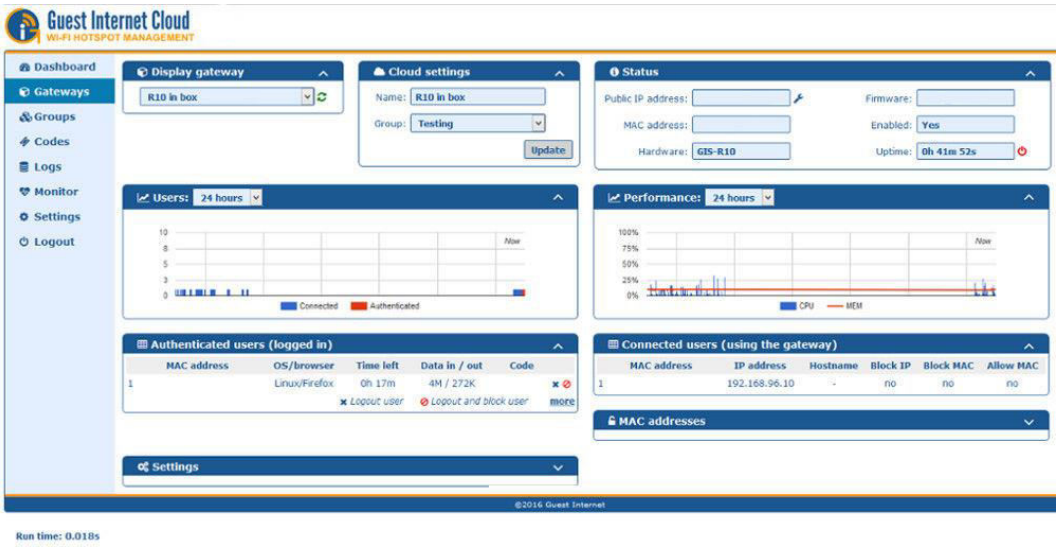
Manage many as one

The GIS Cloud permits many products to be managed as one group. Look at the groups stats, change the group settings. It's like having one big GIS product spread over many locations.



The Cloud advantage

The Cloud portal can send an email alarm when any product fails to connect to the Cloud, to facilitate support and maintenance.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Manage on the go

The GIS Cloud portal can be accessed from a 4G tablet or smartphone. Get warnings and correct problems 24 x 7 x 365

Managed services

IT service providers appreciate the value of the GIS Cloud as the ideal platform to offer managed services for their customers.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS Cloud Usage Guide

This guide is designed to help you make the most of the GIS cloud and utilise all its features.

If you run into any difficulty get in touch here

If you need help setting up your cloud account, please see the quickstart guide

Dashboard

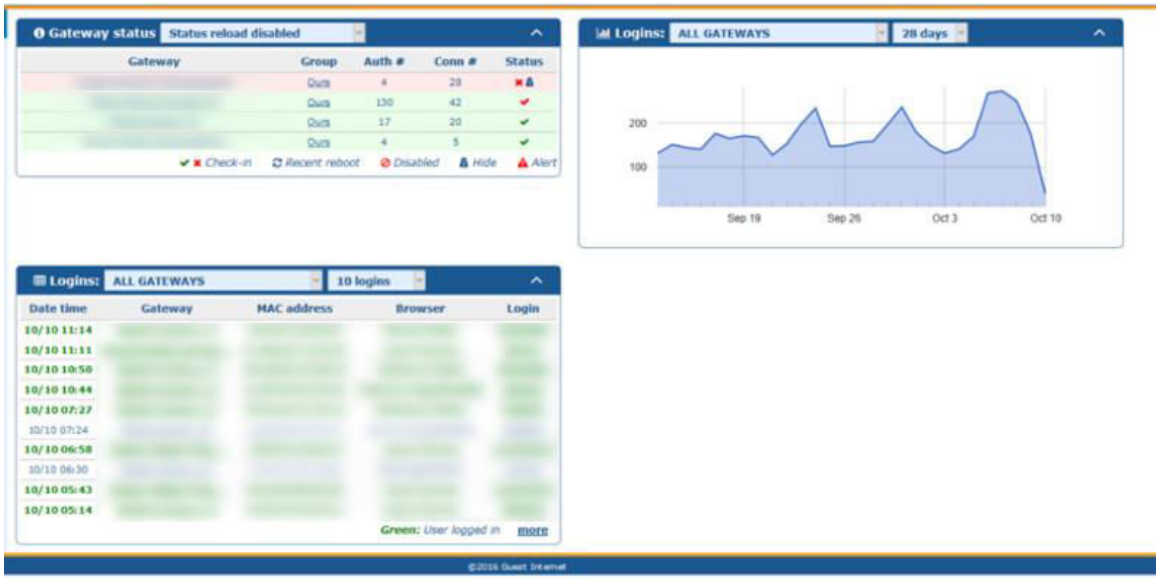
This page shows basic information for all your units

Here you will find all you need to know at-a-glance to help you check for any problems with your network.

- The Status box shows a list of your registered GIS units, their status and the group they are in (if any).

Note: When red, this shows the unit has failed to check-in or is offline; these units will always be shown at the top of the table.

- The Logins graph plots the numbers of logins.
- The Logins table shows detailed information about the most recent logins.



Clicking on a Gateway's name will take you to the Gateway page for this unit.

Gateways

This page gives detailed information about one of your GIS units, and allows you to manage your gateways

When you first open this page you will see very little information. You first need to select one of your registered units from the dropdown menu (you will have at least 1). See the next figure.

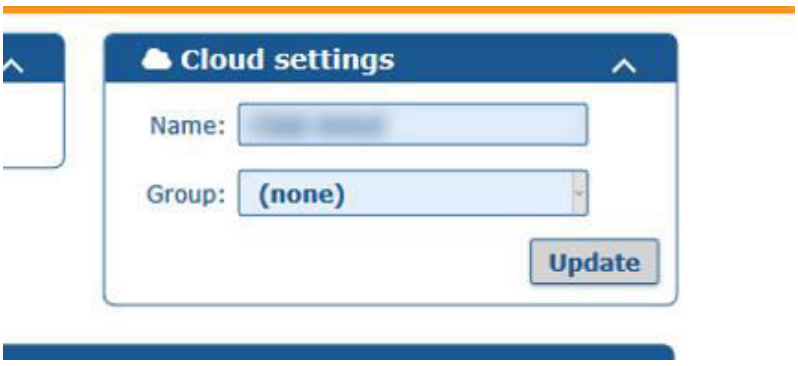
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Once selected you will be able to view the gateway's Status, graphs showing the Connected Users and WAN usage, list of Authenticated users and list of Connected users.

You can also modify basic settings on this page and set allowed/blocked MAC addresses.

Cloud Settings

Allows you to change the name of your gateway and add your gateway into a group.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

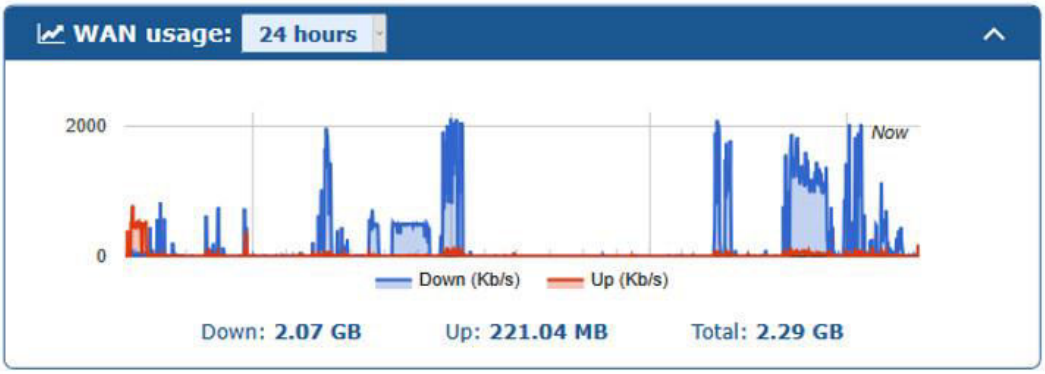
Status

Shows information about your GIS unit itself (MAC address, current firmware etc)

It also shows the unit's uptime and whether it is currently enabled. If you have remote access enabled, you will be able to access the unit here using the spanner icon.

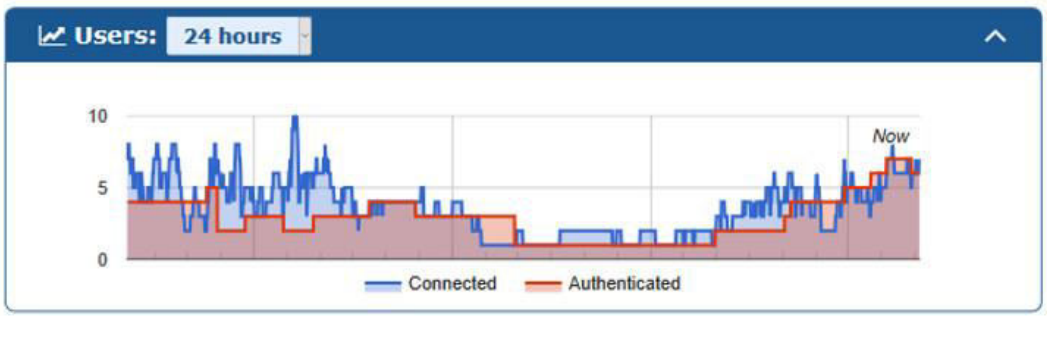
WAN usage

Shows the Kbps up and down on your unit over time. The timeframe can be altered to show more or less information, and hovering over the graph will give you absolute values.



Connected/Authenticated Users

Users Graph: The Users graph shows the connected and authenticated users over time.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Connected users: Users who have connected to the gateway, but not logged in.

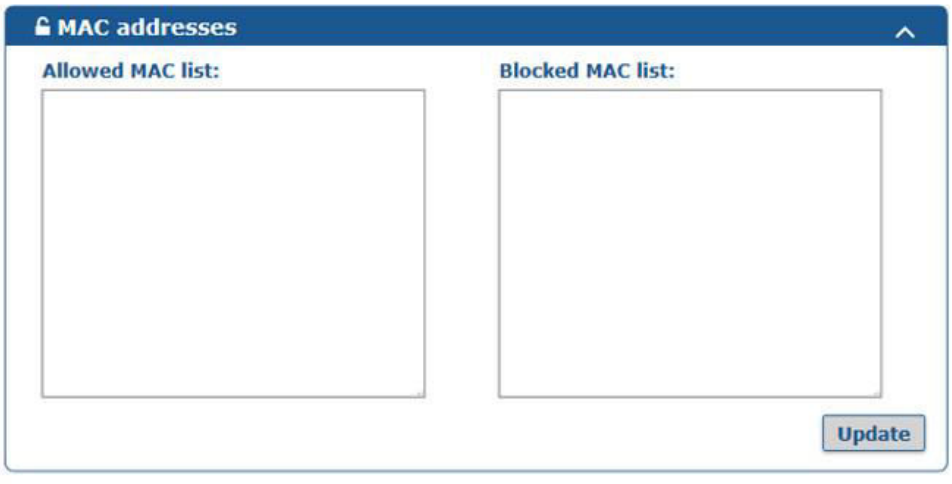
The Connected users table shows the MAC addresses, hostnames and assigned IP addresses of connected users.

Authenticated users: Users who have logged in to the gateway and have access to the Internet.

The Authenticated users table shows the MAC addresses, browser, time left, data up/down and code used to log in for each authenticated user. Here you can ban a user or log a user out.

Allowed/Blocked MAC: This shows the current Allowed MAC and Blocked MAC addresses.

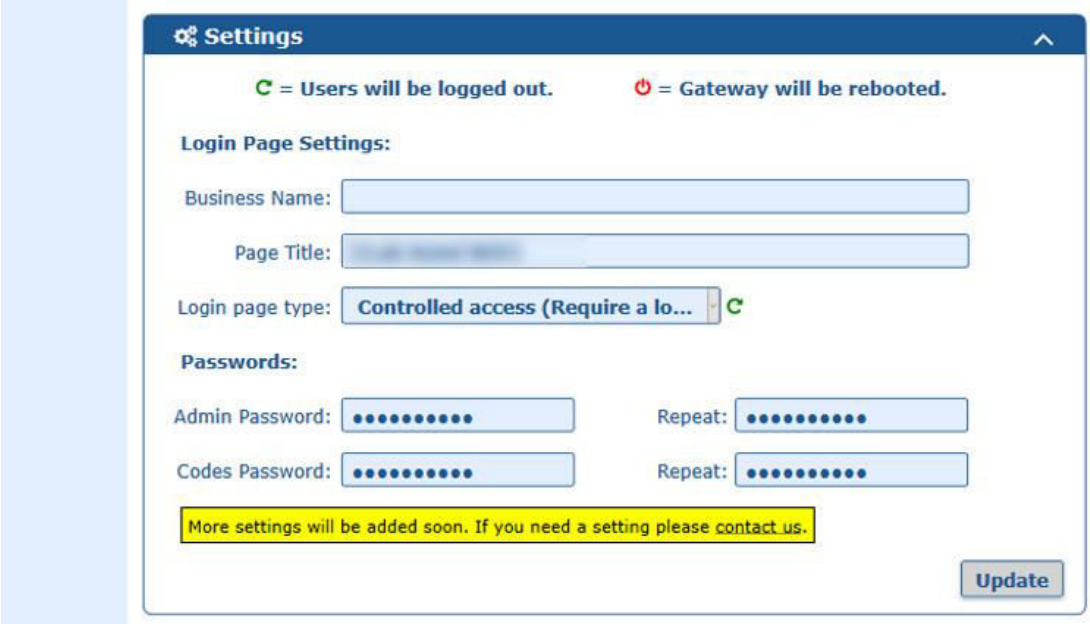
Allowed MACs allow a device to bypass the login page and have full Internet access at all times. Blocked MACs will prevent this device from logging in altogether. You can update this table and click the "update" button to edit this.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Settings

Here you can edit basic settings on your unit.



Adding another GIS unit

When you set up your account, the GIS unit you signed up with is automatically added to your account. If you wish to add further units to your account, simply enter the ID of the unit into the "Add a Gateway" box, then click "Add gateway".

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Removing GIS unit from the Cloud

If you wish to remove a GIS unit from your Cloud account, on the Gateway page, under "Delete a Gateway", simply select the ID of the unit you wish to remove, and click "Delete Gateway"

Groups

Create code groups (sharing codes across multiple GIS units)

With groups you can create codes to be used across multiple GIS units. Groups also allow for easier management and monitoring of multiple units. To use groups you must first create a group using a unique group name.

Once created you can add gateways to the group by selecting the group in the Cloud Settings on the Gateways Page. You can now create group codes which will be shared across any GIS unit in the group. These are created on the Codes page

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

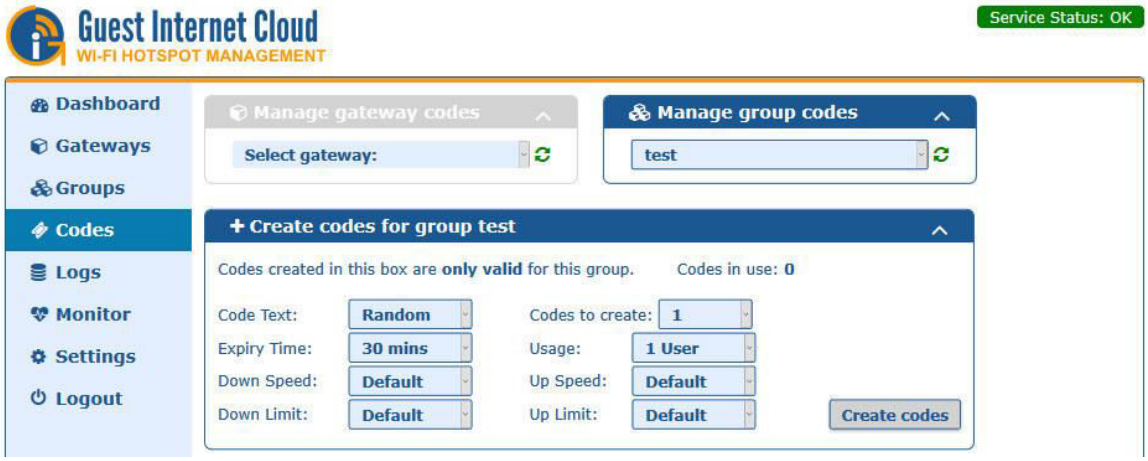
Codes

Create codes for single GIS units or groups

You can create codes as usual for a single unit using the same method as on your local GIS admin interface.

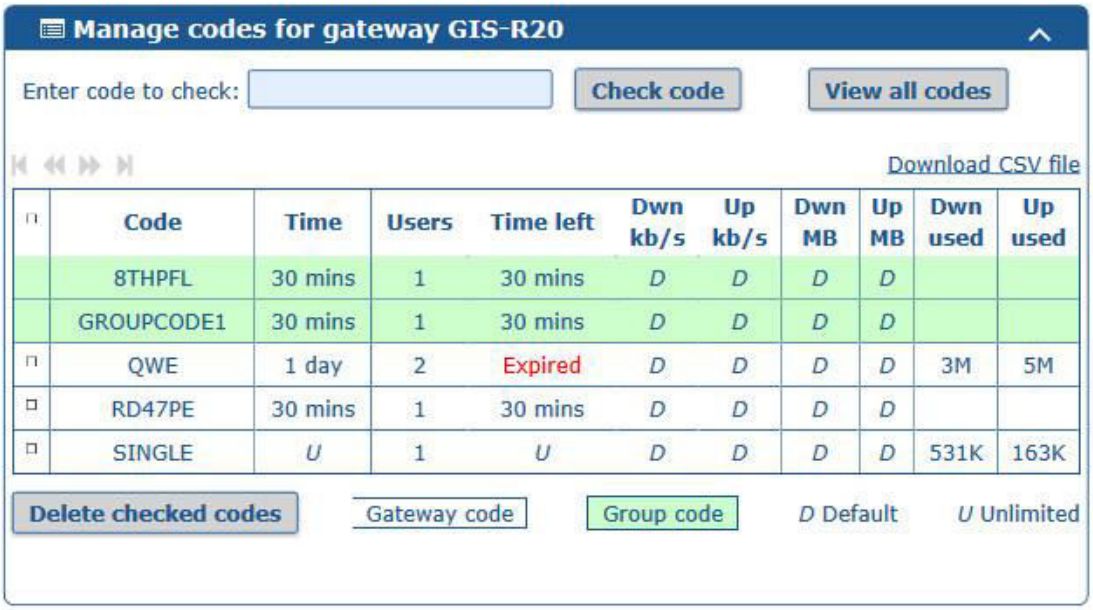
- Code Text - The name of your code ("Random" creates alphanumeic random code)
- Number of codes to create - The number of random codes to create
- Expiry time - The amount of time you wish to give to the user
- Usage - Number of users for a single code (1-5 or unlimited)
- Down speed - Max allowed Mb/s down
- Up speed - Max allowed Mb/s up
- Down limit - Max allowed data downloaded
- Up limit - Max allowed data uploaded

You can also select a group to create codes for. Group codes are created in the same way as individual gateway codes.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

You can also view all codes on this page for the selected unit or group. Group codes will be shown highlighted in green. (this will be the same on your GIS unit's local admin interface > Manage codes page.)



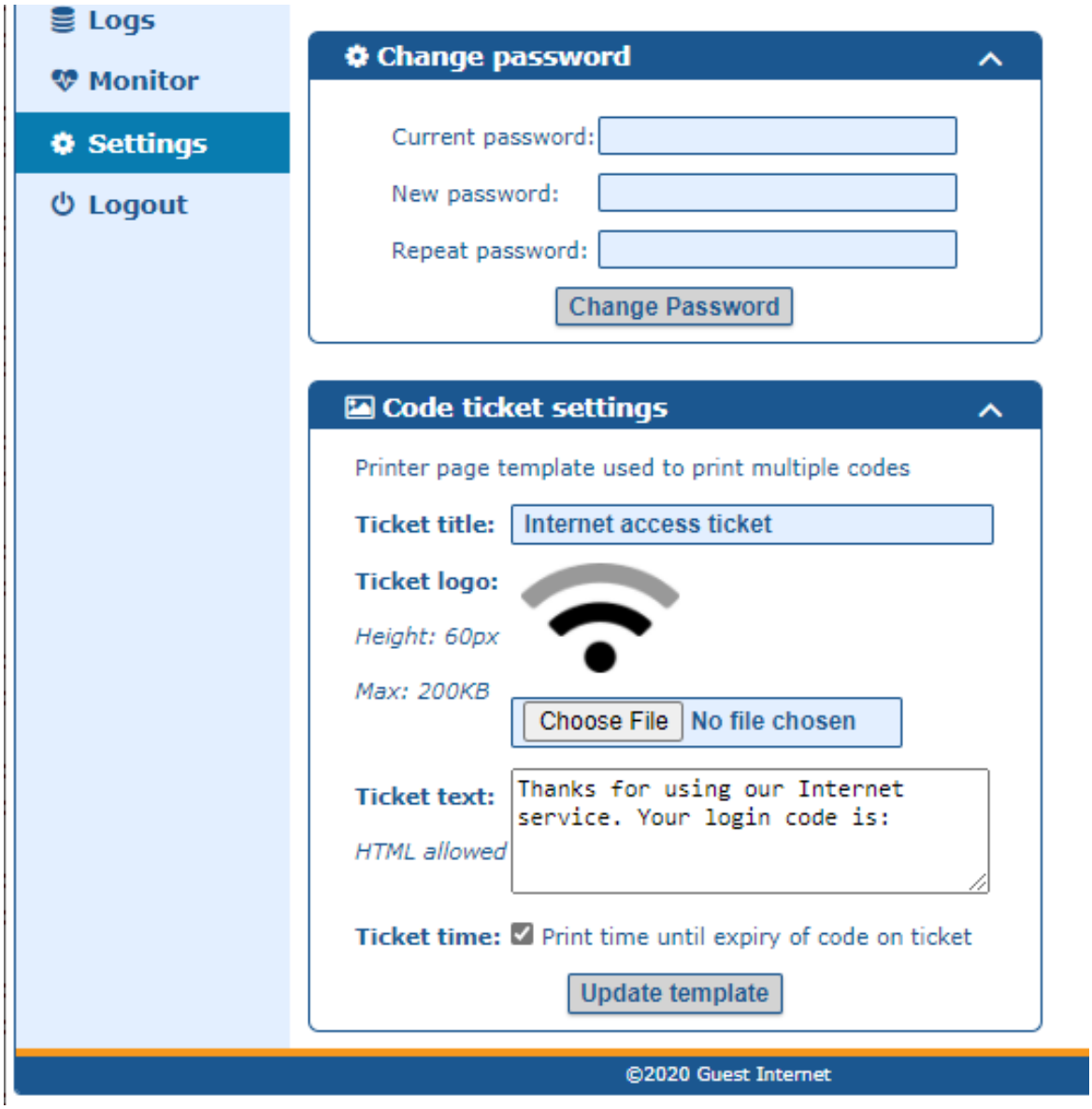
Code	Time	Users	Time left	Dwn kb/s	Up kb/s	Dwn MB	Up MB	Dwn used	Up used
8THPFL	30 mins	1	30 mins	D	D	D	D		
GROUPCODE1	30 mins	1	30 mins	D	D	D	D		
QWE	1 day	2	Expired	D	D	D	D	3M	5M
RD47PE	30 mins	1	30 mins	D	D	D	D		
SINGLE	U	1	U	D	D	D	D	531K	163K

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Cloud Voucher Printing

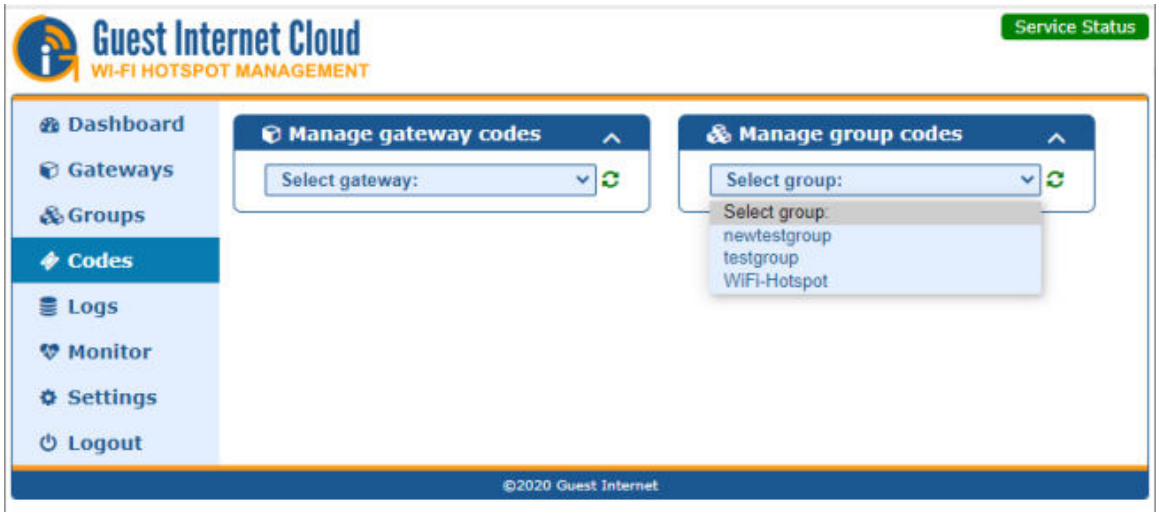
When access codes are generated with the cloud the codes can also be printed as vouchers on a Letter size page in a 4 x 4 grid. This is identical to the voucher-printing feature in the Guest Internet firmware. However the codes can be group codes that can be authenticated by any gateway that has been added to the group. This might be thousands of gateways spread throughout a city or country.

The first time that vouchers are to be printed the voucher design is created. Go to the settings menu entry then configure the code ticket settings. Add the text and the logo that will be printed on the voucher

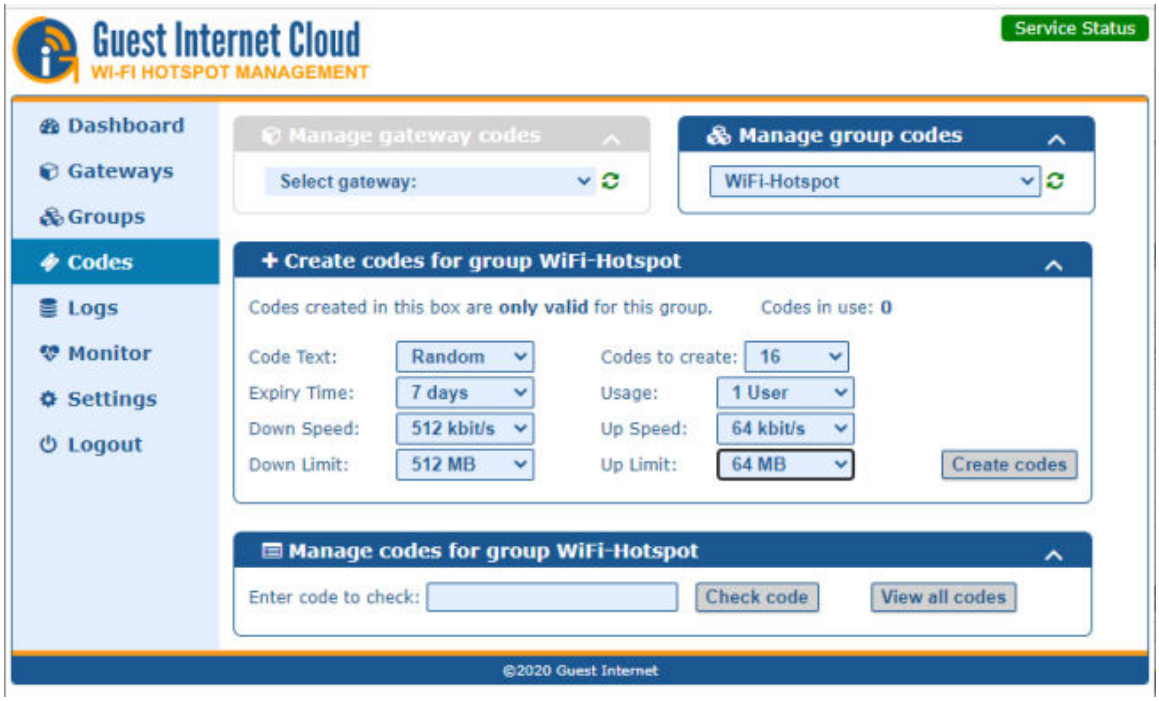


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Next select the group that the voucher codes will be printed for.

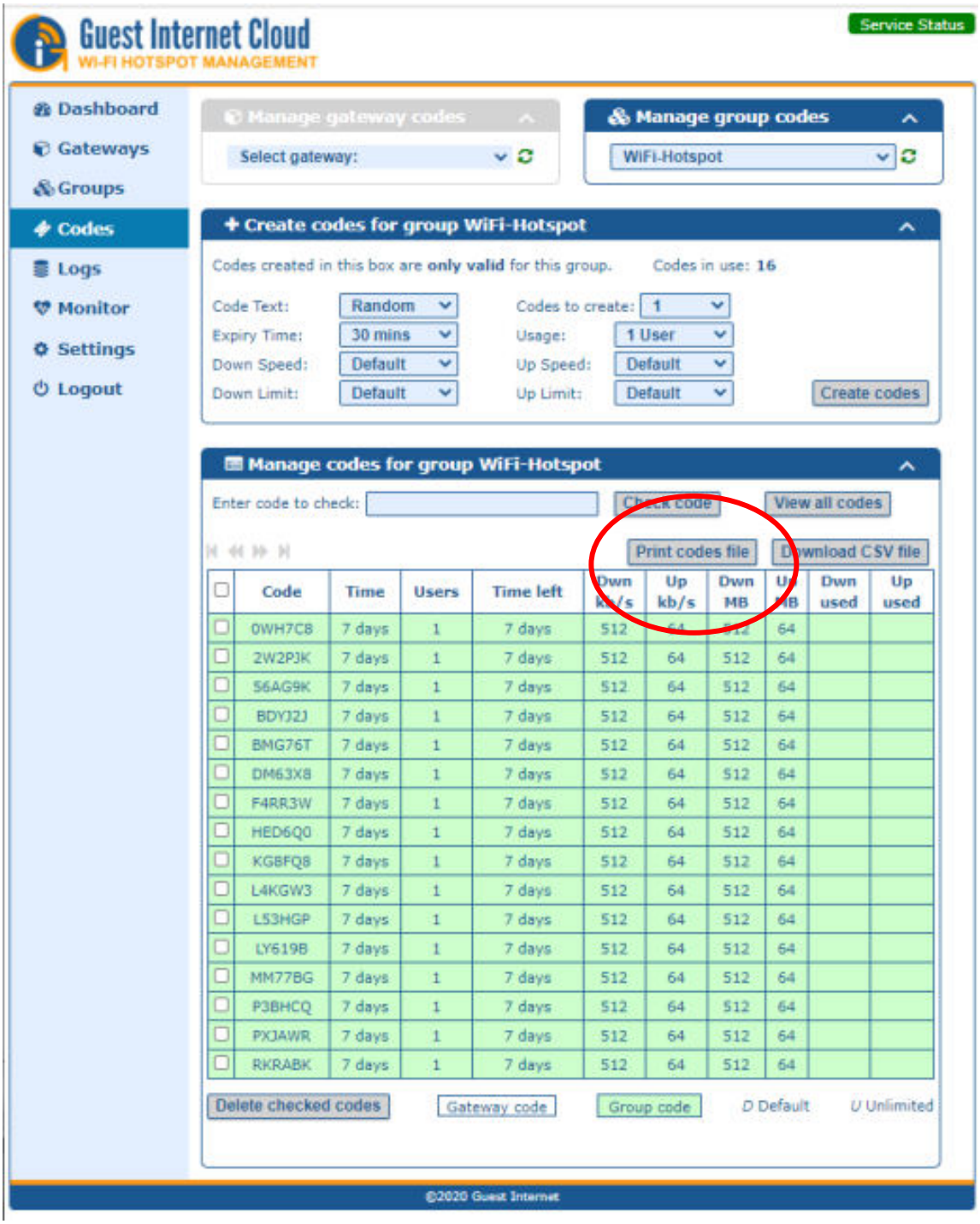


Set the code parameters and the number of vouchers that will be printed



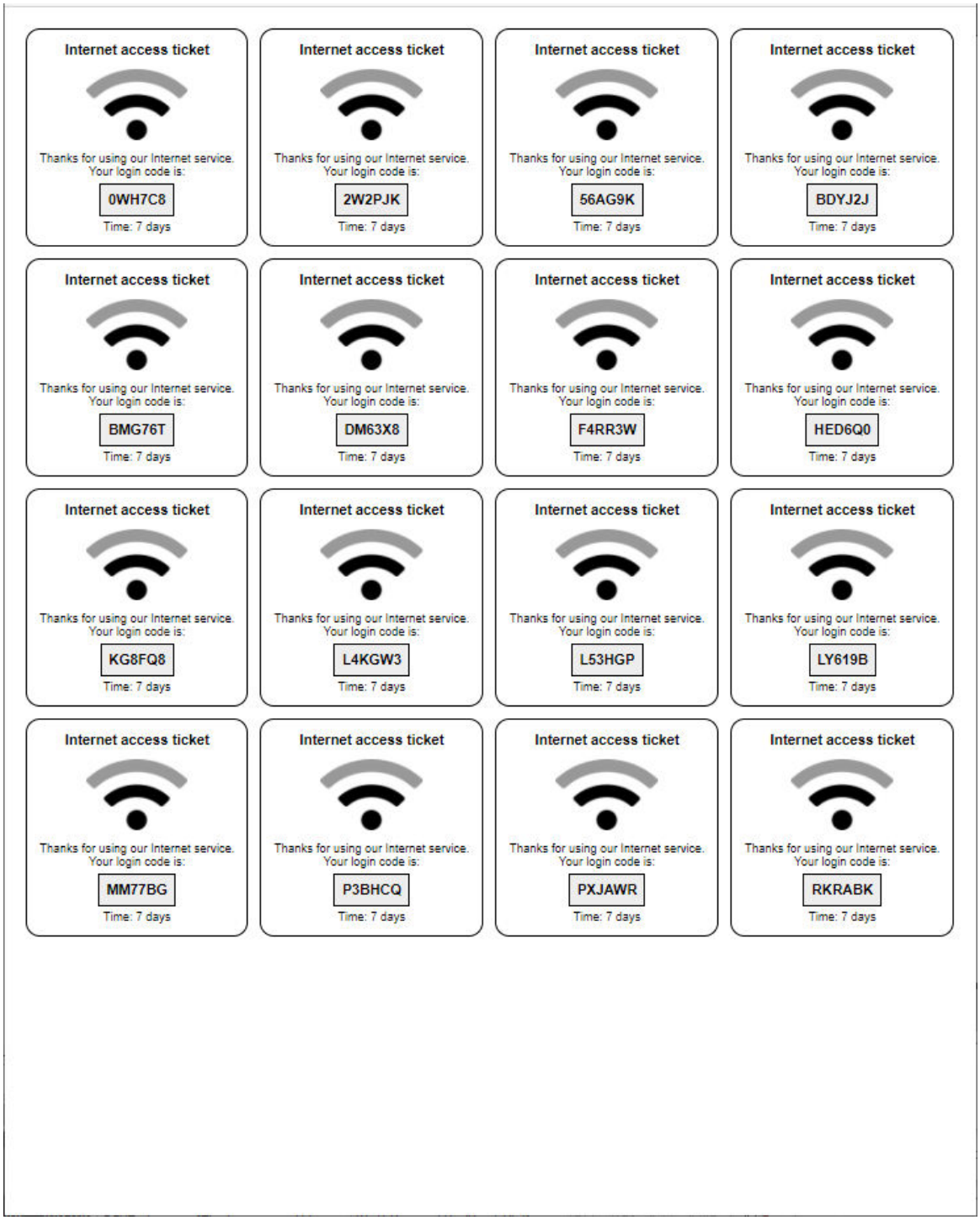
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

When the codes are generated they will be listed on the page. The green background indicates that the codes are group codes.



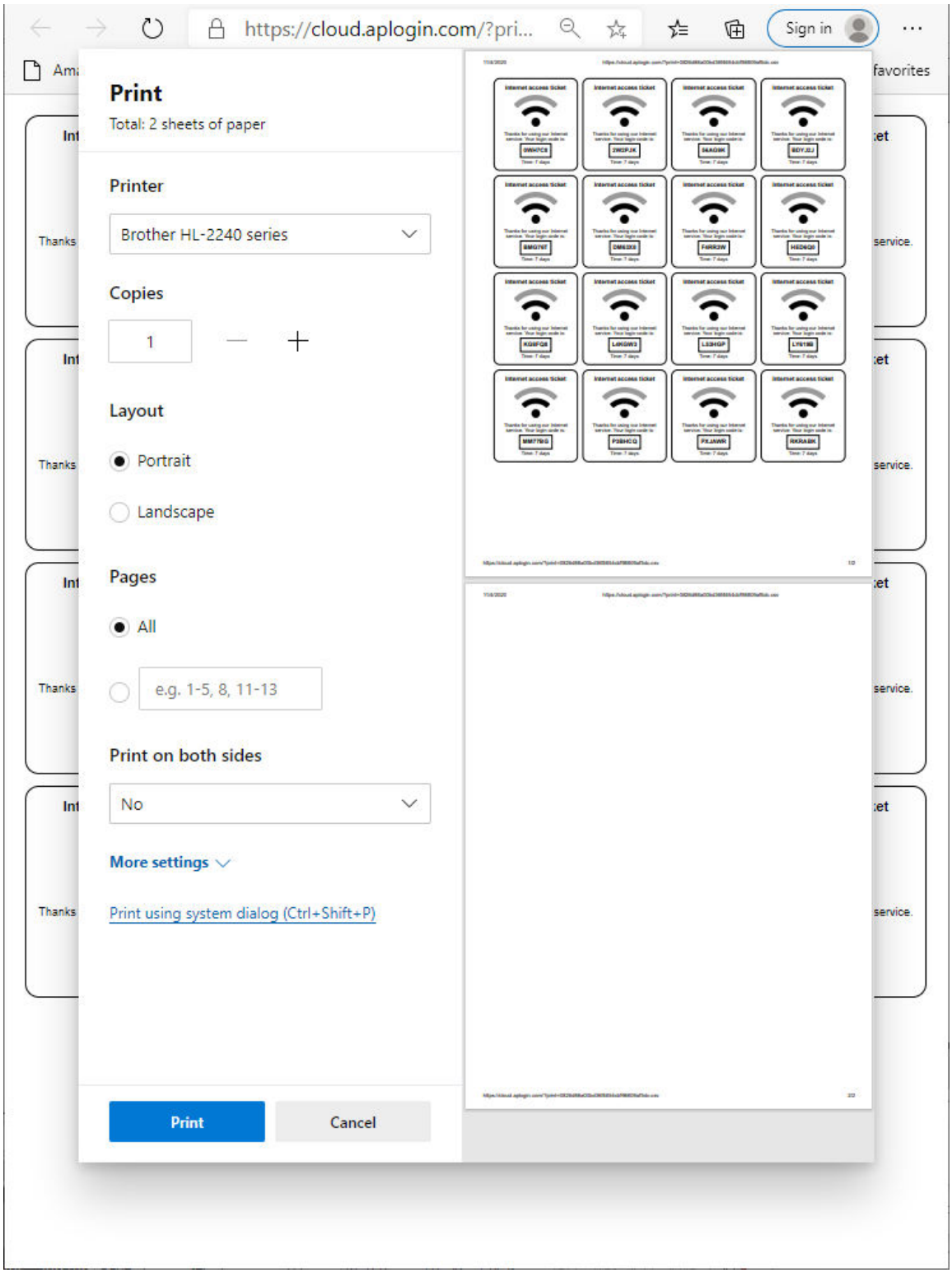
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

When the print codes file button is clicked the page of vouchers will be displayed as this will be printed onto a Letter size page in 4 x 4 format



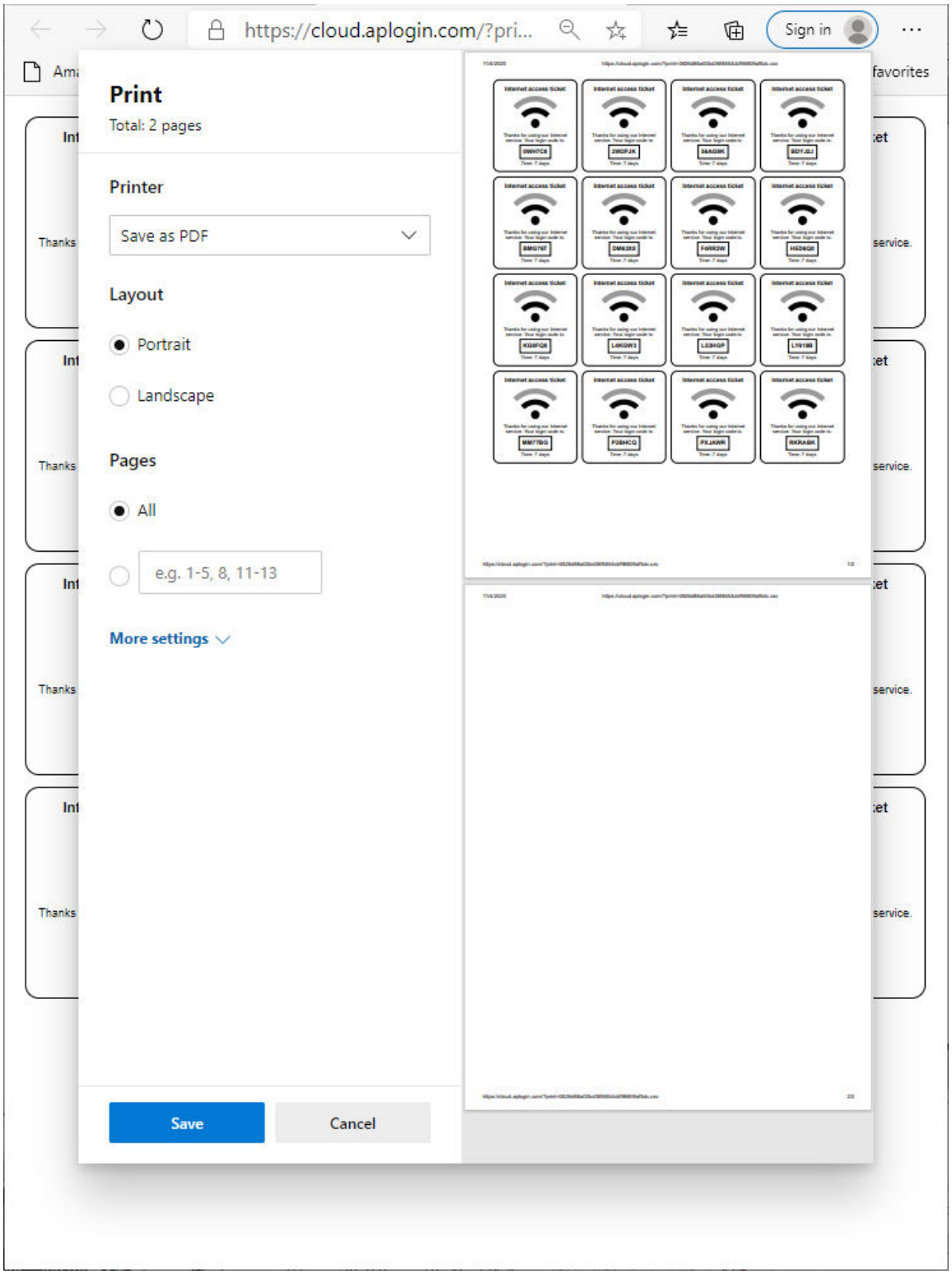
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The vouchers can be sent to a printer, and then cut up into individual vouchers.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Alternatively the vouchers can be stored as a PDF file and sent to a printer to print onto a card, or to create a scratch-off card.



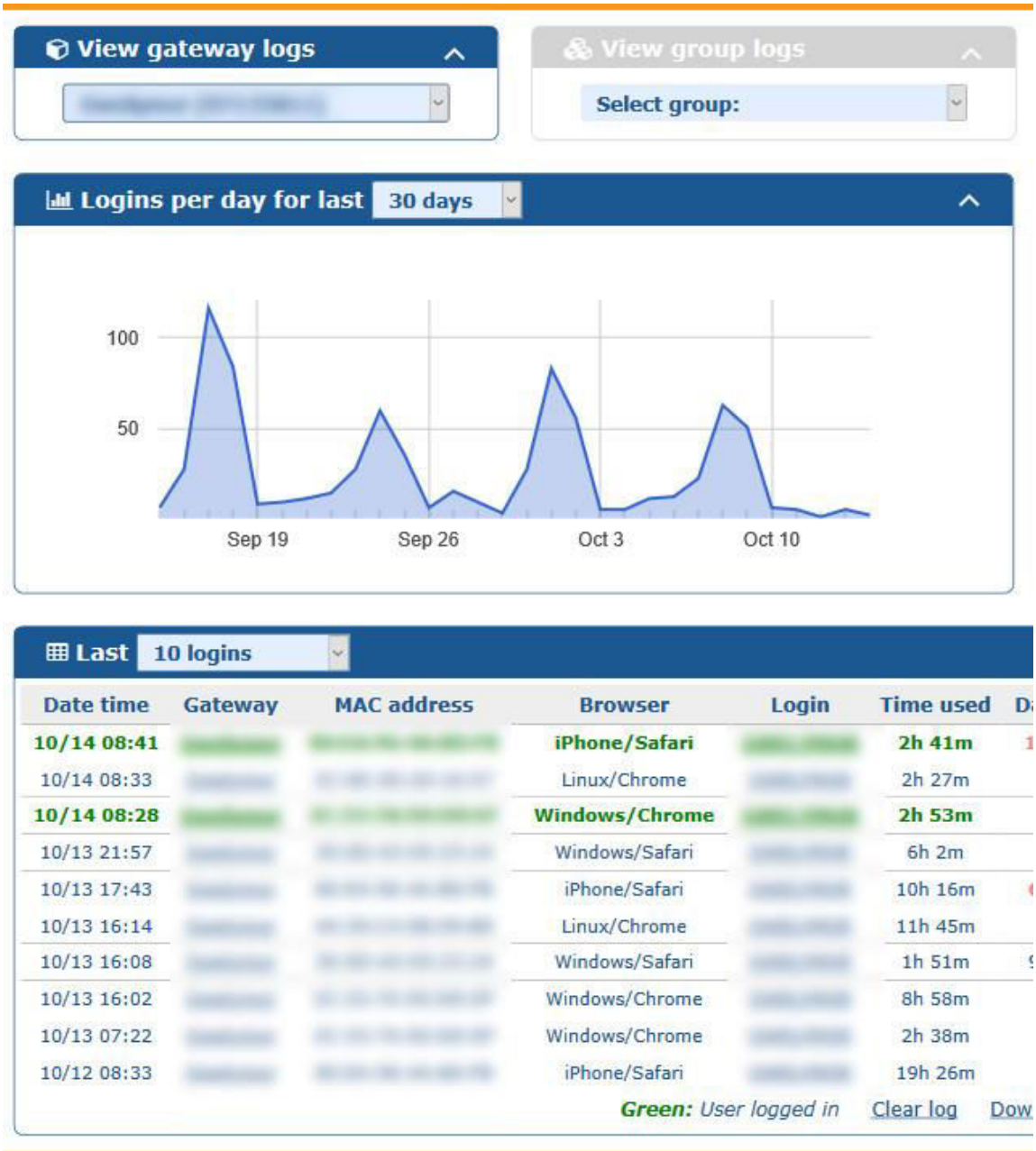
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Logs

View logs (usage reports)

On this page you monitor usage using the graph of past usage for a single unit or a group of units.

You can also see a table of the latest connections for a single unit or group, much like the Usage reports on your GIS unit's local admin interface. You can choose which unit you wish to show logs for. The Users Graph/Table is shown on the following page.



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The Cloud Group Graph and Table is shown below.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Monitor

Monitor Unit Status and set up Alerts

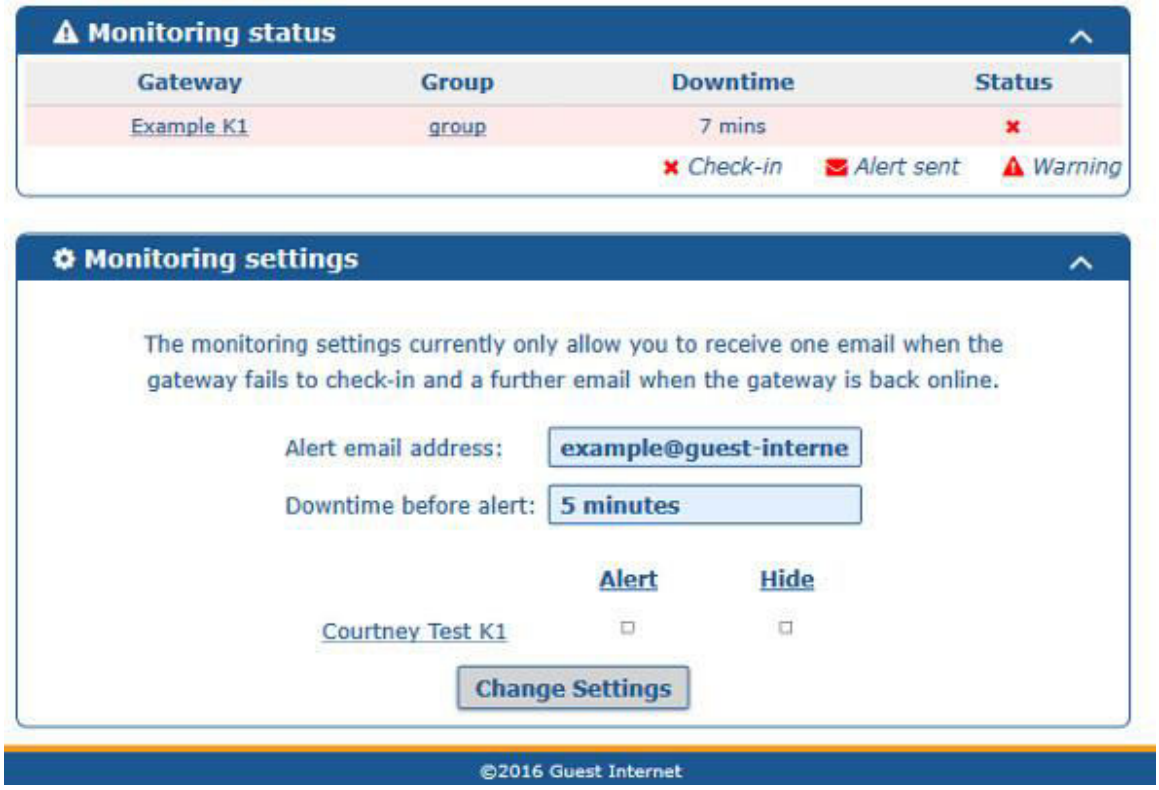
The live monitor status shows any unit which is not currently checking in with the Cloud, and shows how long it has been down for.

Tip: You can hover over the cross or tick under "Status" to see when the unit last checked in.

You can also create automatic email alerts, to let you know as soon as one of your units goes offline.

When selected, if a unit does not check-in for 5 minutes and alert email will be sent to the address you signed up with. A second email will be sent when it comes back online.

Next to each registered unit you will see a checkbox for both Alert and Hide options. When Alert is selected, an email alert will be sent if this unit goes offline. If hide is selected, this will remove it from the gateways page.



Settings

Allows you to change your password

This page allows you to change your password. Further settings may be added in future.

Failure to check-in/offline

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

What it means if your unit shows as offline

Failure to check-in/offline

X If your unit is showing red on the dashboard or on the monitor page it means your unit is either offline or that it has not checked in with the cloud in over 5 minutes.

/ If you see a red tick next to your unit, this means it has not checked in for over a minute, but below the 5 minute cut-off period to be shown as being offline. This would indicate a potential issue with the unit reporting to the cloud.

In either of the above cases, this does not necessarily mean the unit is not working; just that it has not reported to the cloud. Potential causes are that either the unit has lost access to the Internet, has an error preventing it from contacting the cloud or that it is not working altogether.

If your unit shows as being offline, you will need to investigate to find the cause. If the unit seems to be working correctly, but not reporting to the cloud, please contact us via the support page.

Mobile

On mobiles the interface will alter slightly

On mobiles and tablets, to maximize on available space, the menu will be moved to the top and will display Icons rather than text. The icons left to right are in the same order as top to bottom as on the Desktop view.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Cloud FAQ

Frequently Asked Questions

Q: How do I set up a new account?

A: See the setup guide here.

Q: How do I add another unit to my account?

A: Simply enter your units ID into the "Add a gateway" box on the Gateways page. See here.

Q: How do I create a code/group code?

A: Codes are created in the same way as on your GIS unit's local admin pages. Select the code settings and click "create codes". This can be done on the codes page. See here.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Additional Information

Reset to Factory Default

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.

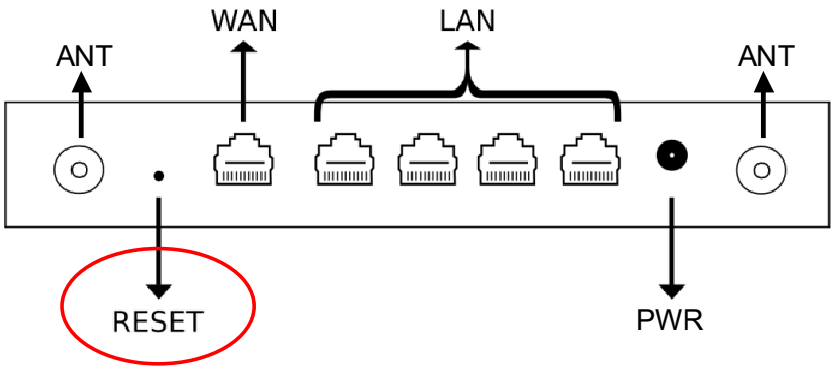
This section describes procedures to reset all the necessary product parameters to factory defaults so that the product can be accessed once more.

If you want to erase all data from your unit, see information here.

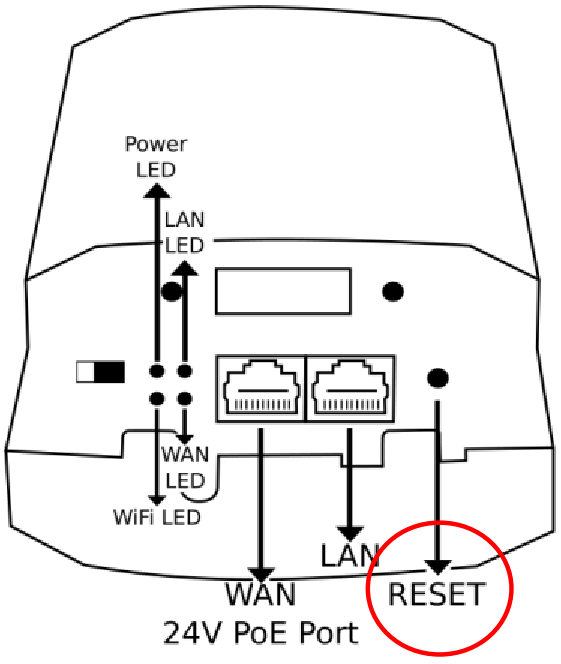
Reset to defaults as follows:

1. Power up the gateway unit and locate the hole in the enclosure for the reset button.
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.

GIS-K1

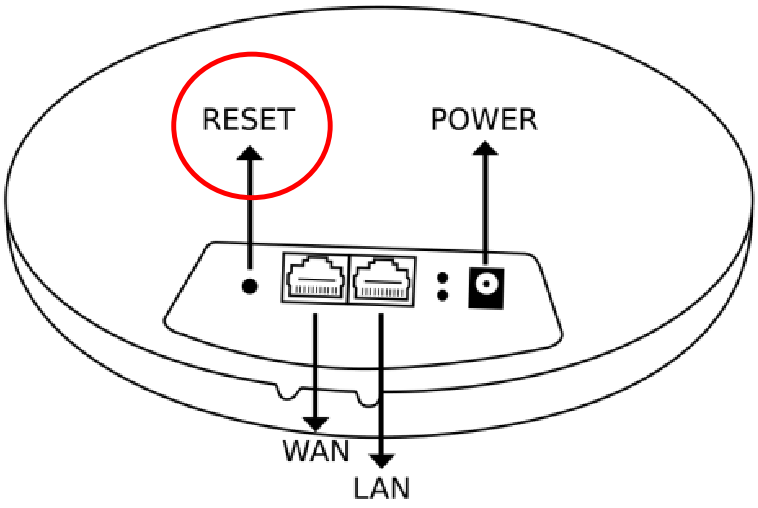


GIS-K3

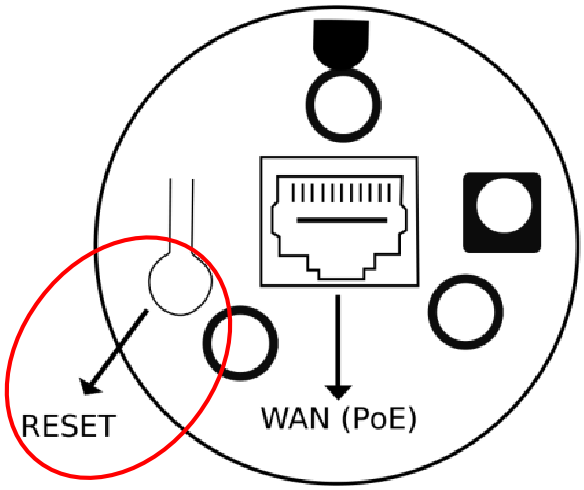


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

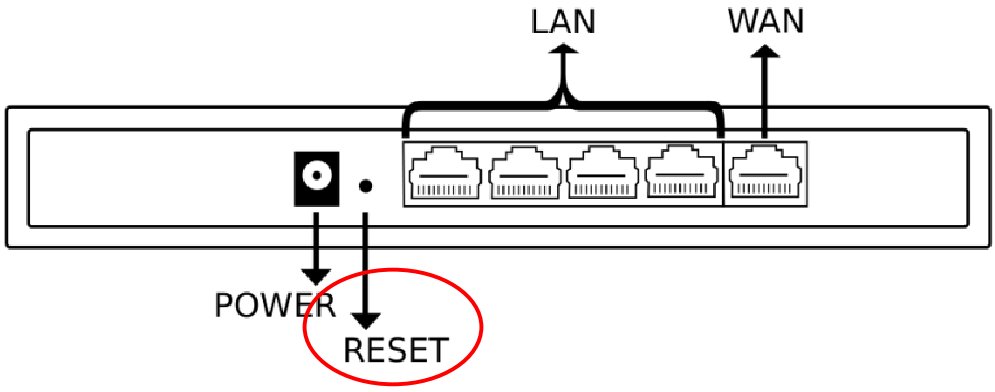
GIS-K5



GIS-K7

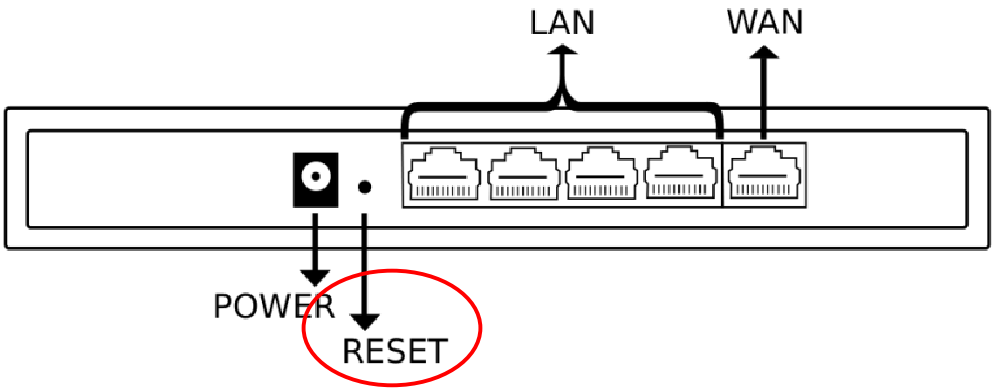


GIS-R2

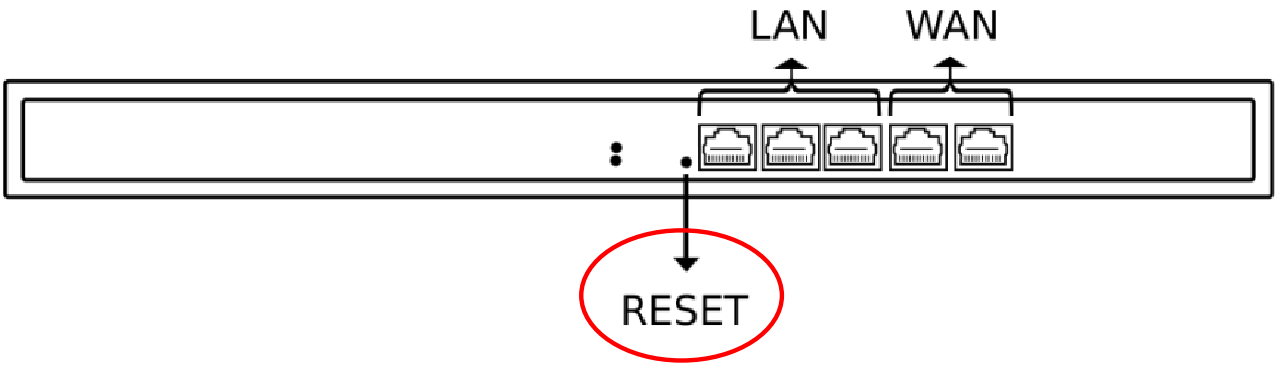


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-R4



GIS-R6



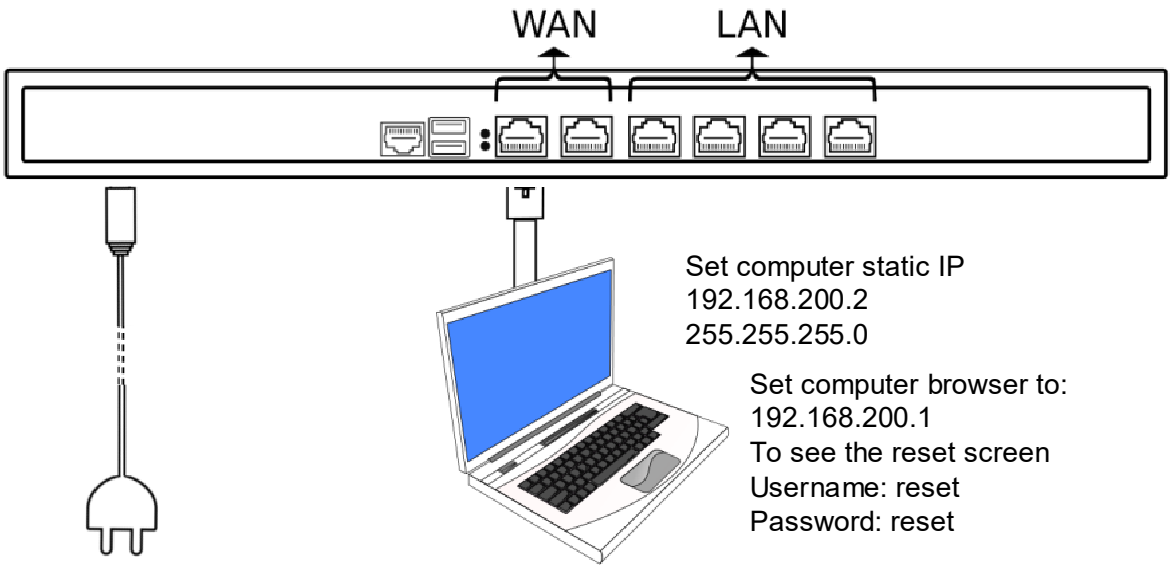
Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

The GIS-R10, GIS-R20, and GIS-R40 products do not have a reset button.

To reset to the factory default configuration:

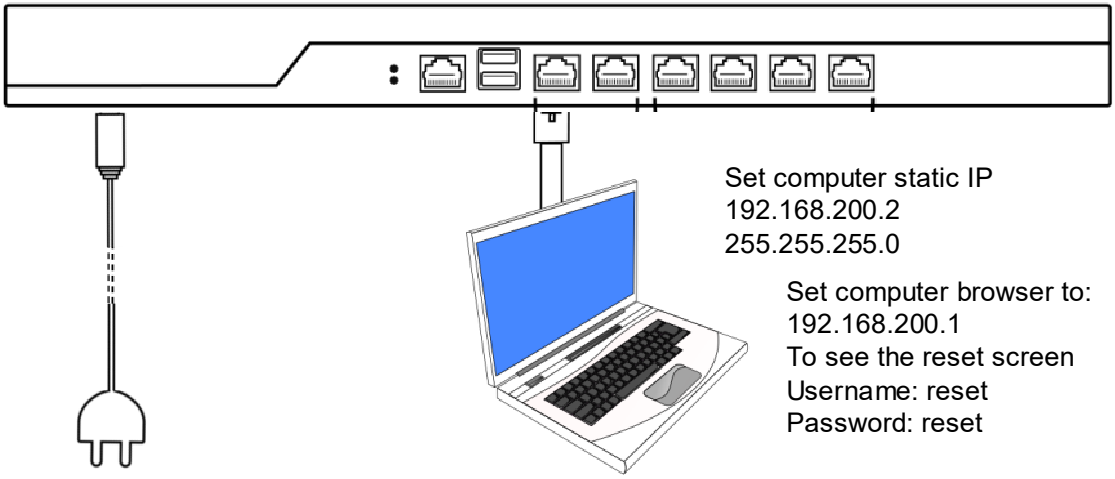
1. Connect a computer to the primary WAN port of the device.
2. Set the computer Ethernet port to an IP of **192.168.200.2** and Subnet Mask **255.255.255.0**.
   To learn how to set a static IP address on your device, click here.
3. Open the browser at an IP address of: **192.168.200.1**.
4. Type the username **reset** and the password **reset**.
5. Click on *enter*, another page will appear.
6. Click on the Reset to defaults button and then wait two minutes.
7. Switch the product power off then on.
8. Proceed to reconfigure the product using the wizard as described in an earlier section.

GIS-R10

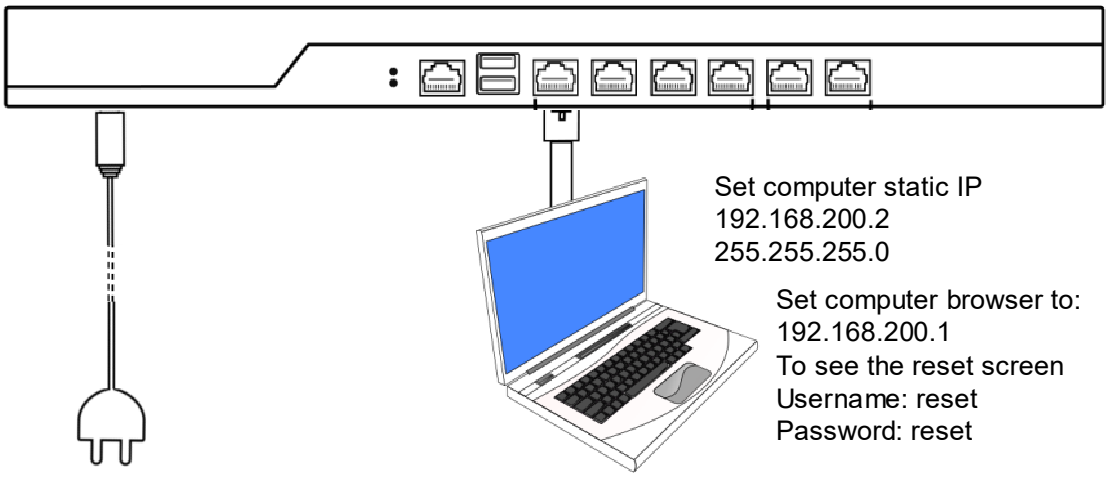


Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

GIS-R20



GIS-R40



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Troubleshooting your GIS

Unit stuck on "System Test Please Wait..."

If your unit is stuck on "System Test Please Wait..." the first thing you need to do is reset to factory defaults.

If after reseting your unit, it still does not work, please contact us, as the unit will need to be sent back for repairs.

Unit does not have access to the Internet

The GIS units will run a number of checks for potentially quite some time to determine if the Internet connection is stable enough to return, to avoid complaints from your guests having issues with internet connection, but no error from the GIS unit.

Please follow the steps below:

1. Check Internet access with your router
2. Check that your router is plugged to the WAN port of your GIS unit
3. On the System Preferences page of the admin interface, check if you are gettin an IP on the WAN port

If you are having continued issues with this, please contact us, so we can look further into the issue.

I can't get to the admin interface

First check you are connected directly to the unit via ethernet (this is preferable for troubleshooting), then visit http://aplogin.com/admin.

If this fails, check you are getting an IP from the unit. If so, please visit the GIS unit's LAN IP address manually (by default on LAN1 this is 192.168.96.10).

If not, please reboot the unit and check all connections.

If the issue persists, attempt a factory reset.

If you are still having problems, please contact us.

Users cannot see login page

Check if the user is actually connected to the unit and check they see the login page when manually visiting http://aplogin.com.

Redirection is a problem when the users home page is encrypted (https) which is becoming increasingly common.

If an attempt is made to redirect an encrypted connection then the browser will show a message that the computer is being hacked, or similar. Redirection of an encrypted connection is called a 'man-in-the-middle' attack.

For this reason if the user tries to establish a https connection behind the login page then we do not respond, in the hope that the user will try a http connection.

Please instruct your guests to use an HTTP or you could advice to go to http://aplogin.com

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Most modern devices will open a browser by default when recognizing connection behind a captive portal and open their default browser or mini-browser at a http page, to allow for redirection. This will be the case for most users.

Only one concurrent user can connect to the internet

When only one user can be logged in at any one time, so each user will get internet access, but will be dropped as soon as another connects. Most admins would not notice this, and would instead see that users can log in for a short period of time, and are then logged out.

This means that your Access Point is not set on bridge mode, so all the users are getting the same IP address. Therefore only one user can get access.

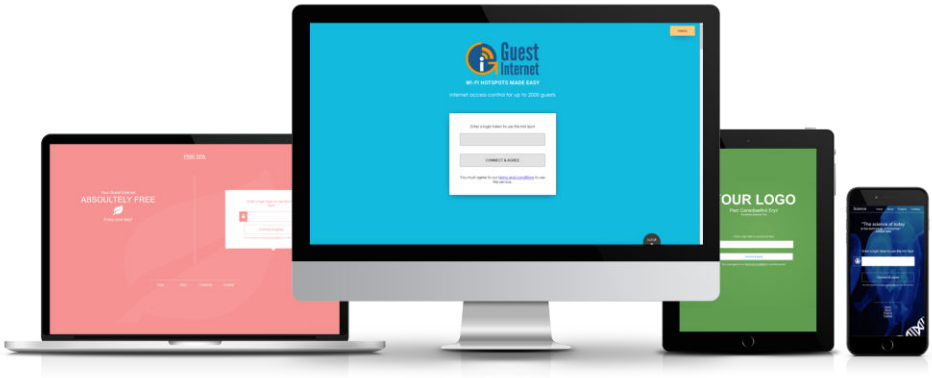
We have set a few examples on how to setup your Access Point correctly in bridge mode, to read more, please click here

This could also be the issue if users are seeing the **"There was an error"** generic message.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Captive Portal

A Captive Portal is a web page that requires a login method before network access is granted. The login methods can be simply viewing and agreeing to a disclaimer, connecting via email, paid access with PayPal® or using an access code.



Benefits

The first and most important benefit of the Captive Portal is to free you from resposability in case of any illegal activties by a guest. Using a captive portal also gives you control over your bandwidth, you can set limits (time, bandwidth or speed) for each user that connects to your network.
Captive Portal is an excellent marketing opportunity as your Login Page can be fully customised with your company logo, information and promotions.

1. Identify your business. By identifying your business, you prevent users to connect to a hacker's network.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

2. Promote your business

You can create a personalized Login Page and display information about your business, with offers.

You can also collect users data and use it for marketing. For example: you can collect users email address and add them to a mailing list with offers.

3. Protect your business

As you are providing open access, some risks are introduced to your network.

If a guest does something illegal you can block the user and keep the users MAC address as well as other information.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

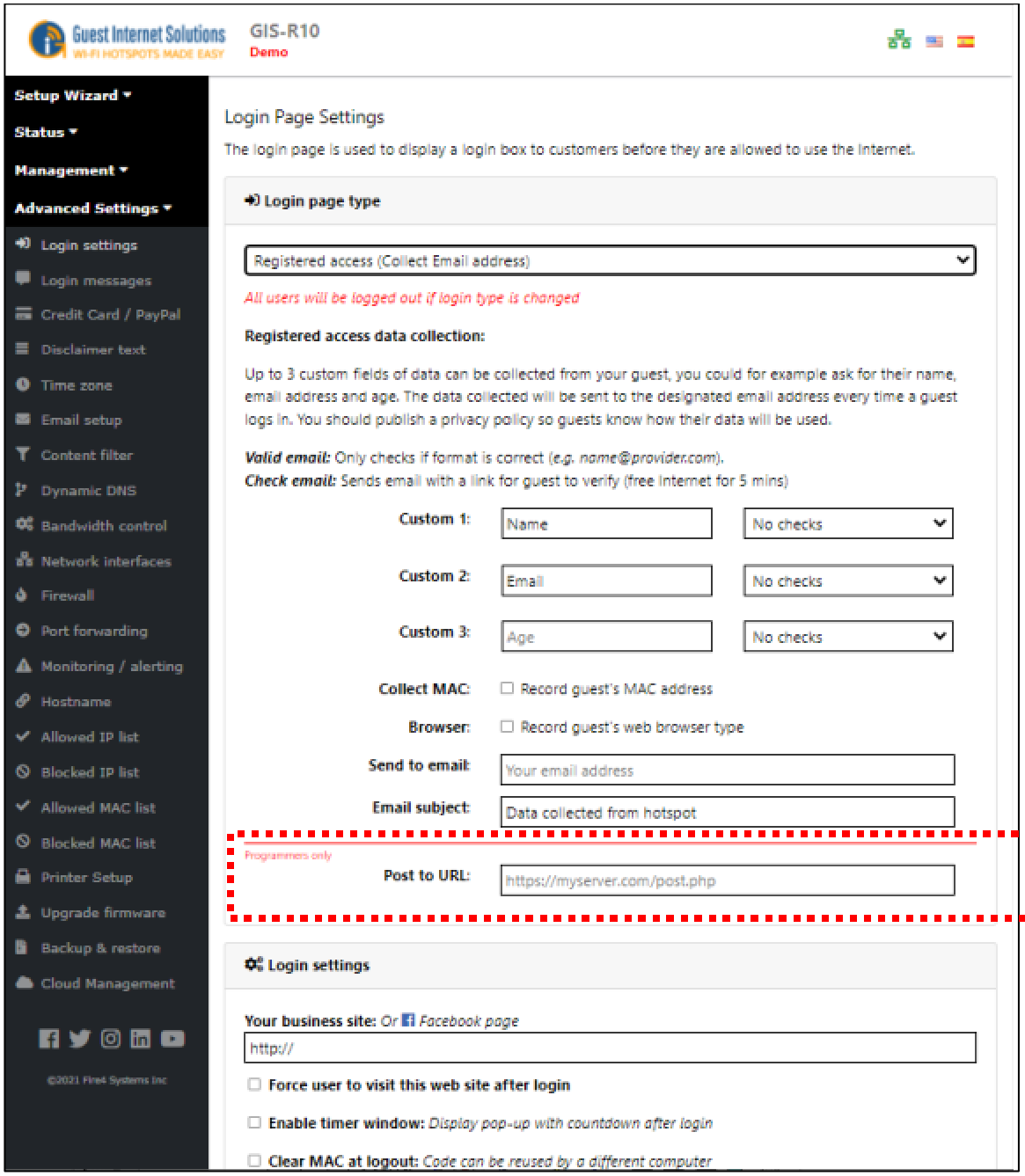
CSV

A **Comma Separated Values** (CSV) stores tabular data in plain text. Files ".csv" can be imported to and exported from any spreadsheet program.

Each line of the file is a record and record is made of fields that are separated by commas.

HTTP Post

Data collection with the GIS unit is set up on the 'Login settings page':
http://aplogin.com/admin/loginpage.cgi



Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

This information can be sent to an email address, or sent to be processed by a script running on your server.

This script can be written in many different web-based languages, however the below basic example is done using PHP.

The data is sent by HTTP POST from the GIS unit when the user presses the ‘Connect & agree’ button to the URL you provide on the ‘Login settings page’. The URL should be the location on your server of the script you are using to make use of this data.

An example would be:

http://www.myserver.com/example.php

The following data is sent:

Up to 3 key/value pairs defined on the login settings page. key = name defined on Login settings page

Login time/date key/value pair	key = “LOGIN”
Hotspot ID key/value pair	key = “HOTSPOT_ID”
MAC address key/value pair	key = “MAC_ADDRESS” (if selected)
Browser type key/value pair	key = “BROWSER” (if selected)

These are all contained in the $_POST array.

You can access the key/value pairs in the $_POST array by requesting the value using the “key”. This is done with the following:

```
$_POST[“key”];
```

Where “key” is an example key of a key/value pair.

This can be passed to a variable with the following:

```
$example_variable = $_POST[“key”];
```

$example_variable now contains the value associated with the key value pair of the given key. This variable can now be used as you wish, e.g. to pass to your database. You can also get a dump of all the information from the $_POST array using the following:

```
var_export($_POST, true);
```

Or

```
var_dump($_POST);
```

The following example takes the $_POST information and passes each value from the key/value pairs to variables, and also does a var_export of the $_POST to see all the data contained within it. It then appends these variables to a text file located in the same directory as the php script, so you can easily see the output.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Example Code

```
<?php
//set variable $file to be the text file located on server
$file = 'test.txt';

//set variables to take the value of $_POST based on the "key" given for that value
$name = $_POST["Name"]; //name set by user
$age = $_POST["Age"]; //name set by user
$favorite_colour = $_POST["FavoriteColour"]; //name set by user
$login = $_POST["LOGIN"];
$hotspotID = $_POST["HOTSPOT_ID"];
$mac = $_POST["MAC_ADDRESS"]; // Needs to be selected on login settings page
$browser = $_POST["BROWSER"]; // Needs to be selected on login settings page

//Exports all the key/value pairs from $_POST
$all = var_export($_POST, true);

//Append the values of the above variables to a file $file
file_put_contents($file, "Name:$name\n
Age:$age\n
Favourite Colour:$favorite_colour\n
Login:$login\n
Hotspot ID:$hotspotID\n
MAC address:$mac\n
Browser:$browser\n\n
Everything from the var_export $all\n\n\n" , FILE_APPEND | LOCK_EX);
//The End
?>
```

This should write something similar to the following to the test.txt file located in the same directory as the PHP script:

```
Name:Mike
Age:25
Favourite Colour:Blue
Login:2015-08-03 07:36:33
Hotspot ID:152axxx
MAC address:00:00:00:00:00:00
Browser:Linux/Firefox

Everything from the var_export array (
'LOGIN' =       > '2015-08-03 07:36:33',
'HOTSPOT_ID' =       > '152axxx',
'Name' =       > 'Mike', 'Age' =       > '25',
'FavoriteColour' =       > 'Blue',
'MAC_ADDRESS' =       > ‘00:00:00:00:00:00’,
'BROWSER' =       > 'Windows/Firefox',

)
```

This is not very easy to read, nor very useful, however it shows the basic concept of receiving the information from the GIS unit and saving it to your server to then make use of.

Rather than printing these variables to a text file you can pass them to your database and use them as you wish to provide analytical data about your users and their internet usage.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

API

The access code request API is implemented in all GIS firmware versions and is available to PoS vendors and other systems integrators upon request.

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.

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

Creating Codes

Codes can be added to the system via a single HTTP call, the URL 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.

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.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Parameters to pass are shown in the following table:

Parameter	Values	Comments
code	Create a name to the code	Argument is optional and is not necessary for the call
num	Number of codes to create	Argument must be included in the call. The maximum number of codes is limited by the codes available on the gateway
time	Time in minutes	Argument must be included in the call.
type	Type of code: **n**=normal/single user **m**=multi-user	Argument must be included in the call.
download	Download limit(kbps)	Argument is optional and is not necessary for the call
upload	Upload limit (kbps)	Argument is optional and is not necessary for the call
downlimit	Download data limit (mbps)	Argument is optional and is not necessary for the call
uplimit	Upload data limit(mbps)	Argument is optional and is not necessary for the call

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

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Deleting Codes

Codes can be deleted from the system via a single HTTP call, the URL to use is:
http://aplogin.com/codes/deletecode.cgi

Parameters to pass include:

Parameter	Values	Comments
code	code to be deleted	Argument must included in the call.

An example call would be:
http://aplogin.com/codes/deletecode.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.

CODE	TIME	TYPE	USED	LEFT	DOWN	UP
113DRW	2	n	Yes	Expired	*	*
1AT1AQ	30	t	No	30	*	100
3B0AQ0	2	n	Yes	Expired	*	*
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

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

Get list of allowed MACs

http://aplogin.com/admin/macmanage.cgi?list=allowed

Get list of blocked MACs

http://aplogin.com/admin/macmanage.cgi?list=blocked

Block a MAC

The MAC address needs to be written in the colon separated format.
http://aplogin.com/admin/macmanage.cgi?mac=00:11:22:33:44:55&action=block

Allow a MAC

The MAC address needs to be written in the colon separated format.
http://aplogin.com/admin/macmanage.cgi?mac=00:11:22:33:44:55&action=allow

Enable Remote Management

Remote management can be enabled by substituting aplogin.com for the IP address of the gateway.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

PCI DSS

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.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

FAQs

Q. How do I get the latest firmware?

A. See the firmware request box on the support page. Provide the following information: product model, current firmware version, serial number and your email address. We will respond and send you the correct firmware for your product. Note that some email providers may not permit you to receive a binary file via email.

Q. How do I determine which gateway product is the best one for my application?

A. Each product has a maximum bandwidth capacity and can be selected for the Internet circuit. There is no limit to the numbers of users

Unit	Internet Circuit and Number of users
GIS-K1:	Up to 50 Mbps circuit
GIS-K3:	Up to 75 Mbps circuit
GIS-K5:	Up to 75 Mbps circuit
GIS-K7:	Up to 75 Mbps circuit
GIS-R2:	Up to 100 Mbps circuit
GIS-R4:	Up to 150 Mbps circuit
GIS-R6:	Up to 200 Mbps circuit
GIS-R10:	Up to 400 Mbps circuit
GIS-R20:	Up to 600 Mbps circuit
GIS-R40:	Up to 800 Mbps circuit

Q. Can I sell Internet access by charging Internet users using credit cards?

A. All units, apart from the GIS-R2, will permit a Hotspot operator to charge for Internet access. The Hotspot operator will have to obtain a PayPal® account to receive payments.

Q. I have a motel and I just received a letter from my DSL service provider telling me that my service will be cut off due to illegal file downloads. How can I stop my guests downloading illegal files?

A. All units, apart from the GIS-R2, have the ability to block the software that is used for illegal downloads of copyrighted material. The ISPs can detect when a peer-to-peer file sharing program, such as bittorrent is being used. Note that when file share blocking is activated then the maximum number of users is reduced.

Q. How do I prevent guests looking at X-rated web sites in the hotel lobby?

A. All our gateway products have content filtering, which can be activated during installation. The content filter requires an account with OpenDNS, the leading content filtering service.

Q. Can I access the gateway remotely after I have installed it?

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved

A. Yes you can. All our gateway products have a check box as part of the firewall configuration to permit remote access. The gateway will have to be configured with a fixed IP and the DSL or Cable router will have to be configured for port forwarding. If the DSL or Cable service has a fixed IP then remote access just requires the IP address and the port number allocated to the gateway. If the DLS or Cable IP address is dynamic then the gateway DynDNS service can be used. An account is required with DynDNS and their service permits the gateway IP to be obtained.

Q. How do I isolate users to prevent one from accessing the information of another?

A. User isolation is implemented by configuring each wireless access point for WVLAN operation. Commercial grade access points support WVLAN configuration, including those manufactured by Engenius and Ubiquiti. All our gateway products provide support features for advanced wireless access point operation, including port forwarding for remote configuration, and failure monitoring.

Copyright (c) Fire4 Systems Inc., 2005 to 2025. All Rights Reserved