

GuestGate MK II – Firmware 2.15



INTELLINET[™]
NETWORK SOLUTIONS



GUESTGATE[™] **MK II**

GuestGate MK II – Firmware 2.15

CONTENTS

1. Installation	3
2. Change log	4
3. New functions explained	6
3.1 Welcome page preview	6
3.2 Session & traffic log updates	7
3.3 DYNDNS.ORG, DNS-O-MATIC and OpenDNS	8
3.4 Adjustable HTTP port number	9
3.5 Banning users permanently	9
4. Important tech support notes	10
4.1 The iPad vs. GuestGate issue	10
4.2 GuestGate hardware reset does not work?	10
4.3 How to repeat the GuestGate wireless signal	10

GuestGate MK II – Firmware 2.15

1. INSTALLATION

Note: None of GuestGate’s settings will be overwritten by the new firmware.

- a. Uncompress the “guestgate_524827_fw215.zip” file.
- b. Verify that the file “524827-2.15.img” is 3.33 MB in size (3,502,828 bytes).
- c. Logon to GuestGate’s admin web interface

d. Click on  [Device Settings](#)

- e. Click on “Browse” and select the firmware file (see step b.)
- f. Click on “Install” to begin the upgrade

Firmware	
Upgrade Firmware:	<input type="text"/> <input type="button" value="Browse.."/>
<input type="button" value="Install"/>	

g. You’ll see the following message.

Firmware is being upgraded
The firmware is being upgraded at the moment. After the upgrade is complete, the device will restart automatically.
Please be patient and do not restart the device before the upgrade is complete as this will destroy the device permanently!

h. Allow the process to complete. This takes several minutes.

GuestGate MK II – Firmware 2.15

2. CHANGE LOG

Changes 2.15:

- Additional bandwidth control values of 5 and 10 Mbps (previously the maximum was 2 Mbps)
- Ability to ban clients based on their MAC address
- HTTP clear link error message fixed when used in web browser
- Removed duplicate MAC address entries from status page

Changes 2.10:

- Fixed bug in function “Access Control: Individual Passwords” which prevented the use of the function “Maximum numbers of users” (only one user was able to use the password at a time)

Changes 2.09:

- Access Control: Individual passwords can now be deleted properly
- Individual user password valid from and valid until fields can now be left blank. E.g., if valid until is not filled out, the password will never expire.

Changes 2.08:

- HTTP Web Server Port can be changed from 80 to a different port
- Support for DNS-O-Matic
- Support for OpenDNS via DNS-O-Matic
- Lease time for IP addresses changed from 10 minutes to 2 hours
- Session log contains client’s MAC address, username / password used and user agent information

GuestGate MK II – Firmware 2.15

Changes 2.05:

- HTTP Web Server Port can be changed from 80 to a different port
- Support for DYNDNS.ORG
- Added HTTP link to download and delete traffic and session log
- Duplicate MAC addresses on status page should no longer occur

Changes 2.04:

- Resolved bug in walled garden function that prevented inputting a network range
- NTP update process more robust, GuestGate should not lose time after a reboot, unless the NTP server is truly offline
- Resolved bug in DHCP server causing problems with certain Windows 7 systems (the double-login caused problems with user-defined passwords)
- Resolved problem with MAC addresses of connected clients sometimes showing up multiple times on the status page
- Added preview function for advanced welcome page editing

GuestGate MK II – Firmware 2.15

3. NEW FUNCTIONS EXPLAINED

3.1 WELCOME PAGE PREVIEW

While you are designing the welcome page, you can now check the progress with the preview function. You no longer need to reboot GuestGate and log in as a guest to see the modified welcome page. This makes the design process much easier and quicker.

Welcome HTML Code

```
<html>
<head>
  <title>INTELLINET NETWORK SOLUTIONS - GUESTGATE™ MK II -
  Welcome</title>
  <link rel="SHORTCUT ICON" href="/img/favicon.ico">
  <link href="/img/styles.css" rel="stylesheet"
  type="text/css">
  <meta http-equiv="Content-Type" content="text/html;
  charset=UTF-8">
  <script language="javascript" type="text/javascript">
    function enter_submit_form(f) {
      if (window.event && window.event.keyCode == 13)
        f.submit();
      else
        return true;
    }
  </script>
</head>
<body>
  <form method="GET" name="welcomeform">
```

INTELLINET
NETWORK SOLUTIONS

GUESTGATE™ MKII

Dear Guest,

We're pleased to provide you with Internet Access using the Intellinet GUESTGATE™ MK II Hotspot Gateway.

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.

Please note that your Internet activities may be monitored.

By continuing you agree to those terms.

Password:

Copyright © INTELLINET NETWORK SOLUTIONS 2006-2011 - www.intellinet-network.com

April 25th, 2013

www.intellinet-network.com

GuestGate MK II – Firmware 2.15

3.2 SESSION & TRAFFIC LOG UPDATES

a. Session Log Updates

Additional information is stored in the session log.

- username / password

- User agent (e.g., Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101 Firefox/6.0.2)

The session log also contains the login and logout time, as well as the MAC address of the client. The MAC address provides the link to the traffic log.

b. Download and deletion of session and traffic log via HTTP command

Log	
Enabled:	enabled ▾
HTTP Download:	enabled <input type="button" value="Regenerate key"/> <input type="button" value="Deactivate"/>
Session Log:	<input type="button" value="Download"/> <input type="button" value="Clear"/> (HTTP Download Link) (HTTP Clear Link)
Traffic Log:	<input type="button" value="Download"/> <input type="button" value="Clear"/> (HTTP Download Link) (HTTP Clear Link)

With the new firmware you can remotely download and also delete the session and traffic log off GuestGate. In order to use the function, you first need to generate a key. This key is a randomly generated string, which looks something like this: "FAF9D99766676112FB547B6EAB15D3B0". Why do we use this string instead of the administrator user name and password you may ask? The reason is security. As GuestGate currently does not support SSL encryption, all requests sent to the device can be potentially read by a third party. We therefore do not include the admin credentials in the HTTP links. In case something is reading the traffic, he'd only receive the key, which does not give access to GuestGate's administrator interface.

You will end up with 4 links:

1. Session Log HTTP Download Link
2. Session Log HTTP Clear Link
3. Traffic Log HTTP Download Link
4. Traffic Log HTTP Clear Link

The links will look like this:

`http://111.222.333.444/cgi-bin/config.cgi?auth_key=FAF9D99766676112FB547B6EAB15D3B0&session_log=download`

`http://111.222.333.444/cgi-bin/config.cgi?auth_key=FAF9D99766676112FB547B6EAB15D3B0&traffic_log=clear`

GuestGate MK II – Firmware 2.15

3.3 DYNDNS.ORG, DNS-O-MATIC AND OPENDNS

GuestGate’s host configuration page of features a new area called “DYNAMIC DNS”.

Dynamic DNS:	
DNS Service:	DynDNS <input type="text"/>
DNS Alias:	example.dyndns.org <small>(e.g. domain.dyndns.org)</small>
Username:	dyndns_username
Password:	dyndns_password

DNS Service: Choose between DynDNS or DNS-O-Matic

DNS Alias: Enter the DDNS domain name

Username: The DynDNS or DNS-O-Matic account name goes here.

Password: The DynDNS or DNS-O-Matic account password needs to be entered here.

Which service do I use, and how can I use OpenDNS with GuestGate?

a. DynDNS

If you select DynDNS, GuestGate will update the public IP address with the DynDNS database, so that you can reach your GuestGate from a remote site, even if it is connected behind a dynamic Internet address that changes often. Most DSL services utilize IP addresses that are highly dynamic and change as often as once every 24 hours. Cable modem services typically keep the IP address assigned to a user for a longer period of time; e.g., up to 30 days. In any case, after a certain amount of time the IP address of your network will change unless you have a more business-type Internet service that provides a permanent, static IP address.

Why does it matter if the IP address that the ISP assigns to you changes? If you never want to access the GuestGate remotely over the Internet, it wouldn’t and you do not need DynDNS. If you want to connect to your GuestGate from outside your network, the changing IP addresses will make this task very complicated, as you never know under which IP address you can reach your GuestGate device. DynDNS is the solution to the problem. DYNDNS.ORG allows signing up for a free account and setting up domain names like “myguestgate.dyndns.org.” The DDNS service assigns the current IP address that your ISP has assigned to you to the domain name you have set up, so that you can always reach your device at [http:// myguestgate.dyndns.org](http://myguestgate.dyndns.org) (example).

Note that the DynDNS address does not necessarily match the IP address, which GuestGate shows as its “Device IP Address: “ on the host configuration page. Especially in installations where GuestGate is installed behind another router, this is a very likely possibility.

GuestGate MK II – Firmware 2.15

b. OpenDNS and DNS-O-Matic

DNS-O-Matic is a free service for distributing your dynamic IP changes to multiple services with a single update. Those services include DynDNS, and among others, OpenDNS. OpenDNS is an Internet security and DNS service that allows for sophisticated methods of content filtering. Read more about OpenDNS' content filtering abilities here: <http://www.opendns.com/school/contentfiltering>

It is easy to see why using the OpenDNS service in combination with GuestGate is a powerful solution. In order to use OpenDNS with GuestGate, you need to use the DNS-O-Matic service, which is owned by OpenDNS. The authentication is done via DNS-O-Matic, and then GuestGate will automatically switch to the OpenDNS primary and secondary DNS servers 208.67.222.222 and 208.67.220.220. These cannot be bypassed by the user, even if the connected guest computer uses custom DNS settings.

3.4 ADJUSTABLE HTTP PORT NUMBER

In the past GuestGate's web administrator interface was limited to running on the standard HTTP port 80. With the new firmware you can now change that port. The setting can be found under HOST CONFIGURATION.

Administrator IP Address:	<input type="text"/>	Use This Client's Address
Configuration HTTP Port:	<input type="text" value="85"/>	

3.5 BANNING USERS PERMANENTLY

Introduced in firmware 2.15, this feature allows to permanently block a user's computer based on the MAC address of the device he or she's been using. You can block a network client either from the status page, or the guest configuration page.

Connected Guest Computers			new / neu
Ethernet Address	IP Address	Logged In	
c0:cb:38:35:15:e2	192.168.2.102	0 day(s), 00:00:12 (hh:mm:ss)	<input type="button" value="Disconnect"/> <input type="button" value="Details"/> <input type="button" value="Bann"/>

Status Page

Banned Ethernet Addresses:	<input type="text" value="c0:9f:42:0c:60:86"/>	<input type="button" value="Remove"/>
Add Ethernet Address:	<input type="text"/>	<input type="button" value="Add Address"/>

Guest Configuration Page

GuestGate MK II – Firmware 2.15

4. IMPORTANT TECH SUPPORT NOTES

4.1 THE IPAD VS. GUESTGATE ISSUE

iPad cannot connect to the Internet when I am connecting with GuestGate

When GuestGate's default DHCP mode is activated each guest computer operates in its own network and the iPad will not be able to connect to the Internet. This problem occurs on all versions of GuestGate (MKI and MKII, regardless of the firmware version installed on the GuestGate unit).

- **Update the iPad / iPad 2 to version 4.3.3**

Open the Apple iOS update page here: <http://www.apple.com/ios/>

4.2 GUESTGATE HARDWARE RESET DOES NOT WORK?

You try to reset GuestGate to factory defaults by pressing the reset button for 15 seconds, but it does not work. You need to follow the steps below and it will work without problems.

1. Disconnect the power cable from the rear of the GuestGate MKII
2. Plug the power cable back in to the GuestGate MKII
3. When you see one green light on the Guestgate, press and hold down the reset button located on the rear of the router until you see the lights flash
4. Release the button.
5. The device is now set to factory defaults.

In short: Power on GuestGate, count to 5, then press the reset button for 15 seconds.

4.3 HOW TO REPEAT THE GUESTGATE WIRELESS SIGNAL

If you need to expand the wireless network, additional Access Points may be required. It is recommended to hardware additional Access Points to the network as it is a faster and more reliable connection. If you have no choice but to use an Access Point as a wireless repeater, you need make one change to the configuration of GuestGate. You need to change the DHCP mode of GuestGate on the guest configuration page to "same network for all clients".

Guest Configuration:

same network for all clients (automatic) ▼

The standard mode "separate network for each client" causes problems when the wireless signal is repeater by other Access Points.