

GUESTGATE™ HOTSPOT GATEWAY USER MANUAL

MODEL 523240



TABLE OF CONTENTS

section	page
1. Introduction	3
Function Description	3
Installation Examples	5
GuestGate™ Function Basics	5
2. Installation	7
Recommended Setup	7
Advanced Setup	10
3. Configuration Options	13
Status Screen	13
Guest Configuration Screen	14
Host Configuration Screen	16
Welcome Screen	17
Device Settings Screen	18
Firmware Upgrade Process	19
Exit Screen	19
4. Questions & Answers	20
5. Service & Support	22
6. Specifications	22
7. Appendix	23

FCC Regulatory Statements

Electromagnetic Compatibility (EMC)

This equipment generates radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a different circuit than the receiver.
- Consult your dealer or an experienced radio/TV technician for help.
- Check that shielded (STP) network cables are being used with this unit to ensure compliance with EMC standards.

This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

This digital equipment fulfills the requirements for radiated emission according to limit B of EN55022/1998, and the requirements for immunity according to EN55024/1998 residential, commercial and light industry.

Safety

This equipment complies with EN 60950, Safety of Information Technology equipment.

Radio Transmission Regulatory Information

This equipment generates and radiates radio frequency energy, and must be installed and operated while maintaining a minimum distance of 20 cm between the radiator and your body.

Tested to comply with FCC Standards FOR HOME OR OFFICE USE.

This product must be installed and used in strict accordance with the instructions given in the user documentation.

This product complies with the following radio frequency and safety standards:

Europe — EU Declaration of Conformity. This device complies with the requirements of the R&TTE Directive 1999/5/EC with essential test suites as per standards EN 301489: General EMC requirements for radio equipment; and ETS 300328: Technical requirements for radio equipment.

USA — Federal Communications Commission (FCC): This device complies with Part 15 of FCC Rules.

Operation of the device is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference that may cause undesired operation.

1. INTRODUCTION

Thank you for your purchase of the INTELLINET NETWORK SOLUTIONS™ GuestGate™ HotSpot Gateway, Model 523240. GuestGate connects guests to your network, allowing them to access only the Internet (Web, email, chat and other applications). GuestGate protects your existing network from unauthorized access by the connected guest computers and, if required, even provides shielding for the guest computers among themselves. Furthermore, GuestGate features enhanced IP PnP (Plug and Play) technology: It automatically adjusts to the guest computer's TCP/IP settings, eliminating time-consuming client IP reconfigurations.

GuestGate seamlessly integrates into your existing network and, in most applications, a configuration of GuestGate is not necessary: GuestGate provides the core functionality right out of the box!

FUNCTION DESCRIPTION

Internet Access for Guests

GuestGate is primarily designed to provide configuration-free Internet access for your guests. GuestGate uses the existing Internet connection of your network to provide Web and email access for computers connected in a conference room, a hotel or a public place with wireless network connectivity. GuestGate does not stop here, however. It addresses security-related concerns of the network administrator by shielding the existing network from access attempts from the connected guests. In short, this means that guests can access the Internet, but your own network — i.e., your network file server, email or application server — is off limits.

Password-Protected Internet Access for Guests

You, the network administrator, can make it mandatory for your guests to enter a password before Internet access is granted. This is an important function in case you offer Internet access as a paid service or in situations where an open, unprotected wireless access point is connected to GuestGate and you wish to keep unauthorized users from using your bandwidth.

Configurable Welcome Screen for Your Guests

You can set up your own welcome screen in seconds. Change the wording and formatting, and upload your own banner image. The welcome screen is displayed when a guest connects to the Internet for the first time. The welcome screen can be utilized to make the guest agree to your terms and conditions, and can be completely deactivated if required.

IP PnP

In many situations, it is necessary for the network administrator to change the TCP/IP settings of guest computers because the existing settings are not compatible or your network has advanced requirements. GuestGate eliminates this step completely. GuestGate automatically adjusts to the guest computer's TCP/IP settings, providing a true zero guest configuration.

Bandwidth Control

GuestGate controls how much of your Internet connection speed is dedicated to the guest network. Upload and download bandwidth can be configured individually.

True Layer 3 Virtual VLAN Function

In a public location with a public wireless access point, there are often concerns about security. GuestGate not only protects the host network from unauthorized access by your guests, it takes security one step further. When the "separate network for each client" option is activated, no guest computer can access any other guest computer. In this mode, GuestGate randomly assigns each guest computer its own network. This option is activated by default.

Packet Filter

Block access to certain Web sites or entire IP ranges.

4-Port 10/100 Auto-Sensing LAN Switch

GuestGate provides four 10/100 Mbps LAN switch ports for the connection of PCs, notebooks, or other switches or wireless access points.

Web-Based Administrator Interface

The configuration is fully Web-browser based. For security reasons, the Web administrator menu is only accessible from the host network.

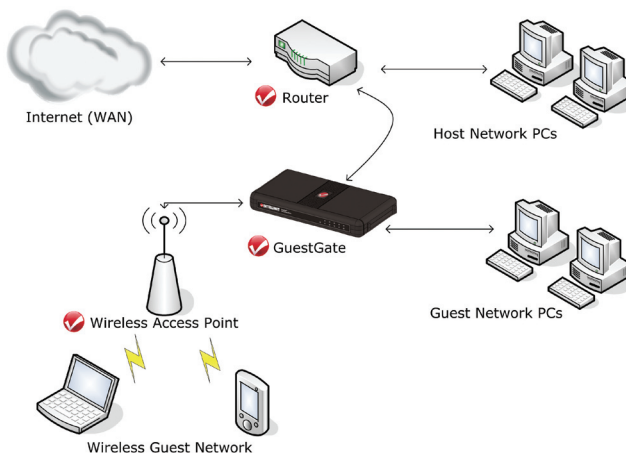
Firmware Updates via Web Browser

Quickly and conveniently upgrade firmware of your GuestGate HotSpot Gateway from INTELLINET NETWORK SOLUTIONS with the Web browser of your choice.

INSTALLATION EXAMPLES

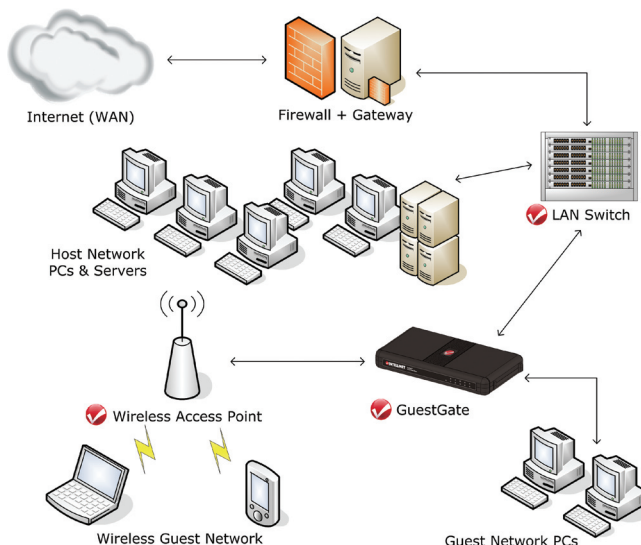
GuestGate in a SOHO Network Environment

This is a typical setup in which the Internet connection is established through an NAT router with an integrated firewall.



GuestGate in an SMB Environment

In larger networks, GuestGate connects to any available switch port behind the firewall/gateway/router.



GUESTGATE FUNCTION BASICS

Ports

GuestGate features a total of five 10/100 RJ-45 ports. One port is for the connection of GuestGate to the host network (host port), four ports are

available for guest connections (guest ports). The guest ports can be connected to hubs, switches, wireless access points, PCs or notebooks.

Host Ports

By default, GuestGate obtains an IP address from a DHCP server already present in the network. GuestGate analyzes the network and obtains all information necessary for Internet access. The DHCP server log reveals the host IP address of GuestGate.

In the event that no DHCP server is present, GuestGate reverts to its default IP address: 192.168.2.1. In this case, a manual configuration of the host IP settings is necessary.

Guest Ports

GuestGate assigns IP addresses to the connected guest computers. IP PnP technology ensures that no configuration on the guest computer is necessary. The default DHCP IP address range is 172.16.xxx. Changing the guest IP settings is possible via the Web administration interface.

Guest Ports with Virtual VLAN Enabled

If Virtual VLAN is enabled, GuestGate assigns a different IP network (subnet) to each connected guest computer. Since this assignment is random, it makes it virtually impossible for a hacker to guess the other guest computer's IP settings to try to gain access. Virtual VLAN is enabled by default. It can be disabled in the guest configuration screen of the administrator Web interface. The option is "separate network for each client (automatic)."

Accessing the Administrator Web Interface

The configuration of GuestGate is entirely Web based. Any standard Web browser is supported. For security reasons, GuestGate can only be configured from the host port. GuestGate rejects all connection attempts which originated from the guest side.

Internet Access for Guests and Welcome Page

When a guest computer tries to access the Internet for the first time, a welcome page is shown in the Web browser. This welcome page can be configured and altered in the administrator Web interface. Guests have to accept the terms and conditions in order to access the Internet. If the guest password option is enabled, a password must be provided by the guest to gain Internet access. This authorization procedure is only required once. GuestGate memorizes all authorized guest computers until GuestGate is restarted. After a restart of GuestGate, guests again will be shown the welcome page.

2. INSTALLATION

RECOMMENDED SETUP

This setup method for the INTELLINET NETWORK SOLUTIONS GuestGate HotSpot Gateway assumes that a DHCP server such as a router is present in your network.

Connecting to the Host Network

Connect a standard RJ-45 network cable to GuestGate's host port and to an RJ-45 port on your existing network (Ethernet switch port, router switch port, etc.).

Turn on GuestGate and verify that the network connection is active (host LED must be lit on GuestGate). **NOTE:** The startup process takes up to 30 seconds.

Connecting Guests

Using standard RJ-45 network cables, you can now connect PCs, notebooks, Ethernet switches, hubs or wireless access points to GuestGate's guest ports. Each port has its own status LED. Verify that the network connection is active on each port you connect.

Testing Internet Access

Start up a PC or notebook that is connected to one of the guest ports. Launch a Web browser and open an Internet Web site, such as <http://www.intellinet-network.com>. You will then see GuestGate's welcome page.

Provide the password if required and click on "continue." You will then be forwarded to the Web page you originally entered in the Web browser's address bar.

INTELLINET
NETWORK SOLUTIONS

BRINGING NETWORKS
TO LIFE

Welcome to our Network!
Dear Guest,

We're happy to provide you with Internet Access using the INTELLINET NETWORK SOLUTIONS GuestGate™ Internet Access Device. You agree to comply with the company's terms of use. In particular access to any illegal content is strictly prohibited. Violation of this can result in legal prosecution.

By continuing you agree to those terms.

Enter your password to continue:

Copyright © INTELLINET NETWORK SOLUTIONS 2006 - www.guestgate.com

NOTE: In order to get Internet access, you must first open a Web browser and open a Web page. Other applications, such as chat programs (ICQ, MSN Messenger, Skype, etc.), will not be able to connect to the Internet unless the welcome page has been confirmed in the Web browser.

Accessing the Administrator Web Interface from the Host Interface

1. Open the log of your DHCP server to find the IP address of GuestGate. GuestGate's MAC (media access control) address can be found on the bottom of the device. Find this MAC address in your DHCP server's client log to determine the IP address.

Below is an example of a DHCP log file:

IP Address	MAC Address	Time Expired(s)
192.168.0.100	00:50:fc:be:48:58	169576
192.168.0.101	00:0f:a3:1d:a3:da	114749

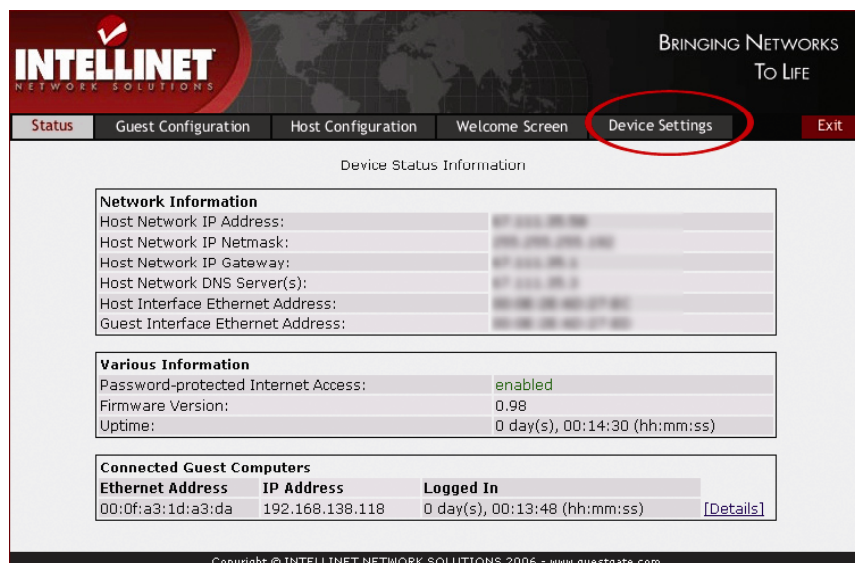
2. Launch your Web browser and open the IP address shown in the DHCP client log. You will then see the administrator Web interface. The default password is 1234.



The image shows the login page of the Intellinet Network Solutions administrator interface. It features the Intellinet logo on the left and the tagline "BRINGING NETWORKS TO LIFE" on the right. In the center, there is a text input field labeled "Enter your password to login:" and a "login" button. At the bottom, a copyright notice reads "Copyright © INTELLINET NETWORK SOLUTIONS 2006 - www.questgate.com".

Changing the Administrator Password

1. Click on "Device Settings."



The image shows the "Device Settings" page of the Intellinet Network Solutions administrator interface. The "Device Settings" tab is highlighted with a red circle in the navigation bar. The page displays "Device Status Information" with three sections: "Network Information", "Various Information", and "Connected Guest Computers".

Network Information		
Host Network IP Address:	192.168.138.118	
Host Network IP Netmask:	255.255.255.255	
Host Network IP Gateway:	192.168.138.1	
Host Network DNS Server(s):	192.168.138.1	
Host Interface Ethernet Address:	00:0f:a3:1d:a3:da	
Guest Interface Ethernet Address:	00:0f:a3:1d:a3:da	

Various Information	
Password-protected Internet Access:	enabled
Firmware Version:	0.98
Uptime:	0 day(s), 00:14:30 (hh:mm:ss)

Connected Guest Computers		
Ethernet Address	IP Address	Logged In
00:0f:a3:1d:a3:da	192.168.138.118	0 day(s), 00:13:48 (hh:mm:ss)

[Details]

Copyright © INTELLINET NETWORK SOLUTIONS 2006 - www.questgate.com

2. Enter the old password (1234).
3. Enter a new password (up to 20 characters long).
4. Retype the new password.
5. Click on "Exit" (upper right corner).

6. Check "Save settings."
7. Check "Reboot device."
8. Click on "Exit."

GuestGate now reboots. This takes about 25 seconds. After the reboot, you'll be redirected to GuestGate's login page. You can now login with the new password.

NOTE: The administrator Web Interface is designed to let you make changes on all four screens without saving each change individually. Once you are done programming GuestGate, you need to click on "Exit" and reboot the device. The changes will only take effect after GuestGate has been rebooted. Closing the Web browser without saving the configuration changes will result in a loss of the changed configuration.

If you've successfully performed the above steps, you can skip the next section.

ADVANCED SETUP

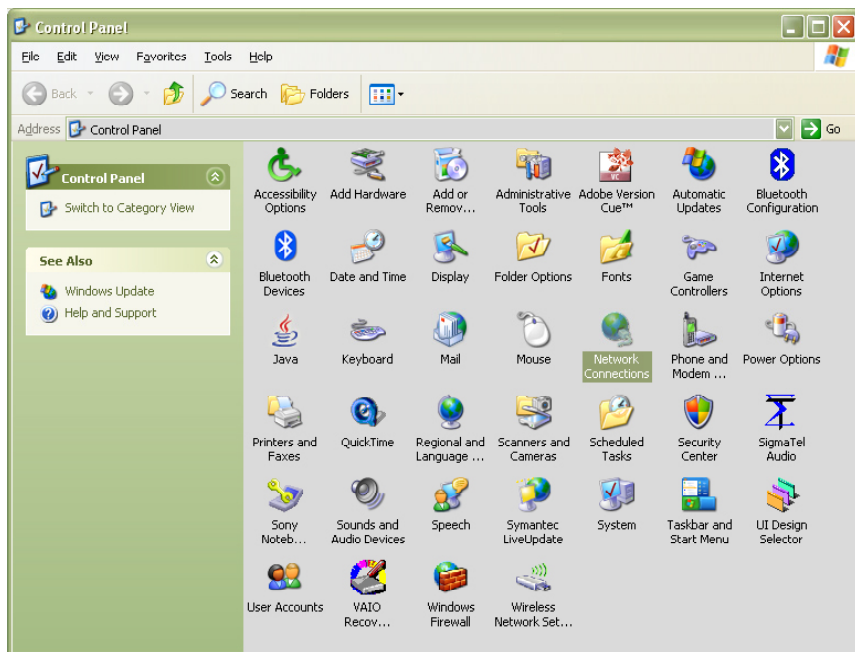
The standard installation of GuestGate is based on the assumption that a DHCP server is present in your network. If this is not the case, you can still configure GuestGate manually. To do this, you need to turn GuestGate on while it is disconnected from the network. If no DHCP server can be found after three minutes, GuestGate will fall back to its default IP address: 192.168.2.1.

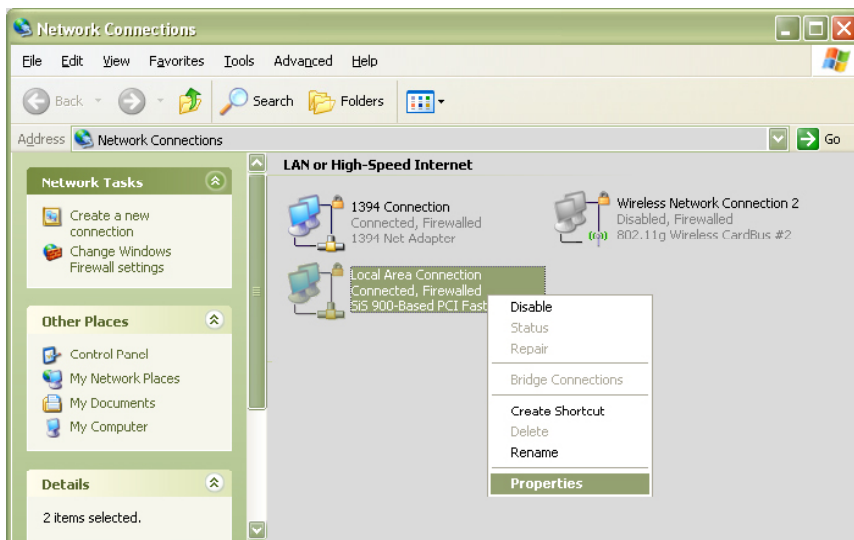
Advanced setup requires:

- A network adapter correctly installed in your computer;
- User rights that allow manual configuration of TCP/IP-related settings on your PC; and
- GuestGate connected with an RJ-45 cable to the network adapter in your PC.

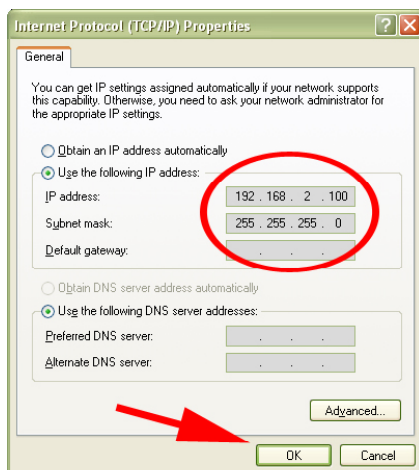
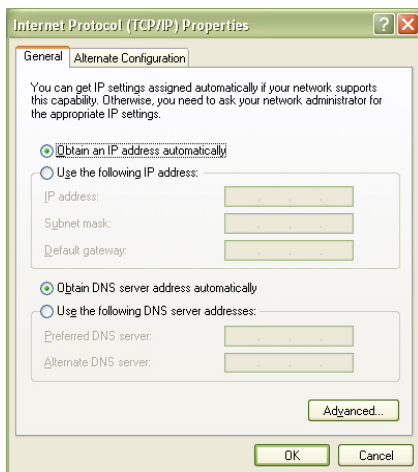
Changing the IP Address of Your PC

1. Click on "Start" → "Settings" → "Control Panel."
2. Double-click the "Network Connections" icon.



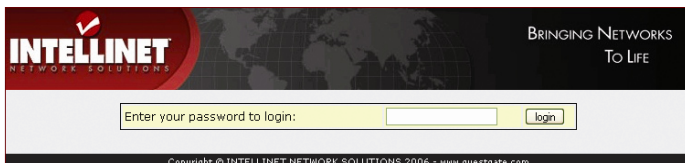


3. Right-click the "Local Area Connection" icon and select "Properties" from the context menu.
 4. In the "Local Area Connection Properties" window, highlight "Internet Protocol (TCP/IP)" and click on "Properties." When the "Internet Protocol (TCP/IP) Properties" window opens, make the changes as shown.
 5. Click "OK" when done.
 6. Close the previous windows by clicking "OK," as well.
- Your TCP/IP settings are now compatible to GuestGate.



Connecting to GuestGate via a Web Browser

1. Start your Web browser and open the address <http://192.168.2.1>. The administrator Web interface login screen then appears.
2. Enter the password (1234) and click on "login."

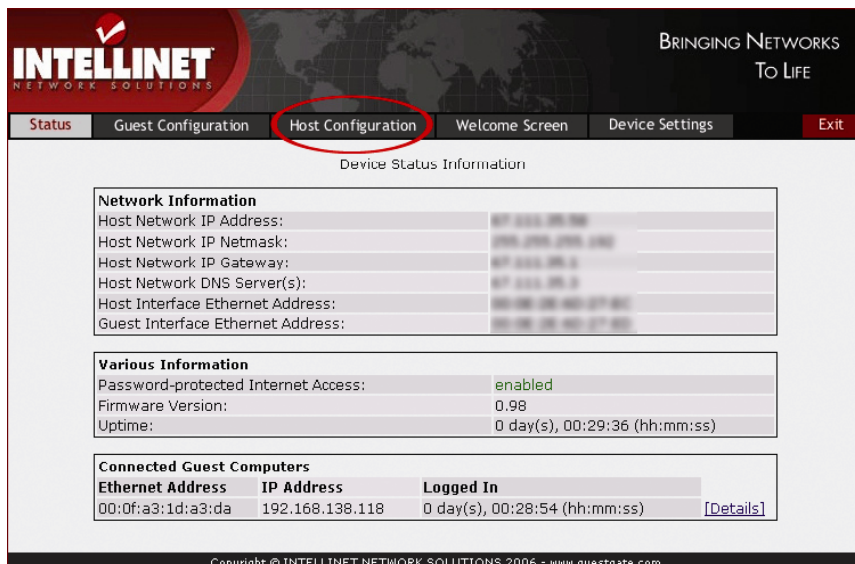


The login screen features the Intellinet logo and the tagline 'BRINGING NETWORKS TO LIFE'. It includes a text input field for the password and a 'login' button. The footer contains the copyright notice: 'Copyright © INTELLINET NETWORK SOLUTIONS 2006 - www.guestgate.com'.

NOTE: At this point, it is recommended that you change the administrator password as described in the previous section.

Host Configuration

1. Click on "Host Configuration."

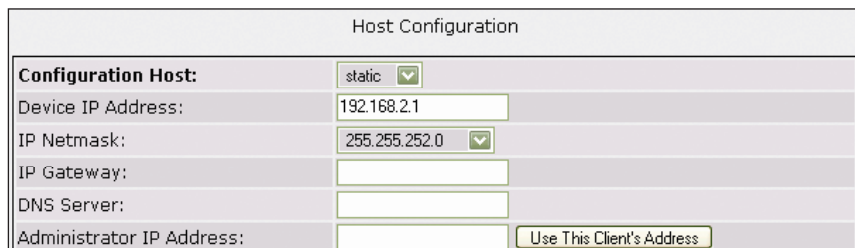


The Host Configuration page shows the 'Host Configuration' tab selected in the navigation bar. It displays device status information, including network and various settings.

Network Information		
Host Network IP Address:	192.168.138.118	
Host Network IP Netmask:	255.255.252.0	
Host Network IP Gateway:	192.168.138.2	
Host Network DNS Server(s):	192.168.138.2	
Host Interface Ethernet Address:	00:0f:a3:1d:a3:da	
Guest Interface Ethernet Address:	00:0f:a3:1d:a3:da	

Various Information	
Password-protected Internet Access:	enabled
Firmware Version:	0.98
Uptime:	0 day(s), 00:29:36 (hh:mm:ss)

Connected Guest Computers		
Ethernet Address	IP Address	Logged In
00:0f:a3:1d:a3:da	192.168.138.118	0 day(s), 00:28:54 (hh:mm:ss) [Details]



The Configuration Host window allows setting network parameters for the device.

Configuration Host:	static
Device IP Address:	192.168.2.1
IP Netmask:	255.255.252.0
IP Gateway:	
DNS Server:	
Administrator IP Address:	<input type="text"/> <input type="button" value="Use This Client's Address"/>

2. With the Configuration Host window displayed, specify the device IP address, IP netmask, IP gateway (Internet connection gateway, router) and DNS server.

Device IP Address: A free IP address in your network. This is the IP address you assign to GuestGate.

IP Netmask: Enter the same netmask (or subnet mask) you use in your network.

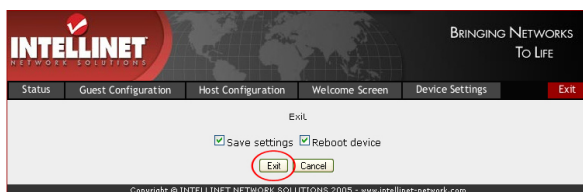
IP Gateway: The IP address of your Internet gateway (such as a router).

DNS Server: Domain name service as required by your ISP. You can add multiple DNS servers by separating the different entries with a space.

Administrator IP Address: When specified, only this IP address is allowed to connect to the administrator interface of GuestGate. The function "Use this client's IP address" automatically populates the field with the IP address of the computer currently used to connect to the administrator menu.

When done, click on "Exit" (upper right corner).

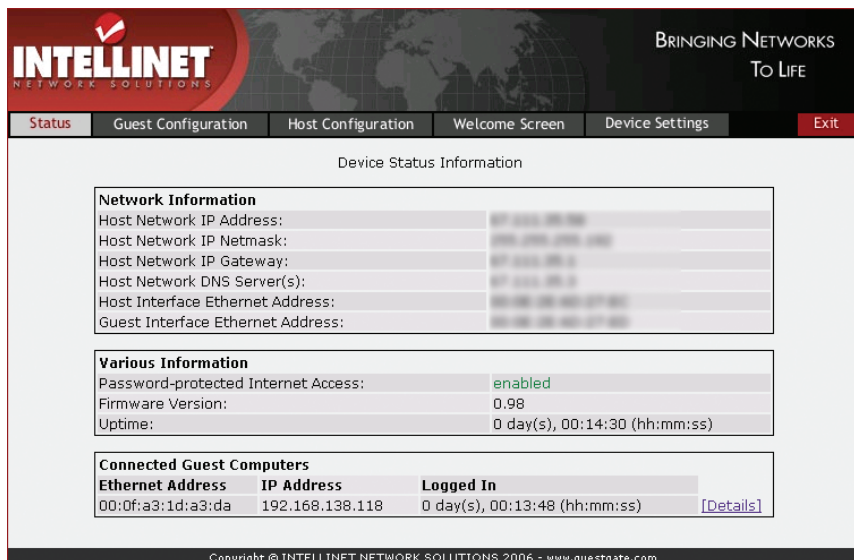
3. Click on "Exit" to save the configuration and restart GuestGate.



3. CONFIGURATION OPTIONS

STATUS SCREEN

The status screen shows three types of information.



Network Information: Basic information about the host network interface.

Various Information: Display of the current firmware version, the system's uptime and the status of the password-protected Internet access.

Connected Guest Computers: GuestGate shows all of the connected guest computers, including the MAC address, the assigned IP address and the connection time. Click on "[Details]" to view individual statistics for each connected PC, including the bandwidth consumed (Mbytes).

GUEST CONFIGURATION SCREEN

This page shows the configuration options for the connected guest computers.

INTELLINET
NETWORK SOLUTIONS

BRINGING NETWORKS
TO LIFE

Status **Guest Configuration** Host Configuration Welcome Screen Device Settings Exit

Guest Configuration

Configuration Guest: ☒ separate network for each client (automatic) ☒

Device IP Address: 172.16.254.254

IP Netmask: 255.255.255.0

Dynamic Range: 172.16.254.1 through 172.16.254.253

Security

Welcome Screen: ☒ enabled ☒

Guest Password: (leave empty for no password)

Bandwidth Download Limit: 1024 kbit/s ☒

Bandwidth Upload Limit: 1024 kbit/s ☒

Trusted Ethernet Addresses: ☒ Remove

Add Ethernet Address:

Copyright © INTELLINET NETWORK SOLUTIONS 2006 - www.guestgate.com

Configuration Guest

Option "separate network for each client (automatic)": This operational mode is called "Virtual VLAN." If this option is activated, GuestGate randomly assigns different networks to each connected guest computer. This option should be activated if you want to prevent guest computers from seeing and accessing each other (Virtual VLAN = on). It is activated by default.

Option "same network for all clients (automatic)": GuestGate automatically assigns IP addresses to the guest computers. All guest computers operate in the same network (Virtual VLAN = off).

Option "same network for all clients (enter manually)": If this option is enabled, you can manually define the network for the connected guest computers (Virtual VLAN = off).

Welcome Screen

Enable or disable the welcome page for guests. (Default = enabled.)

Guest Password

If you require your guests to enter a password to access the Internet, you can define it here. If left empty, no password is required (Default = no password).

Bandwidth Download Limit

Control the maximum download speed available for the connected guest computers here. Available options are from 32 kbps (kilobits per second) up to 2048 kbps (= 2 Megabits per second; Default = unlimited).

Bandwidth Upload Limit

Bandwidth control for the upload speed (sending files to the Internet) is here, with options the same as above.

Trusted Ethernet Addresses

If you wish to permanently authenticate a guest computer, you can add its MAC address to GuestGate's configuration. GuestGate will not show the welcome page to any computer that has been entered here.

You can obtain the MAC address of a connected computer from the GuestGate status screen, or you can perform the following steps (example: Windows 2000/XP).

1. Click on "Start" → "Run."
2. Type in "cmd"; press "Enter."
3. At the DOS command prompt, type "ipconfig /all" and press "Enter."

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : 802.11g Wireless CardBus
Physical Address. . . . . : 00-0F-A3-1D-A3-DA
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.10.10.89
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 10.10.8.1
DHCP Server . . . . . : 10.10.8.10
DNS Servers . . . . . : 10.10.8.10
                        10.10.8.21
```

Example Output

The physical address is the MAC address that needs to be entered in the configuration of GuestGate.

The format is: xx:xx:xx:xx:xx:xx (not xx-xx-xx-xx-xx-xx).

HOST CONFIGURATION SCREEN

This page shows the configuration options for the host interface of GuestGate.

INTELLINET
NETWORK SOLUTIONS

BRINGING NETWORKS
TO LIFE

Status Guest Configuration **Host Configuration** Welcome Screen Device Settings Exit

Host Configuration

Configuration Host: DHCP ☒

Device IP Address: 67.111.35.58

IP Netmask: 255.255.255.192

IP Gateway: 67.111.35.1

DNS Server: 67.111.35.3

Administrator IP Address:

Packetfilter

Blocked Addresses: ☒ Remove

Add Host Address:

Add Network Address: / 255.255.255.0 ☒

Blocked Ports: ☒ Remove

Add Port Number:

Permit Addresses: 67.111.35.0/26 ☒ Remove

Add Host Address:

Add Network Address: / 255.255.255.0 ☒

Copyright © INTELLINET NETWORK SOLUTIONS 2006 - www.guestgate.com

Configuration Host

Option "DHCP": GuestGate automatically receives the IP address, netmask, gateway and DNS server information from the DHCP server in your network, typically a router. This is the default and recommended setting.

Option "static": In larger networks, a manual configuration of the IP settings may be necessary. Select "static" and enter the IP address, netmask, gateway IP address and DNS server IP addresses manually.

Multiple DNS servers can be entered by separating them with a space; e.g., 111.222.333.444 999.888.777.666.

Administrator IP Address: Restrict access to GuestGate's administration menu to the IP address you enter in this field. This can be any local or public IP address.

Packet Filter

Blocked Ports: If you wish to block certain IP addresses, domain names or an entire network, you can enter this here.

"Add Host Address" is used to enter domain names such as guestgate.com or intellinet-network.com.

"Add Network Address" is used to enter an IP address. To specify the range, you can select the appropriate network mask from the drop-down list.

Blocked Addresses: This option lets you specify which outgoing TCP/IP ports you wish to block. Enter the port number and click on "Add Port." GuestGate blocks both TCP and UDP protocols.

A list of common service ports can be found in the appendix at the back of this manual. If you wish to remove a port, simply select the desired port from the drop-down list and click on "Remove."

NOTE: You can only add and remove single ports. Port ranges are not supported.

Permitted Addresses: By default, GuestGate blocks access to all PCs in the host network. This function lets you define exceptions.

Add Host Address: Enter a single IP address — e.g., the IP address of your Intranet Web server — and click on "Add Host." Repeat this step if you wish to enter more IP addresses.

Add Network Address: Enter an IP address and a subnet mask to define a range of IP addresses permitted to your guests.

WELCOME SCREEN

This page shows the welcome screen configuration options of GuestGate.

INTELLINET
NETWORK SOLUTIONS

BRINGING NETWORKS
TO LIFE

Status Guest Configuration Host Configuration **Welcome Screen** Device Settings Exit

Welcome Screen Configuration

Banner Graphic

Banner: Default Image

Upload your own Banner Image: Browse... Upload

Welcome Text

Welcome to our Network!

Dear Guest,

We're happy to provide you with Internet Access using the
INTELLINET NETWORK SOLUTIONS GuestGate™ Internet Access Device.
You agree to comply with the company's terms of use. In particular
access to any illegal content is strictly prohibited. Violation of
this can result in legal prosecution.

By continuing you agree to those terms.

Copyright © INTELLINET NETWORK SOLUTIONS 2006 - www.guestgate.com

Banner Graphic

You can replace the default banner image with your own image, such as the

logo of your company. Click on "Browser" to select the file you wish to upload. Click on "Upload" to replace the default banner image. After the upload, the text "Default Image" changes into "Custom Image."

NOTE: The banner image file type must be in the form of a JPG, GIF or PNG; the image size must not exceed 60 kb; the image dimensions, though not limited, should not exceed 1024 pixels. The banner image only displays on the guest welcome screen. It does not replace the banner in the administrator Web interface.

Welcome Text

You can overwrite the default text with your own custom text. GuestGate supports HTML tags to format your text. Below is a small selection.

- `bold text`
- `red text`
- `green text`
- `<u>underlined text</u>`
- `<u>red bold underlined text</u>`

Other HTML commands, such as `<TABLE>`, `<tr>`, `<td>` and `` tags and many more, are also supported.

DEVICE SETTINGS SCREEN

This page shows the device settings of GuestGate.

INTELLINET
NETWORK SOLUTIONS

BRINGING NETWORKS
TO LIFE

Status Guest Configuration Host Configuration Welcome Screen **Device Settings** Exit

Device Status Information

Admin Password

Old password:

New password:

Retype new password:

Firmware

Upgrade Firmware:

Copyright © INTELLINET NETWORK SOLUTIONS 2006 - www.questgate.com

Admin Password

To change the administrator password, you need to enter the old password and the new password. You also must confirm the new password by retyping it.

Click on “Change” to save the changes. GuestGate’s default password is 1234. The password can be up to 20 characters in length.

Firmware

To benefit from new functions in the future, you may wish to upgrade the firmware. More information on how to obtain and upgrade firmware appears in the next section.

FIRMWARE UPGRADE PROCESS

Where to Obtain New Firmware

There are two ways to find out if new firmware is available for the INTELLINET NETWORK SOLUTIONS GuestGate HotSpot Gateway.

- Check GuestGate’s status page. GuestGate checks if new firmware is available whenever you login to the administrator menu. If a new version is found, a test message appears on the status screen. Click on the link “Click here for more information” to open the Web page with details, instructions and the new firmware image.
- Check the download section manually at <http://www.guestgate.com>.



Upgrade Process

Open the device settings screen of the administrator menu.

Click on “Browse” to select the new firmware image, then click on “Install” to begin the upgrade process. The upgrade may take several minutes depending on your connection speed to GuestGate.

GuestGate will automatically restart after the upgrade process. After you see the restart message, you need to wait one minute before you can access GuestGate again.

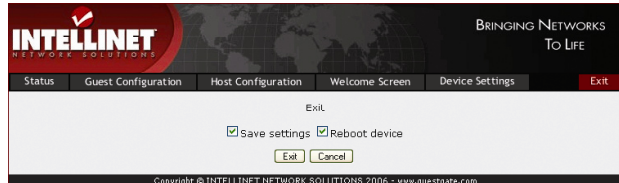
IMPORTANT: The upgrade process must not be interrupted! A network connection failure or a crash of your local computer during the upgrade process will result in the destruction of GuestGate. Ideally, you want to perform the upgrade from within the local host network whenever possible.

EXIT SCREEN

This page lets you save the new configuration.

Save Settings

All changes you made to the configuration will only be memorized if you save the changes by activating this check box. If you made changes in some of the configuration screens and fail to perform this step before closing the Web browser, all changes will be lost.



Reboot Device

In order to activate the new configuration, you must also check this box.

NOTE: Saving the settings does not automatically activate them. It is necessary to reboot GuestGate for the new configuration to become active. This way, you can make changes to the configuration (e.g., a new guest password) now and then activate them at a later time. Rebooting GuestGate will also enforce a re-authentication of all connected guest computers.

4. QUESTIONS & ANSWERS

- Q: I have a server in my network that my guests are not allowed to access. Which settings do I need to activate in GuestGate to prevent my guests from accessing this server?
- A: You do not need to activate any settings. GuestGate provides this functionality by default. Should a guest try to access a server or computer in your network, GuestGate will deny the request and display a warning message in the guest's Web browser window.
- Q: What if I want to allow my guests access to my network (e.g., my Intranet Web server)?
- A: Add the IP address of your Intranet server in GuestGate's host configuration page under "Permit Addresses" and GuestGate will no longer block access to that server.
- Q: Can I control the amount of bandwidth available for my guest network?
- A: Yes. Upload and download bandwidth can be controlled in the guest configuration section of the Administrator Web Interface.
- Q: I wish to display my own welcome page for my guests. Can I change the default welcome page?
- A: Yes. The welcome page can be changed in the welcome page configuration section of the administrator Web interface. You can change the welcome message and upload your own banner image.

Q: Can I use HTML code in my custom welcome page?

A: Yes. GuestGate does not limit you in any way. If you are an HTML Web developer, you can create an enhanced welcome page simply by pasting the HTML code into the welcome page configuration field.

Q: Does GuestGate support PHP, ASP or Perl?

A: No. GuestGate does not support server-side scripting.

Q: I have changed some settings in the administrator Web interface, but the changes show no effect. Why?

A: You may have forgotten to save the configuration through the exit page of the administrator Web interface.

Q: What is the option "separate network for each client (automatic)" in the guest configuration screen used for?

A: This is the Virtual VLAN function of GuestGate. If this option is activated, GuestGate will prevent the connected guest computers from accessing each other by assigning random TCP/IP network settings to the guest computers. This way, each guest operates in its own "Virtual LAN." The two examples below illustrate how it works.

1. Guest configuration set to "same network for all clients (automatic)":

Guest computer 1 receives IP address 172.16.254.253.

Guest computer 2 receives IP address 172.16.254.252.

Guest computer 3 receives IP address 172.16.254.251.

[...]

In this mode, all guest computers operate in one network and are therefore able to access each other. This is the standard mode of virtually any router and DHCP server on the market.

2. Guest configuration set to "separate network for each client (automatic)" (Virtual VLAN enabled):

Guest computer 1 receives IP address 192.168.17.42.

Guest computer 2 receives IP address 172.16.25.12.

Guest computer 3 receives IP address 10.10.8.178.

Guest computer 4 receives IP address 10.10.4.18.

Guest computer 5 receives IP address 192.168.8.178.

[...]

In this mode, each guest computer operates in its own network and therefore can not access any other device except for the Internet. Since this function is random, it is next to impossible for an attacker to know or guess which IP addresses the other guests have been assigned, making a hacking attempt more difficult.

If you are concerned with the security of your guests or are worried about potential liability issues, you should activate this option (it is activated by default).

- Q: Some of my guests wish to play a network game or share files and folders, but that doesn't work. Why can't the connected guest computers communicate with each other?
- A: Because, by default, Virtual VLAN is activated. You need to disable it to allow network communication between the connected guest computers. (See the previous Q&A.)
- Q: How often does a guest need to authenticate at the welcome page?
- A: Only once. As long as GuestGate is not restarted, the guest will never again be prompted to enter the password and agree to your terms and conditions.
- Q: Can I access the administrator menu of GuestGate from one of the guest ports?
- A: No. For security reasons this is not possible. Access to the administrator menu can only be gained through the host port.

5. SERVICE & SUPPORT

Additional information about GuestGate is available on the web at

<http://www.guestgate.com/>.

On this page you can:

1. Find answers to common questions (FAQ);
2. Obtain the latest firmware versions; and
3. Get in contact with our technical support team.

In case of technical problems, we always recommend checking with your local authorized INTELLINET NETWORK SOLUTIONS dealer first. Contact with our technical support team can be made on the Web site, as well.

6. SPECIFICATIONS

- Guest network: 1 x 10/100 Mbps RJ-45 port
- Host network: 4 x 10/100 Mbps RJ-45 ports
- Reset button
- LEDs: 1 x Power; 1 x Link/Activity for host network; 4 x Link/Activity for guest ports
- AC adapter 12 V / 0.5 A
- Dimensions: H: 45 mm; W: 220 mm; D: 120 mm
- Humidity: 0 – 90% (non-condensing)
- Temperature: 10 – 55°C
- EMI certification: FCC Class B, CE Mark, C-T

7. APPENDIX

Below is a sample list of common TCP/IP service ports that can be entered in the host configuration of GuestGate to block access to certain services.

Port Number	Service Name / Description
21	FTP
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Outgoing Mail, Sendmail Server Port)
69	TFTP (Trivial File Transfer Protocol)
70	Gopher
79	Finger
80	HTTP (Standard Web Port for Web Sites)
110	POP3 (Incoming Mail)
115	SFTP (Simple File Transfer Protocol)
119	NNTP (Newsgroups)
123	NTP (Network Time Protocol)
135	RPC service, used for NET SEND command
137, 138, 139	NETBIOS (Filesharing, MS Windows Network)
143	IMAP (Interim Mail Access Protocol)
161	SNMP (Simple Network Management Protocol)
194, 6665-6669	IRC (Internet Relay Chat)
443	HTTPS (Secure Web Transfer, used by SSL)
514	SHELL
515	LPR (Line Printer Remote), LPD (Line Printer Daemon)
631	IPP (Internet Printing Protocol)
1080, 3127, 3128, 10080	Trojan: Used by MyDoom
1723	PPTP (used for VPN Connections)
1863	MSN Messenger
2535, 2745, 8866	Trojan: Used by Beagle
3389	Windows XP Remote Desktop Port
3410	Trojan: OptixPro, also used by NetworkLens SSL Event
3689	iTUNES by Apple, DAAP
4899	RADMIN, Remote Control
5000, 5001	YAHOO Messenger Voice Chat
5100	YAHOO Messenger Video (Webcam)
5190, 5191, 5192, 5193	AOL (America On Line via TCP)
5554	Trojan: Sasser Family, also used for SGI ESP HTTP.
5800+, 5900+	VNC
12345	Trojan: Used by Netbus, Italk Chat System and Trend/Micro OfficeScan antivirus
27374	Trojan: Used by SubSeven



INTELLINETTM

N E T W O R K S O L U T I O N S

BRINGING NETWORKS TO LIFE

INTELLINET NETWORK SOLUTIONSTM offers a complete line of active and passive networking products.

Ask your local computer dealer for more information or visit

www.intellinet-network.com

Copyright © INTELLINET NETWORK SOLUTIONS

All products mentioned are trademarks or registered trademarks of their respective owners.