

# Igaware User Guide

Software Version 9.0.0 (last updated 27/05/11)



## Contents

Welcome to Rock Solid Computing	3
A Choice of Services	4
Installation	5
Configuration	5
Connecting to a local area network (LAN)	6
Connecting to the Internet (WAN)	6
Enable Internet access for computers on your network	6
Internet access controls	7
Web access controls	7
Adding Users & Groups	8
Sending and Receiving Email	8
Email Filtering	9
File Serving	9
Web Serving	9
Sending & Receiving FAXes	9
Desktop Anti-Virus	10
Remote Working VPN	10
Groupware	10
Zarafa	10
Horde	11
Open-Xchange	11
Server Backup	11
Reports	12
System Tools	12
Updates and Change Log	13
Status Console	13
Support	13
Hardware Upgrades	14
Online Resources	14
Appendix	15

## Welcome to Rock Solid Computing

We bid you a very warm welcome to the **Igaware Server** - a powerful multi-functional Network Server Appliance that delivers a choice of managed IT services. Combined with Igaware's product support, it delivers unrivalled reliability and ease of use. As an Igaware customer you should expect to have few if any problems with your Igaware Server. **It has been engineered to be rock solid.**


The key to Igaware's rock solid reliability is three fold;

- **It is well engineered** - it is robust and reliable.
- **It is continuously updated** - product support includes continuous updates to the operating system and all applications, including new features and security measures. This ensures your server is always secure and up-to-date. Furthermore, these updates are automatic so you don't have to do a thing and can say goodbye to manual firmware updates.
- **Our support is world class** - should you have a problem an engineer can undertake remote diagnostics and support. If the problem doesn't lie with the Igaware Box, we won't leave you in limbo. Instead, we will do our best to help you identify the problem whether, for example, it is a faulty ADSL line or a misconfigured switch. The Igaware Server has a built in tool box for diagnosing problems on your network.

As a rule, if your box is plugged in and switched on, it's most likely to be working fine. So please, if you suspect a problem, **don't switch it on or off**, please call Igaware support on 0191280 4013..

This guide covers the basic installation and configuration of your Igaware Server to take advantage of the wide range of available services it can deliver. It also covers how to undertake daily tasks such as, for example, adding new users and monitoring Internet use.

This guide should be used in conjunction with the extensive on-line help that is found throughout the Igaware Server configuration interface.

* Points shown like this is are to make you aware of advanced configuration options that may be relevant for your setup.*

The Igaware Server is easy to use, making configuration within the capability of anyone with a basic understanding of computer networking. If you should need clarification on anything, please drop an email to [support@igaware.com](mailto:support@igaware.com) or call Igaware support on 0191 2804013 and we will be pleased to assist.

## A Choice of Services

The Igaware Server is a multi-functional Server engineered to deliver a choice of IT services. Some organisations use just one service, others a combination and some use all of the services.

Services are enabled according to the service fees you pay. If you want to use additional services please contact your Igaware dealer.

### **Remote Working**

Giving you easy access to documents, emails and applications, while you are out and about, using your laptop, pda and mobile phone.

### **Email Servicing**

Give all your staff an email address @yourcompany.co.uk to improve communication with colleagues, customer and suppliers. Built in tools allow you to monitor and control email use and archive emails.

### **File Servicing**

Store documents and databases centrally on a secure server and share them with authorised colleagues. Anti-virus and data backup systems are available to protect your data.

### **Groupware**

Share contacts, diaries and tasks, improving staff productivity and communication.

### **Internet Security**

Protects confidential data, documents and customer information from Internet threats including hackers, viruses and spyware. Prevent downtime and legal implications of a security breach.

### **Email Filtering**

Protects against harmful emails including viruses, spam, phishing and pornography that can cost you money in terms of downtime, lost productivity, damaged reputations, harassment cases and employee claims.

### **Web Filtering**

Gives you the critical controls needed to prevent and monitor harmful and inappropriate web surfing by your staff, protecting against lost productivity, system downtime and legal liability.

### **Backup/Disaster Recovery**

Protects your business against data loss from fires, floods, accidental damage and theft. Delivering peace of mind.

## Installation

The Igaware server has a minimum of two Ethernet ports, one marked 'LAN', the other marked 'WAN'. The LAN port is used to connect the server to your local area network and the WAN port is used to connect it to the Internet (via a broadband modem/router).

Multi-WAN capabilities mean more than one Internet connection can be specified. Additional connections can use a range of connectivity options including Ethernet modem/routers, 3G USB dongles and serial modems. Automatic failover and load balancing can be configured where you have more than one Internet connection.

*☞ Multi-LAN is also supported to create DMZs etc. Go to Administration => Network.*

The Server should be installed in a well ventilated location and requires a single power point. The use of an uninterruptible power supply (UPS) is recommended to protect against power outages and surges. The server supports APC UPS units - the USB port on the Server can be connected to one of these units, enabling automatic safe shutdown before the UPS battery runs dry.

The power button is on the front of the Server along with a reset button. Please don't power the unit off or reset it using these buttons unless asked to do so by an Igaware engineer. If you need to power the unit down it should only be done via the configuration interface under System => Shutdown or Reboot. Although the unit shouldn't be damaged by being powered off it's always preferable to follow the shutdown procedure.

**Note:** When an Igaware server is powered on for the first time the orange hard disk light will remain on for an hour or so while the disk RAID system synchronises.

## Configuration

The Server has a factory default IP address of 192.168.2.252 and DHCP is enabled. To start configuring the server you can simply connect a computer using a cross over Ethernet cable plugged into the server's LAN port. The Server can then be configured by opening a web browser and surfing to <https://192.168.2.252>.

This address will open up the login page for the Igaware configuration interface. Login using the user name and password supplied with the Server.

Before you start configuring the Igaware Server please go to System => Register/Licence => Registration. You will be asked to enter the system user name and password (supplied with the Server). Registration must be completed for the Server to fully function.

**Note:** There is on-screen help available throughout the configuration interface.

**IMPORTANT:** Any configuration changes made are only activated after 'Commit Changes' has been run (found on the left hand menu of all configuration pages).

### **Connecting to a local area network (LAN)**

To add the Server to your LAN go to Administration => Network and select 'Ethernet #0' give it an IP Address on your LAN and complete all fields using the on screen help. By default DHCP is enabled.

*👉 One Handed Mode is available to give the Server an Internet connection over the LAN. In this mode the Server only requires one Ethernet connection to the LAN and no separate connection to the Internet.*

### **Connecting to the Internet (WAN)**

The Igaware Server can be connected directly to the Internet using an Ethernet router, an Alcatel USB SpeedTouch modem, or a serial modem. It also supports ADSL modems using PPPoE. There is also the option to connect over the LAN using 'One-Handed Mode'. To configure Internet access, go to Administration => Network and select Ethernet #1 and Add New ISP Connection.

If a router is used, it must be configured to allow the Igaware Server unrestricted Internet access inbound and outbound otherwise the Igaware Server may not be able to operate correctly.

Once you have configured Internet access, you can test that it is working by going to System => Tools => Test Internet Connection.

*👉 If the Igaware Server is installed in 'One Handed Mode' (see 2.2.1 above) then your existing firewall must be configured to allow the Server unrestricted outbound Internet access. Inbound access from the Internet to the following ports on the Server must be provided:*

- SSH 22 (This allows remote support services).
- SSL 443 (This allows remote access to the Igaware administration interface. If port 443 is already in use then use port 666).

***Note:** You may need to forward additional ports to enable some services. E.g. if the Igaware Server is being used to filter email that is delivered via SMTP you will need to forward traffic on port 25 to the Igaware Server. If the Igaware Server is installed as the router/firewall then things are much simpler.*

### **Enable Internet access for computers on your network**

By default, all outgoing Internet access from the LAN is blocked. To enable Internet access for machines on the LAN, go to Administration => Access Controls => Outbound Firewall => Individual Computers.

The Individual Computers page is used to configure Internet and Web access for machines on the LAN. Any computers or devices not listed here will not be allowed Internet access.

*👉 The default "blocking" policy can be changed by selecting a derestricted access policy e.g. Web Access Only etc.*

The 'default' machine listed, on this page, defines the default Internet access policy that will be applied to machines added to this list. Click on this and check the settings before adding machines.

The quickest way to add machines to the list is to click on the 'Scan LAN Network' button. The scan will find machines on your network and apply the default Internet access policy.

**Note:** Machines with a software firewall enabled may not be found. Disable firewalls and try again. Any machines that are not picked up by the scan can be added manually. Once listed, you can click on a machine to change the default Internet and Web access policies:

### **Internet access controls**

It is recommended not to give all the machines on your LAN unrestricted Internet access unless it is really necessary; most security breaches come from internal staff innocently downloading and accessing malicious content on the Internet. Prevention is a lot cheaper than cure.

Access is controlled by applying an access policy such as 'Web Only' or 'Web & FTP'. There are several pre-defined policies that cover the majority of user requirements.

*☞ Additional access policies can be created using the left-hand menu options;*

- *Service Port List (configure Internet ports that are used to define LAN Access Policies).*
- *LAN Access Policies (define Internet Access Policies that can then be applied to machines on the LAN).*

### **Web access controls**

Access to the web can be controlled in a number of ways by checking appropriate boxes on the Individual Computer configuration page. Options include:

- Limit access to only the sites listed in the company white list
- Allow access to any web site except those in site categories you select (e.g. pornography), and the company black list.
- Block access to certain file types that may be 'dangerous' e.g. executable files.
- Control access according to the time of day

Web access control through the Igaware Server requires the default gateway on LAN machines to be set as the LAN IP address of the Igaware Server. This can be done automatically using DHCP.

*☞ Web authentication can be enabled to force users to login with a user name and password when they open their web browser. Useful if users share computers.*

*☞ If you are using Active Directory, users can be synchronised to the Igaware Server to allow single sign on. To enable ADS integration go to Administration => Servers => Windows Services => PDC/ Domain Member Configuration => PDC/ ADS Member*

## Adding Users & Groups

### Users

Users only need to be added once for them to be able to use the different services on the Server. To add users go to Administration => Users/Groups => Users and click on the 'Add User' and follow the on-screen help.

### Groups

If you have a large number of users it may be easier to administer access to the web or file server shares according to local group policies. Local groups can be created in Administration => Users/Groups => Groups.

*☞ If you are using an Active Directory Server, users can be synchronised with this. To enable ADS integration go to Administration => Servers => Windows Services => PDC/ Domain Member Configuration => PDC/ ADS Member*

## Sending and Receiving Email

The Igaware Server can handle both incoming and outgoing email. In addition to ensuring email gets to its destination the Igaware server filters email to remove malicious payloads including viruses, dangerous content, fraud attempts (phishing) and spam.

To configure the Igaware Server for email go to Administration => Servers => Email.

Select 'General' from the menu and set which user will be the 'Postmaster'. The 'Postmaster' can receive various notifications from the Server about, for example, emails that can't be delivered. On the same page enter the outgoing SMTP server; this should be the outgoing SMTP server address given to you by your ISP.

**Note:** The Igaware Server can relay outgoing mail directly but some anti-spam systems will reject emails sent by a server using a public IP address that is part of a block allocated to an ISP.

The Igaware Server can be configured to receive email for multiple domains using POP3, IMAP and SMTP. You can configure this in Administration => Servers => Email => Internet Accounts.

To allow email to be received via SMTP, open port 25 in Administration => Access Controls => Port Input.

Incoming email is distributed to users' mail boxes (created when a user is added to the Server). Email aliases or mailing lists can be configured, and email received for these will be delivered to users you select in Administration Servers => Email => Aliases.

Users can access email on the Igaware Server using any client software that supports POP3 or IMAP e.g. Outlook, Mozilla Thunderbird. Client software should have the incoming and outgoing mail servers set as the Igaware server's IP address on the LAN.

The user name and password for the incoming mail server is the same as that set on the Igaware server when the user was created.

Email can also be accessed using Web based groupware. For more about groupware see page 10.

*✎ A global Outgoing Email Signature can be defined in Administration => Servers => Email => Outgoing Email Signature*

*✎ By default only users on the local LAN can send (relay) email through the Server. To enable remote users to relay email when connected by VPN go to Administration => Servers => Email => SMTP Relay.*

### **Email Filtering**

The Igaware Server filters email for viruses, spam, phishing attempts and other malicious content. To configure email filtering go to Administration => Servers => Email => Email Filtering.

*✎ You can block emails to and from specific email addresses and/or domains by going to Administration=>Servers=>Email=> Blocking List.*

*✎ Emails can be forwarded on to another Email server, such as MS Exchange, This is configured by using Administration => Servers => Email => SMTP Forward*

### **File Serving**

The Igaware Server provides central file serving with access to public and private file shares that you define. Users can logon to the file server as a member of an MS domain or a workgroup. The file server is configured in Administration => Servers => Windows Services.

*✎ A number of options exist to backup data held on the file server. See 'Server Backup' on page 11.*

*✎ File server space can be used as iSCSI Storage. This allows you to effectively add additional hard disk storage to existing servers. This is enabled in Servers => ISCSI Storage.*

### **Web Server**

The Igaware Server can be used to host web pages that can be made publicly accessible by opening port 80 in Administration => Access Controls => Inbound Firewall => Port Input. The Web server runs Apache, MySQL and PHP, enabling the hosting of dynamic, data driven websites. To configure the Web server go to Administration => Servers => Web Server.

### **Sending and Receiving FAXes**

The Igaware Server can send and receive faxes providing it is connected to a telephone line using a Fax Modem. We recommend that you use a US Robotics 56K External Fax modem V.92 (USR015630D). Incoming faxes are converted to PDF and sent as attachments to emails to the fax recipients specified for the 'FAX recipients' alias in Administration => Servers => Email => Aliases.

Outgoing faxes can be sent via the fax printer on the Igaware server or via email.

To configure faxing go to Administration => Servers => FAX Server

### **Desktop Anti-Virus**

Desktop anti-virus software from Kaspersky can be configured to update directly from the Igaware Server. To enable desktop updates go to Administration => Servers => Anti-Virus => Desktop Updates => Kaspersky

Kaspersky client software should be configured to update from [http://\[serverip\]/kavupdates](http://[serverip]/kavupdates) (e.g. <http://192.168.2.252/kavupdates>).

Client software can be obtained directly from Kaspersky ([www.kaspersky.co.uk](http://www.kaspersky.co.uk)).

Note: We don't endorse or supply Kaspersky software.

### **Remote Working/VPN**

The Igaware Server supports PPTP, IPSec and SSL VPN protocols that enable you to create secure connections to your Network over the Internet.

To connect remote offices together over the Internet we recommend using IPSec. This can be setup to connect to another Igaware Server or any IPSec compliant device. To setup IPSec VPN go to Administration => Network => Virtual Private Networking (VPN) => IPSec VPN.

If you are out of the office, working from home or on a train, for example, you can create a secure connection to the Igaware server in your office using PPTP VPN. Most computers have a PPTP client as standard – for MS Windows this is called “VPN Adapter”. To setup PPTP VPN go to Administration => Network => Virtual Private Networking (VPN) => PPTP.

### **Collaborative Groupware**

The Igaware Server has three groupware options all of which provide web access to email, diaries, contacts and tasks.

#### **Zarafa (Exchange alternative)**

Zarafa allows you to share e-mail and calendars via Outlook, on your PDA or through Webaccess. The Zarafa Webaccess features the familiar Outlook 'Look & Feel' interface, and you can keep using the features in Outlook that have always allowed you to work efficiently. It also works with Active Sync and Mail for Exchange (nokia) enabling synchronisation with mobiles and PDAs (including Blackberrys).

To enable Zarafa go to Administration => Servers => Collaborative Groupware => Zarafa


 Note: There is a Zarafa Setup Guide available from <http://www.igaware.com/support>.

## Horde

Horde is an enterprise ready, browser based communication suite. Users can read, send and organize email messages and manage and share calendars, contacts, tasks and notes.

To enable Horde go to Administration => Servers => Collaborative Groupware => Horde.

Once enabled, login to Horde by pointing a web browser at <http://serverip/groupware> (where *serverip* the IP address of the Server on your LAN. You can login remotely over the Internet using <https://publicip/groupware>, where *publicip* is the public IP address of the Igaware server. You can find your public IP address by looking in Administration => Network => ISP Settings.

 *Note: Port 443 (https) is opened in Administration => Access Controls => Inbound Firewall => Port Input. This allows users to login remotely over the web to groupware using SSL (https://)*

When you login to Horde for the first time, you must set an 'Identity' in 'Personal Information'. If not, you will be unable to send emails. To set your Identity; When in Email click on Options and select Personal Information. Fill in at least the first 3 fields and the "Sent mail folder". Click on "Save Options" when finished. Go back to Personal Information and set "Your Default Identity". Click on "Save Options" when finished.

## Open-Exchange (OX)

**This service is now deprecated in favour of the Zarafa server. We don't recommend any new installations of Open-Exchange Server.**

## Server Backup

The Igaware Server offers a number of ways to backup data held on it. Data can be stored to tape, an external USB/Firewire hard drive, a Windows share on your network, or offsite to a remote Rsync server. All settings are available in System => Backup where you can configure a 'Main' and a 'Secondary' backup.

The Igaware Server can be used as an Rsync Server and receive data from other Igaware Servers. E.g. If you have several offices, each with an Igaware Server, you can back these up centrally to your head-office Igaware Server that has been enabled as an Rsync Server. Enable in System => Backup => Rsync Server.

Note: The system configuration is automatically backed up offsite to Igaware's data center, daily. This ensures that if your Server is, for example, destroyed in a flood etc, another Igaware Server can be supplied pre-configured with all of your settings.

## Reports

The Igaware Server makes a number of reports available in 'Activity Reporting'. These include:

- **Email Summary**  
This report shows a summary of email activity for the last 7 days including the total number of emails sent and received, the number of viruses detected and the number of spam emails filtered.
- **Email Usage Report**  
This report provides details of emails sent and received by users for date ranges you select.
- **Site Blocking Report**  
This report shows attempts to access web sites blocked by web filtering policies.
- **Web Visits Report**  
This report shows details of web surfing activity.
- **Network Traffic**  
Graphs show network traffic on each of the network interfaces in use.
- **PPTP VPN Report**  
This report shows information about past and present remote PPTP connections.

Reports can be viewed within your web browser, or exported to be saved as an MS Excel file.

## System Tools

If you go to System => Tools you will find a number of options that can help you monitor and diagnose network problems. Here's a summary of the tools and what they provide:

- **Network/Host Monitoring**  
You can monitor devices on the LAN or WAN and receive email alerts if they should become unavailable.
- **Log Viewer**  
One of the many advantages of an Igaware Server is that it is very verbose about what it is doing. The logs tell you what is going on, taking the guess work out of support.
- **Ping Scan LAN**  
This utility will tell you what devices the Igaware Server can see on your network.
- **Network Vulnerability Scanner**  
This option allows you run a Nessus scan on local or remote networks to identify security vulnerabilities. See <http://www.nessus.org/>
- **Network Query Tool**  
A tool for discovering Host Information e.g. DNS, WHOIS etc, and checking Host Connectivity e.g. PING, TRACEROUTE etc.

- **Test Internet Connection**  
Does what it says.
- **Ntop Server**  
This is a network discovery tool that provides a graphical web interface through which you can see exactly what is happening on the network. See [www.ntop.org/overview.html](http://www.ntop.org/overview.html).

## Updates and Change Log

What makes Igaware different from other products is that the whole software bundle, including the operating system and all applications, are constantly updated to provide new features and protect against new security threats. An unsupported security product will soon become vulnerable to security threats. Not only should Spam, AV and Web Filtering databases be updated, for example, but you should also update the software engines and add new techniques that become available. Because of our approach your Igaware Server is secure and robust. To view the latest updates, click on the ‘change log’ link on the home page of the administration interface. For boredom control we only detail significant updates.

## Status Console

When you first login to the Igaware Server configuration interface, you are presented with live system status information. This status console provides a heads up to any current issues, such as disk space running low, and also provides statistics on, for example, email filtering. More detailed information can be accessed by using the ‘Full Info’ links.

Alerts can be configured to be emailed using the ‘Config’ links.

The status console can be accessed anytime in System Status => Status Console.

## Support

If you have a problem, please don’t reset the server (switch the server on and off) - this will not fix anything but it may well make diagnosis of the problem much harder, and in could result in a damaged file system. If a unit loses power (powercut/unplugged/reset), when it is powered back on it will run file system checks which can take several minutes - resetting at this point can seriously damage the file system.

Let’s say, for example, that you are not receiving email. This could be down to a whole number of factors; your domain has expired, your ISP mail server could have a problem, your MX record has been misconfigured, your personal computer has a problem, your internal network has a problem, your Internet connection is down, or it could even be that no-one has sent you any email today. Re-booting the Server will not resolve any of these



issues. Please call for support if you have any problems and we'll work with your dealer to resolve them in the minimum possible time.

## **Hardware Upgrades**

Igaware Servers are available in a number of different specifications and upgrades are available as and when required. You can request upgrade information from your Igaware dealer. The system status console (see above) can alert you if hard disks, for example, need upgrading sometime soon.

## **Online Resources**

The Igaware website at <http://www.igaware.com> provides extensive product information. There is also a support section with the latest version of this and other guides.

## **Appendix**

### **Resetting an Igaware Server to Factory Defaults**

To reset, attach a key board and screen and switch on.

At the login prompt, login with user name 'factorydefaults' and enter the reset password and follow the instructions on screen. If you require the reset password, please contact us.