getbusi
CREATING SMART CONNECTIONS

ALERT/ADVANCE USER GUIDE

Level 1, 61 Davey St   Hobart, TAS 7000   T (03) 6165 1555   www.getbusi.com

Table of Contents

1 Introduction

Getbusi is excited to provide you with the very best of today's technology in web access management, full of intelligent and well-designed features. We have designed our product with our end-users in mind, striving to make it intuitive and easy-to-use. In our efforts to constantly improve our product, we welcome feedback from our customers. If you would like to provide us with suggestions or feature requests, please don't hesitate to send an email to: support@getbusi.com.

As you know, the Internet is a vital resource for all organisations. Like any resource, it needs careful management, especially in today's online environment. Organisations are faced with a number of issues when providing Internet access, including cost, productivity, bandwidth limitations and legal duty of care. Most organisations declare an Acceptable Usage Policy without an effective means of implementation. The Getbusi system solves this problem by providing a cost-effective, easy-to-use, and reliable Web Access Management solution.

The Getbusi system allows organisations the ability to enforce Internet Usage Policy, while reducing the real costs of providing Internet access. The Getbusi software provides a comprehensive set of features within a single, elegant, browser-based interface that can be easily administered by anyone who is responsible for an organisation's Internet access management.

The key benefits of Getbusi include:

- A browser-based interface that may be managed by non-technical staff.
- Content filtering to block access to undesirable sites through Getbusi managed filters, seamless upstream website classification as well as customisable good, bad, expression-based and file-type filters.
- Download quotas aggregated on a daily, weekly and monthly basis.
- Customisable cost assignment to bandwidth usage as well as a ticketing subsystem allowing users to purchase additional access.
- Quota bypass for designated sites.
- Maximum file size to limit the maximum size of an individual downloaded file.
- Bandwidth-throttling to control an individual's, or group of individuals' bandwidth usage.
- Customisable access policies for an individual or group.
- Time-based policies to allow different access restrictions based on the day-of-week, a date range, time range, or any combination thereof.
- Restrictions based on file types using Getbusi's default set, and the ability to add custom file types.
- Comprehensive reporting features complete with graphs and charts and the ability to save reports in Adobe™ PDF format.
- Easy implementation into your existing IT infrastructure with seamless integration with your existing authentication and security infrastructure.
- Enterprise reliability based on the Red Hat® Enterprise Linux 5 platform.
- Scalability for the enterprise, with the ability to replicate settings to slave proxies from a master server.
- Full disaster recovery features.
- A focus on quality service and support.

2 About This Manual

This manual is intended for your organisation's designated Getbusi Administrator. An in-depth knowledge of IT concepts is not required to administer the Getbusi solution, however the Getbusi Administrator should read this guide to understand the full capabilities of the software. This guide provides the Getbusi Administrator with the knowledge to administer the Getbusi software, and manage your organisation's Internet access. This manual assumes that the Getbusi software has been successfully installed, and the Getbusi console is accessible via a web-browser. If that is not the case, please refer to the Installation and Server Configuration Guide, also found on your installation media.

For assistance in the configuration of your Getbusi software, please first refer to the step-by-step instructions contained in this guide. You may also contact Getbusi support for additional assistance, if required:

Via email: support@getbusi.com
Telephone (Australia): (03) 6165 1555 Telephone
(International): +61 3 6165 1555

3 Initial Software Configuration and Setup

This section documents the necessary steps to configure your Getbusi software for the first time. The software should be installed on your Getbusi server, and the server properly configured for your network.

3.1 Pre-Installation Checklist

Prior to configuring your Getbusi software, you should have at your disposal, some information about your organisation's authentication system, if any. Supported authentication systems include: NTLM Seamless/Basic (Windows 2000, 2003, 2008 and NT), various LDAP (Lightweight Directory Access Protocol) implementations.

You also need to know how many client workstations (or number of users) that are going to use your Getbusi proxy. The following checklists will help you determine which authentication settings to configure for your Getbusi server. Only use the checklist that pertains to your authentication method.

3.1.1 Seamless/Basic Authentication (Windows® Active Directory®) Checklist

Prior to filling out the checklist, please read the section entitled: Authentication: Seamless/Basic Authentication for a detailed explanation each of the items in the checklist, especially regarding the Authentication User.

Number of Workstations: ______________________________

Administrator User Name: ______________________________

Administrator Password: ______________________________

Windows Server IP Address: ______________________________

Windows Server Netbios Name: ______________________________

Authentication User: ______________________________

Authentication User Password: ______________________________

Windows Domain: ______________________________

Other Domains to Trust: ______________________________

3.1.2 LDAP (POSIX®, Apple® OS X, Novell® eDirectory®) Checklist

Implementations of LDAP for POSIX, Apple OS X and Novell eDirectory are very similar. Please read the corresponding documentation in the Authentication section for a detailed explanation of each item in the checklist. Note that not all fields will be required, depending on LDAP implementation.

Number of Workstations: ______________________________

LDAP Server IP Address: ______________________________

LDAP Search Base: ______________________________

LDAP Bind Distinguished Name: ______________________________

LDAP Password: ______________________________

LDAP Version: Auto / LDAPv2 / LDAPv3

Secure Connection on TLS: Yes / No

3.2 Connecting to the Getbusi Server

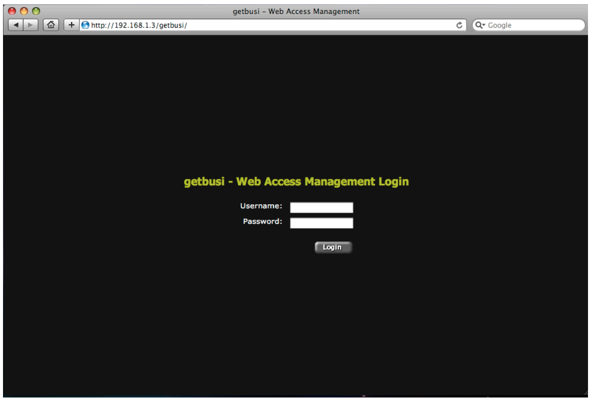
You can access the Getbusi server from any desktop computer on your local area network (LAN). You can connect to your Getbusi server either by its IP address, or by name, if there is an entry for the Getbusi server in your DNS. Open a browser and connect to:

When navigating by IP address: http://<your Getbusi server's IP address>

When navigating by name: http://<your Getbusi server's DNS name>

Figure 1 shows the login screen that is presented when you connect to the Getbusi server.

NOTE: On some versions of Mac OS X Server 10.5 the Apache module for PHP is disabled by default. If you are having trouble connecting to the Web Interface please ensure the Web module named *php5_module* is enabled in Server Admin.



getbusi – Web Access Management

http://192.168.1.3/getbusi/

getbusi - Web Access Management Login

Figure 1

- The Getbusi administrator Username is: **admin**
- The default Getbusi administrator Password is: **test**

Do not worry at this time about changing the default password. You will be instructed on how to change the password later in this document.

3.3 License Agreement

The next screen you are presented with is a License Agreement. You should carefully read the terms of the Getbusi License. If you accept the terms of the license, select the radio button that corresponds with: **I accept the conditions of the license agreement**. If you do not accept the terms of the license agreement, you will not be allowed to continue. Click the grey **Continue** button to proceed to the next screen.

3.4 Organisation Categorisation

The next screen displayed after accepting the Getbusi License Agreement is the Organisation Categorisation screen. This screen allows you to select a type of organisation that best represents your organisation. This information is used to determine the default policies that are configured into your system. For example, if you select **Education**, there will be a Student policy loaded by default into your system, which will not appear if you select **Corporate**, or **Government**. None of the default policies are immutable; you may add, modify or delete policies at a later time, overriding any default configurations set here.

Select the radio button corresponding with an organisation that best describes your own, and click on the grey **Continue** button to proceed.

The system notify you that it is being set up, which could take up to ten minutes. When the system notifies you that the setup process is complete, click on the grey **Continue** button to proceed.

3.5 Installing your Getbusi License

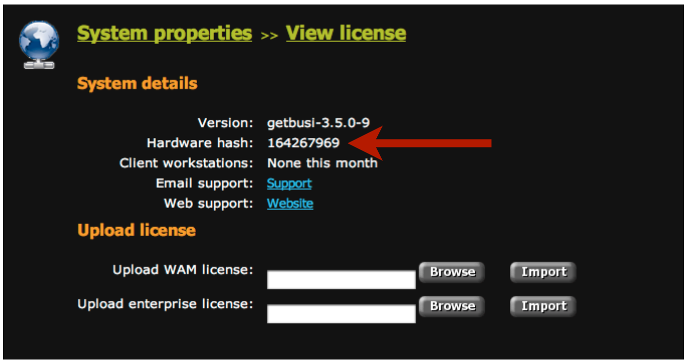
The next screen allows you to install a Getbusi license. This is a three-part process: requesting your license, obtaining your license and installing your license. Please note that you must be on workstation with access to the Internet.

3.5.1 Requesting your License

The first step of installing a license for your Getbusi system involves obtaining a license from Getbusi support. You should have the following information available when you request your Getbusi license:

1. Hardware Hash: The red arrow in Figure 2 shows where you can find your machine's hardware hash. Your hardware hash is unique to your machine, and is calculated based on a number of factors defined by the hardware on your machine. Please do not use the hardware hash provided in this example, as it will not work for your machine.

2. Number of Workstations: This is the number of clients that will be using Getbusi as a proxy for your organisation.



System properties >> View license

System details

Version: getbusi-3.5.0-9
Hardware hash: 164267969
Client workstations: None this month
Email support: Support
Web support: Website

Upload license

Upload WAM license:
Upload enterprise license:

Figure 2

You can either call or email Getbusi Support to have a license generated for your Getbusi server. If you purchased Getbusi through an authorised reseller, then you should request a license through that reseller.

3.5.2 Obtaining your License

Once you have contacted Getbusi Support with the information from the preceding step, a license will be generated for you. You will receive an email with instructions on how to retrieve your license from the Getbusi website. If you purchased Getbusi through a reseller, you should receive directions from them on how to obtain your Getbusi license from the Getbusi website.

You should download your license from the website and save it to a known location on your workstation. You are now ready to upload your license to the Getbusi server.

1. Click on the grey **Browse** button that corresponds to the **Upload WAM license** field.

2. Once you have browsed and selected a license to upload, the path to that license will appear in the text box that corresponds with: **Upload WAM license.** Then click on the corresponding grey **Import** button.

3. Once you have imported your license, the page will refresh and display your license in the area entitled: **License Details**. Click the **Next** button located in the top right-hand corner of your browser window to proceed.

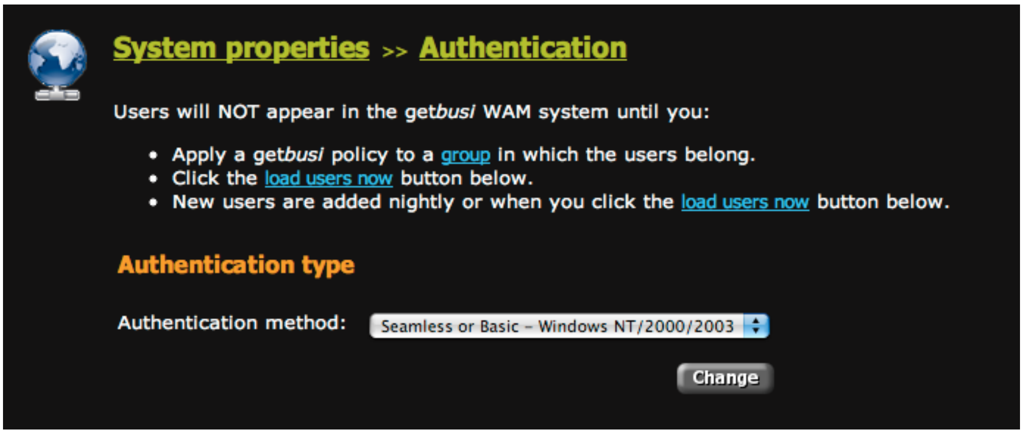
3.6 Authentication Settings

The next step in configuring your Getbusi system is selecting and configuring the authentication method that best suits your organisation's existing authentication infrastructure (if any). The authentication method determines what type of directory service the Getbusi system will use to retrieve user and group information. If you do not have a pre-existing authentication infrastructure and wish to use the built-in Getbusi LDAP, please see the **Getbusi Built-In LDAP Guide** before proceeding.

Please use the information identified in your Authentication Checklist to help you properly set up and configure authentication for your Getbusi system.

3.6.1 Selecting Authentication Type

Under the **Authentication Type** heading, a drop-down menu listing the supported authentication types allows you to select the one best suited for your organisation. Select the type of authentication you wish to set for your Getbusi system and click the grey **Change** button. Upon page refresh, the form fields being displayed on the rest of the page may change to reflect the correct options for the selected authentication type.



System properties >> Authentication

Users will NOT appear in the get*busi* WAM system until you:

- Apply a get*busi* policy to a group in which the users belong.
- Click the load users now button below.
- New users are added nightly or when you click the load users now button below.

Authentication type

Authentication method: Seamless or Basic - Windows NT/2000/2003

Figure 3

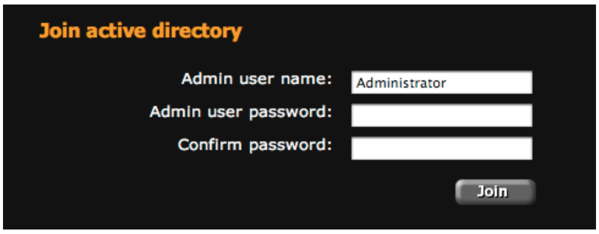
3.6.2 Active Directory Authentication

In Windows Active Directory environments, you may choose to either have seamless or basic authentication. With seamless authentication, your users will not be prompted for a username and password when using a browser to surf the web. Seamless authentication uses the authentication tokens from a user's Windows desktop login to allow access to Internet resources. In order for seamless authentication to work, the Getbusi system must be allowed to join your organisation's Windows Active Directory domain.

If you do not wish the Getbusi system to join Active Directory, you can still have users authenticate against Active Directory for web access, but users will be prompted with a username/password dialogue box when accessing Internet resources.

3.6.2.1 Join Active Directory

The information used to join Active Directory is neither recorded nor saved by the Getbusi system, and does not compromise the security of your Windows network. If you do not wish for Getbusi to join Active Directory, skip these steps and proceed to entering your Authentication Details.



Join active directory

Admin user name: Administrator

Admin user password:

Confirm password:

Figure 4

1. In the **Admin user name** field, enter the user name of an administrative user. This user must have the required privileges to allow the Getbusi system to join the domain. Typically, this is the Administrator user.

2. In the **Admin user password** field, enter the administrative user's password.

3. In the **Confirm password** field, retype the administrative user's password.

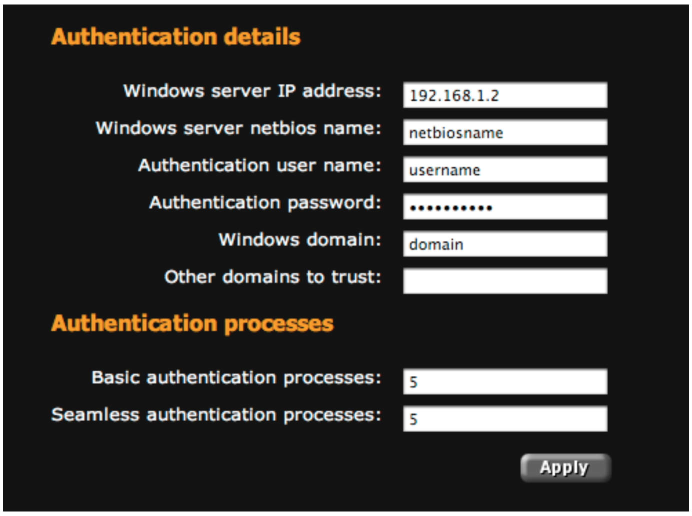
4. Click the grey **Join** button to join Active Directory. You will be provided feedback on whether the Getbusi system successfully joined the domain. If your browser is configured to block pop-ups this notification may not appear.

3.6.2.2 Authentication Details

The Authentication Details section is required for Getbusi to get the groups and users from Active Directory.

Prior to configuring Getbusi to integrate into your Microsoft Windows domain, you should create an Authentication User for Getbusi on your Windows server. If you are running Windows 2000, 2003 or 2008 Server, this user must be made part of the "Pre-Windows 2000 compatible access" group. No other access privileges for this user are required.

Although you may use your Administrator User for this purpose, this practice is **seriously discouraged**, as the username and password are written to a configuration file on the Getbusi server, and could lead to a security compromise of your Windows Domain Controller.



Authentication details

Windows server IP address: 192.168.1.2

Windows server netbios name: netbiosname

Authentication user name: username

Authentication password: ••••••••••

Windows domain: domain

Other domains to trust:

Authentication processes

Basic authentication processes: 5

Seamless authentication processes: 5

Figure 5

1. In the **Windows server IP Address** field, enter the IP address of a Windows Domain Controller for your Windows domain.

2. In the **Windows server NetBIOS name** field, enter the NetBIOS name of the same Windows Domain Controller from step 1.

3. In the **Authentication user name** field, enter the username of the Authentication User you created for the Getbusi system.

4. In the **Authentication password** field, enter the password corresponding the Authentication User you created for the Getbusi system.

5. In the **Windows domain** field, enter the top-level name of your Windows domain. If you have an Active Directory domain named *mydomain.local*, you only need to enter *mydomain*.

6. In the **Other domains to trust** field, you may optionally supply a comma-separated list of trusted Active Directory domains, allowing Getbusi to serve users from those trusted domains. The following conditions need to be satisfied:

    - A two-way trust must exist between the domain controller identified in step 1 and the domain controllers serving the trusted domains listed.
    - User accounts for all users in the trusted domains must exist in the domain controller identified to Getbusi.
    - Passwords for these users must match across all of the domains.

3.6.2.3 Authentication Processes

The following two fields control the number of authentication processes to run on the Getbusi server. These authentication processes allow client access to Internet resources.

The calculation to establish the number of authentication processes for each of the authentication types can be determined by dividing the number of workstations using the Getbusi system by 5. **Even if you are using seamless authentication, the minimum recommended number of basic authentication processes is 5**, which corresponds to 25 workstations. Do not set the number of Basic authentication processes to 0, because it will disable the Temporary Users feature of your Getbusi system, as well as disable access for clients not in Active Directory. The maximum recommended value for basic authentication processes is 50 (450 workstations).

If you are not using seamless authentication, you may set the value for seamless authentication processes to 0. The maximum number of seamless authentication processes is 50 (450 workstations).

1. In the **Basic authentication processes** field, enter the number of Basic authentication processes to be run on your Getbusi system.

2. In the **Seamless authentication processes** field, enter the number of seamless authentication processes to be run on your Getbusi system.

3. Click the grey **Apply** button to save your settings.

4. At the top of the screen, you will see an indication that the system is processing your parameters. When the processing is complete, click the grey **Next** button in the upper right-hand corner of your browser window.

You have now finished configuring authentication for Active Directory (Seamless or Basic - Windows NT/2000/2003/2008). Proceed to the section entitled: Setting Group Policies.

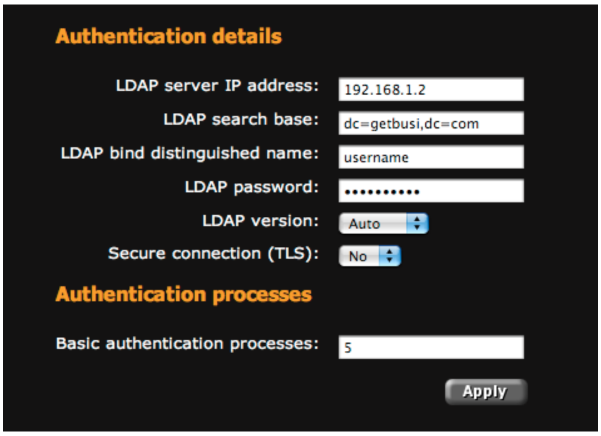
3.6.3 LDAP Authentication (POSIX, Mac OS X, Novell only)

This section documents how to configure the LDAP-based authentication methods.

The **LDAP - POSIX** authentication type is suitable for environments using an authentication scheme based on OpenLDAP.

The **LDAP - Mac OS X Open Directory** is suitable for environments running Apple Macintosh OS X Server's built-in Open Directory services.

The **LDAP - Novell eDirectory** is suitable for environments running Novell's eDirectory LDAP directory services.



Authentication details

LDAP server IP address: 192.168.1.2

LDAP search base: dc=getbusi,dc=com

LDAP bind distinguished name: username

LDAP password: ••••••••••

LDAP version: Auto

Secure connection (TLS): No

Authentication processes

Basic authentication processes: 5

Figure 6

3.6.3.1 Authentication Details

1. In the **LDAP server IP address** field, enter the IP address of the LDAP server against which you are authenticating.

2. In the **LDAP search base** field, enter the search base for your LDAP directory. The search base defines the location in the directory from which the LDAP search begins.

3. In the **LDAP bind distinguished name** field, enter the user name to connect to your LDAP services with.

   - For most LDAP implementations, this may be left blank, as most allow anonymous binding.
   - If you implement Novell eDirectory, if the username is required, it must be fully qualified. For example, if your username is *admin* and your search base is *o=mysite*, then the LDAP bind distinguished name will be: *cn=admin, o=mysite*.

4. In the **LDAP password** field, enter the password corresponding with the username you are using to connect to your LDAP services. Leave this blank if you are not using a username.

5. In the **LDAP version** drop-down list, set this to the version of LDAP running on your authentication server, or leave this set to *Auto*. Not all versions of LDAP require this to be set.

   - If you are running Mac OS X Open Directory, set this to *LDAPv3*.

6. In the **Secure connection (TLS)** drop-down list, select *Yes* if you use TLS (Transport Layer Security) when authenticating against your LDAP services.

3.6.3.2 Authentication Processes

The following determines the number of basic authentication processes to run on the Getbusi server. These authentication processes allow client access to Internet resources.

The calculation to establish the number of basic authentication processes can be determined by dividing the number of workstations using the Getbusi system by 5. The recommended minimum number basic authentication processes is 5, which corresponds to 25 workstations. The maximum recommended value for basic authentication processes is 50 (450 workstations).

1. In the **Basic authentication processes** field, enter the number of Basic authentication processes to be run on your Getbusi system.

2. Click the grey **Apply** button to save your settings.

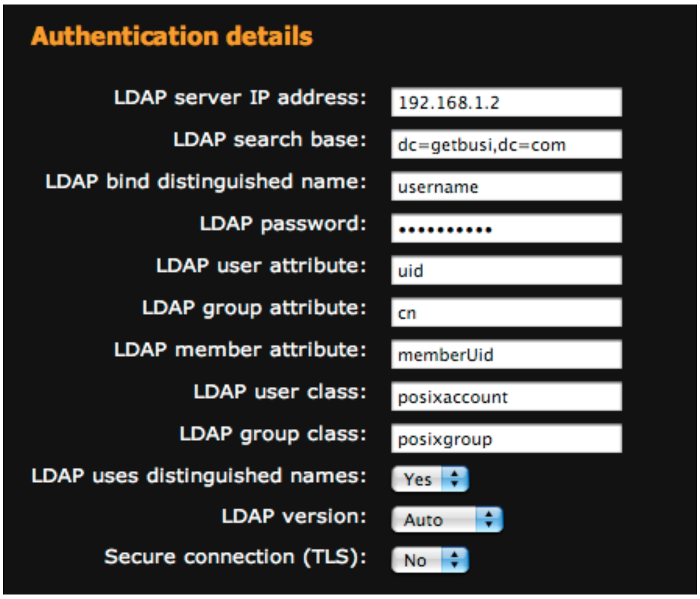
3. At the top of the screen, you will see an indication that the system is processing your parameters. When the processing is complete, click the grey **Next** button in the upper right-hand corner of your browser window.

You have now finished configuring authentication for LDAP (POSIX, Mac OS X or Novell eDirectory only). Proceed to the section entitled: Setting Group Policies.

3.6.4 LDAP Authentication (Other)

Use the **LDAP - Other** authentication method for LDAP implementations that are neither based upon OpenLDAP nor are POSIX compliant.

3.6.4.1 Authentication Details



Authentication details

LDAP server IP address:	192.168.1.2
LDAP search base:	dc=getbusi,dc=com
LDAP bind distinguished name:	username
LDAP password:	••••••••••
LDAP user attribute:	uid
LDAP group attribute:	cn
LDAP member attribute:	memberUid
LDAP user class:	posixaccount
LDAP group class:	posixgroup
LDAP uses distinguished names:	Yes
LDAP version:	Auto
Secure connection (TLS):	No

Figure 7

1. In the **LDAP server IP address** field, enter the IP address of the LDAP server against which you are authenticating.

2. In the **LDAP search base**, enter the search base for your LDAP directory. The search base defines the location in the directory from which the LDAP search begins.

3. In the **LDAP bind distinguished name** field, enter the user name to connect to your LDAP services with. This may be left blank if your LDAP server allows anonymous binding.

4. In the **LDAP password** field, enter the password corresponding with the username you are using to connect to your LDAP services. Leave this blank if you are using anonymous binding in step 3.

5. In the **LDAP user attribute** field, enter the attribute identifying a user name within the organisational unit containing users.

6. In the **LDAP group attribute** field, enter the attribute identifying a group name within the organisational unit containing groups.

7. In the **LDAP member attribute** field, enter the attribute identifying a user as being part of a group within the organisational unit containing users.

8. In the **LDAP user class** field, enter the name identifying the class of organisational unit representing users.

9. In the **LDAP uses distinguished names** drop-down list, select *yes* if a group member uses their distinguished name to identify them as part of a group.

10. In the **LDAP version** drop-down list, select set this to the version of LDAP running on your authentication server, or leave this set to *Auto*. Not all versions of LDAP require this to be set.

11. In the **Secure connection (TLS)** drop-down list, select *Yes* if you use TLS (Transport Layer Security) when authenticating against your LDAP services.

3.6.4.2 Authentication Processes

The following determines the number of basic authentication processes to run on the Getbusi server. These authentication processes allow client access to Internet resources.

The calculation to establish the number of basic authentication processes can be determined by dividing the number of workstations using the Getbusi system by 5. The recommended minimum number basic authentication processes is 5, which corresponds to 25 workstations. The maximum recommended value for basic authentication processes is 50 (450 workstations).

1. In the **Basic authentication processes** field, enter the number of Basic authentication processes to be run on your Getbusi system.

2. Click the grey **Apply** button to save your settings.

3. At the top of the screen, you will see an indication that the system is processing your parameters. When the processing is complete, click the grey **Next** button in the upper right-hand corner of your browser window.

4. You have now finished configuring authentication for **LDAP - Other**. Proceed to the section entitled: Setting Group Policies.

3.6.5 LDAP - Getbusi

For LDAP - Getbusi, the only value that needs to be set is the number of basic authentication processes. These authentication processes allow client access to Internet resources.

The calculation to establish the number of basic authentication processes can be determined by dividing the number of workstations using the Getbusi system by 5. The recommended minimum number basic authentication processes is 5, which corresponds to 25 workstations. The maximum recommended value for basic authentication processes is 50 (450 workstations).

1. In the **Basic authentication processes** field, enter the number of Basic authentication processes to be run on your Getbusi system.

2. Click the grey **Apply** button to save your settings.

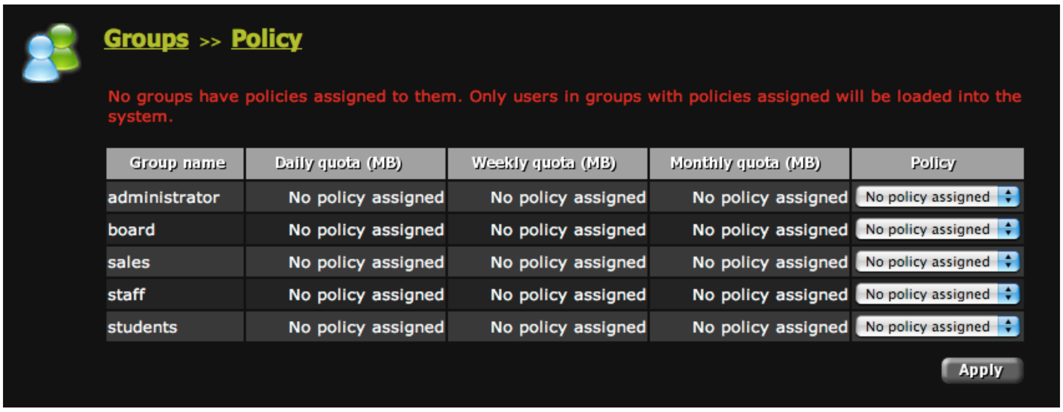
3. At the top of the screen, you will see an indication that the system is processing your parameters. When the processing is complete, click the grey **Next** button in the upper right-hand corner of your browser window.

You have now finished configuring authentication for **LDAP - Getbusi**. Proceed to the section entitled: Setting Group Policies.

3.7 Setting Group Policies

The Group Policy screen allows you to assign specific policies that govern Internet access by group. The groups are retrieved from your organisation's authentication server. The type of organisation you previously selected in the Organisation Categorisation section determined the set of default policies. At this stage of your setup, you may not create custom policies, but you may do so once the initial setup is complete.

Figure 8 depicts a table similar to the one you should see in your web browser window. By default, no policies are assigned to your groups.



No groups have policies assigned to them. Only users in groups with policies assigned will be loaded into the system.

Group name	Daily quota (MB)	Weekly quota (MB)	Monthly quota (MB)	Policy
administrator	No policy assigned	No policy assigned	No policy assigned	No policy assigned
board	No policy assigned	No policy assigned	No policy assigned	No policy assigned
sales	No policy assigned	No policy assigned	No policy assigned	No policy assigned
staff	No policy assigned	No policy assigned	No policy assigned	No policy assigned
students	No policy assigned	No policy assigned	No policy assigned	No policy assigned

Figure 8

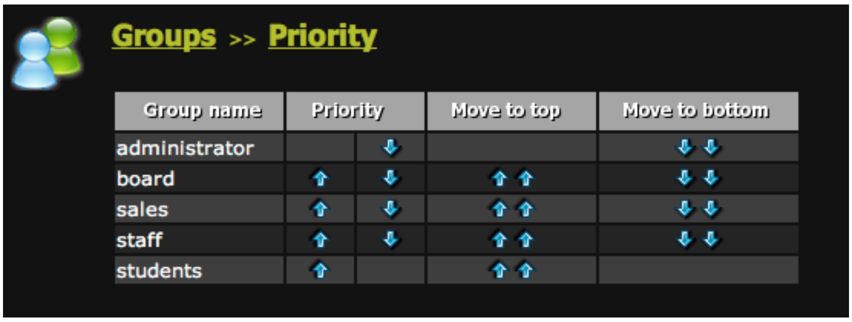
- The groups retrieved from your Authentication server are listed in the left-most column of the table, under the heading: **Group name**.
- The available policies are selectable from each group's corresponding drop-down menu in the right-most column of the table, under the heading: **Policy**.
- Select a policy for a group and click on the grey **Apply** button to apply the policy to the group. The table will update to show the effect of the selected policy on the quotas for that group. You may apply policies to multiple groups before clicking on the **Apply** button, or you may apply policies individually.
- If a group has no policy applied to it, users contained within that group will be denied access to the Internet.
- Once you have finished applying policies to groups, click on the grey **Next** button in the upper right-hand corner of your browser window.

You have now finished assigning your Policies to your Groups. Proceed to the section entitled: Setting Group Priorities

3.8 Setting Group Priorities

The Group Priority screen allows you to set the priority for groups. Group priorities are only used when users belong to multiple groups. When a user belongs to multiple groups, the user will be granted access based on the policy corresponding to the group with the highest priority.

For example, *fred* belongs to the *staff* group and the *board* group. If the *staff* group has daily, weekly and monthly quotas set, but the *board* group has no quotas set, and the *board* group has a higher priority than the *staff* group, then *fred* will have no quotas on his Internet access. However, if the *staff* group is given a higher priority, then *fred* will have the same Internet access quotas as other members of the *staff* group.



Groups >> Priority

Group name	Priority		Move to top	Move to bottom
administrator		↓		↓↓
board	↑	↓	↑↑	↓↓
sales	↑	↓	↑↑	↓↓
staff	↑	↓	↑↑	↓↓
students	↑		↑↑	

Figure 9

Figure 9 shows the Group Priority screen. Groups are ordered in priority from top to bottom, with the top being the highest priority, and the bottom being the lowest. The arrows in a group's row indicate the direction the group will move when clicked. Single arrows move a group one step. The double arrows will move the group to either the top or bottom of the table.

Please note that the Group Priority screen will not give one group priority in accessing Internet resources over another. It is only used to determine which policy applies to users when they belong to multiple groups.

When you have finished prioritising your groups, click on the grey **Next** button in the upper right-hand corner of your screen. You will be directed back to the Authentication screen to continue the configuration process.

3.9 Loading Users

To load users from your Authentication system into Getbusi's database, click on the grey **Load** button at the bottom of the Authentication screen. When you click on the grey **Load** button, the screen will refresh and an activity indicator will indicate that the system is loading your users. When the activity indicator displays a *Complete* message, click on the grey **Next** button in the upper right-hand corner of your browser window.

Please note: Usernames with characters other than those listed below will not be recognised by Getbusi and therefore not loaded into the database.

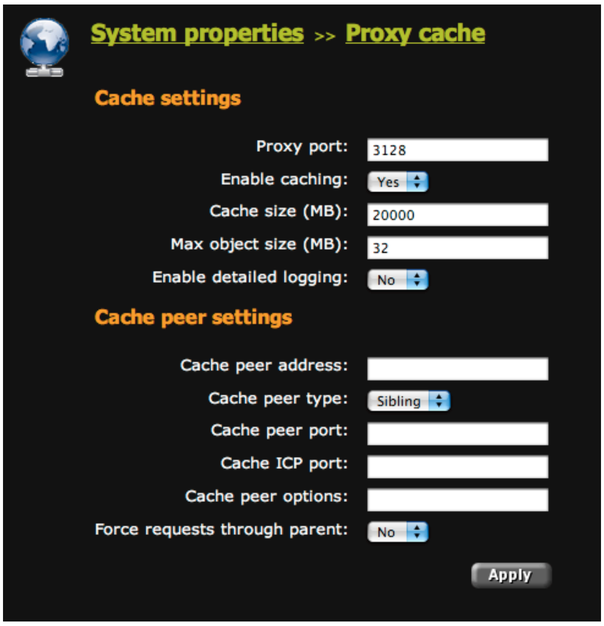
Allowable Username Characters					
-	.	_	a – z	A – Z	0 – 9

3.10 Proxy Cache Settings

You Getbusi server is a caching proxy. This means that whenever possible, it will cache (store) previously served requests so that subsequent requests for that resource will be served from it's cache, rather than retrieving the request from the original source. This can greatly improve your Internet performance while reducing your upstream bandwidth usage.

The Proxy Cache screen allows you to set parameters associated for the proxy. The screen is split into two sections: **Cache Settings** and **Cache Peer Settings**. **Cache Settings** are used to tune the actual proxy cache, and may affect the performance of your Getbusi server.

For those who have a separate external upstream proxy, provided by either your organisation or your Internet Service Provider, the **Cache Peer Settings** allow you to configure the Getbusi system so that it uses that external upstream proxy for access to Internet resources.



System properties >> Proxy cache

Cache settings

Proxy port: 3128
Enable caching: Yes
Cache size (MB): 20000
Max object size (MB): 32
Enable detailed logging: No

Cache peer settings

Cache peer address:
Cache peer type: Sibling
Cache peer port:
Cache ICP port:
Cache peer options:
Force requests through parent: No

Figure 10

3.10.1 Cache Settings

- The **Proxy port** field allows you to set the port on which your Getbusi system serves requests. The default port is *3128*, but some have a preference for *8080*. This port is the one you will also specify in your browser settings when setting up browsers to use your Getbusi system for Internet access.
- The **Enable caching** drop-down menu allows you to enable or disable caching. The default is to enable caching. Set this to *No* if you don't want your Getbusi system to cache requests.
- The **Cache size (MB)** field allows you to set the amount of disk space (in megabytes) the proxy cache uses. It is recommended that you restrict this value to no more than half of your hard disk drive's capacity, unless you have a dedicated hard drive for your proxy cache. In that event, it is recommended that you set this to no more than 80% of your hard disk drive's capacity. The default setting for this field is 20000 MB (20 GB).
- The **Max object size (MB)** field allows you to set the maximum file size that your Getbusi system will cache. If a file exceeds this setting, your Getbusi will not cache the file. The minimum setting for this field is 4 MB, and the default is 32 MB.
- The **Enable detailed logging** drop-down menu allows you to enable or disable detailed logging of the proxy cache subsystem. This field is for troubleshooting, and should be left at the default value of *No*.

3.10.2 Cache Peer Settings

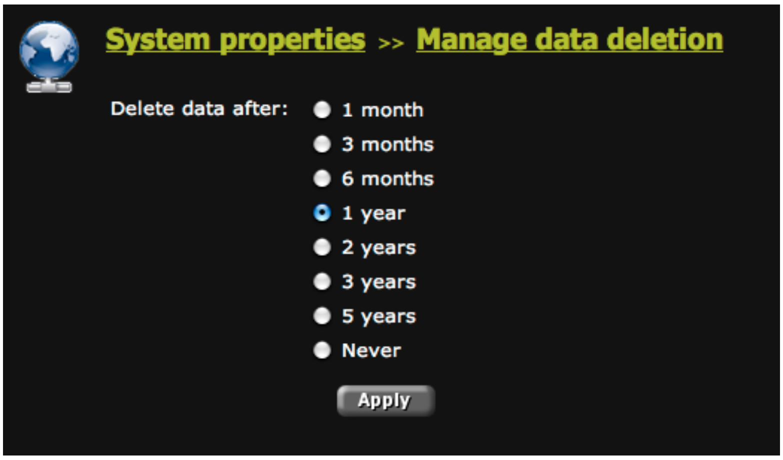
- The **Cache peer address** field allows you to identify an external proxy with which to peer. If you wish to peer with an external proxy, enter its IP address in this field. Leave blank if you are not peering.
- The **Cache peer type** drop-down list allows you to select the type of peering to implement. Select *Parent* if you are peering to a parent (or upstream) proxy to gain access to Internet resources. Select *Sibling* if your proxy is working in tandem with another sibling caching proxy. Note that non-ICP neighbours should be specified as a *Parent*.
- The **Cache peer port** field should be set to the port number on which your peering proxy (if set) is listening.
- The **Cache ICP port** field should be set if your Getbusi proxy is working co-operatively with other peers. If your Getbusi proxy is not working cooperatively with other peers, it should be set to *0.* The standard port number for ICP is *3130*.
- The **Cache peer options** field may take multiple, comma-separated values. Some of the options are:
  - If your upstream proxy requires proxy authentication from a single username and password, enter: *login=username:password*. Please note that if your username contains spaces, use the URL escape: *%20* to represent the space. For example, if the username is: *john smith*, then the value would be: *login=john%20smith:password*.
  - If each of your users need to individually authenticate against your upstream proxy, then enter: *login=PASS*. Please note that this will expose your user's password to the upstream proxy. Please use with caution.
  - If you need to pass just the username to your upstream proxy, but with a fixed password for all users, enter: *login=*:password*. This scenario is meant to be used when your peer is in another administrative domain, but still needs to identify each user. The asterisks may optionally be followed by extra information which is added to the username, helping identify the Getbusi server to the peer.
  - If you wish to prevent user's bandwidth restrictions affecting the connection between the Getbusi server and the upstream proxy, enter: *no-delay*.
  - If the upstream proxy is not being used with ICP, enter: *no-query* to prevent ICP queries from occurring.
  - If you do not wish to locally cache objects that are already in the upstream proxy's cache (to prevent duplication), then enter: *proxy-only.*
  - If you wish to limit the number of connections that the Getbusi system will open with the upstream proxy, enter: *max-conn*.
- The **Force requests through parent** drop-down list allows you to select if all requests should go through the upstream proxy, or just requests that can be cached. Some requests, like search engine results cannot be cached. If you set this to *No*, then non-cacheable requests will bypass the upstream proxy, improving performance. If you set this to *Yes*, then all requests, including non-cacheable requests, will utilise the upstream proxy.

Once you have configured your cache and cache peer settings properly, click on the grey **Apply** button to save your settings. To proceed, click the grey **Next** button in the upper right-hand corner of your browser window.

3.11 Manage Data Deletion Settings

Your Getbusi system logs all of the Internet activity for all of your users. Over time, this data grows to a considerable size and could become the largest consumer of disk space on your system. Additionally, as your database grows, reporting functions could take longer to generate, and the overall performance of your Getbusi system could eventually be impacted.

You may manage your data by choosing to delete it after a period of time. Remember that unless you keep your data backups, once the data is deleted from the database, it is irretrievable. The default is to retain data for one year.



System properties >> Manage data deletion

Delete data after:
○ 1 month
○ 3 months
○ 6 months
● 1 year
○ 2 years
○ 3 years
○ 5 years
○ Never

Figure 11

- Select the radio button that corresponds with the amount of data you wish to retain on your system.
- Click on the grey **Apply** button to save your setting.
- To proceed, click the grey **Next** button in the upper right-hand corner of your browser window.

You have now finished configuring your Data Deletion settings. Proceed to the section entitled: Custom Message Settings

3.12 Custom Messages Settings

Certain events like users being over quota, or pages getting blocked by filters, will generate redirection error messages informing the user of the event. You may customise these messages to your preference. On the **Custom Messages** page, a list of all of the redirection error messages are displayed, each with a corresponding text box containing the default message (if any). The following list describes the name of the error message, and the event that would trigger it:

- **Filtered Message**: This message appears if there is an attempt to view a site that is being blocked by any of the filters applied to a policy.
- **Whitelist Message**: For policies being implemented to only allow access to sites in a local good list, this message appears when there is an attempt to view a site not specifically approved by the local good list.
- **Banned File Type Message**: This message appears if there is an attempt to download a file that has been banned by a policy.
- **Over Quota Message**: For policies that implement quotas, this message appears when a user exceeds either their daily, weekly or monthly quota.
- **Computer Denied Message**: For machine-based policies, this message appears when a machine has been denied access to Internet resources.
- **Computer Over Quota Message**: For machine-based policies, this message appears when a machine has exceeded its daily, weekly or monthly quota.

To customise any of the aforementioned errors, type the message you wish to be displayed when that error is triggered in the error's corresponding text box. Click on the grey **Apply** button that corresponds to the error and text box. You may also click on the corresponding grey **Test** button, to generate a test of the message. When you click the **Test** button, a new browser window will appear with the text for that error.

When you have completed customising your error messages, click on the grey **Next** button located in the upper right-hand corner of your browser window.

You have now finished configuring your Custom Message settings. Proceed to the section entitled: Miscellaneous settings

3.13 Miscellaneous Settings

The miscellaneous settings page allows you to set some general settings for your Getbusi system.

3.13.1 General Details

- The **Site Name** field allows you to set a name for your Getbusi system that will appear on email feedback reports. Although you may simply set this to the hostname of your Getbusi server, you may also set this to any name you wish.
- The **Report Email Address** field allows you to designate an email address to which you deliver email reports. You should set this to a valid email address that you check regularly, as your Getbusi system will email you reports about its health and other status updates.
- The **SMTP (Email) Server** field allows you to set the IP address of your email server. This is the email server that the Getbusi will deliver email through. This could be your internal email server, or that of your ISP.
- The **Process reporting data when the system load is** allows you to customise the load threshold for processing data. If the load threshold is exceeded, your system will delay writing Internet usage and quota usage to the database until the system load drops back below the threshold. This feature allows the system to cope with temporary spikes in load during periods of high usage. The default and recommended value is *2*.
- The **System Scale** drop-down list allows you to customise which unit of measurement you wish to use for reporting. The scale may be set to either *Kilobytes* (KB), or *Megabytes* (MB).
- The **Default Price** field allows you to set a price per megabyte for data being downloaded through your Getbusi system. By default, this price is set to $0.00. This setting allows you to bill and credit your users, as well as issue tickets for users wishing to purchase bandwidth.

To apply your settings, click the corresponding grey **Apply** button at the end of the **General Details** section.

3.13.2 Filtering

This section allows Getbusi Advance customers to select a Filtering Type. If you are not using Getbusi Advance please proceed to section 3.13.2.1: Getbusi Managed Filters.

The drop-down list allows you to select from three filtering types, each incorporating real-time website classification. You also have the option of using the Managed Filters maintained by Getbusi (detailed in the following section).

1. The **Getbusi Advance** option will utilise a local cache of previously classified websites in conjunction with locally managed Good / Bad / Expression lists. When an unclassified website is accessed your Getbusi machine will automatically seek a category from an upstream Category Name Server, this action is seamless within the request.
2. The **On-demand Filters** option will ignore the local cache of previously classified websites as well as the locally managed Good / Bad / Expression lists and categorise all websites on-the-fly. Each time a request is made through the Getbusi proxy, the website will be seamlessly categorised against an upstream Category Name Server.
3. The **URL Classification Only** option will disable the redirection of Users. Instead, every request will be categorised and listed in the Prohibited Attempts report. This option is for those that wish to sacrifice access control for classification of all traffic.

3.13.2.1 Getbusi Managed Filters

In order to keep your filter lists up-to-date, your Getbusi system can automatically download managed filters from the Getbusi website. These filter lists are constantly being updated by Getbusi, so it is highly recommended that you do not disable this feature.

- The **Update Time** drop-down menus allow you to set the time of day that you want your Getbusi system to retrieve managed filters. Your Getbusi system will download the latest managed filters every day at the time you set.
- The **Do not update manage filters** check-box allows you to disable the automatic managed filters update feature. This is not recommended.
- The **Update managed filters now** button allows you to perform a one-off, unscheduled update of managed filters.
- The **Allow Getbusi to classify the sites visited (beta)** check-box enables a feature (currently in beta testing) that sends a weekly report to Getbusi. The report contains a full listing of all visited domains and a listing of all of the manually blocked and unblocked sites on your system. If any of the domains your users have visited have not been classified, Getbusi staff will categorise the domains. Getbusi does not record where the domain information was sent from or which user made the request. This feature helps us improve our domain classification and filter lists. The collective gathering of domain information provides a greater level of domain classification and improved reports on Internet usage for our clients on their Getbusi systems. To enable this feature, click on the check-box. This feature is disabled by default.

To apply your settings, click the corresponding grey Apply button at the end of the **Filtering** section.

3.13.2.2 Redirection Processes

The Redirection processes field allows you to set the number of redirection processes. These processes are used to check client requests against filtering policies. You should configure one redirection process for every 10 workstations simultaneously using the Getbusi system. The minimum recommended number of redirection processes is *5*, and the maximum is *80*.

Note: Getbusi Advance's real-time filtering will increase the load on the Redirection Processes. If you are using Getbusi Advance you should configure 1 process for every 5 workstatisons simultaneously using the Getbusi system.

3.13.3 Changing Your Administrative Password

Your default Getbusi admin password is *test*. We highly recommend you change this password, since anyone with the admin password can reconfigure your Getbusi system.

1. In the **Old Password** field, enter the existing admin password. By default, this is *test*.
2. In the **New Password** field, enter a secure password for your admin user.
3. In the **Confirm Password** field, re-enter the password from step 2.

To apply your settings, click the corresponding grey **Apply** button at the end of the **Admin Password** section.

When you have finished, click on the grey **Next** button located in the upper right-hand corner of your browser window.

3.14 System and Network Status

The system and network status page allows you to check the server's health and ensure that the network and system services are running as expected. The status page contains a number of sections, network checks, file system checks, system load checks and authentication checks.

3.14.1 Network Checks

The network check section contains an area to add network checks, and an area to view the status of the configured network checks. By default, there are no network checks configured in the system. Network checks allow you to check to make sure that your Getbusi server is properly connected to your network. It can also help you determine if your network is functioning properly.

3.14.1.1 Add Network Check

Network checks utilise the ping utility to see if there is network access to the configured target host. You can add as many network checks as you wish, but there are three recommended ones.

The first recommended network check is to identify a known, fixed-ip host on your local area network, like your default gateway, a mail server or a file server. This test tells you if your Getbusi machine has access to your local area network.

The second recommended network check is to identify a known, fixed-ip host outside of your network. A good candidate might be your next-hop router outside of your network, like your ISP's router. In order for this to work, your firewall will need to allow outbound ICMP packets.

The third recommended network check is to identify a known website, like google, which will respond to ping requests. This not only tests your external Internet access, but also tests to ensure that DNS is working properly.

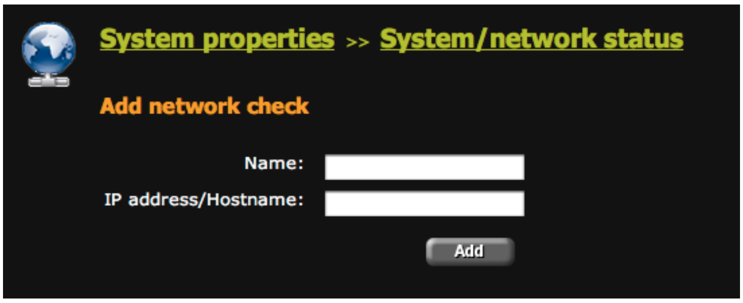


Figure 12

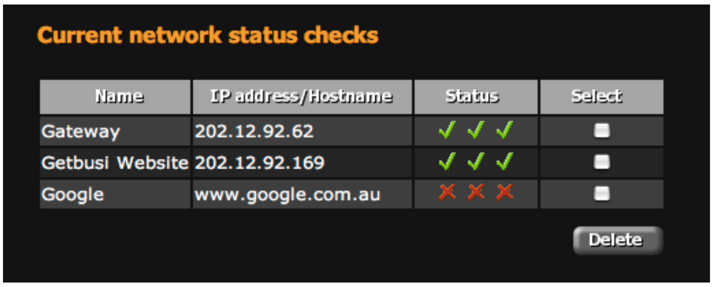
1. Enter a unique name for the network check in the **Name** field.

2. Enter either an IP address, a fully-qualified hostname, or a URL in the **IP address/Hostname** field.

3. Click the grey **Add** button to add your network check. Repeat steps 1 - 3 to add additional network checks.

3.14.1.2 Viewing the Status of Network Checks

The **Current network status checks** area shows you the status of all configured network checks in your Getbusi system. Green checks indicate a successful check. Red x's indicate a failed network check.



Current network status checks

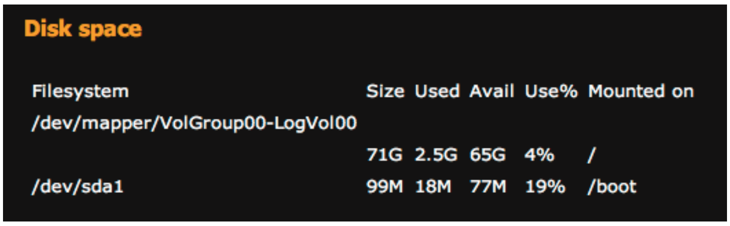
Name	IP address/Hostname	Status	Select
Gateway	202.12.92.62	✓ ✓ ✓	□
Getbusi Website	202.12.92.169	✓ ✓ ✓	□
Google	www.google.com.au	✗ ✗ ✗	□

Figure 13

To delete a configured network check, click in the check-box that corresponds with the network check you wish to delete from the system and click the grey **Delete** button. You may delete more than one network check at a time. When the page refreshes, the **Current network status checks** status area should no longer show the deleted network check(s).

3.14.2 Disk Space

The **Disk space** section provides you with information about the amount of space being used on your hard disk(s). This information can help with decisions determining your data retention policy or how much disk space to configure for your cache. We recommend never allowing your partitions to fill beyond 90% of their capacity.



Disk space

```
Filesystem                          Size  Used  Avail  Use%  Mounted on
/dev/mapper/VolGroup00-LogVol00
                                    71G   2.5G  65G    4%    /
/dev/sda1                           99M   18M   77M    19%   /boot
```

Figure 14

Figure 14 shows a sample of a disk space check. The only partition of interest is the root, or "/" partition. This is the partition that would contain the proxy cache and the database. If you configured your system to have the database on a separate partition, it would appear on a separate line.

3.14.3 System Load

The **System Load** section displays the number of waiting processes for the last minute, 5 minutes and 15 minutes. Under normal conditions, the 5 and 15 minute values should remain under 3. If you have a dual processor or Hyper-Threading processor, this value should remain under 6. If you are running reports, or are in the process of reconfiguring the system, these values may rise above recommended levels for short periods of time. You will also see short bursts of high load in times of high usage.

3.14.4 Authentication Groups

The **Authentication Groups** section allows you to see if the system can retrieve group information from the authentication system being used. An empty table is indicative of communication problems between your Getbusi server and the authentication system.

3.14.5 External Network Connections

The **External Network Connections** section allows you to test various external connections. These checks not only test that external connections are available, but that they're allowed through your firewall. To run external network connection tests, click on the grey **Test** button. It can often take a short amount of time to return the results of the tests. The returned values show the result of testing:

- DNS resolution: DNS is required to resolve names (like www.google.com) to IP addresses. Without DNS, you will not be able to access external websites by commonly known names.
- RSYNC access: RSYNC is required if you wish to receive managed list updates from Getbusi.
- FTP access: FTP is required if you wish to be able to automatically update your system software.
- HTTP access: HTTP is required for access to regular web sites on the Internet
- HTTPS access: HTTPS is required for access to secure web sites on the Internet
- SSH access (only outbound is required): SSH access is used by Getbusi support to help you troubleshoot problems.
- FILTERING access: This protocol is required for Getbusi Advance systems to communicate with the upstream Category Name Servers which provide on-the-fly classification of websites.
- SMTP access: SMTP is required to allow your Getbusi server to send email reports.
- NTP access: NTP is required to keep your system's clock properly synchronised. Disallowing NTP access will adversely affect Time-based Policies because your system's clock can become increasingly inaccurate over time.

3.15 Updates

The **Updates** page allows you to view and install available updates for your Getbusi system and kernel.

To check for updates, click the grey **View** button. If there are system updates available, they will be listed under the **System updates** section. If there are kernel updates available, they will be listed under the **Kernel updates** section.

If there are available updates, you may configure your system to update itself at night. In the drop-down menu that corresponds with *Update system tonight*, select *yes* if you wish to have your system update overnight and click the grey **Apply** button. If you select *no*, then your system will not update itself.

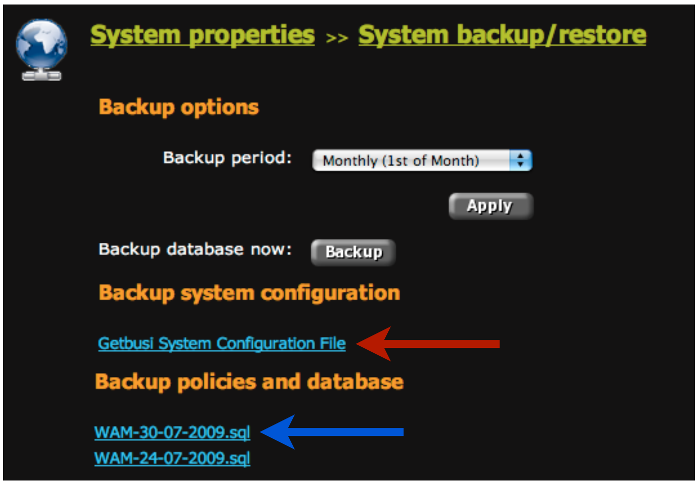
You may choose to manually update your system by clicking on the grey **Update** button. It is generally recommended that you choose to update your system overnight. If you want to update your system immediately, then you should choose a time when your system is not experiencing high load.

3.16 System Backup and Restore

The **System backup/restore** page allows you to back up or restore two critical components of your Getbusi system: your system configuration and your system's database.

3.16.1 Backing Up your Database

You may configure the system to automatically backup your database on a pre-determined schedule, or you may manually backup your system.


System properties >> System backup/restore
Backup options
Apply
Backup database now:
Backup
Backup system configuration
Getbusi System Configuration File
Backup policies and database
WAM-30-07-2009.sql
WAM-24-07-2009.sql

Backup period: Monthly (1st of Month)

Figure 15

- To configure your database backup frequency, select the frequency in the drop-down menu, and click the grey **Apply** button.
- To perform a one-time on-demand backup of your database, click on the grey **Backup** button. It is important to not backup your database during periods of high activity or load.
- To download your Getbusi configuration file to your desktop machine, click the **Getbusi System Configuration File** link. The red arrow in Figure 15 shows where the link is located.
- To download a database backup to your desktop, click one of the **WAM-<date>.sql** files. The blue arrow in Figure 15 shows where those links are located. Note that there will be up to five links, each downloading the backup that was made on the date indicated in the link.

3.16.2 Restoring Your Getbusi Server

To restore either your Getbusi server configuration or your database, click on the grey **Browse** button and navigate to where you've saved the backups on your local system. Click on the grey **Import** button to import the file. The system will automatically restore the configuration file or database.

3.17 Finishing the Initial Setup

After you have configured your backup policy, click on the grey **Next** button in the upper right-hand corner of your browser window. You will be redirected to the main Getbusi Administration Console login screen. Login with a username of: admin, and with the password you set in the section entitled, Changing Your Administrative Password. If you did not change your administrative password in that section, the default password is: test.

4 Getbusi Administration Concepts

The Getbusi system allows you to manage Internet access for groups of users, groups of computers, or individual users. For the purposes of clarity, **Groups** refer only to groups of users, and not groups of computers. Groups of computers are referred to as **Computer Groups**.

The Getbusi system extracts group and user information from your existing authentication infrastructure. You may not create a **Group** or groups of **Users** with the Getbusi system. They must already exist in your authentication infrastructure. You may however, create **Computer Groups** within the Getbusi system, and assign computers to them by inputting individual IP addresses, or IP address ranges.

A **Policy** controls the rules of Internet access for groups, users and computer groups. Policies may control:

- Internet access - if Internet access is allowed or prohibited.
- Access filtering - determining which websites may be accessed, and which are prohibited. Access may be controlled by managed filter lists, custom filter lists, expression filters or any combination thereof.
- Filetype filtering - determining which file types may be accessed or downloaded.
- Quotas - determining how much bandwidth may be consumed on a daily, weekly and monthly basis, and if access is to be shaped or disabled after those limits are reached.
- Pricing - determining the price per megabyte for downloads.
- Users' reporting and administration privileges.

A policy may be applied to individual users, groups and computer groups. Each may have a single policy applied at any one time. Even if a user belongs to a group which has a specific policy, you may override the user's group policy and apply a different policy for that individual user. If a user belongs to multiple groups, and the user does not have a specific policy, then the policy for that user will be determined by the group with the highest priority, as described in the section entitled, Setting Group Priorities.

If you wish to have multiple policies applied to a group based on time, you may create **Time-Based Policies** for groups. Only groups may have time-based policies. Users which have individual policies applied to them are not affected by their group's time-based policy.

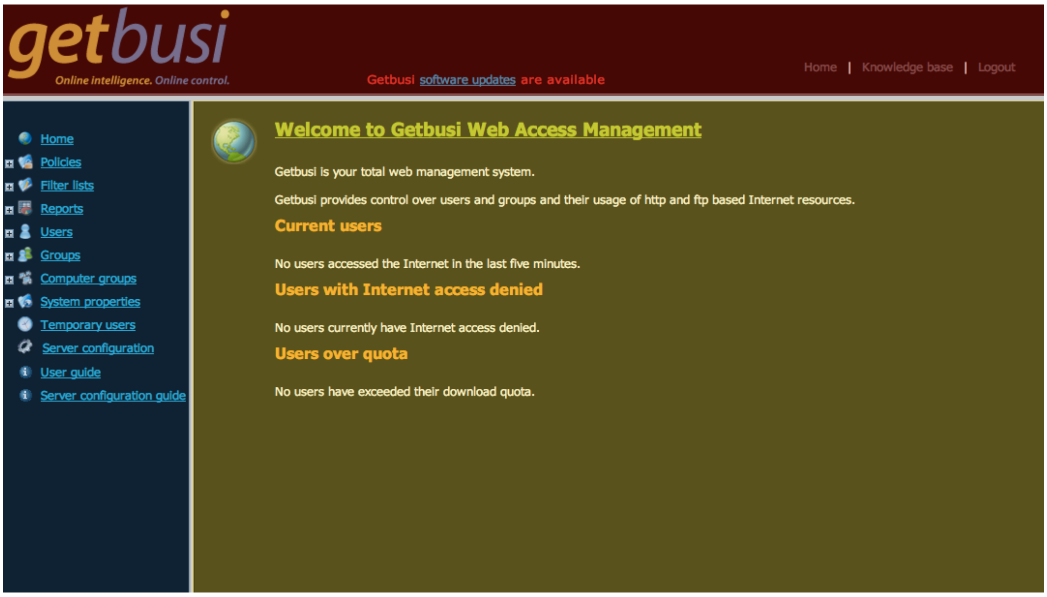
Computer group policies override group and user policies. If you implement computer groups in addition to user groups, and a user is accessing Internet resources from a computer belonging to a computer group, then the policy applied to the computer group will override any policies applied to the user or the user's group(s).

The Getbusi system implements a "deny unless allowed" strategy, which means that in the absence of a policy specifically allowing Internet access, the Getbusi system will deny all requests. This means that if a user is not known by the Getbusi system, and that user is accessing from a computer that has not been given access, then neither the user nor the computer will be allowed access to Internet resources.

Important: Your Getbusi system cannot manage Internet access if the computers on your network are not configured to use Getbusi as a proxy. If computers on your network can bypass the Getbusi system and are allowed to have direct access to the Internet through your firewall, then the Getbusi system cannot manage your organisation's Internet access. For more information, see the section entitled "Network Configuration" of your Installation and Server Configuration Guide on how to configure your network firewall.

5 The Getbusi Interface

The Getbusi administration console interface is designed for ease of use. Figure 16 shows the main page of the administration console.


getbusi
Online intelligence. Online control.
Getbusi software updates are available
Home | Knowledge base | Logout
Home
Policies
Filter lists
Reports
Users
Groups
Computer groups
System properties
Temporary users
Server configuration
User guide
Server configuration guide

Welcome to Getbusi Web Access Management

Getbusi is your total web management system.

Getbusi provides control over users and groups and their usage of http and ftp based Internet resources.

Current users

No users accessed the Internet in the last five minutes.

Users with Internet access denied

No users currently have Internet access denied.

Users over quota

No users have exceeded their download quota.

Figure 16

The console is split into 3 areas. The area shaded in red is the header pane. The header pane has links to *Home*, *Knowledge Base* and *Logout.* The *Home* link will take you to the initial page after logging into the administration console. The *Knowledge Base* link will open a new browser window and directs you to the Getbusi website. The *Logout* link logs you out of the console. The header pane will also notify if new software updates are available.

The area shaded in blue is the navigation pane. The navigation pane allows you to easily navigate to different functional areas of the administration console. You can expand the different headings in the navigation pane for quick access subsections of the functional areas by clicking on the ⊞ icon next to each functional area heading.

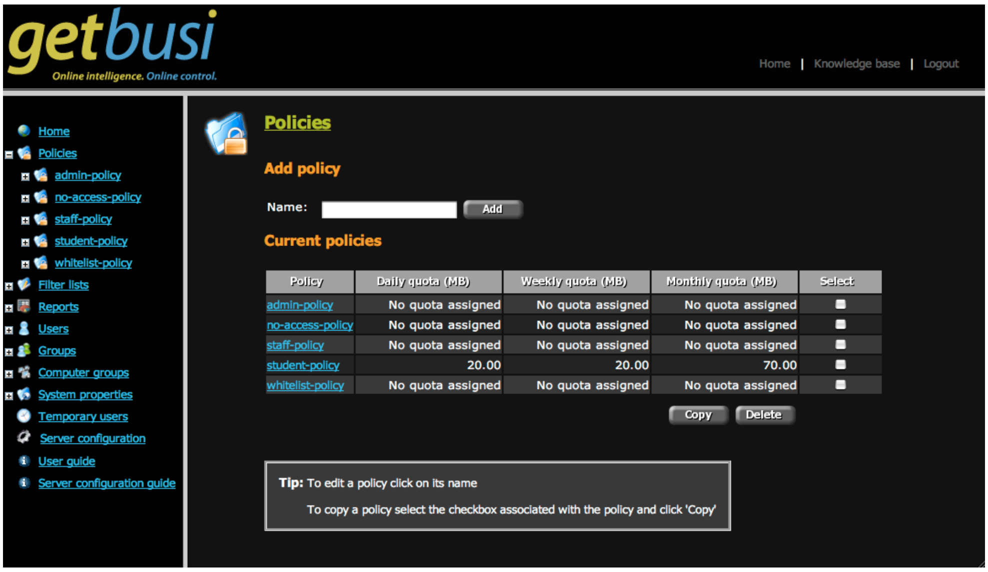
The area shaded in yellow is the configuration pane. The configuration pane will present configuration options depending on which functional area is selected. If the functional area has multiple configuration options, the configuration pane will present tabs along the top to aid in navigation.

When configuring Getbusi, each configurable item will have its own corresponding **Apply** button to apply that configuration setting. When reconfiguring the system, it can take several seconds before the changes come into effect. If a configuration change takes a long time, the Getbusi console will provide feedback. If your system is under high load, you may wish to delay any configuration changes. Many configuration changes cause the system load to rise considerably.

6 Policies

Figure 17 shows the main Policies screen. From this screen, you may configure existing policies or add a new policy to the system. Note that you have direct access to each of your existing policies in the navigation pane.

Each existing policy within your system will be displayed in the *Current Policies* table. The table will also identify any quotas associated with the policy. Quotas are displayed in megabytes (MB).



Policy	Daily quota (MB)	Weekly quota (MB)	Monthly quota (MB)	Select
admin-policy	No quota assigned	No quota assigned	No quota assigned	□
no-access-policy	No quota assigned	No quota assigned	No quota assigned	□
staff-policy	No quota assigned	No quota assigned	No quota assigned	□
student-policy	20.00	20.00	70.00	□
whitelist-policy	No quota assigned	No quota assigned	No quota assigned	□

Tip: To edit a policy click on its name

To copy a policy select the checkbox associated with the policy and click 'Copy'

Figure 17

6.1 Adding, Copying and Deleting Policies

- To add a new policy, type the policy name in the *Name* text box, and click the grey **Add** button. When the page refreshes, you should see your new policy in the Policy table.
- To delete an existing policy, click on its associated check-box in the *Select* column of the table and then click on the grey **Delete** button. You may delete multiple policies simultaneously. When the page refreshes, you should no longer see the policy/policies you've deleted.
- To copy an existing policy, click on its associated check-box in the *Select* column of the table and then click on the grey **Copy** button. You may copy multiple policies simultaneously. When the page refreshes, you should see the copy/copies of the policies you've duplicated. The copied policy/policies will be named after the original policy and appended with "*-1*".

6.2 Configuring Policies

To configure a policy, either click on the policy's name in the *Current Policies* table. If you have expanded the policies heading in the navigation bar, you can also navigate directly to a policy from the navigation bar.

As previously stated, policies control the rules of Internet access for groups, users and computer groups. Any changes to a policy will affect all entities to which the policy is applied. The Getbusi administrator can choose to apply the default policies, customise any policy in the system, or create their own customised policies.

All policies have the following configurable options and are accessible from the grey tabs located at the top of the configuration pane when a specific policy is selected:

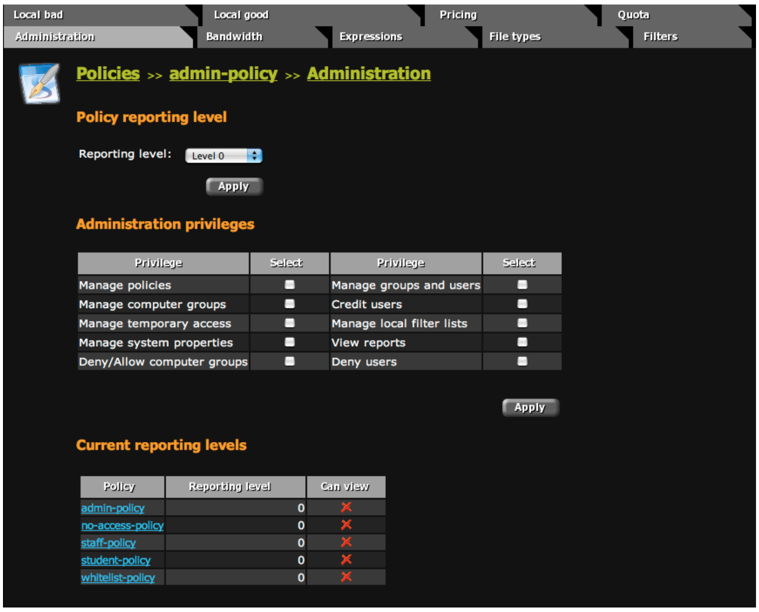
- **Administration**: Allows the delegation of administrative privileges to users within that policy. Additionally, users within the policy may be granted access to view certain reports.
- **Bandwidth**: Configure and apply bandwidth restrictions on a policy.
- **Expressions**: Create and apply URL filters based on expressions.
- **File Types**: Modify and apply filters based on file-type.
- **Filters**: Apply Getbusi managed filters, or ban all access except for sites permitted in a *Local Good* list.
- **Local Bad**: Create and apply filters banning sites.
- **Local Good**: Create and apply filters allowing sites.
- **Pricing**: Set a price per megabyte (MB) for all users of the policy.
- **Quota**: Configure and enforce daily, weekly or monthly quotas; maximum download size restrictions; and enable or disable Internet access for a policy.

6.2.1 Administration

Figure 18 shows the **Administration** option for a policy. From this screen, you may configure administrative access for users of the selected policy, as well as give access to certain reports from the Getbusi system.

The Getbusi administrator has unrestricted access to all management areas of the Getbusi administration console, granted through the *admin* account. Only the Getbusi administrator, through the *admin* account, may delegate certain administrative privileges to a policy, and therefore to all users (or groups) to whom the policy is applied. Administrative access is not granted to computer groups, even if the policy is applied to computer groups.

For example, an organisation might wish to have a small group of administrators who can manage the Getbusi system. Rather than give all members of the group the *admin* password, those users could have the admin policy applied individually to their user names. If all administration privileges are granted to the admin policy and the reporting level set to *Super User*, the each account with the admin policy would have the same access privileges of the *admin* user account.



Policies >> admin-policy >> Administration

Policy reporting level

Reporting level: Level 0

Apply

Administration privileges

Privilege	Select	Privilege	Select
Manage policies	□	Manage groups and users	□
Manage computer groups	□	Credit users	□
Manage temporary access	□	Manage local filter lists	□
Manage system properties	□	View reports	□
Deny/Allow computer groups	□	Deny users	□

Apply

Current reporting levels

Policy	Reporting level	Can view
admin-policy	0	✗
no-access-policy	0	✗
staff-policy	0	✗
student-policy	0	✗
whitelist-policy	0	✗

Figure 18

6.2.1.1 Administration Reporting Level

The administration reporting level defines the level of reporting available to a user with that policy applied. If a policy has the appropriate administrative privileges (see Administration Privileges in the next section), its users can view reports on any user of a policy with a *lower* access level, but not of the *same* or *higher* access level. Please note that the administration reporting level only determines the hierarchy of the different policies. Setting a hierarchy alone does not grant privileges to a policy. You must still grant the specific privileges, as explained in the next section: Administration Privileges.

For example, a school might wish to allow staff access to reporting on students, but not other staff members. By giving the staff policy a higher reporting level than the student policy *and* giving the staff policy the ability to view reports, users with the staff policy could view reports on all users with the student policy, but not view reports on other members with the staff policy.

To configure the reporting level for a policy, select the desired reporting level for that policy from the *Reporting level* drop-down menu, and click the grey **Apply** button. A reporting level of 0 cannot view any reports on any other policies. A reporting level of *Super User* may view reports on all other policies. When the browser refreshes, the *Current reporting levels* table at the bottom of the configuration pane will reflect the reporting levels of all policies in the system.

6.2.1.2 Administration Privileges

The administration privileges table lists the administrative privileges of users with that policy. The privileges the Getbusi Administrator may grant to users of a policy are:

- **Manage Policies**: the ability to manage all other policies in the Getbusi system. The only area of policy management that is not delegated is the Administration section, so that users may not promote their own, or any other policy's Administration privileges. However, all other areas of policy management for *all* of the other policies in the system are available. Please be very careful when delegating this privilege.
- **Manage computer groups**: the full ability to create and manage computer groups.
- **Manage temporary access**: the ability to create a temporary user, and grant that user access to Internet resources.
- **Manage system properties**: the ability to reconfigure the system, and perform other maintenance tasks.
- **Deny/Allow computer groups**: the ability to control all configured computer groups' access to Internet resources.
- **Manage groups and users**: for groups, this allows the ability to assign and change the policy that is applied for all groups. For users, this allows the ability to control *the policy* for users belonging to a policy with a lower reporting level. If you promote a user to a reporting level higher than your own policy level, you will lose the ability to manage that user.
- **Credit users**: the ability to credit users belonging to policies with a lower reporting level than the policy being granted the credit users privilege.
- **Manage local filter lists**: the ability to create, alter or delete all local filter lists available on the system.
- **View reports**: the ability to view reports for users belonging to a policy with a lower reporting level.
- **Deny users**: the ability to deny access to Internet resources for users belonging to a policy with a lower reporting level.

To grant privileges, click on the unchecked check-box in the *Select* column that corresponds to the privilege you wish to grant. A check will appear in the check-box. You may grant multiple privileges simultaneously. To apply your changes, click the grey Apply button under the *Administration Privileges* table. When the page refreshes, only the privileges granted will be indicated by checked boxes.

To revoke privileges, click on the checked check-box in the *Select* column that corresponds to the privilege you wish to revoke. The check in the check-box will disappear. You may revoke multiple privileges simultaneously. To apply your changes, click the grey **Apply** button under the *Administration Privileges* table. When the page refreshes, only the privileges granted will be indicated by checked boxes.

6.2.2 Bandwidth

The Bandwidth configuration screen allows you to manage the bandwidth consumption for users of a policy. Bandwidth restrictions only apply to *miss* data, which is data retrieved by your Getbusi server (like Internet data). *Hit* data, which is data currently in your Getbusi server's cache, is delivered at the full speed of your local area network.

Bandwidth restrictions apply to all requests from a given machine. If a user has multiple browser windows open, the bandwidth restrictions apply to all traffic to that machine, with all of the open browser windows sharing the bandwidth. Users therefore cannot circumvent their bandwidth restrictions by having multiple browser windows open on the same machine. However, if a user has browser windows open on two different machines, each machine has the full bandwidth allocated to the user, effectively doubling that user's bandwidth allocation.

Bandwidth is measured in kilobits per second (kbps). To convert this to megabytes per second (MB/s), use the following formula:

$$\text{MB/s} = \frac{0.125 \text{ x kbps}}{1024}$$

For example, a popular bandwidth restriction is 56 kbps, or what a user would experience on a typical dial-up connection. This translates into 0.0068 MB/s. **Do not use a MB/s value when configuring bandwidth restrictions!** The following table shows how long 1 MB of data will take to download using various settings:

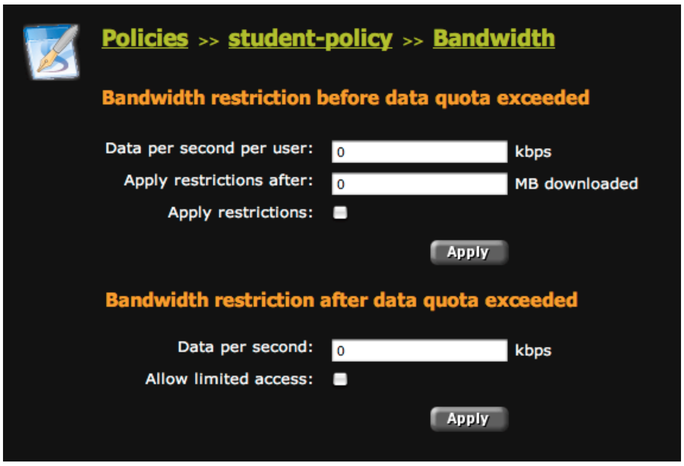
Bandwidth restriction (kbps)	Time to download 1 MB of data
28	4.88 minutes
56	2.44 minutes
128	1.07 minutes
256	0.53 minutes
512	0.27 minutes

Bandwidth restrictions may be enforced in three ways:

1. You may enforce bandwidth restrictions on all access, regardless of how much data has been downloaded.

2. You may set up restrictions to be enforced after a certain amount of data has been downloaded.

3. You may set up restrictions (rather than denying all access) to be enforced after a user's quota has been exceeded.


Policies >> student-policy >> Bandwidth

Bandwidth restriction before data quota exceeded

Data per second per user: 0 kbps

Apply restrictions after: 0 MB downloaded

Apply restrictions: ☐

Bandwidth restriction after data quota exceeded

Data per second: 0 kbps

Allow limited access: ☐

Figure 19

To create bandwidth restrictions on a policy before a user's quota has been reached, enter the following values in the *Bandwidth restriction before data quota exceeded* section:

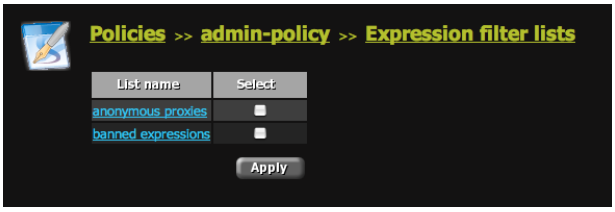
- In the *Data per second per user* text box, enter the desired bandwidth restriction in kbps. **A zero in this text box will effectively deny access**.
- In the *Apply restrictions after* text box, enter the amount of data allowed to be downloaded (at full speed) before the bandwidth restriction is enforced.
- Click the *Apply restrictions* check-box, and click on the grey **Apply** button for the *Bandwidth restriction before data quota exceeded* section.

To create bandwidth restrictions on a policy after a user's quota has been reached, enter the following values in the *Bandwidth restriction after data quota exceeded* section:

- In the *Data per second* textbox, enter the desired bandwidth restriction in kbps. **A zero in this text box will effectively deny access.**
- Click the *Allow limited access* check-box and click on the grey **Apply** button for the *Bandwidth restriction after data quota exceeded* section.

6.2.3 Expressions

The Expressions configuration screen allows you to apply existing expression filter lists to your policy. You must have existing expression filter lists already configured. By default, there are no pre-configured expression filter lists in your system. To learn how to create an expression filter list, please read section 7.3: Expression Lists.


Policies >> admin-policy >> Expression filter lists

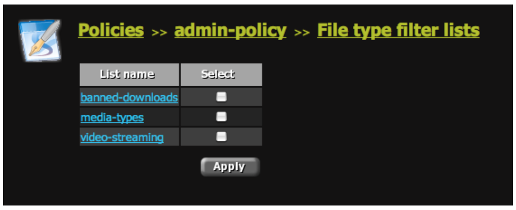
List name	Select
anonymous proxies	☐
banned expressions	☐

Figure 20

A list of all existing expression filter lists created in your system will appear in the expression filter list table. To apply an expression filter list to your policy, click on the filter's corresponding check-box and click the grey **Apply** button. You may apply multiple filters to a policy, and you may apply the same filter(s) to multiple policies.

6.2.4 File Types

The File types screen allows you to apply existing file type filters to your policy. By default, there are three file type filters configured in your Getbusi system: banned-downloads, media-types and video-streaming. You may wish to review which file types are filtered by these categories prior to applying the filter to your policy. You may also create a new file type filter to apply to your policy. For information on how to create or modify a file type filter, please read section 7.4: File Type Lists.



Policies >> admin-policy >> File type filter lists

List name	Select
banned-downloads	☐
media-types	☐
video-streaming	☐

Figure 21

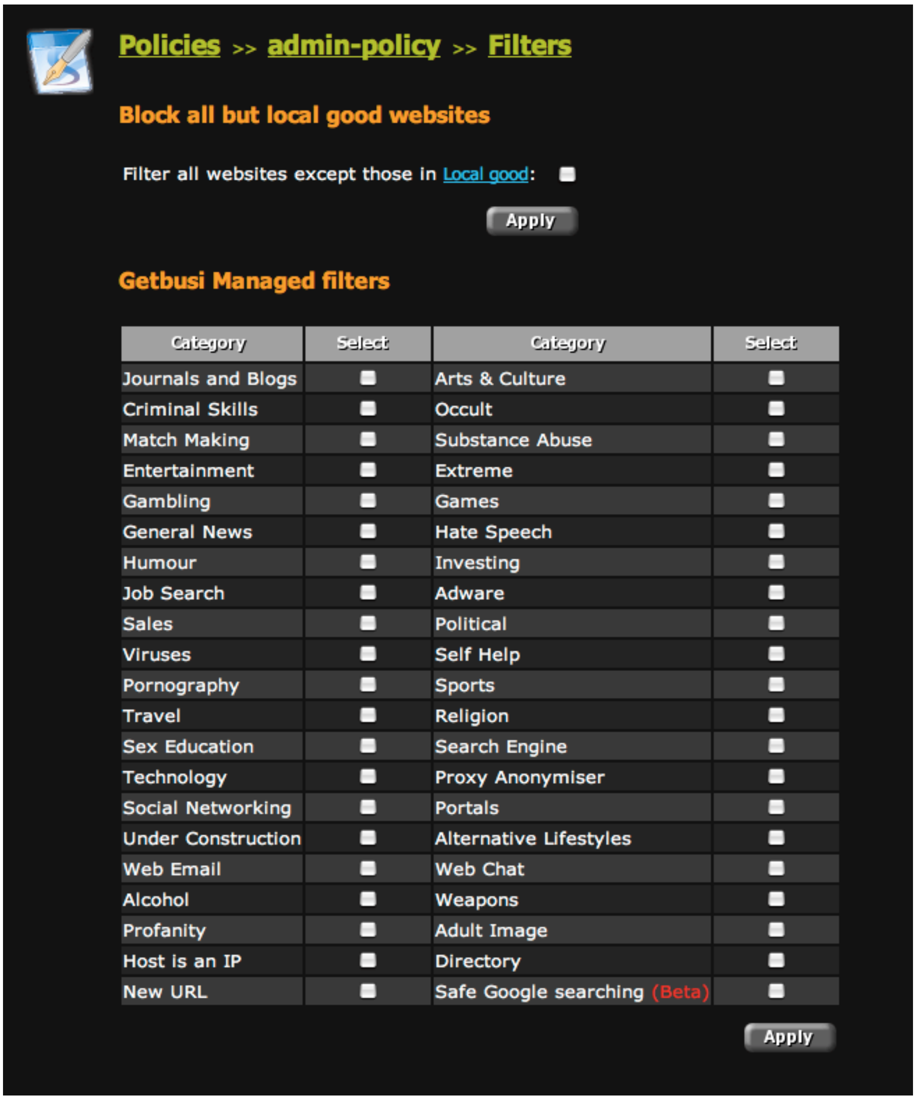
To apply a file type filter to your policy, click on the check-box that corresponds to the name of the file type filter you wish to apply. You may apply multiple file type filters to a policy, and you may apply the same filter(s) to multiple policies. Click on the grey **Apply** button to apply the filter(s) to your policy.

Please proceed to the section entitled: Filters

6.2.5 Filters

The **Filters** screen allows you to apply managed filters to your policy. Getbusi maintain its own Managed Filter lists, however, Getbusi Advance filtering is maintained by Netsweeper, Getbusi's technology partner.

You may also choose to block all sites except for those expressly allowed by one of your own local good filter lists, but you must have already created at least one local good filter list, and have it applied to the policy, or you will effectively block all Internet resources. For information on how to create a local good filter list, please read section 7.5: Good Lists. For information on how to apply a local good filter list to your policy, please read section 6.2.7: Local Good.



Policies >> admin-policy >> Filters

Block all but local good websites

Filter all websites except those in Local good: □

Getbusi Managed filters

Category	Select	Category	Select
Journals and Blogs	□	Arts & Culture	□
Criminal Skills	□	Occult	□
Match Making	□	Substance Abuse	□
Entertainment	□	Extreme	□
Gambling	□	Games	□
General News	□	Hate Speech	□
Humour	□	Investing	□
Job Search	□	Adware	□
Sales	□	Political	□
Viruses	□	Self Help	□
Pornography	□	Sports	□
Travel	□	Religion	□
Sex Education	□	Search Engine	□
Technology	□	Proxy Anonymiser	□
Social Networking	□	Portals	□
Under Construction	□	Alternative Lifestyles	□
Web Email	□	Web Chat	□
Alcohol	□	Weapons	□
Profanity	□	Adult Image	□
Host is an IP	□	Directory	□
New URL	□	Safe Google searching (Beta)	□

Figure 22

To block all websites except the local good filter(s) applied to your policy, click on the *Filter all websites except those in Local good* check-box and click on the corresponding **Apply** button.

To apply a managed filter list to your policy, click on the check-box corresponding to the managed filter list category. You may apply as many managed filter lists to your policy as you wish. To apply your selection to the policy, click on the grey **Apply** button under the managed filter table.

6.2.5.1 Managed Filter Categories

The following is a list of each Managed Filter category and what it blocks. Descriptions are provided by Netsweeper and have been edited where appropriate:

- **Journals and Blogs:** Includes websites that range from personal and medical to literary and culturally-oriented publications.
- **Criminal Skills:** Includes websites that reference instructions or methods that promote, encourage, or provide the skills to do anything that is generally considered to be illegal, criminal, harmful to the general public, and/or that are forbidden by laws, as well as websites promoting academic cheating.
- **Match Making:** Websites in this category include topics related to dating services, dating advice and tips, relationships, listings or personal advertisements, and on-line dating services.
- **Entertainment:** Includes websites pertaining to music, recreation, amusements, fan clubs, gossip, celebrities, movies, or any other form of casual diversion. This category also includes personal websites devoted to movies and television shows.
- **Gambling:** includes websites that directly provide the ability to place a bet or to determine the outcome of a bet, as well as websites that promote or facilitate gambling.
- **General News:** Includes websites which involve the reporting of current events by local, regional, or mass media in the form of newspapers, television, radio programs, and websites on the World Wide Web.
- **Humour:** Includes websites featuring jokes, funny pictures, comic pages, comedy clubs etc. This category could include some profane humour.
- **Job Search:** Includes websites which allow people to search and apply for employment positions. Topics may also include resume writing and interviewing skills, career information, classified advertising, job databases, and job application pages.
- **Sales:** Includes any website offering consumers the ability to purchase products or services online.
- **Viruses:** Includes known or suspected websites associated with computer viruses. Selecting this as a category to block does NOT guarantee that all virus-infected websites will be blocked. You should take additional precautions to avoid viruses.
- **Pornography:** Includes websites that reference, discuss, or show pornography, pictures, videos, or sexually oriented material. Excludes sex education websites.
- **Travel:** Includes websites that have discussions of favorite travel destinations, discounts for travelers, special events in different cities, travel guides, vacations, accommodation, transportation, regulations, maps, weather, and bookings.
- **Sex Education:** Includes websites that describe the various stages of reproduction including the conception, the embryo, the fetus, and the birth of the baby. It also includes topics such as sexually transmitted diseases, abortions, contraception, abstinence and sex advice.
- **Technology:** includes websites that pertain to technology related content. It also includes websites that offer a software download, either for free as a trial or for purchase.
- **Social Networking:** Includes websites that allow members to connect and communicate with friends, family, business contacts, and individuals who share similar interests. Social networking sites are also used to share photos and videos, plan events, schedule meetings, and share information.
- **Under Contruction:** Includes websites that have been identified by the owner as being incomplete or under construction.

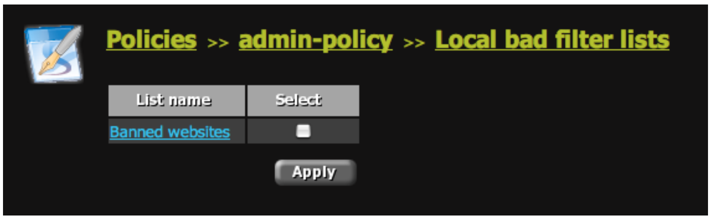
- **Web Email:** Includes websites that permit users to send and receive text, HTML, images, and other data files to each other.
- **Alcohol:** This category includes websites that reference information related to alcohol, including wine, spirits, beer, cocktail recipes, homemade alcohol, or any other alcoholic drink.
- **Profanity:** Includes websites with words that are generally considered obscene, vulgar, or derogatory.
- **Host is an IP:** Includes websites that are accessed via an IP Address rather than a domain/host name.
- **New URL:** This category is for websites which have not yet been categorised. Websites can remain uncategorised from 2 minutes up to 24 hours depending on your filtering type.
- **Arts & Culture:** Includes websites that reference art, artists and culture. Including museum and art gallery websites.
- **Occult:** Includes websites involving the study of secret or hidden knowledge such as: cults, supernatural forces and events, occult lore, vampires, astrology, witchcraft, mysterious symbols, and other 'paranormal' phenomena.
- **Substance Abuse:** Includes websites that provide information on illegal drugs used for recreational rather than medical purposes, or that promote the abuse of legal drugs. excludes informational websites that are clearly intended to provide description of drugs and substances, their negative effects, and addiction potential.
- **Extreme:** These websites are usually violent and may depict or promote torture, mutilation, eating disorders, or other dangerous or disturbing activities. This category does not include pornographic fetishes or widely accepted "extreme sports", such as rock climbing, skiing, or other achievements.
- **Games:** Includes websites that have games or information about games, electronic games, computer games, card games, board games, Internet games etc.
- **Hate Speech:** Includes websites intended to degrade, intimidate, or incite violent or prejudicial actions against someone based on race, ethnic affiliation, nationality, gender, sexual orientation, religion, disability, or profession.
- **Investing:** Includes websites about stocks and quotes, money management, online publications, banks, discount brokerage services, mutual funds, and portfolio management.
- **Adware:** Includes URLs that are advertisements. If you block the adware category, many portal pages may appear broken - when in fact the imbedded advertising URLs are being blocked.
- **Political:** Includes websites related to the structure or affairs of government, politics, or the state.
- **Self Help:** Includes websites which provide the information or support for an individual or a group to better themselves economically, intellectually, physically, or emotionally.
- **Sports:** Includes websites relating to all kinds of Sport including athletics, racing, hunting, baseball, football, basketball, soccer, hockey, etc.
- **Religion:** Includes websites related to or dealing with religious beliefs, practices, faith, churches, worship, etc.
- **Search Engine:** Includes only websites whose sole purpose is Internet search.
- **Proxy Anonymiser:** Includes websites that allow a user to mask their identity online. These websites can be used to bypass the Getbusi proxy and its filtering restrictions.
- **Portals:** Portals are web-based applications that provide a single starting point to retrieve information from multiple sources. For Example, the content of a portal could

include web searching, news, free-email, discussion groups, online shopping, references, and other services.

- **Alternative Lifestyles:** Includes websites that reference habits or behaviors related to social relations, dress, or recreation.
- **Web Chat:** Includes websites that contain computer programs that enable two-way communication between users within an active browser window.
- **Weapons:** Includes websites with information related to the promotion, sale, or discussion of weapons.
- **Adult Image:** This category differs from the Pornography category in that the Adult Image category is based on image scanning and the Pornography category is based on textual content.
- **Directory:** Includes URLs that produce a directory listing instead of a default html page. This page is generated by the remote web server if no default html page is available and directory browsing is enabled.
- **Safe Google™ searching (beta)**: A special type of filter that forces Google searches to use the highest level of content filtering. Getbusi cannot guarantee that this filter will always work as Google™ will regularly alter this system.

6.2.6 Local Bad

The local bad screen allows you to apply your own custom local bad filter lists to a policy. Local bad filters allow you to create a customised list of sites or domains that you specifically wish to prohibit. If your policy implements both local bad and local good lists, the Internet resources prohibited by your local bad list(s) will **override** those granted by your local good list(s). In order to apply a local bad custom filter list to a policy, one must already be created. For information on how to create a local bad custom filter, please read section 7.2: Bad Lists.



Policies >> admin-policy >> Local bad filter lists

List name	Select
Banned websites	□

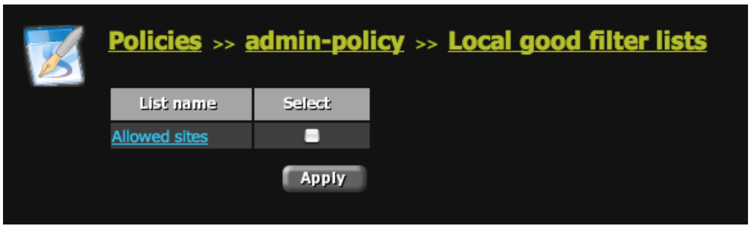
Figure 23

To apply a custom local bad filter list to your select the check-box that corresponds to the list you wish to apply. If you have multiple filter lists, you may apply any combination of lists to your policy. When you have selected the list(s) you wish to prohibit in your policy, click the grey **Apply** button.

6.2.7 Local Good

The local good screen allows you to apply an existing local good filter list, allowing access to sites that is blocked by a managed filter. If your policy implements managed filter lists, local bad lists and local good lists, Internet resources allowed by a local good list **override** those blocked by the managed filter(s), but **do not override** those blocked by local bad lists. For information on creating a local good custom filter, please read section 7.5: Good Lists.

You may also use your local good list(s) as an "allow-only" policy, where only those Internet resources in your local good list(s) will be accessible. For information on how to configure a policy to only allow resources listed in a local good list, please see section 6.2.5: Filters.



Policies >> admin-policy >> Local good filter lists

List name	Select
Allowed sites	□

Figure 24

To apply an existing local good list to your policy, click on the check-box that corresponds with the list you wish to allow. If you have multiple lists, you may select any combination to allow. Click the grey **Apply** button to apply the configuration.

6.2.8 Pricing

The pricing screen allows you to set a price per megabyte for data downloaded by users of a policy. This setting allows a per-policy override of the global price per megabyte that can be set for your Getbusi system (see section 3.13.1: General Details) The value for price paid per MB is the price at which a user with this policy assigned can purchase additional data once over-quota. It is also the rate at which data is charged in billing and reporting.

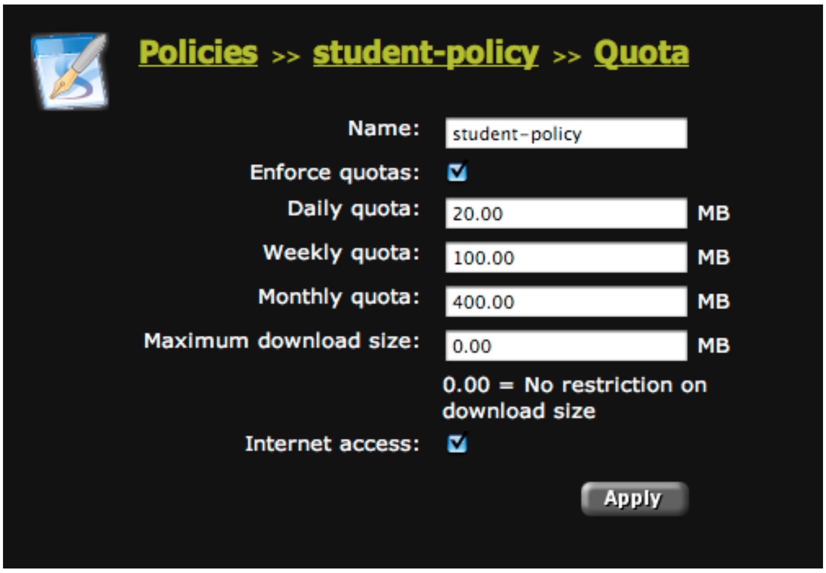
Enter the price per megabyte you wish to set for your policy and click the grey **Apply** button to save your settings.

6.2.9 Quota

The quota screen allows you to:

- Rename the policy that is selected.
- Enforce quotas on the selected policy.
- Set daily, weekly and monthly quotas for users of the selected policy.
- Set a maximum download size for users of the selected policy.
- Enable or disable Internet access for users of the selected policy.

Note: Quota limits are displayed in megabytes (MB) or kilobytes (KB) depending on the system scale (please see section 3.13: Miscellaneous Settings).



Name: student-policy

Enforce quotas: ☑

Daily quota: 20.00 MB

Weekly quota: 100.00 MB

Monthly quota: 400.00 MB

Maximum download size: 0.00 MB

0.00 = No restriction on download size

Internet access: ☑

Figure 25

- To rename the currently selected policy, enter the new name in the *Name* text box.
- To enforce quotas on the policy, click the *Enforce quotas* check-box. Uncheck the check-box to disable quotas on the policy.
- To set a daily quota on the policy, enter the quota in the *Daily quota* text box. The scale is displayed to the right of the field.
- To set a weekly quota on the policy, enter the quota in the *Weekly quota* text box.
- To set a monthly quota on the policy, enter the quota in the *Monthly quota* text box.
- To set a maximum download size on the policy, enter a value in the *Maximum download size* text box.
- To enable Internet access for the policy, click on the *Internet access* check-box. Uncheck the check-box to disable Internet access on the policy.
- Click the grey **Apply** button to save your settings for the policy.

Note: If you wish to *only* enforce a daily, weekly or monthly quota limit you must still enforce all other quota values. Failing to do this will result in Users being automatically over-quota.

For example, if you wish to apply a 500MB Monthly quota limit **only,** to the policy you will still need to apply Weekly and Daily quotas. Therefore, you would apply 500MB quotas to Daily and Weekly.

6.2.9.1 Calculating Quotas

Quotas can be difficult to calculate if you do not have an unlimited Internet access plan. We recommend you monitor your organisation's Internet usage and then tailor your policies to suit.

As a rough guide, you should decide on the total quantity of data you wish your users to download per month. You should factor in how much your non-web traffic consumes (like email services, DNS overhead, organisation web servers).

In the following example, Organisation X has a 50 GB/month Internet access plan. Organisation X 10 employees, an email server which consumes an average of 5 GB/month and a corporate web server which consumes an average of 2 GB/month. Since Organisation X has their own caching DNS server, their DNS overhead is only 10 MB/month. Organisation X does not provide external access to their network, so there is no overhead for remote access services.

Organisation X has a total server overhead of 7.1 GB/month.

Organisation X has 42.9 GB/month available for employee access. A good value for a monthly quota is 42.9 GB/10 employees, or 4.29 GB/employee/month. Rounding down builds overhead into the figures, so the monthly quotas should be set at 4 GB (4000 MB). Weekly quotas should be set at 1 GB (1000 MB), and daily quotas should be set at 200 MB (since employees don't work weekends).

Since Organisation X's ISP implements shaping, there is no financial penalty for exceeding their monthly plan. However, since Organisation X depends on the Internet for their business, there can be productivity losses incurred due to shaping. There is some overhead built into the figures to allow for variations in server consumption.

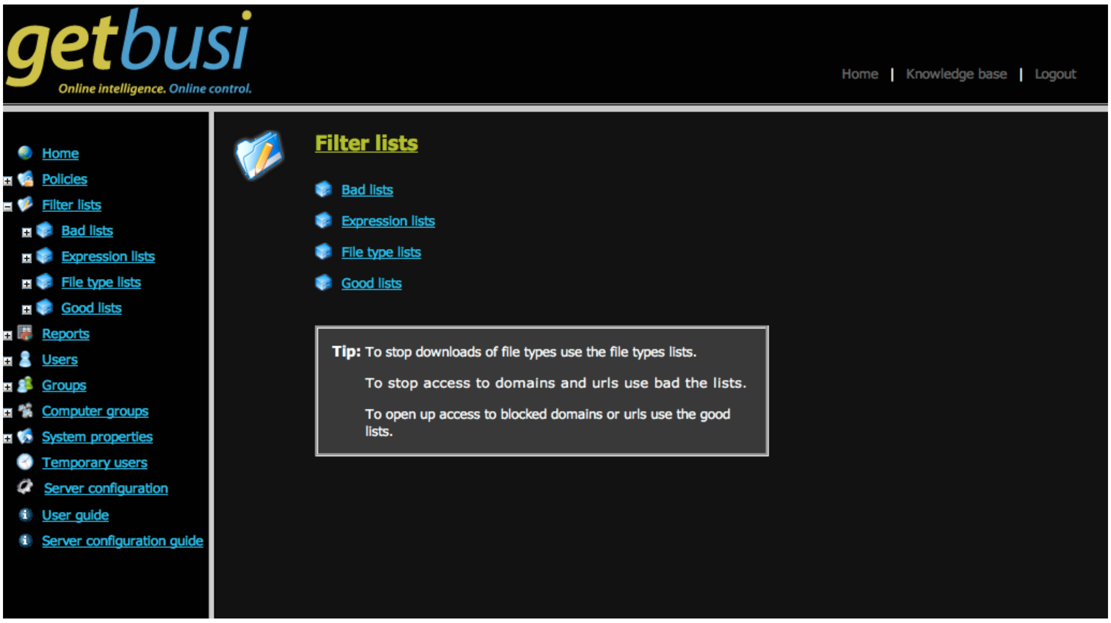
To fine tune Organisation X's quotas, users could be divided into high-usage and low-usage. A mailroom clerk may not require as much access as a computer programmer. If you create low usage plans with low quotas and high usage plans with high quotas, you can further increase your productivity by allocating the right amount of quota to those who need it.

Please proceed to section 7: Customised Filter Lists

7 Customised Filter Lists

The Getbusi system allows you to create your own customised filter lists that can either allow access or deny access to Internet resources. There are four types of customised lists you can create: Bad lists, Expression lists, File type lists and Good lists. Bad lists, Expression lists and File type lists are *blocking* lists; they block access based on the information they contain. Good lists *allow* access; you can use them to override resources that are being blocked by a managed filter list, or you can restrict access to only those resources contained within them. Good lists however, do not override resources being blocked by Bad lists, Expression lists or File type lists.

You may create customised lists by clicking on the **Filter lists** link in the navigation pane, which displays the different filter lists in the configuration pane. Alternatively, if you expand the **Filter lists** link in the navigation pane, you may navigate directly to one of the aforementioned list types.



Tip: To stop downloads of file types use the file types lists.

To stop access to domains and urls use bad the lists.

To open up access to blocked domains or urls use the good lists.

Figure 26

7.1 Valid List Entries

Each list type has criteria which determine a valid entry for that list. Bad lists and good lists can accept Domain Names and URLs. Expression and File type lists only accept a certain range of characters. When making entries into filter lists, your entries must conform to the rules that govern those lists.

7.1.1 Domain Names

The Internet is simply a vast network of computers, each with a numeric Internet Protocol (IP) Address. However, navigation by IP address would make connecting to websites a difficult process, because it is hard for people to remember long sequences of numbers. The Domain Name System aids navigation by associating easily-remembered names to those IP addresses, serving as a "phone book" for the Internet.

The DNS infrastructure is based upon a hierarchy, or an upside-down "tree" of labels. A domain name usually consists of two or more labels separated by dots. Each label to the left specifies a subdivision, or *subdomain* of the domain above it. The DNS system implements a series of *top-level* domains, like *com, net, org, edu, au, us, uk.*

When organisations register a domain name for their website, they get their names from the institutions that control the top-level domains.

For example, Getbusi's domain is *getbusi.com*. The top level domain is *com*, and the sub-domain that is registered to Getbusi is *getbusi*. When reading domain names, always read from right to left. As you read left, each label after a dot is a sub-domain of the label to its right.

Keep this hierarchy in mind when adding a domain to a bad or good list. If you block (or allow) domains at too high of a level, you will also block (or allow) all of the sub-domains of the domain you've specified.

For example, if you were to add *edu.au* to a bad list, you would effectively block every educational institution in Australia, because they are all subdomains of *edu.au*.

7.1.2 Uniform Resource Locators (URLs)

It is important that you understand the parts of a URL in order to tune your filter lists to block (or allow) exactly what you want to filter and no more.

In its strictest technical definition Uniform Resource Locator (URL) is an identifier that is a means to locate an Internet resource by describing its network location. What this means is that a URL contains all of the information a browser needs to access a document being served by a web server.

For example, the address: http://www.somewhere.com/path/to/document/file.html

contains the following information:

- Protocol the server uses to host the document: *http*
- Name of the server hosting the document: *www*
- Sub-domain to which the server belongs: *somewhere*
- Top level domain hosting the subdomain: *com*
- Directory location of the document: */path/to/document*
- Name of the document: *file.html*

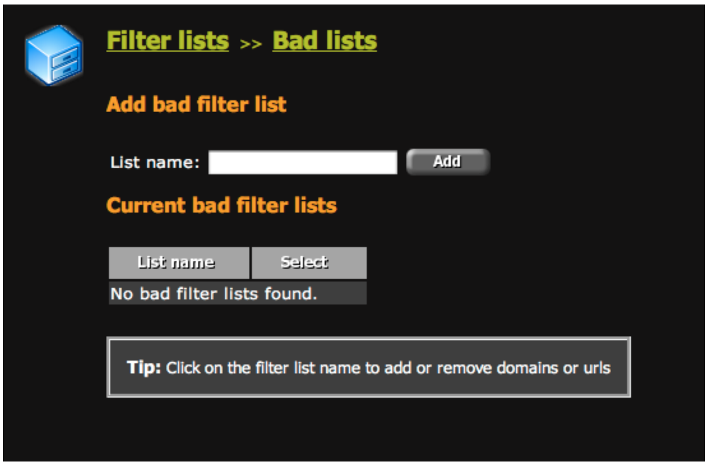
As you can see, the URL describes everything your browser needs to retrieve the document *file.html* from the server *www* in the domain *somewhere.com*.

When inputting URLs into a good or bad filter list, there are some sections of a URL that are not needed by the Getbusi system. You do not need to include the protocol identifier, or *http://* part of the URL into the list. If you do, the Getbusi system will strip it out, and only display the part of the URL after the protocol identifier. The Getbusi system will also strip out any references to specific files. In the preceding example of the URL, the Getbusi system would strip out the name of the document.

The Getbusi system **only** uses the domain parts and the directory location in a URL filter. Using the example URL: http://www.somewhere.com/path/to/document/file.html, the entry for the URL filter would be: somewhere.com/path/to/document. This filter would block (or allow) all documents (and sub-directories) in the path */path/to/document* for documents being served by the domain *somewhere.com*. If the website *somewhere.com* was serving documents in the */path* or */path/to* directories, they would not be blocked (or allowed), because they are parent paths of the directory *document*.

7.2 Bad Lists

As previously mentioned, you may create your own customised bad lists to block access to Internet resources, and apply them to any of your policies. For instructions on applying existing bad lists to a policy, see section 6.2.6: Local Bad.



Filter lists >> Bad lists

Add bad filter list

List name: [Add]

Current bad filter lists

List name	Select
No bad filter lists found.	

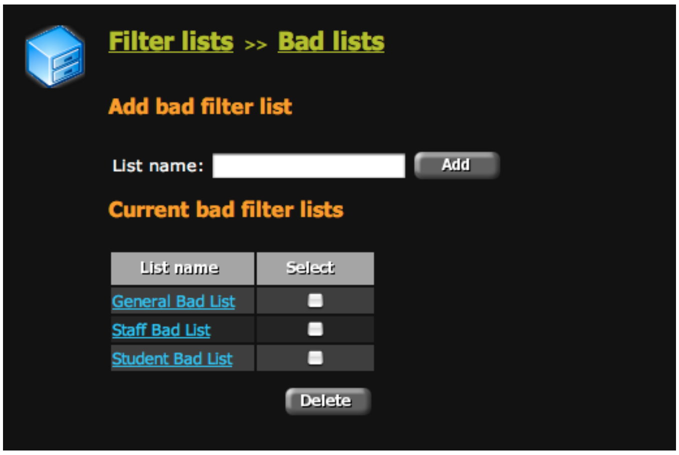
Tip: Click on the filter list name to add or remove domains or urls

Figure 27

Figure 27 shows the bad lists configuration pane. The bad lists configuration pane allows you to add new bad filter lists, and displays the names of all existing bad lists in the *Current bad filter lists* table. If there are no bad lists configured in your system, then the table will display: *No bad filter lists found.*

7.2.1 Creating and Deleting Bad Lists

Prior to adding Internet resources to bad lists, you must first create one. You may create as many bad lists as you wish. It is recommended that when creating bad lists, you name them based on either the category of Internet resources it is designed to block. If you are creating a general bad list that will only apply to a specific policy, you may wish include that policy's name in the bad list's name.



Filter lists >> Bad lists

Add bad filter list

List name: [Add]

Current bad filter lists

List name	Select
General Bad List	□
Staff Bad List	□
Student Bad List	□

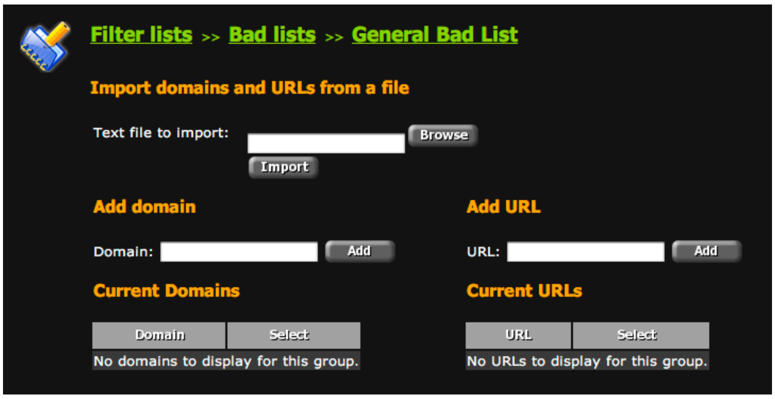
[Delete]

Figure 28

- To create a new bad list, type the list's name in the *List name* text box and click the grey **Add** button. The *Current bad filter lists* table will display the new bad list name when the page refreshes.
- To delete an existing bad list, click on the check-box that corresponds with the list you wish to delete. You may select multiple bad lists for deletion. Click on the grey **Delete** button to delete the list(s) from your system. Note: when you delete a list from your system, all information contained within the list will be irreversibly lost.

7.2.2 Modifying Bad Lists

As seen in Figure 29, there are two ways to add Internet resources to a bad list. You may import a text file containing Internet resources, or you may manually add each resource through the administration console interface.



No domains to display for this group.

No URLs to display for this group.

Figure 29

There are two types of Internet resources you may block with a bad list: domains and URLs. Blocking domains is a powerful way of blocking all content on a website, but is a very indiscriminate way of blocking. For finer-grained control, URL blocking allows you to block specific areas of a website.

Important: Please read section 7.1: Valid List Entries for information about domain names and URLs, and how to craft valid entries in your Bad list.

7.2.2.1 Importing Bad Lists from a File

1. Using your favourite text editor, create a new text document.

2. Using one entry per line, add as many domains or URLs as you wish.

3. Save the document **as a plain text file** (.txt) to a location you can find again on your computer. Do not save the document in a proprietary document format (like Microsoft Word Document), or in rich text format. The document **must** be a plain text document with no formatting, or the Getbusi system will not be able to read the document.

4. Click on the grey **Browse** button and select your text document. Once you've selected the document, the path to the document will appear in the *Text file to import* text box.

5. Click the grey **Import** button to import the text file. The contents of the file will automatically be added to your list, and displayed in the *Current Domains* or *Current URLs* tables.

7.2.2.2 Manually Adding Resources

- If you are adding a domain, type the domain name in the *Domain* text box and click the corresponding grey **Add** button.
- If you are adding a URL, type the URL in the *URL* text box and click the corresponding grey **Add** button.
- Your entry will be displayed in the corresponding table when the browser refreshes.

7.3 Expression Lists

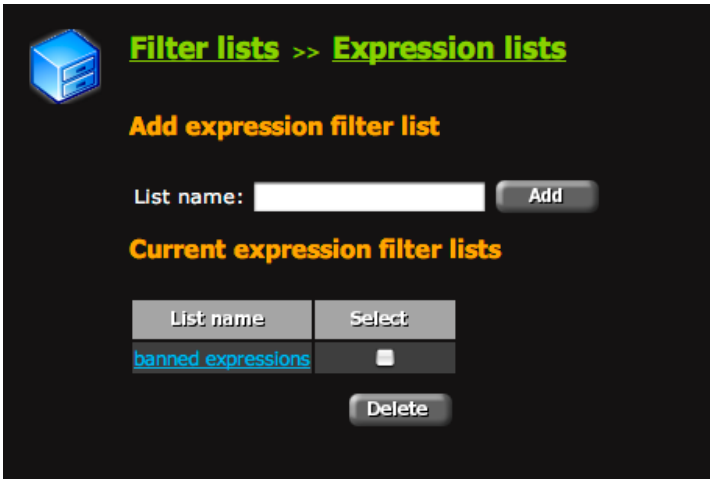
Expression lists allow you to create customised filters that evaluate the address being requested in the address bar of your browser and apply them to your policies. If a user has a policy implementing expression list filtering, any address typed into the address bar of the browser will be parsed for a match against the list. If there is a match, access will be filtered, depending on how the list is applied (either allowed or denied). For instructions on applying existing expression lists to a policy, see section 6.2.3: Expressions.

Expression lists are a powerful filtering tool, but are indiscriminate. Since they are based on pattern matching, you must be careful in how you apply them. There are five types of expression lists filters: a filter when an expression is *contained* anywhere within a URL; a filter when a URL *ends with* the expression; a filter specifically parsing *IP Addresses* in the URL; a filter that can filter a specified *Port* (like 443); and a filter that parses the *Query* section. The query section (if present) of a URL is the part following a question mark. These are typically found in URLs of pages that implement forms.

There are many uses for expression lists, but their implementation must be carefully thought out. For example, you may wish to block eBay and eBay-related sites. If you create an expression list blocking the URLS which **contain** *ebay*, you will also block sites like *rosebay*, because it contains the word *ebay*.

7.3.1 Creating and Deleting Expression Lists

To create an expression list, type the name of the list in the *List name* text box and click on the grey **Add** button. The newly created expression list will appear in the *Current expression filter lists* table when the page refreshes.


Filter lists >> Expression lists
Add expression filter list
List name:
Add
Current expression filter lists
Delete

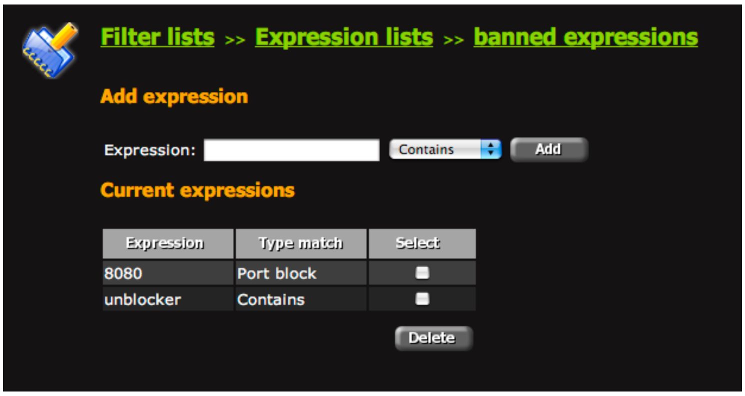
List name	Select
banned expressions	□

Figure 30

To delete an existing expression list, click on the list's corresponding check-box in the *Current expression filter lists* table. You may delete multiple lists simultaneously by clicking on their corresponding check-boxes. Click the grey **Delete** button to delete the lists. Deleted lists cannot be retrieved at a later time.

7.3.2 Modifying Expression Lists

To modify the entries in an expression list, click on the expression list in the *Current expression filter lists* table.



Filter lists >> Expression lists >> banned expressions

Add expression

Expression: Contains Add

Current expressions

Expression	Type match	Select
8080	Port block	□
unblocker	Contains	□

Delete

Figure 31

- To add a new expression to your expression list, enter the expression you want to filter for in the *Expression* text box. Using the drop-down menu, select the appropriate option you wish to enable. Click on the grey **Add** button to save the expression.
- To remove an existing expression in your expression list, click on the check-box that corresponds to the expression in the *Current expressions* table. You may delete multiple expressions simultaneously. Click on the grey **Delete** button to remove the expressions from the list.

7.3.3 Combating Circumventing Proxy Websites

The explosive growth of publicly available circumventing proxy websites have become a major issue for organisations who employ web filtering software (like Getbusi) to control, filter and manage their Internet access. Anonymous proxy websites are a problem because they allow an organisation’s users to effectively bypass their web access management system’s filters and controls, providing unrestricted, untraceable and unmonitored access to Internet content. Since building an anonymous proxy website is a trivial task for anyone with rudimentary computing skills and broadband Internet access, traditional list-based filtering methods cannot stay ahead of the increasing number of proxy sites.

Getbusi Advance’s new filtering technology eliminates the weaknesses of relying on a blacklist-based system by seamlessly classifying any URL that has not already received a classification from the upstream Category Name Servers.

For example, user *Fred* accesses an anonymous proxy website that he has set up and is hosting on his home ADSL connection. *Fred*, quite rightly, assumes that his personal webpage will not be on any of the anonymous proxy blacklists being maintained around the world because he just set it up yesterday. The first time *Fred* accesses the website through the Getbusi proxy it receives the classification “New URL” and is not redirected as this category is not checked in his Policy. As soon as this website is classified as a “New URL” the address is sent to an upstream Category Name Server where the page’s contents are analysed and subsequently classified in the “Proxy Anonymiser” category. Several minutes later, when *Fred* attempts to access the website again, he is redirected because his Policy has the “Proxy Anonymiser” category checked.

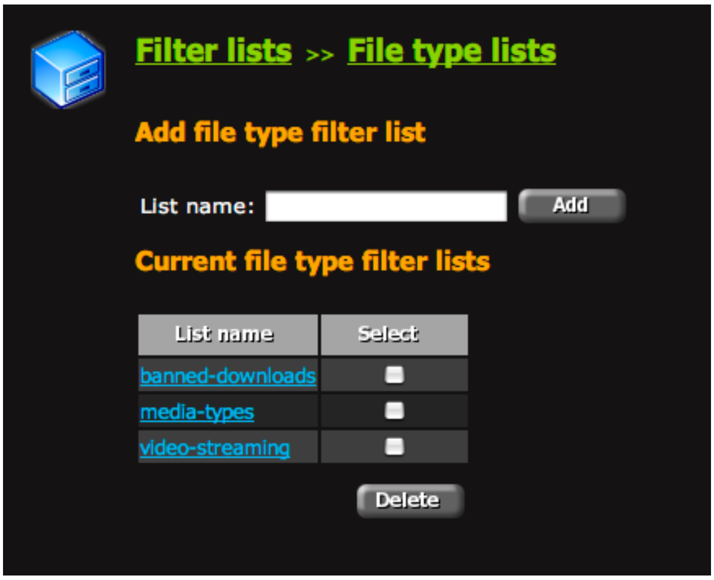
Getbusi Advance is the most effective Getbusi product for combating access to Anonymous Proxy websites and is the one that we recommend. However, there are several methods available in the standard version of **Getbusi** that can assist in blocking these sites, using Expression filters in conjunction with the standard Getbusi Managed Filters. For more information please refer to the Anonymous Proxy White Paper.

7.4 File Type Lists

File type lists may be used to block users from accessing many types of files available on the Internet. File type lists can not only prevent users from downloading banned file types, but can also prevent browsers from displaying inline content, like streaming media. For information on how to apply file type lists to a policy, see section 6.2.4: File Types.

By default, there are three pre-configured file type lists in your Getbusi system: banned-downloads, media-types and video-streaming. The banned-downloads category is configured to block .exe and .zip files. The media-types category is configured to block common movie and music files. The video-streaming category is configured to block common video-streaming formats. Before applying these pre-configured lists to a policy, you should review which file types are being blocked to ensure that you want that list applied. You may also customise these lists to your liking. If you wish, you may also add your own customised file lists.

7.4.1 Creating and Deleting File Type Lists



Filter lists >> File type lists

Add file type filter list

List name:

Current file type filter lists

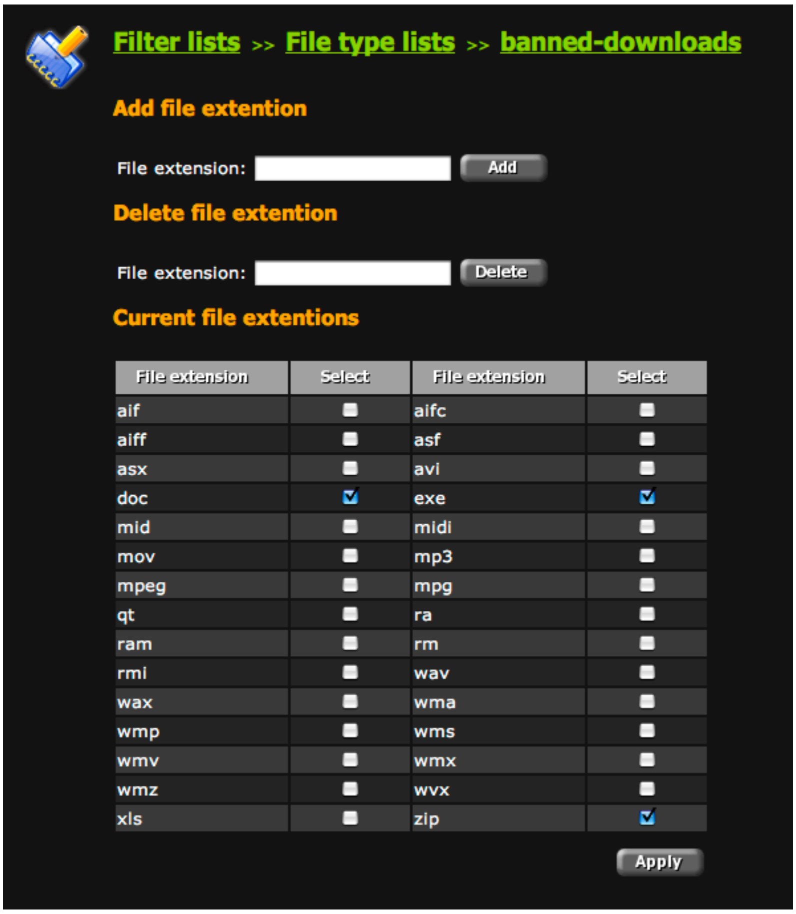
List name	Select
banned-downloads	□
media-types	□
video-streaming	□

Figure 42

- To add a new file type list, type the name of the list in the *List name* text box, and click on the grey **Add** button. Your newly created file type list will appear in the *Current file type filter lists* table when the page refreshes.
- To delete an existing file type list, click on the check-box that corresponds with the list you wish to delete. You may delete multiple lists simultaneously. Click on the grey **Delete** button to remove the list from your Getbusi system. Deleted lists cannot be recovered at a later time.

7.4.2 Modifying File Type Lists

You may modify the types of files being denied by a file type list. The *Current file extensions* table lists a number of pre-configured file types for you to add to the list. If the file type you wish to block does not exist in the table, you may add a new file type to the table.



Filter lists >> File type lists >> banned-downloads

Add file extention

File extension:

Delete file extention

File extension:

Current file extentions

File extension	Select	File extension	Select
aif	□	aifc	□
aiff	□	asf	□
asx	□	avi	□
doc	☑	exe	☑
mid	□	midi	□
mov	□	mp3	□
mpeg	□	mpg	□
qt	□	ra	□
ram	□	rm	□
rmi	□	wav	□
wax	□	wma	□
wmp	□	wms	□
wmv	□	wmx	□
wmz	□	wvx	□
xls	□	zip	☑

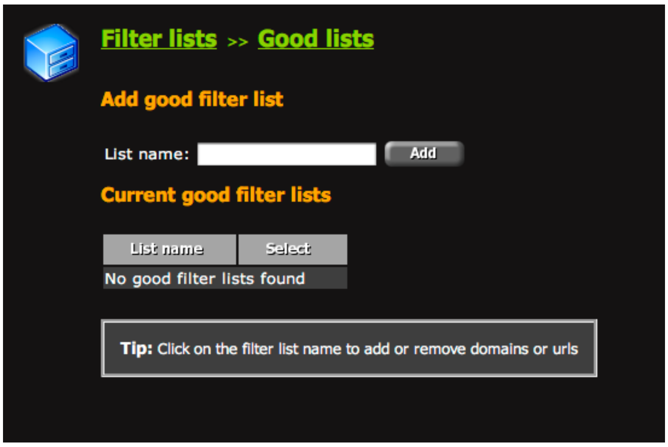
Figure 43

7.4.3 Modifying File Type Lists

- To add a new file type to filter against, enter the file type extension in the *File extension* text box and click on the grey **Add** button. The new file type will be displayed in the table when the browser refreshes.
- To delete a file type from the *Current file extensions* table, enter the file type extension in the *File extension* text box and click on the grey **Delete** button. The file type will be removed from the table when the browser refreshes.
- To apply a file type to the file type filter you're editing, click on the file type's corresponding check-box in the *Current file extensions* table. You may check multiple file types simultaneously. Click on the grey **Apply** button to add the file types to your list.
- To remove a file type from the file type filter you're editing, click on the checked file-type check-box. You may remove multiple file types simultaneously. Click on the grey **Apply** button to remove the file types from your list.

7.5 Good Lists

As previously mentioned, you may create your own customised good lists to allow access to Internet resources, and apply them to any of your policies. For instructions on applying existing good lists to a policy, see section 6.2.7: Local Good.



Add good filter list

List name:

Current good filter lists

List name	Select
No good filter lists found	

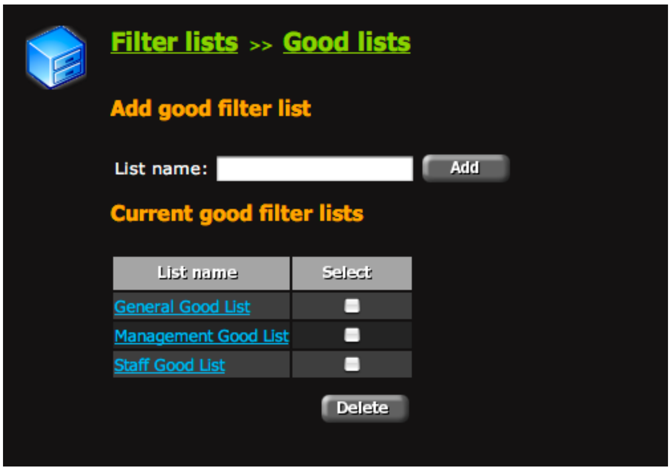
Tip: Click on the filter list name to add or remove domains or urls

Figure 44

Figure 44 shows the good lists configuration pane. The good lists configuration pane allows you to add new good filter lists, and displays the names of all existing good lists in the *Current good filter lists* table. If there are no good lists configured in your system, then the table will display: *No good filter lists found.*

7.5.1 Creating and Deleting Good Lists

Prior to adding Internet resources to good lists, you must first create one. You may create as many good lists as you wish. It is recommended that when creating good lists, you name them based on either the category of Internet resources it is designed to allow. If you are creating a general good list that will only apply to a specific policy, you may wish include that policy's name in the good list's name.



Add good filter list

List name:

Current good filter lists

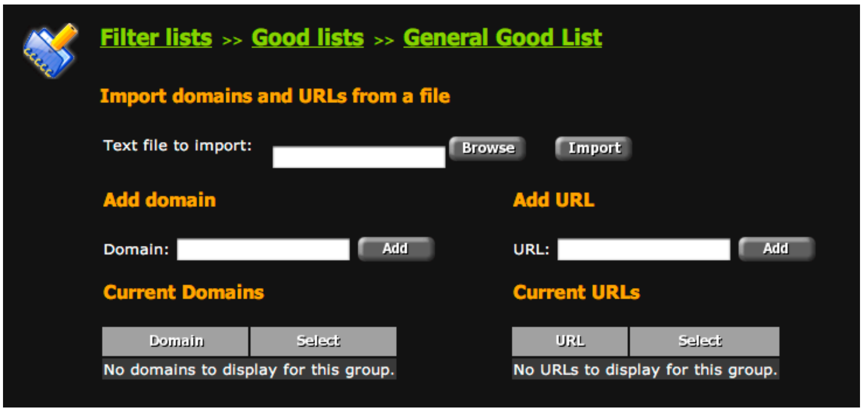
List name	Select
General Good List	□
Management Good List	□
Staff Good List	□

Figure 45

- To create a new good list, type the list's name in the *List name* text box and click the grey **Add** button. The *Current good filter lists* table will display the new good list name when the page refreshes.
- To delete an existing good list, click on the check-box that corresponds with the list you wish to delete. You may select multiple good lists for deletion. Click on the grey **Delete** button to delete the list(s) from your system. Note: when you delete a list from your system, all information contained within the list will be irreversibly lost.

7.5.2 Modifying Good Lists

As seen in Figure 46, there are two ways to add Internet resources to a good list. You may import a text file containing Internet resources, or you may manually add each resource through the administration console interface.



No domains to display for this group.

No URLs to display for this group.

Figure 46

There are two types of Internet resources you may allow with a good list: domains and URLs. Allowing domains is a powerful way of allowing all content on a website, but is indiscriminate. For finer-grained control, adding a URL allows you to only allow specific areas of a website.

Important: Please read section 7.1: Valid List Entries for information about domain names and URLs, and how to craft valid entries in your Good list.

7.5.2.1 Importing Good Lists from a File

1. Using your favourite text editor, create a new text document.

2. Using one entry per line, add as many domains or URLs as you wish.

3. Save the document **as a text file** to a location you can find again on your computer. Do not save the document in a proprietary document format (like Microsoft Word Document), or in rich text format. The document **must** be a plain text document with no formatting, or the Getbusi system will not be able to read the document.

4. Click on the grey **Browse** button and select your text document. Once you've selected the document, the path to the document will appear in the *Text file to import* text box.

5. Click the grey **Import** button to import the text file. The contents of the file will automatically be added to your list, and displayed in the *Current Domains* or *Current URLs* tables.

7.5.2.2 Manually Adding Resources

- If you are adding a domain, type the domain name in the *Domain* text box and click the corresponding grey **Add** button.
- If you are adding a URL, type the URL in the *URL* text box and click the corresponding grey **Add** button.

Your entry will be displayed in the corresponding table when the browser refreshes.

8 Reports

The Getbusi system implements a large array of reports to help you manage your organisation's Internet resources. You may access the various reports by clicking on the *Reports* link in the navigation pane, which will display the list of reports in the configuration pane. Alternatively, if you wish to directly access a report, you can expand the *Reports* link in the navigation pane to show direct links to the specific reports.

The results of a report are presented in tables. Many of the tables implement sortable columns, allowing you to sort the data in the table by column name. If a table's columns are sortable, the column names will be clickable.

Many of the reports also allow you to save the report as a PDF file. If a report can be saved as a PDF, then a grey **PDF** button will be rendered on the report's page. Clicking on the **PDF** button will produce a PDF version of the report in a new browser window.

Some reports also allow you to graph the information in the table. If the data on the table can be graphed, then a grey **Graph** button will be rendered on the report's page. Clicking on the **Graph** button generates a graph of the data in a new browser window.

Only those users having the correct permission levels are able to view reports. For information on how to configure user access to reports, see section 6.2.1: Administration.

8.1 Active Requests

The active requests report shows a snapshot of all current Internet activity of users accessing Internet resources through your Getbusi system at the time of the report. The report lists the URL being accessed, the amount of data downloaded for each request, the workstation that the user is accessing the Internet from, and the time the download started. No user information is available from this report.

8.2 Billing

The billing report may be generated for groups or for users. The report will display the groups or individual users as well as the total data used by that group or user, multiplied by the pricing set in that group's or user's policy.

8.3 Computer Groups

The Computer groups report provides information on the total data downloaded for each computer group for the period selected. The report also provides three links to extract greater detail on each computer group.

The link in the *Total Data(MB)* column generates a report that shows the total amount of data used by a computer group by day. This report, in turn, provides links to data reports on the average data per day and per hour downloaded by the computer group.

The *Workstation Info* link generates a report that provides information downloaded by each individual computer in the computer group. This report, in turn, provides links to data reports on the average data per day and per hour downloaded by each machine in the computer group.

The *Site Info* link generates a report that generates a list of sites and downloaded data visited by all machines within the computer group.

8.4 CSV

The CSV reports are downloadable report files in CSV (Comma Separated Values) format, and provide information about the overall traffic through your Getbusi system, and information about Internet requests that were prohibited by your Getbusi system. Once generated, the CSV reports can be downloaded to your local machine and displayed in your favourite spreadsheet application. Each report will be saved in your Getbusi system, with the size of the report and the date it was generated. If you do not wish to save reports in the system, you can choose to delete it.

8.4.1 Traffic

The traffic report allows you to generate a customised report about all of the requests being handled by your Getbusi system. You must generate a report for a specific date/time range, and filter the results to only show any combination of the following categories:

- Date/Time of each request.
- User making the request.
- Workstation making the request.
- Miss data: the amount of data downloaded from the Internet for the request.
- URL: the url being requested.
- From cache: if the data was served from the Getbusi system's cache.
- Hit data: the amount of data served from the Getbusi system cache for the request.
- Host: The name of the Internet host the data was being requested from.

8.4.2 Prohibited Attempts

The prohibited attempts report allows you to generate a customised report about any Internet access attempts that were prohibited by your Getbusi system. You must generate a report for a specific date/time range. Additionally, you may filter the results to only show any combination of the following categories:

- Date/Time of the request.
- User making the request.
- Policy responsible for prohibiting access.
- Workstation making the request.
- URL: the URL that was prohibited.
- Filter: The specific filter that blocked access.

8.5 Data

There are four data reports you can generate to see the amount of data that has been downloaded through your Getbusi system. All data reports require a date range to report on. The reports show the amount of data downloaded and the proportion of hit data (data served from your Getbusi server's cache) and miss data (data downloaded from the Internet).

8.5.1 All Data

The *All* data report displays the total amount of hit data, miss data and the combined total data that has been downloaded by workstations during the selected time period.

8.5.2 Total Data by Date

The *Total by date* data report displays the total amounts of hit data, miss data and combined data downloaded for each individual day in the selected time period.

8.5.3 Average Data by Day

The *Average by day* data report displays hit data, miss data and combined data that has been downloaded, averaged for each day of the week during the selected time period. This allows you to easily view trends of daily usage over a time period.

8.5.4 Average Data by Hour

The *Average by hour* data report displays the hit data, miss data and combined data that has been downloaded each hour, averaged each hour of the day during the selected time period. This allows you to easily view trends of usage by hour over a time period.

8.6 Deleted Users

The *Deleted users* report shows those users who have been deleted from the system during the specified date range. If the date range is inclusive of the current day, then the report will also show which users are scheduled to be deleted overnight. The report contains the date and time the user was set to be deleted, the user name to be deleted, and the name of the administrator who initiated the deletion.

8.7 Failed Ticket Attempts

The *Failed ticket attempts* report shows those users who attempted to credit their account with the ticketing system, but input an invalid ticket number. The report shows the date and time when the failed attempt was made, the user making the attempt, the IP address of the Getbusi host and the access code that was inputted.

This allows you to ensure that users aren't randomly inputting ticket codes to credit their account quotas.

8.8 File Type

The *File type* report provides information on the total amount of data downloaded for each file type in the file type list. For information about how to add file types to the file type list, please see section 7.4: File Type Lists.

The *File type* report shows each file type that has been downloaded within the specified date range, the total amount of data (MB) for each file type, a link to show the sources of the file type downloads and the users which downloaded the file type.

8.9 Groups

The *Groups* report provides information on the total data downloaded for each group within the specified date range. For each groups listed in the group table, there are three links which run additional reports to extract greater details. Clicking on the link in the *Total data (MB)* column runs data report that shows (within the specified date range) the aggregate data downloaded for all users in the group, ordered by date. The *Site info* link shows the sites visited by users within the group, and the aggregate data downloaded from each site within the specified time period. The *User info* link lists users in the group and the aggregate amount of data downloaded within the specified time period.

8.10 Over Quota

There are two Over Quota reports that can be generated: Users and Computers.

8.10.1 Users

The Users over quota report lists those users who have exceeded their weekly or monthly quota, and the amount of data actually downloaded by that user.

8.10.2 Computers

The Computers over quota report lists those computers which have exceeded their weekly or monthly quota, and the amount of data actually downloaded to that computer.

8.11 Previously Credited Users

The previously credited users report provides information on those users who have been previously credited with a monetary value. The report sows the date and time the user was credited, the user name of the person who was credited, the amount credited and the user name of the administrator who completed the credit.

8.12 Previously Denied Users

The previously denied users report provides information on those users who have been previously denied Internet access. The report shows the date and time the user was denied, the user name of the person who was denied, the period of time the user was denied for and the user name of the administrator who completed the denial. The report also provides a link from the administrator's user name to details on the public and private note set for the denial.

8.13 Previously Denied/Allowed Computer Groups

The previously denied/allowed computer groups report provides information on computer groups whose Internet access has been denied or allowed. The report shows the date and time the computer group was denied or allowed, the name of the relevant computer group, the previous and current access status and the user name of the administrator who made this change.

8.14 Prohibited Attempts

Prohibited attempts reports may be generated in three ways: by category, by user and by workstation.

Each report shows the prohibited attempts for that category.

8.14.1 By Category

The prohibited attempts by category report contains a summary of filter categories and the number of attempts to access sites or files contained within those categories. It also contains two links: one to user information and one to site information. These links provide greater detail on the users' access attempts to sites in this category and the sites to which access attempts were made.

8.14.2 By User

The prohibited attempts by user report contains a summary of users and the number of attempts to access prohibited sites. The report also contains a link to information on those categories the user attempted to access and which sites or files the user attempted to access.

8.14.3 By Workstation

The prohibited attempts by workstation report contains a summary of workstations and the number of attempts to access prohibited sites that were made from these workstations. The report lists the fully qualified domain name of the machine, if available, otherwise it lists the machine's IP address. The report also contains a link to information on those categories access attempts were made on and the total number of attempts. By selecting the link in the total attempts column you can access further detail about the workstation including user and site information relevant to this machine and the prohibited access attempts.

8.14.3.1 Prohibited Attempts: URL Classification Only

If you have enabled the Filtering option *URL Classification Only*, the Prohibited Attempts report will contain records of **all internet access**, though no requests will have been prohibited. For more information on Filtering options see the section entitled Filtering.

8.15 Time

Time reports may be generated three ways: by groups, by users or by all combined users. Time reports show the estimated amount of time spent accessing Internet resources. Please note that time reports only count the minutes where a requests have been made. The time report cannot estimate the amount of time a user spends reading a page result. Additionally, if a user opens a page that constantly refreshes, the report will show higher time usage.

8.15.1 Groups

The time report by group contains a summary of the minutes spent surfing the Internet by any group of users defined in your authentication system. Note that a group will only appear if a Getbusi policy is applied to it. The report also contains links to 'Time by date', 'Time by day' and 'Time by hour' reports. The 'Time by date' report shows the time spent surfing the Internet by the chosen group, day by day for the period chosen. The 'Time by day' report shows the average time spent surfing the Internet by the chosen group for each day of the week. The 'Time by hour' report shows the average time spent surfing the Internet by the chosen group for each hour of the day.

8.15.2 Users

The time report by users contains a summary of the minutes spent surfing the Internet by any user defined in the Getbusi system. The report also contains links to 'Time by date', 'Time by day' and 'Time by hour' reports. The 'Time by date' report shows the time spent surfing the Internet by the chosen user, day by day for the period chosen. The 'Time by day' report shows the average time spent surfing the Internet by the chosen user for each day of the week. The 'Time by hour' report shows the average time spent surfing the Internet by the chosen user for each hour of the day.

8.15.3 All Users Combined

The time report for all users combined contains a summary of the minutes spent surfing the Internet by all users as a combined total. The report also contains links to 'Time by date', 'Time by day' and 'Time by hour' reports. The 'Time by date' report shows the time spent surfing the Internet by all users as a total, day by day for the period chosen. The 'Time by day' report shows the average time spent surfing the Internet by all users as a total for each day of the week. The 'Time by hour' report shows the average time spent surfing the Internet by all users as a total for each hour of the day.

8.16 Users

User reports may be generated three ways: by date, by date and time and current users. All of the user reports provide similar information, but for different time ranges.

8.16.1 Users by Date

The users data by date report provides information on the data downloaded by day for this user for the selected period. This report displays the total data for each day for the user and selected period. The report also contains links to 'Data by day' and 'Data by hour' reports. The 'Data by day' report shows the average data downloaded from the Internet by the chosen group for each day of the week. The 'Data by hour' report shows the average data downloaded from the Internet by the chosen group for each hour of the day.

8.16.2 Users by Date/Time

The users data by date/time report provides information on the data downloaded by day for this user for the selected date and time period. This report displays the total data for each day for the user and selected period. The report also contains links to 'Data by date and 'Data by hour' reports. The 'Data by day' report shows the average data downloaded from the Internet by the chosen group for each day of the week. The 'Data by hour' report shows the average data downloaded from the Internet by the chosen group for each hour of the day.

8.16.3 Current Users

The current users generates a report based on the period filter. You may select a period ranging from the last 5 minutes to the last 24 hours. This report displays the total data for each day for the user and selected period. The report also contains links to 'Data by date and 'Data by hour' reports. The 'Data by day' report shows the average data downloaded from the Internet by the chosen group for each day of the week. The 'Data by hour' report shows the average data downloaded from the Internet by the chosen group for each hour of the day.

8.17 Todays Users

The todays users report lists the users which have accessed the Internet on the day the report is generated. The report shows userid and total data downloaded. The report also has links to site information reports and total users for the period reports.

8.18 Users (Current Status)

The Users (Current Status) report shows an alphabetical table by which you can navigate to any user in the system. When clicking on a letter in the table, it will generate a report for all user IDs starting with the selected letter. The report shows the user ID, week to date downloads (MB), month to date downloads (MB) and whether or not the users have Internet access.

8.19 Web Sites

The web sites report provides information on the total data downloaded from each website for the period selected. The resultant table includes links to generate further information about each website visited by users. These links provide information about the host name of the website, the total data downloaded from the site, the users who visited the site and the actual resources used from the site.

8.20 Workstations Report

The workstations report shows all of the workstations that have been used to access Internet resources through the Getbusi system. The report provides details on the amount of data downloaded to the workstation and links to view which sites were accessed, and the user ID of the users who used the workstation to access Internet resources.

Please proceed to the section entitled Users

9 Users

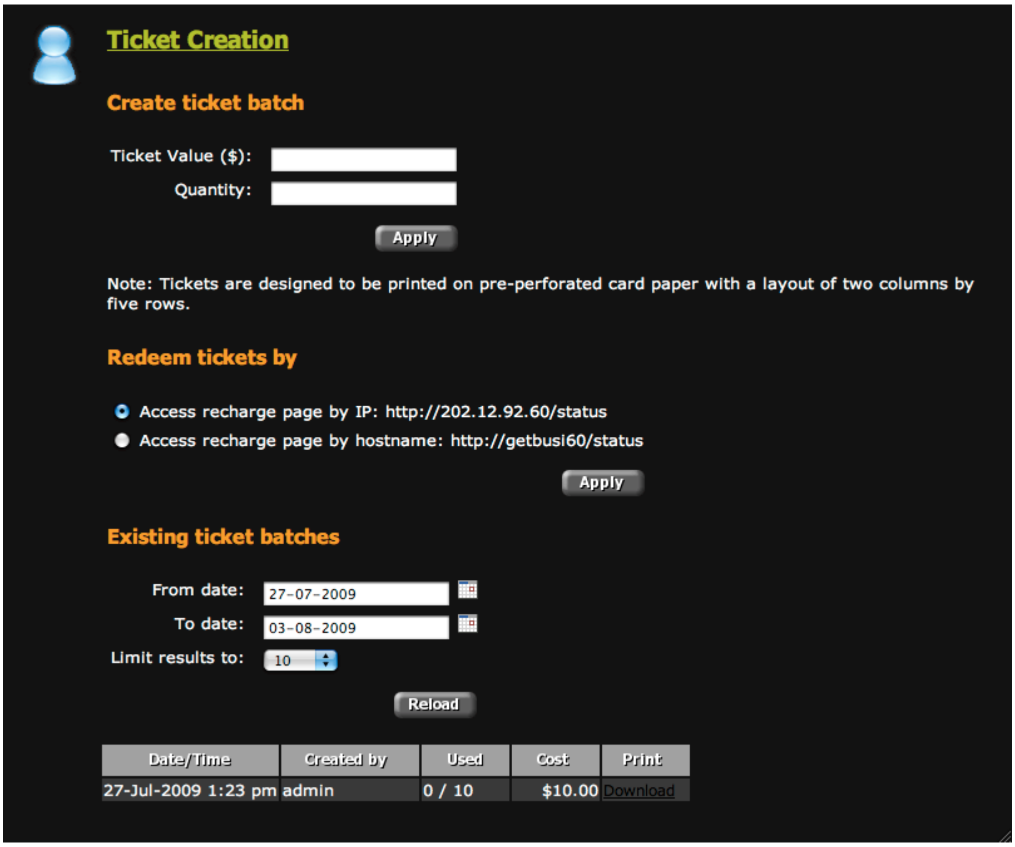
The Getbusi system certain aspects of user access at a more granular level. You may directly manage a user's quotas, change a user's policy and view a report on an individual user's activity. Additionally, through the users link in the navigation pane, you may access the ticketing subsystem which allows you to generate tickets for users to add credit to their accounts.

You can access the user functions through the *Users* link in the navigation pane, which will display the list of functions which apply to users in the configuration pane. Alternatively, if you wish to directly access a user function, you can expand the *Users* link in the navigation pane, which shows direct links to user functions.

9.1 Tickets

The Getbusi system implements a method by which you may generate dollar denominated tickets which users can use to purchase Internet access. Tickets are only applicable for policies that are configured for pricing. The amount of quota purchased by a ticket is dependent on the pricing of the policy to which the ticket is being applied. Tickets are not generated for any specific policy; they can be applied to any policy which has implemented pricing. A $10 ticket used by a user on a policy configured for $0.10 per megabyte will purchase 100MB of quota. The same ticket used by a user with a policy configured for $1.00 per megabyte will only receive 10MB of quota.

Tickets are designed to be printed on pre-perforated card paper with a layout of two columns by five rows (10 tickets per page).



Ticket Creation

Create ticket batch

Ticket Value ($):

Quantity:

Note: Tickets are designed to be printed on pre-perforated card paper with a layout of two columns by five rows.

Redeem tickets by

● Access recharge page by IP: http://202.12.92.60/status
○ Access recharge page by hostname: http://getbusi60/status

Existing ticket batches

From date: 27-07-2009
To date: 03-08-2009
Limit results to: 10

Date/Time	Created by	Used	Cost	Print
27-Jul-2009 1:23 pm	admin	0 / 10	$10.00	Download

Figure 47

9.1.1 Creating Tickets

To create a ticket, you first need to determine how users will access the ticketing system to redeem issued tickets. There are two redeem methods: by IP address, or by the hostname of the system. If you do not have DNS configured to resolve your hostname to your IP address on your network, select *Access recharge page by IP*. If you have DNS properly configured, you may choose either method of redemption. Click on the corresponding grey **Apply** button to set the method of redemption.

Once you have determined the method of ticket redemption, enter the ticket value in the *Ticket Value* text box. Enter the number of tickets you wish to create in the *Quantity* text box and click on the grey **Apply** button. When the page refreshes, you will be presented with a link to download your newly created tickets. Alternatively, the table at the bottom of the page will refresh to include a link to the newly created tickets.

Users may redeem the tickets and credit their own accounts by directing a browser to the link printed on the ticket. They will be prompted to login using their authentication credentials to view the status of their account. For more information about this, see 9.5: Users Viewing Their Own Status.

9.1.2 Viewing Existing Ticket Batches

To view previously created ticket batches, select the date range that would include the ticket batch you're interested in viewing. Click on the grey **Reload** button to update the table. Once the table updates, all ticket batches created within the specified date range will appear. Click on the download link corresponding to the ticket batch to download the tickets as a PDF file. You can then print the tickets you've downloaded.

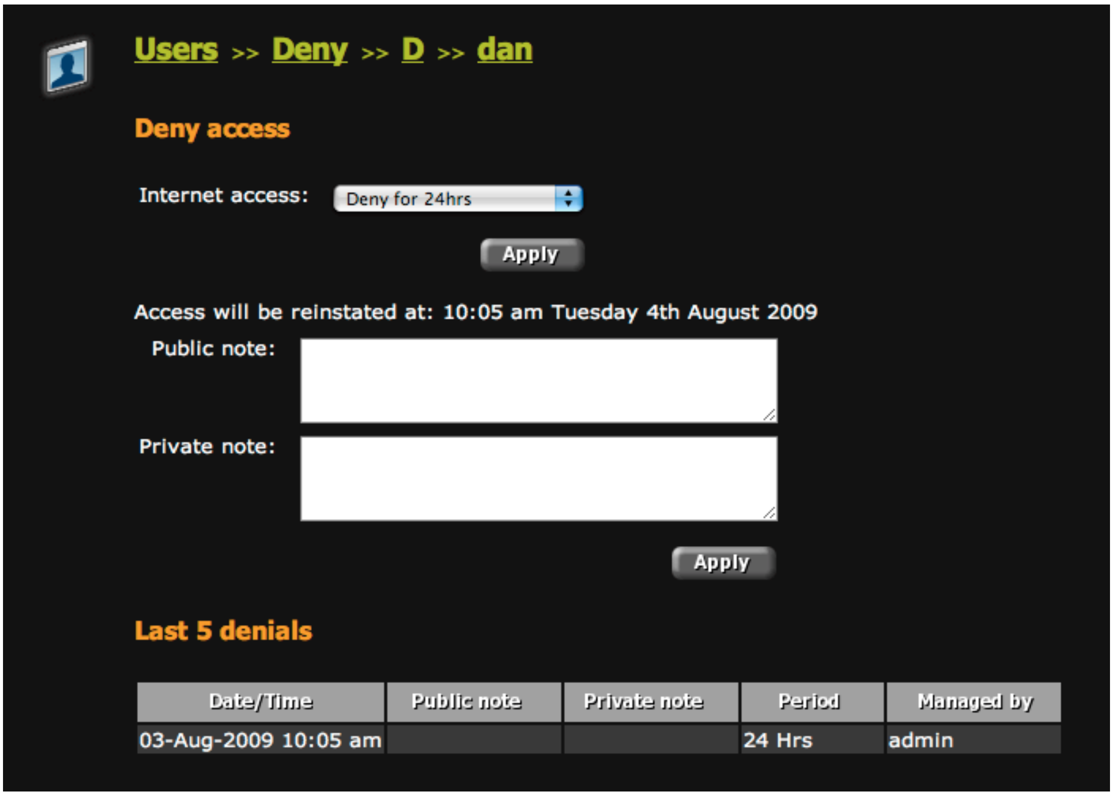
9.2 Crediting Users

Users belonging to policies with a price per megabyte may be credited a dollar amount to increase their quota. If you try to credit a user belonging to a policy that does not implement a price per megabyte, then a red warning message will appear stating that a price of $0.00 per MB has been set on the user's policy. You will have to set a price greater than $0.00 on the policy in order to credit the user a dollar amount.

The user's current credit balance is displayed in the **Credit** configuration screen. To adjust a user's credit by a dollar amount, enter the dollar amount in the *Adjust credit by* text box and click on the grey **Apply** button. The current credit balance will update with the changes when the page refreshes. Additionally, the credit will appear in the *Last 5 credits* table, along with the name of the administrative user who made the credit.

9.3 Denying User Access

If you wish, you may immediately deny any user access to Internet resources. Denying a user's access has no effect on the remaining quota a user may have, and overrides any policies applied to the user's account. Access is simply unconditionally denied. You may permanently deny a user, or deny access for a specified time period.



Internet access: Deny for 24hrs

Access will be reinstated at: 10:05 am Tuesday 4th August 2009

Public note:

Private note:

Date/Time	Public note	Private note	Period	Managed by
03-Aug-2009 10:05 am			24 Hrs	admin

To deny access, select the amount of time to deny access from the *Internet access* drop-down menu and click on the grey **Apply** button. To reinstate access, select *Allow access to the Internet* from the *Internet access* drop-down menu and click the grey **Apply** button.

After you have denied access for a specified time period, the time when access will be reinstated and two text boxes will appear when the page refreshes. The first text box allows you to set a note that the user will see when trying to access the Internet, explaining the reason for denial. The private note may only be viewed by users with Administrative access to the system. To set the notes, enter the notes you wish to be viewed in the text boxes and click the grey **Apply** button. When the page refreshes, the last 5 denials for the user will appear in the table at the bottom of the screen, with the messages you've configured, the period of denial and the name of the Administrative user who denied access for the user.

9.4 General User Management

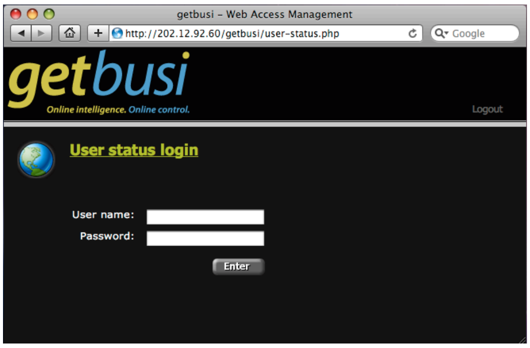
The general management screen allows you to view a user's status and the policy currently applied to the user. The status section shows information about the user's quotas and the amount of quota the user has already used. The *policy* drop-down menu shows the current policy applied to the user. To change a user's policy, select the new policy from the *policy* drop-down menu and click on the grey **Apply** button. When the page refreshes, the drop-down menu will show the new policy of the user. You can use this drop-down menu to override the default policy applied to the user by their group.

9.5 Users Viewing Their Own Status

Getbusi allows users to login to a special page on the Administration Console using their own username and password to view the status of their own account. If a user wishes to view the status of their own account or redeem a ticket, they should navigate to:

```
http://<IP address or hostname of getbusi server>/status
```

where <IP address or hostname of Getbusi server> is the IP address, or the hostname of your Getbusi server. Users should login to the interface with the same username and password that they use for their proxy authentication.



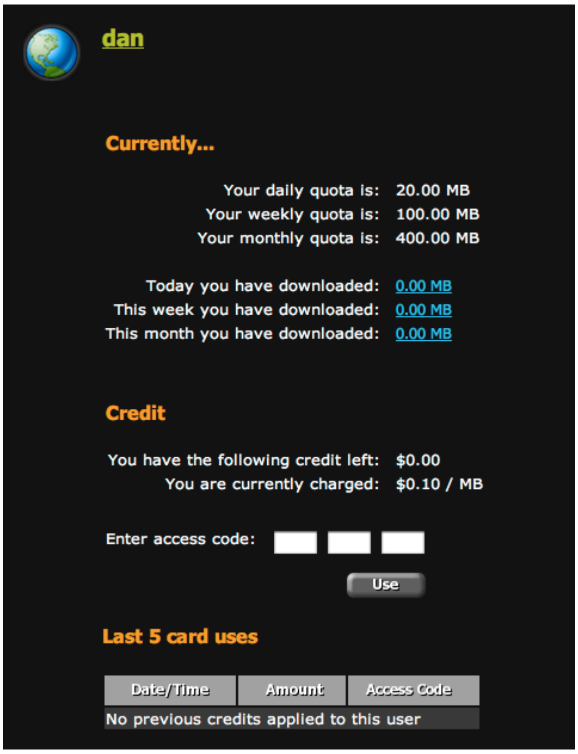
getbusi – Web Access Management
http://202.12.92.60/getbusi/user-status.php
Google
getbusi
Online intelligence. Online control.
Logout
User status login
User name:
Password:
Enter

Figure 48

Once logged in, they will be presented with a status screen showing the current status of their account. Users may use this screen to enter ticket codes to update the credit on their accounts. For information about ticketing functions, see 9.1: Tickets.

Users may also follow the hyper-linked daily, weekly and monthly download totals to view a report on their browsing activity during the respective time period. Users may view complete reports of their activity limited to websites / URLs, time accessed, workstation accessed from and the amount of data that was consumed.

If you wish to disable this feature please contact Getbusi Support.



dan

Currently...

Your daily quota is: 20.00 MB
Your weekly quota is: 100.00 MB
Your monthly quota is: 400.00 MB

Today you have downloaded: 0.00 MB
This week you have downloaded: 0.00 MB
This month you have downloaded: 0.00 MB

Credit

You have the following credit left: $0.00
You are currently charged: $0.10 / MB

Last 5 card uses

Date/Time	Amount	Access Code
No previous credits applied to this user		

Figure 49

9.6 Programmatic Status Interface

Getbusi provides an interface for you to programmatically retrieve user data via the web interface. You may access any user's week-to-date usage, their weekly quota and the amount of credit in their account via the url:

```
http://<IP address or hostname>/getbusi/user-external-data.php?uid=<user id>
```

where <IP address or hostname> is the IP address or hostname of your Getbusi server, and <user id> is the user name of a particular user. For example, if your server's hostname is gbproxy and it's IP address is 192.168.1.4; and you're trying to access the data for the user: bob, then you can retrieve Bob's week-to-date, weekly quota and amount of credit with the following URL:

```
http://gbproxy/getbusi/user-external-data.php?uid=bob
```

or

```
http://192.168.1.4/user-external-data.php?uid=bob
```

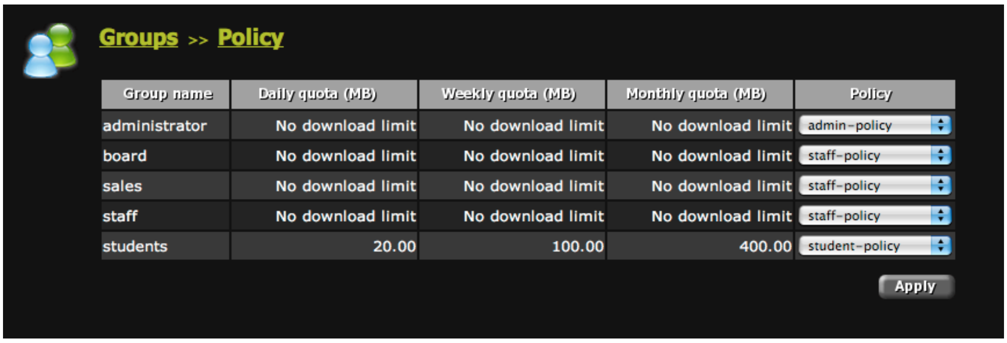
10 Groups

Groups are integral to the way the Getbusi system operates. When your Getbusi system authenticates with your organisation's authentication system, the Getbusi server retrieves all existing groups from your authentication system. Once it has the groups, you can then load users into the system. Your Getbusi system will not load users if they do not belong to a group.

The *Groups* link in the navigation pane allows you to access the functions associated with groups. You may configure group policies, group priorities, or create time-based policies for groups. Expanding the *Groups* link in the navigation pane displays links to these different functions for direct navigation.

10.1 Group Policies

The Group *Policy* screen allows you to assign specific policies that govern Internet access by group. When navigating to the Group *Policy* screen, a table displays all of the groups retrieved from your organisation's authentication system, quotas (if any) imposed by the policies and the name of the policies applied to the groups. The drop-down menus in the **Policy** column will display all configured policies. To add a policy to your system, please see section 6.1: Adding, Copying and Deleting Policies.



Group name	Daily quota (MB)	Weekly quota (MB)	Monthly quota (MB)	Policy
administrator	No download limit	No download limit	No download limit	admin-policy
board	No download limit	No download limit	No download limit	staff-policy
sales	No download limit	No download limit	No download limit	staff-policy
staff	No download limit	No download limit	No download limit	staff-policy
students	20.00	100.00	400.00	student-policy

Figure 50

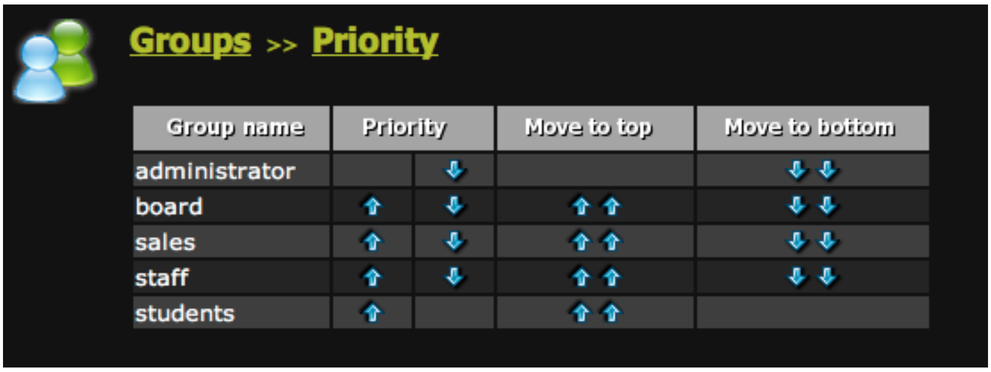
- The groups retrieved from your Authentication server are listed in the left-most column of the table, under the heading: **Group name**. If a group name appears in red, it is no longer accessible from the authentication system.
- The quotas applied by each group's currently assigned policy appears in the three quota columns.
- The available policies are selectable from each group's corresponding drop-down menu in the right-most column of the table, under the heading: **Policy**.
- Select a policy for a group and click on the grey **Apply** button to apply the policy to the group. The table will update to show the effect of the selected policy on the quotas for that group. You may apply policies to multiple groups before clicking on the **Apply** button, or you may apply policies individually. If you wish to remove a group that is no longer accessible from your authentication system (displayed in red text), apply a *No policy assigned* for the group. It will disappear from the table when the page refreshes.
- If a group has no policy applied to it, users contained within that group will be denied access to the Internet.

If you wish, you can override a user's group policy by applying policies to individual users. For information about how to override a user's group policy, see section 9.4: General User Management.

10.2 Group Priorities

The Group Priority screen allows you to set the priority for groups. Group priorities are only used when users belong to multiple groups. When a user belongs to multiple groups, the user will be granted access based on the policy corresponding to the group with the highest priority.

For example, *fred* belongs to the *staff* group and the *board* group. If the *staff* group has daily, weekly and monthly quotas set, but the *board* group has no quotas set, and the *board* group has a higher priority than the *staff* group, then *fred* will have no quotas on his Internet access. However, if the *staff* group is given a higher priority, then *fred* will have the same Internet access quotas as other members of the *staff* group.



Groups >> Priority

Group name	Priority		Move to top	Move to bottom
administrator		⇩		⇩ ⇩
board	⇧	⇩	⇧ ⇧	⇩ ⇩
sales	⇧	⇩	⇧ ⇧	⇩ ⇩
staff	⇧	⇩	⇧ ⇧	⇩ ⇩
students	⇧		⇧ ⇧	

Figure 51

Figure 51 shows the Group Priority screen. Groups are ordered in priority from top to bottom, with the top being the highest priority, and the bottom being the lowest. The arrows in a group's row indicate the direction the group will move when clicked. Single arrows move a group one step. The double arrows will move the group to either the top or bottom of the table. Re-assignment of group priorities take effect immediately.

Please note that the Group Priority screen will not give one group priority in accessing Internet resources over another. It is only used to determine which policy applies to users when they belong to multiple groups.

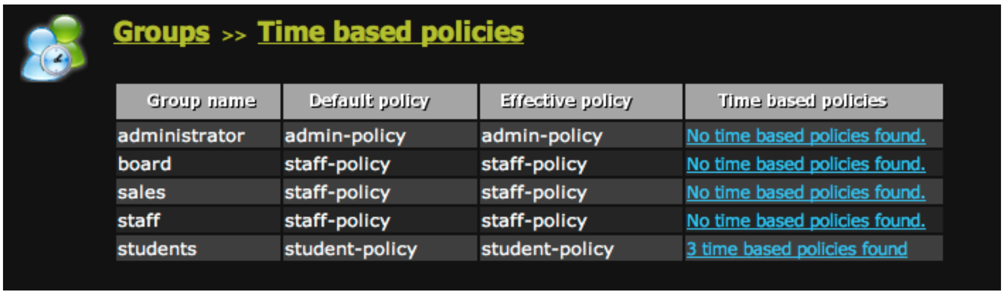
10.3 Time Based Policies

Time based policies allow you to apply enforce different policies to a group depending on time. You may configure time-based policies to be enforced within a specific date range, on specific day-of-week, or any combination of date range/day-of-week. You may further refine the time-based policy to be applied with a time-range within a date or day-of-week range.

Prior to configuring a time based policy, it may be helpful to first create specific policies for the time based policy. For information on how to create customised policies, see section 6.1: Adding, Copying and Deleting Policies.

10.3.1 Creating Time Based Policies

When navigating to *Time Based Policies*, you are first presented with a table listing all groups in the system. The *Default policy* column displays the base policies for the groups. The *Effective policy* column displays the policy currently applied to the groups. If a group has a time based policy, then the policy for the current time will be displayed in the *Effective policy* column. The *Time based policies* column displays the number of time based policies configured for each group, and displays *No time based policies found*, if there are no time based policies configured for a group.

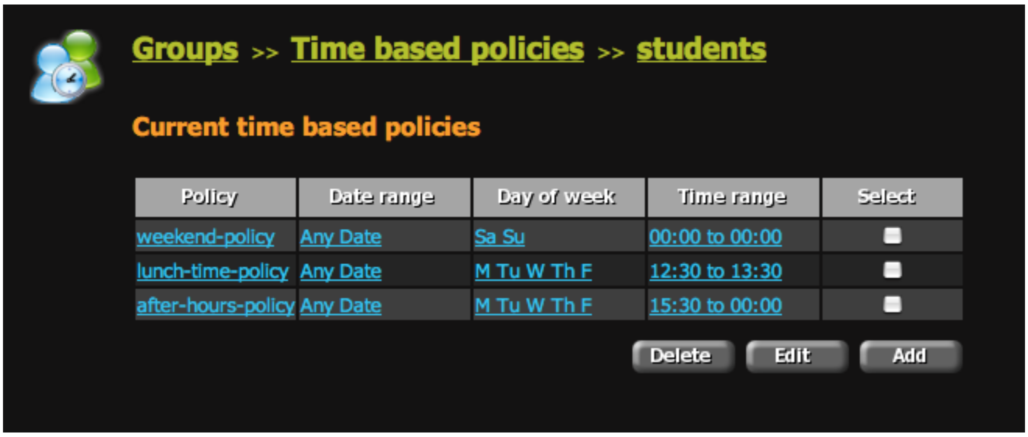


Groups >> Time based policies

Group name	Default policy	Effective policy	Time based policies
administrator	admin-policy	admin-policy	No time based policies found.
board	staff-policy	staff-policy	No time based policies found.
sales	staff-policy	staff-policy	No time based policies found.
staff	staff-policy	staff-policy	No time based policies found.
students	student-policy	student-policy	3 time based policies found

Figure 52

- To create or modify a time based policy for a group, click on the link in the *Time based policy* column that corresponds with the group you are modifying. A new table will display to show the time based policies (if any) that are configured for that group.



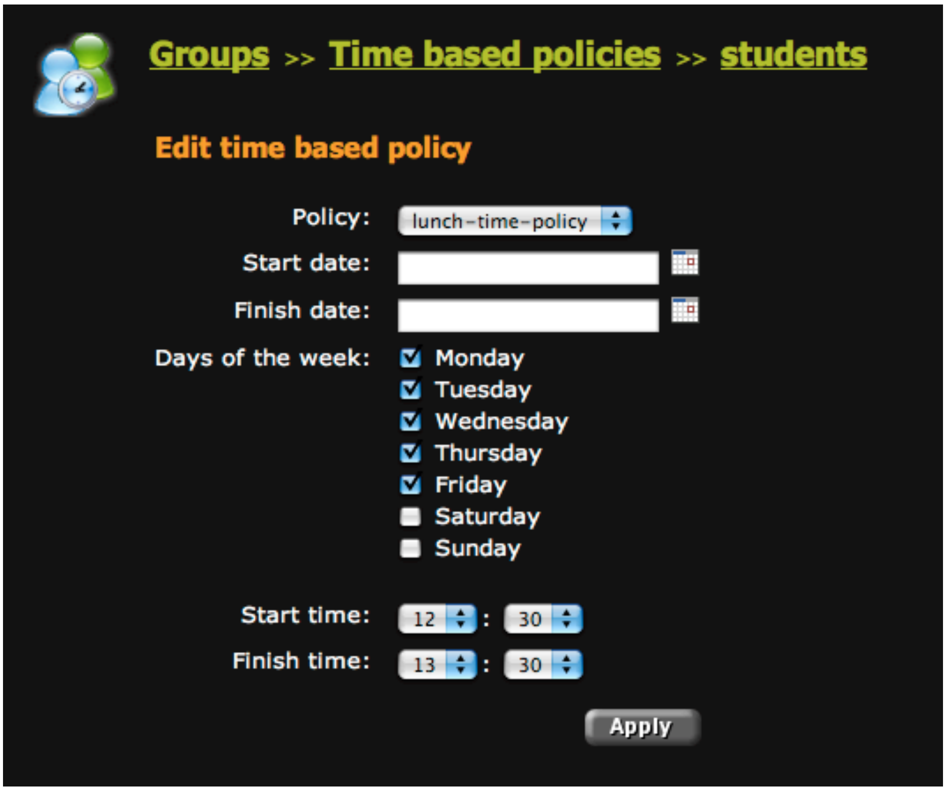
Groups >> Time based policies >> students

Current time based policies

Policy	Date range	Day of week	Time range	Select
weekend-policy	Any Date	Sa Su	00:00 to 00:00	□
lunch-time-policy	Any Date	M Tu W Th F	12:30 to 13:30	□
after-hours-policy	Any Date	M Tu W Th F	15:30 to 00:00	□

Figure 53

- To add a new time based policy for the group, click on the grey **Add** button.
- To delete an existing time based policy, click on the check box that corresponds with the policy you wish to delete, and click on the grey **Delete** key.
- To modify an existing time based policy, click on any of the links corresponding to the time based policy, or check the policy's corresponding check box and click on the grey **Edit** key.
- The time based policy editor will appear when you add a new policy, or modify an existing policy.



Groups >> Time based policies >> students

Edit time based policy

Policy: lunch-time-policy

Start date:

Finish date:

Days of the week:
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
□ Saturday
□ Sunday

Start time: 12 : 30

Finish time: 13 : 30

Figure 54

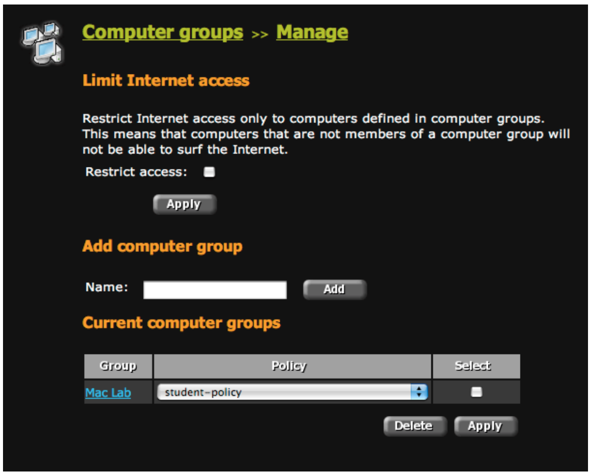
- When the time based policy editor appears, you can select a policy to apply using the *Policy* drop-down menu.
- Select a start date and end date by using the calendar icons next to the *Start date* and *End date* text boxes, if you wish to restrict the policy to a date range. If you don't want a date range, leave these fields blank.
- Select the days of the week you wish to the policy to be applied. If you don't want to use days of the week, leave these check boxes unselected.
- Select the time range you wish the policy to be applied using the drop-down menus. Leaving these selected at their default of 00:00 for the start and end time applies the policy to all hours of the day.
- If you attempt to configure a time based policy that overlaps with a previously configured time based policy, you will be warned of an overlap, and prompted to fix the conflict. You may not configure overlapping time based policies for a group.
- When you have finished configuring the parameters for your time based policy, click on the grey **Apply** button. The *Current time based policies* table will update to reflect your changes when the page refreshes.

11 Computer Groups

Computer groups allow you to configure policies by grouping computers into functional areas. Computer groups may be configured to coexist with users and user group policies, or may have explicit policies applied to them. Please note that when applying an explicit policy to a computer group, that policy will override any policies for users using a workstation belonging to that computer group. Another effect of this configuration is that any reporting will be against the workstation and not against the user.

11.1 Creating, Managing and Deleting Computer Groups

The Getbusi system does not have pre-configured computer groups. In order to apply a policy, or otherwise manage to a computer group, you must first create the group. You may also delete existing computer groups from your Getbusi system.



Computer groups >> Manage

Limit Internet access

Restrict Internet access only to computers defined in computer groups. This means that computers that are not members of a computer group will not be able to surf the Internet.

Restrict access: □

Add computer group

Name:

Current computer groups

Group	Policy	Select
Mac Lab	student-policy	□

Figure 55

- To create a new computer group, type the name of the group in the *Name* text box and click on the grey **Add** button. The *Current computer groups* table will refresh to display the name of your new computer group. By default, no policy will be assigned to the new group.
- To apply a policy to your newly created computer group, or to change the applied policy to an existing computer group, click on the drop-down menu in the *Policy* column that corresponds to the computer group you are configuring. A list of available policies are displayed in the drop-down menu's list. When you have selected the policy you wish to apply to your computer group, click on the grey **Apply** button. The table will refresh to reflect your configuration changes.
- To delete an existing computer group, click on the check box that corresponds with the computer group you wish to delete in the *Current computer groups* table. Click on the grey **Delete** button to permanently delete the computer group from your system.
- To add computers to your computer group, click on the name of the computer group in the *Current computer groups* table. A configuration screen allowing you to add members to your computer group will appear. From that screen, you may add member computers to your computer group by IP Range, or by individual IP address.

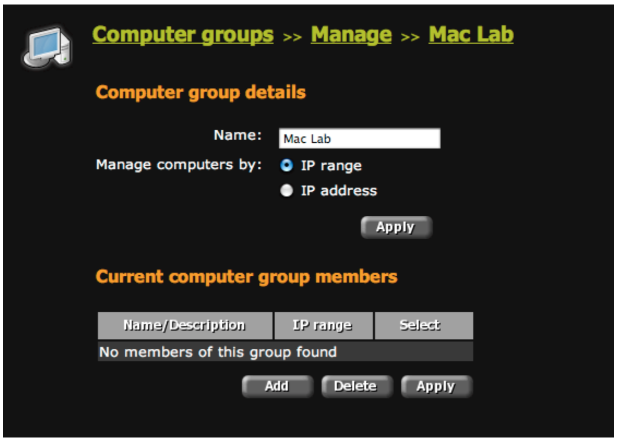
11.1.1 Restricting Access to Computer Group Members

You may choose to restrict Internet access to only those workstations which belong to a computer group. Any workstations not explicitly defined in a computer group will be denied access. If you restrict Internet access to only computer groups, valid users in the system using workstations not belonging to a computer group will be denied access.

Please refer to Figure 55. To restrict access to only those workstations belonging to a computer group, click the *Restrict Access* check-box and click the corresponding grey **Apply** button.

11.1.2 Adding Members by IP Range

To add members to your computer group by range, ensure that the *IP range* radio button is selected. Under the *Current computer group members* table, click on the grey **Add** button to add a new range of computers to your computer group.



Computer group details

Name: Mac Lab

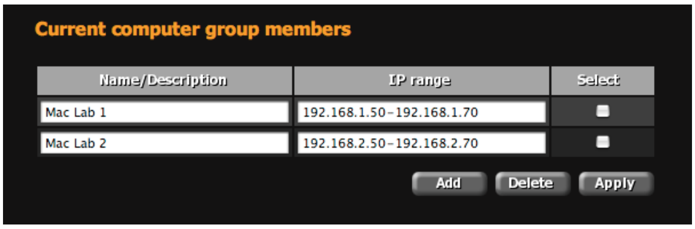
Manage computers by: ● IP range ○ IP address

Current computer group members

Name/Description	IP range	Select
No members of this group found		

Figure 56

In Figure 56, two computer group ranges have been added to illustrate allowable ranges. The first range, named Computer Lab 1, consists of computers on the 192.168.1.x subnet between IP addresses 1 - 254. This range potentially adds 255 computers (if all of those IP addresses are allocated to machines). The second range, named Computer Lab 2, consists of computers on three subnets: 192.168.2.x - 192.168.3.x, which theoretically allows 765 computers. You may configure a range to allow up to 1000 computers in a single range entry.



Current computer group members

Name/Description	IP range	Select
Mac Lab 1	192.168.1.50-192.168.1.70	□
Mac Lab 2	192.168.2.50-192.168.2.70	□

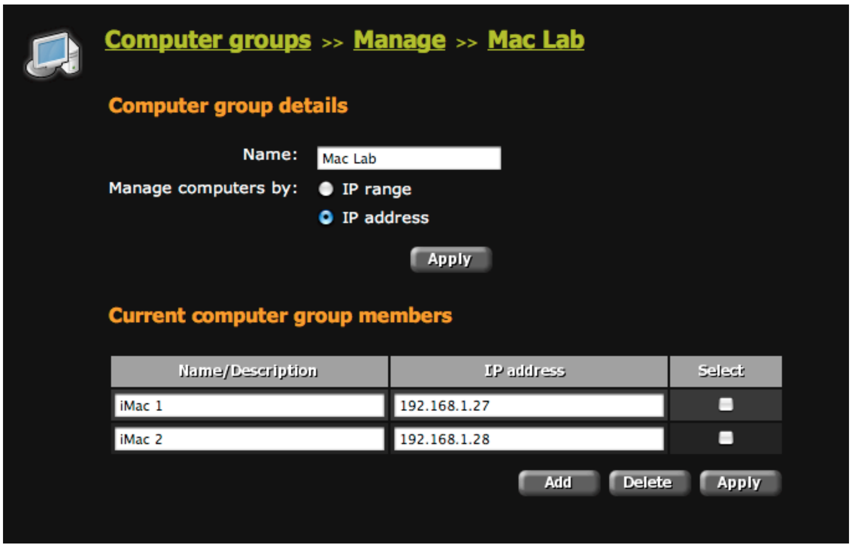
Figure 57

- To add a new range, ensure that the *IP range* button is selected and applied. Click on the grey **Add** button under the *Current computer group members* table. A new row will appear in the table.
- Type a unique name to identify the range of computers you're adding in the *Name/ Description* text field.
- Type in a valid range of IP addresses in the exact format as the example. You may not have spaces nor wildcards in the *IP range* text box.
- To save your newly created range, click on the grey **Apply** button. The table will refresh to show your newly created range.
- To delete a range, click on its corresponding check box and click on the grey **Delete** button. Deleted entries are not retrievable.
- To modify an existing range, simply modify the range in the *IP range* field that corresponds with the range you wish to modify. Click on the grey **Apply** button to save your changes.

11.1.3 Adding Members by IP Address

Selectively adding individual computers to a computer group allows you a fine granularity of control when creating computer groups. In order to add a computer to a computer by IP address, you must **first** ensure that the IP address radio button is selected, and **Applied**.

Please note that if you have previously added an IP address range to your computer group, when you try to add by IP address, all of the computers in the range will be converted to individual computer entries. If your range is large, it will make the *Current computer group members* table very large.



Computer group details

Name: Mac Lab

Manage computers by: ○ IP range ● IP address

Current computer group members

Name/Description	IP address	Select
iMac 1	192.168.1.27	□
iMac 2	192.168.1.28	□

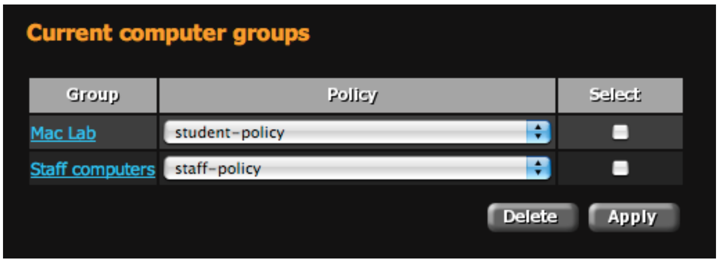
Figure 58

- To add an individual computer's IP address, first ensure that the IP address radio button is selected and click on the grey **Apply** button. See the note above for important information.
- To add a new workstation to your computer group, click on the grey **Add** button beneath the *Current computer group members* table. A new row will appear in the table.
- Add a descriptive name for the workstation you're adding in the *Name/Description* field. A good candidate would be the actual hostname of the computer.
- Add the workstation's IP address in the *IP address* field.
- Click on the grey **Apply** button to apply your changes.
- To modify an existing entry, just change the entry you wish to modify and click on the grey **Apply** button.
- To delete an existing entry, click on the entry's corresponding check box and click on the grey **Delete** button. The entry will be irretrievably removed.

11.2 Assigning Policies to Computer Groups

Once you have created a computer group, you can assign a policy to govern it. To assign a policy, navigate back to the *Computer Groups* link in the navigation pane and then select *Manage*. You will be back on the same page where you initially went to create the computer group, but in the *Current computer groups* table, your computer group will be displayed.

You may choose to assign an explicit policy to a computer group, or you may use user-based policies. If you assign an explicit policy to a computer group, it will override any user policies, and any user may use the workstation (even if they do not exist as a user in your system). If you assign user defined policies to a computer group, only users that exist in the Getbusi system and have a policy assigned will have access to Internet resources.



Current computer groups

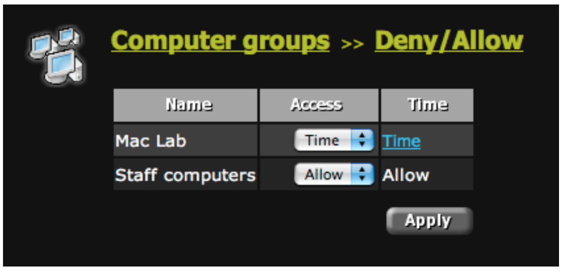
Group	Policy	Select
Mac Lab	student-policy	□
Staff computers	staff-policy	□

Figure 59

- To assign (or reassign) a policy to your computer group, click on the drop-down menu corresponding to the computer group. The drop-down menu will list the available policies in your system. Click on the grey **Apply** button to save your changes.

11.3 Deny/Allow Access and Time Based Denial

By default , when you create a computer group, access to Internet resources is allowed for all members of the group, based on the policies assigned. If you wish, you may quickly disable access for all members of a computer group. You may also deny access based on time for your computer groups. To deny, allow or configure time based denials, click on the *Computer groups* link in the navigation pane, and then click on the *Deny/Allow* link. A table displaying configured computer groups and their access status appears when the page refreshes.



Computer groups >> Deny/Allow

Name	Access	Time
Mac Lab	Time	Time
Staff computers	Allow	Allow

Figure 60

11.3.1 Denying and Allowing Access

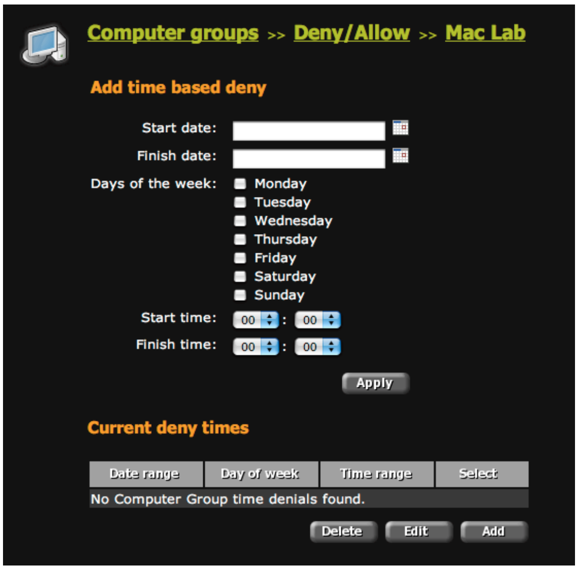
To deny access to a computer group, select *Deny* from the drop-down menu that corresponds to the computer group and click on the grey **Apply** button. Even if a valid user with an undenied access policy tries to access Internet resources from a workstation that has been denied, the user will be denied, but only from that workstation.

To allow access to a denied computer group, or a computer group with a time based denial, select *Allow* from the drop-down menu that corresponds to the computer group and click on the grey **Apply** button.

11.3.2 Time Based Access Denial

To configure your computer group to only have access during certain times of the day, select *Time* from the drop-down menu that corresponds to the computer group and click on the grey **Apply** button.

When the table refreshes, a *Time* link will appear in the table's *Time* column. Clicking on the *Time* link will bring you to a configuration page displaying a *Current deny times* table that shows any configured time-based denials. The grey buttons below the table allow you to **Add**, **Edit**, or **Delete** time-based denials.



Add time based deny

Start date:

Finish date:

Days of the week:
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday
□ Sunday

Start time: 00 : 00

Finish time: 00 : 00

Current deny times

Date range	Day of week	Time range	Select
No Computer Group time denials found.			

Figure 61

11.3.2.1 Adding a Time Based Denial Entry

Clicking on the grey **Add** button displays the time based denial editor.

- If you wish to specify a date range for which to deny a computer group, use the calendar icons next to the *Start date* and *Finish date* text boxes and select the date range from each calendar. The date fields will populate with the selections based on your calendar input. No input in these fields will indicate an unlimited date range.
- If you wish to specify specific days of the week to deny a computer group, use the check-boxes that correspond with the days of the week. No checks in the days of the week indicates all days of the week.
- If you wish to specify a time range, use the hours and minutes drop-down menus that correspond to *Start time* and *Finish time*. If no time ranges are selected, then all hours of the day are chosen.
- Click on the grey **Apply** button to accept your changes.

11.3.2.2 Editing a Time Based Denial Entry

To edit an existing time based denial, select the time based denial link in the *Current deny times* table. The editor will refresh to reflect all properties of the entry. Make the necessary edits and click on the grey **Apply** button to accept your changes.

11.3.2.3 Deleting a Time Based Denial Entry

To delete an existing time based denial, select the check-box in the *Select* column of the *Current deny times* table that corresponds with the entry you wish to delete. Click on the grey **Delete** button to irreversibly delete the entry.

12 System Properties

The System Properties link in the navigation pane allows you to configure the way your Getbusi system functions. You may access subsections of system properties by expanding on the *System Properties* link in the navigation pane, or you can access each section from the configuration pane by clicking on the *System Properties* link. These system properties are the same properties set when the system was initially configured, and when navigating to any system properties, the values will reflect the current system settings.

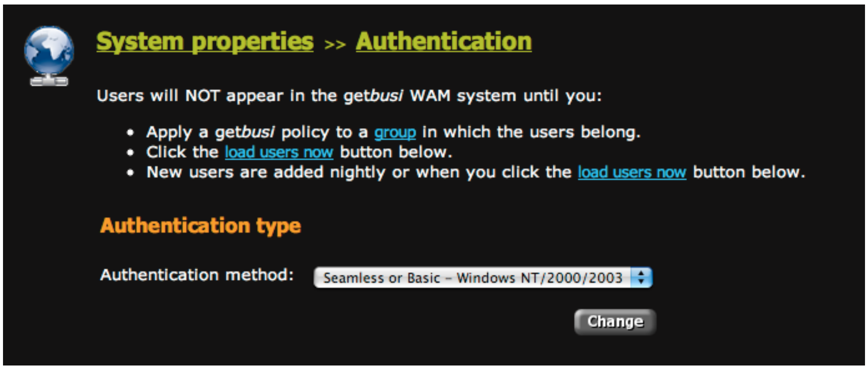
12.1 Authentication

The **Authentication** link allows you to configure the authentication method that best suits your organisation's existing authentication infrastructure (if any). The authentication method determines what type of directory service the Getbusi system will use to retrieve user and group information. If you do not have a pre-existing authentication infrastructure and wish to use the built-in Getbusi LDAP, please see the **Getbusi Built-in LDAP Guide** before proceeding.

Please use the information identified in your Authentication Checklist to help you properly set up and configure authentication for your Getbusi system.

12.1.1 Selecting Authentication Type

Under the **Authentication Type** heading, a drop-down menu listing the supported authentication types allows you to select the one best suited for your organisation. Select the type of authentication you wish to set for your Getbusi system and click the grey **Change** button. Upon page refresh, the form fields being displayed on the rest of the page may change to reflect the correct options for the selected authentication type.



System properties >> Authentication

Users will NOT appear in the get*busi* WAM system until you:

- Apply a get*busi* policy to a group in which the users belong.
- Click the load users now button below.
- New users are added nightly or when you click the load users now button below.

Authentication type

Authentication method: Seamless or Basic – Windows NT/2000/2003

Figure 62

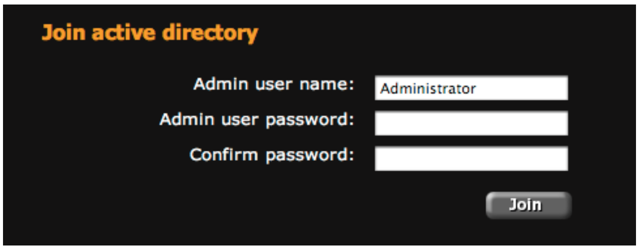
12.1.2 Active Directory Authentication

In Windows Active Directory environments, you may choose to either have seamless or basic authentication. With seamless authentication, your users will not be prompted for a username and password when using a browser to surf the web. Seamless authentication uses the authentication tokens from a user's Windows desktop login to allow access to Internet resources. In order for seamless authentication to work, the Getbusi system must be allowed to join your organisation's Windows Active Directory domain.

If you do not wish the Getbusi system to join Active Directory, you can still have users authenticate against Active Directory for web access, but users will be prompted with a username/password dialogue box when accessing Internet resources.

12.1.2.1 Join Active Directory

The information used to join Active Directory is neither recorded nor saved by the Getbusi system, and does not compromise the security of your Windows network. If you do not wish for Getbusi to join Active Directory, skip these steps and proceed to entering your Authentication Details.



Join active directory

Admin user name: Administrator

Admin user password:

Confirm password:

Figure 63

1. In the **Admin user name** field, enter the user name of an administrative user. This user must have the required privileges to allow the Getbusi system to join the domain. Typically, this is the Administrator user.

2. In the **Admin user password** field, enter the administrative user's password.

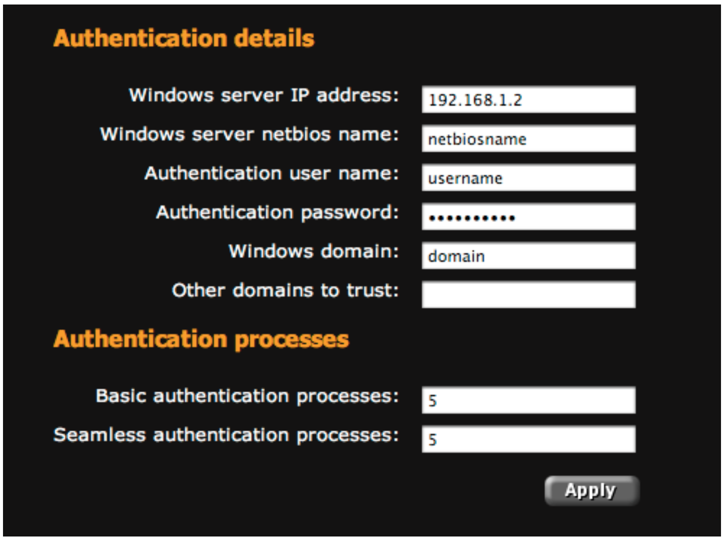
3. In the **Confirm password** field, retype the administrative user's password.

4. Click the grey **Join** button to join Active Directory. You will be provided feedback on whether the Getbusi system successfully joined the domain.

12.1.2.2 Authentication Details

The Authentication Details section is required for Getbusi to get the groups and users from Active Directory.

Prior to configuring Getbusi to integrate into your Microsoft Windows domain, you should create an Authentication User for Getbusi on your Windows server. If you are running Windows 2000 or 2003 Server, this user must be made part of the "Pre-Windows 2000 compatible access" group. No other access privileges for this user are required. Although you may use your Administrator User for this purpose, this practice is **seriously** discouraged, as the username and password are written to a configuration file on the Getbusi server, and could lead to a security compromise of your Windows server.



Authentication details

Windows server IP address: 192.168.1.2

Windows server netbios name: netbiosname

Authentication user name: username

Authentication password: ••••••••••

Windows domain: domain

Other domains to trust:

Authentication processes

Basic authentication processes: 5

Seamless authentication processes: 5

Figure 64

1. In the **Windows server IP Address** field, enter the IP address of a Windows Domain Controller for your Windows domain.

2. In the **Windows server netbios name** field, enter the netbios name of the same Windows Domain Controller from step 1.

3. In the **Authentication user name** field, enter the username of the Authentication User you created for the Getbusi system.

4. In the **Authentication password** field, enter the password corresponding the Authentication User you created for the Getbusi system.

5. In the **Windows domain** field, enter the top-level name of your Windows domain. If you have an Active Directory domain named *mydomain.local*, you only need to enter *mydomain*.

6. In the **Other domains to trust** field, you may optionally supply a comma separated list of trusted Active Directory domains, allowing Getbusi to serve users from those trusted domains. The following conditions need to be satisfied:

    - A two-way trust must exist between the domain controller identified in step 1 and the domain controllers serving the trusted domains listed.
    - User accounts for all users in the trusted domains must exist in the domain controller identified to Getbusi.
    - Passwords for these users must match across all of the domains.

12.1.2.3 Authentication Processes

The following two fields control the number of authentication processes to run on the Getbusi server. These authentication processes allow client access to Internet resources.

The calculation to establish the number of authentication processes for each of the authentication types can be determined by dividing the number of workstations using the Getbusi system by 5. **Even if you are using seamless authentication, the minimum recommended number of basic authentication processes is 5**, which corresponds to 25 workstations. Do not set the number of basic authentication processes to 0, because it will disable the Temporary Users feature of your Getbusi system, as well as disable access for clients not in Active Directory. The maximum recommended value for basic authentication processes is 50 (450 workstations).

If you are not using seamless authentication, you may set the value for seamless authentication processes to 0. The maximum number of seamless authentication processes is 50 (450 workstations).

1. In the **Basic authentication processes** field, enter the number of Basic authentication processes to be run on your Getbusi system.

2. In the **Seamless authentication processes** field, enter the number of seamless authentication processes to be run on your Getbusi system.

3. Click the grey **Apply** button to save your settings.

4. At the top of the screen, you will see an indication that the system is processing your parameters. When the processing is complete, click the grey **Next** button in the upper right-hand corner of your browser window.

You have now finished configuring authentication for Active Directory (Seamless or Basic - Windows NT/2000/2003/2008).

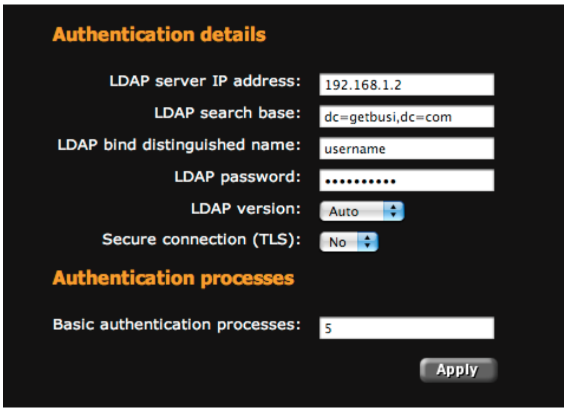
12.1.3 LDAP Authentication (POSIX, Mac OS X, Novell only)

This section documents how to configure the LDAP-based authentication methods.

The **LDAP - POSIX** authentication type is suitable for environments using an authentication scheme based on OpenLDAP.

The **LDAP - Mac OS X Open Directory** option is suitable for environments running Apple Macintosh OS X Server's built-in Open Directory services.

The **LDAP - Novell eDirectory** option is suitable for environments running Novell's eDirectory LDAP directory services.



Authentication details

LDAP server IP address: 192.168.1.2

LDAP search base: dc=getbusi,dc=com

LDAP bind distinguished name: username

LDAP password: ••••••••••

LDAP version: Auto

Secure connection (TLS): No

Authentication processes

Basic authentication processes: 5

Figure 65

12.1.3.1 Authentication Details

1. In the **LDAP server IP address** field, enter the IP address of the LDAP server against which you are authenticating.

2. In the **LDAP search base** field, enter the search base for your LDAP directory. The search base defines the location in the directory from which the LDAP search begins.

3. In the **LDAP bind distinguished name** field, enter the user name to connect to your LDAP services with.

    - For most LDAP implementations, this may be left blank, as most allow anonymous binding.
    - If you implement Novell eDirectory, if the username is required, it must be fully qualified. For example, if your username is *admin* and your search base is *o=mysite*, then the LDAP bind distinguished name will be: *cn=admin, o=mysite*.

4. In the **LDAP password** field, enter the password corresponding with the username you are using to connect to your LDAP services. Leave this blank if you are not using a username.

5. In the **LDAP version** drop-down list, set this to the version of LDAP running on your authentication server, or leave this set to *Auto*. Not all versions of LDAP require this to be set.

    - If you are running Mac OS X Open Directory, set this to *LDAPv3*.

6. In the **Secure connection (TLS)** drop-down list, select *Yes* if you use TLS (Transport Layer Security) when authenticating against your LDAP services.

12.1.3.2 Authentication Processes

The following determines the number of basic authentication processes to run on the Getbusi server. These authentication processes allow client access to Internet resources.

The calculation to establish the number of basic authentication processes can be determined by dividing the number of workstations using the Getbusi system by 5. The recommended minimum number basic authentication processes is 5, which corresponds to 25 workstations. The maximum recommended value for basic authentication processes is 50 (450 workstations).

1. In the **Basic authentication processes** field, enter the number of Basic authentication processes to be run on your Getbusi system.

2. Click the grey **Apply** button to save your settings.

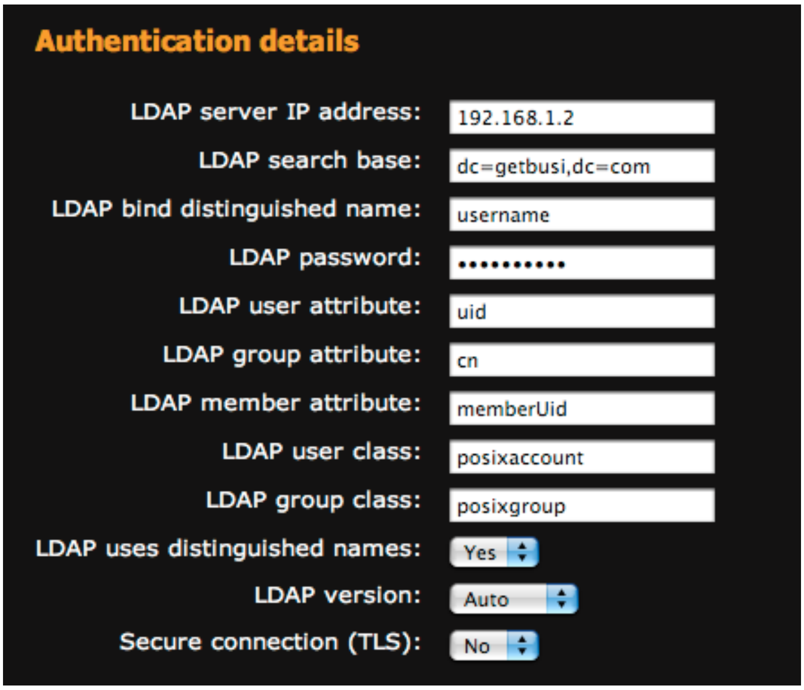
3. At the top of the screen, you will see an indication that the system is processing your parameters. When the processing is complete, click the grey **Next** button in the upper right-hand corner of your browser window.

You have now finished configuring authentication for LDAP (POSIX, Mac OS X or Novell eDirectory only).

12.1.4 LDAP Authentication (Other)

Use the **LDAP - Other** authentication method for LDAP implementations that neither based upon OpenLDAP nor are POSIX compliant.

12.1.4.1 Authentication Details



Authentication details

LDAP server IP address: 192.168.1.2

LDAP search base: dc=getbusi,dc=com

LDAP bind distinguished name: username

LDAP password: ••••••••••

LDAP user attribute: uid

LDAP group attribute: cn

LDAP member attribute: memberUid

LDAP user class: posixaccount

LDAP group class: posixgroup

LDAP uses distinguished names: Yes

LDAP version: Auto

Secure connection (TLS): No

Figure 66

1. In the **LDAP server IP address** field, enter the IP address of the LDAP server against which you are authenticating.

2. In the **LDAP search base**, enter the search base for your LDAP directory. The search base defines the location in the directory from which the LDAP search begins.

3. In the **LDAP bind distinguished name** field, enter the user name to connect to your LDAP services with. This may be left blank if your LDAP server allows anonymous binding.

4. In the **LDAP password** field, enter the password corresponding with the username you are using to connect to your LDAP services. Leave this blank if you are using anonymous binding in step 3.

5. In the **LDAP user attribute** field, enter the attribute identifying a user name within the organisational unit containing users.

6. In the **LDAP group attribute** field, enter the attribute identifying a group name within the organisational unit containing groups.

7. In the **LDAP member attribute** field, enter the attribute identifying a user as being part of a group within the organisational unit containing users.

8. In the **LDAP user class** field, enter the name identifying the class of organisational unit representing users.

9. In the **LDAP uses distinguished names** drop-down list, select *yes* if a group member uses their distinguished name to identify them as part of a group.

10. In the **LDAP version** drop-down list, select set this to the version of LDAP running on your authentication server, or leave this set to *Auto*. Not all versions of LDAP require this to be set

11. In the **Secure connection (TLS)** drop-down list, select *Yes* if you use TLS (Transport Layer Security) when authenticating against your LDAP services

12.1.4.2 Authentication Processes

The following determines the number of basic authentication processes to run on the Getbusi server. These authentication processes allow client access to Internet resources.

The calculation to establish the number of basic authentication processes can be determined by dividing the number of workstations using the Getbusi system by 5. The recommended minimum number basic authentication processes is 5, which corresponds to 25 workstations. The maximum recommended value for basic authentication processes is 50 (450 workstations).

1. In the **Basic authentication processes** field, enter the number of Basic authentication processes to be run on your Getbusi system.

2. Click the grey **Apply** button to save your settings.

3. At the top of the screen, you will see an indication that the system is processing your parameters. When the processing is complete, click the grey **Next** button in the upper right-hand corner of your browser window.

4. You have now finished configuring authentication for LDAP - Other.

12.1.5 LDAP - Getbusi

For LDAP - Getbusi, the only value that needs to be set is the number of basic authentication processes. These authentication processes allow client access to Internet resources.

The calculation to establish the number of basic authentication processes can be determined by dividing the number of workstations using the Getbusi system by 5. The recommended minimum number basic authentication processes is 5, which corresponds to 25 workstations. The maximum recommended value for basic authentication processes is 50 (450 workstations).

1. In the **Basic authentication processes** field, enter the number of Basic authentication processes to be run on your Getbusi system.

2. Click the grey **Apply** button to save your settings.

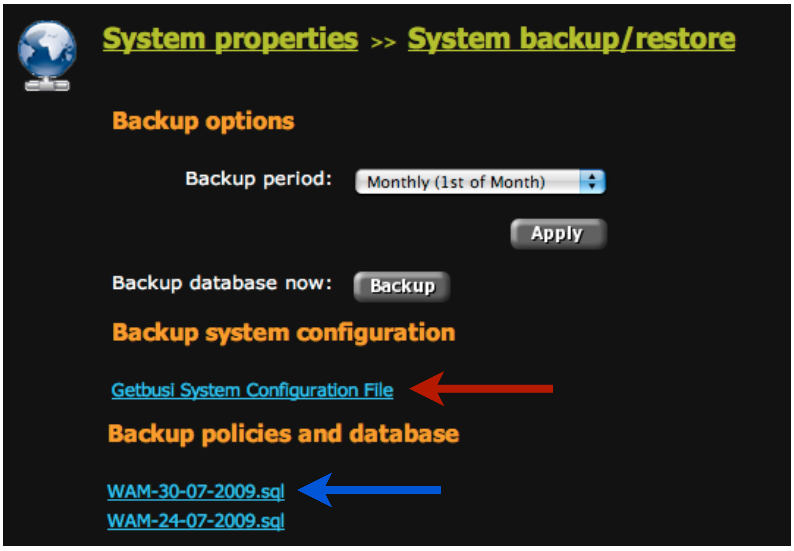
3. At the top of the screen, you will see an indication that the system is processing your parameters. When the processing is complete, click the grey **Next** button in the upper right-hand corner of your browser window.

12.2 Backup / Restore

The **System backup/restore** page allows you to back up or restore two critical components of your Getbusi system: your system configuration and your system's database.

12.2.1 Backing Up your Database

You may configure the system to automatically backup your database on a pre-determined schedule, or you may manually backup your system.



System properties >> System backup/restore

Backup options

Backup period: Monthly (1st of Month)

Backup database now:

Backup system configuration

Getbusi System Configuration File

Backup policies and database

WAM-30-07-2009.sql
WAM-24-07-2009.sql

Figure 67

- To configure your database backup frequency, select the frequency in the drop-down menu, and click the grey **Apply** button.
- To perform a one-time on-demand backup of your database, click on the grey **Backup** button. It is important not to backup your database during periods of high activity or load.
- To download your Getbusi configuration file to your desktop machine, click the **Getbusi System Configuration File** link. The red arrow in Figure 67 shows where the link is located.
- To download a database backup to your desktop, click one of the **WAM-<date>.sql** files. The blue arrow in Figure 67 shows where those links are located. Note that there will be up to five links, each downloading the backup that was made on the date indicated in the link.

12.2.2 Restoring your Getbusi Server

To restore either your Getbusi server configuration or your database, click on the grey **Browse** button and navigate to where you've saved the backups on your local system. Click on the grey **Import** button to import the file. The system will automatically restore the configuration file or database.

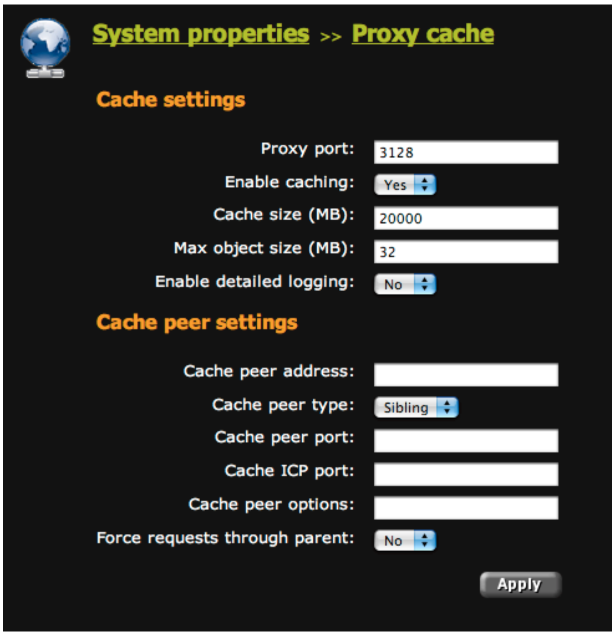
Please proceed to the section 12.3: Cache.

12.3 Cache

You Getbusi server is a caching proxy. This means that whenever possible, it will cache (store) previously served requests so that subsequent requests for that resource will be served from it's cache, rather than retrieving the request from the original source. This can greatly improve your Internet performance while reducing your upstream bandwidth usage.

The Proxy Cache screen allows you to set parameters associated for the proxy. The screen is split into two sections: **Cache Settings** and **Cache Peer Settings**. **Cache Settings** are used to tune the actual proxy cache, and may affect the performance of your Getbusi server.

For those who have a separate external upstream proxy, provided by either your organisation or your Internet Service Provider, the **Cache Peer Settings** allow you to configure the Getbusi system so that it uses that external upstream proxy for access to Internet resources.



System properties >> Proxy cache

Cache settings

Proxy port: 3128

Enable caching: Yes

Cache size (MB): 20000

Max object size (MB): 32

Enable detailed logging: No

Cache peer settings

Cache peer address:

Cache peer type: Sibling

Cache peer port:

Cache ICP port:

Cache peer options:

Force requests through parent: No

Figure 68

12.3.1 Cache Settings

- The **Proxy port** field allows you to set the port on which your Getbusi system serves requests. The default port is *3128*, but some have a preference for *8080*. This port is the one you will also specify in your browser settings when setting up browsers to use your Getbusi system for Internet access. Please be careful not to set this port number to a port number being used by another service.
- The **Enable caching** drop-down list allows you to enable or disable caching. The default is to enable caching. Set this to *No* if you don't want your Getbusi system to cache requests.
- The **Cache size (MB)** field allows you to set the amount of disk space (in megabytes) the proxy cache uses. It is recommended that you restrict this value to no more than half of your hard disk drive's capacity, unless you have a dedicated hard drive for your proxy cache. In that event, it is recommended that you set this to no more than 80% of your hard disk drive's capacity. The default setting for this field is *20000* MB (20 GB).
- The **Max object size (MB)** field allows you to set the maximum file size that your Getbusi system will cache. If a file exceeds this setting, your Getbusi will not cache the file. The minimum setting for this field is *4* MB, and the default is *32* MB.

- The **Enable detailed logging** drop-down list allows you to enable or disable detailed logging of the proxy cache subsystem. This field is for troubleshooting, and should be left at the default value of *No*.

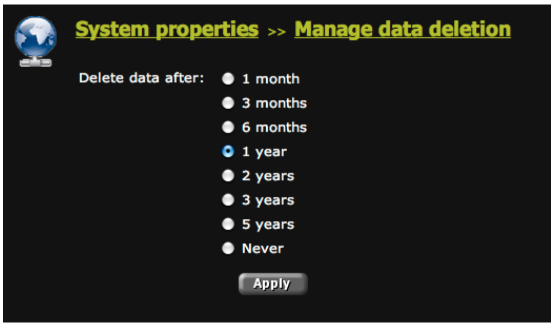
12.3.2 Cache Peer Settings

- The **Cache peer address** field allows you to identify an external proxy with which to peer. If you wish to peer with an external proxy, enter its IP address in this field. Leave blank if you are not peering.
- The **Cache peer type** drop-down list allows you to select the type of peering to implement. Select *Parent* if you are peering to a parent (or upstream) proxy to gain access to Internet resources. Select *Sibling* if your proxy is working in tandem with another sibling caching proxy. Note that non-ICP neighbours should be specified as a *Parent*.
- The **Cache peer port** field should be set to the port number on which your peering proxy (if set) is listening.
- The **Cache ICP port** field should be set if your Getbusi proxy is working cooperatively with other peers. If your Getbusi proxy is not working cooperatively with other peers, it should be set to *0.* The standard port number for ICP is *3130*.
- The **Cache peer options** field may take multiple, comma-separated values. Some of the options are:
  - If your upstream proxy requires proxy authentication from a single username and password, enter: *login=username:password*. Please note that if your username contains spaces, use the URL escape: *%20* to represent the space. For example, if the username is: *john smith*, then the value would be: *login=john%20smith:password*.
  - If each of your users need to individually authenticate against your upstream proxy, then enter: *login=PASS*. Please note that this will expose your user's password to the upstream proxy. Please use with caution.
  - If you need to pass just the username to your upstream proxy, but with a fixed password for all users, enter: *login=*:password*. This scenario is meant to be used when your peer is in another administrative domain, but still needs to identify each user. The asterisk may optionally be followed by extra information which is added to the username, helping identify the Getbusi server to the peer.
  - If you wish to prevent user's bandwidth restrictions affecting the connection between the Getbusi server and the upstream proxy, enter: *no-delay*.
  - If the upstream proxy is not being used with ICP, enter: *no-query* to prevent ICP queries from occurring.
  - If you do not wish to locally cache objects that are already in the upstream proxy's cache (to prevent duplication), then enter: *proxy-only.*
  - If you wish to limit the number of connections that the Getbusi system will open with the upstream proxy, enter: *max-conn*.
- The **Force requests through parent** drop-down list allows you to select if all requests should go through the upstream proxy, or just requests that can be cached. Some requests, like search engine results cannot be cached. If you set this to *No*, then non-cacheable requests will bypass the upstream proxy, improving performance. If you set this to *Yes*, then all requests, including non-cacheable requests, will utilise the upstream proxy.

12.4 Data

Your Getbusi system logs all of the Internet activity for all of your users. Over time, this data grows to a considerable size and could become the largest consumer of disk space on your system. Additionally, as your database grows, reporting functions could take longer to generate, and the overall performance of your Getbusi system could eventually be impacted.

You may manage your data by choosing to delete it after a period of time. Remember that unless you keep your data backups, once the data is deleted from the database, it is irretrievable. The default is to retain data for one year.



System properties >> Manage data deletion

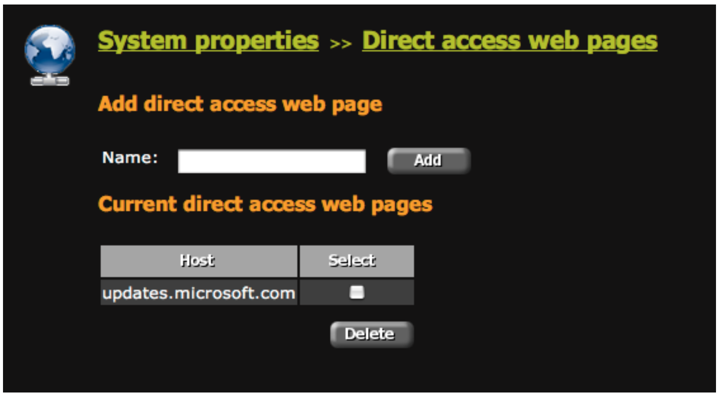
Delete data after:
- ○ 1 month
- ○ 3 months
- ○ 6 months
- ● 1 year
- ○ 2 years
- ○ 3 years
- ○ 5 years
- ○ Never

Figure 69

- Select the radio button that corresponds with the amount of data you wish to retain on your system.
- Click on the grey **Apply** button to save your setting.

12.5 Direct Access

The Getbusi system allows you to configure direct access web pages for those Internet resources which cannot be proxied through a proxy server. For example, the Microsoft Automatic Updates site and certain Apple technologies will not work through a caching proxy system like Getbusi. Direct access pages allow you to bypass the proxy to access these Internet resources.



System properties >> Direct access web pages

Add direct access web page

Name:

Current direct access web pages

Host	Select
updates.microsoft.com	□

Figure 70

- To add a new direct access site, enter the domain or URL of the site in the *Name* text field and click the grey **Apply** button. The table will refresh and display your newly added site.
- To delete an existing direct access site, click on the site's corresponding check box and click on the grey **Delete** button. The table will refresh and display the remaining direct access sites.

12.6 Global Whitelist

The Global Whitelist is a list of unblocked websites that overrides all Local Good and Bad Lists for all policies. This feature is useful for providing more granular control over media websites with intricately designed content serving systems.

For example, YouTube.com uses several different servers, URLs and queries to serve any given video, depending on which way it's being viewed (embedded etc.). Therefore the only way to control access to individual videos is to allow permanent access to the Servers and URLs which serve them. This way, control can be focused on the Video pages themselves rather than the load-balancing systems that work in the background.

- To add a new site to the Global Whitelist, enter the domain or URL of the site in the *URL* text field and click the grey **Add** button. The table will refresh and display your newly added site, the user that added it and the date/time it was added.
- To delete an existing Global Whitelist entry, click on the site's corresponding check box and click on the grey **Delete** button. The table will refresh and display the remaining Global Whitelisted sites.

12.6.1 YouTube Unblocking

The default entries in the Global Whitelist allow access to these content / load balancing servers and URLs, as described above.

With the default entries in place you may add the URLs of individual YouTube videos you wish to allow access to, whilst still blocking access to the rest of the website using the Social Networking filter category or a Local Bad List.

YouTube video URLs must be added to the Global Whitelist in the same format as:

www.youtube.com/watch?v=tgbNymZ7vqY

12.7 Enterprise

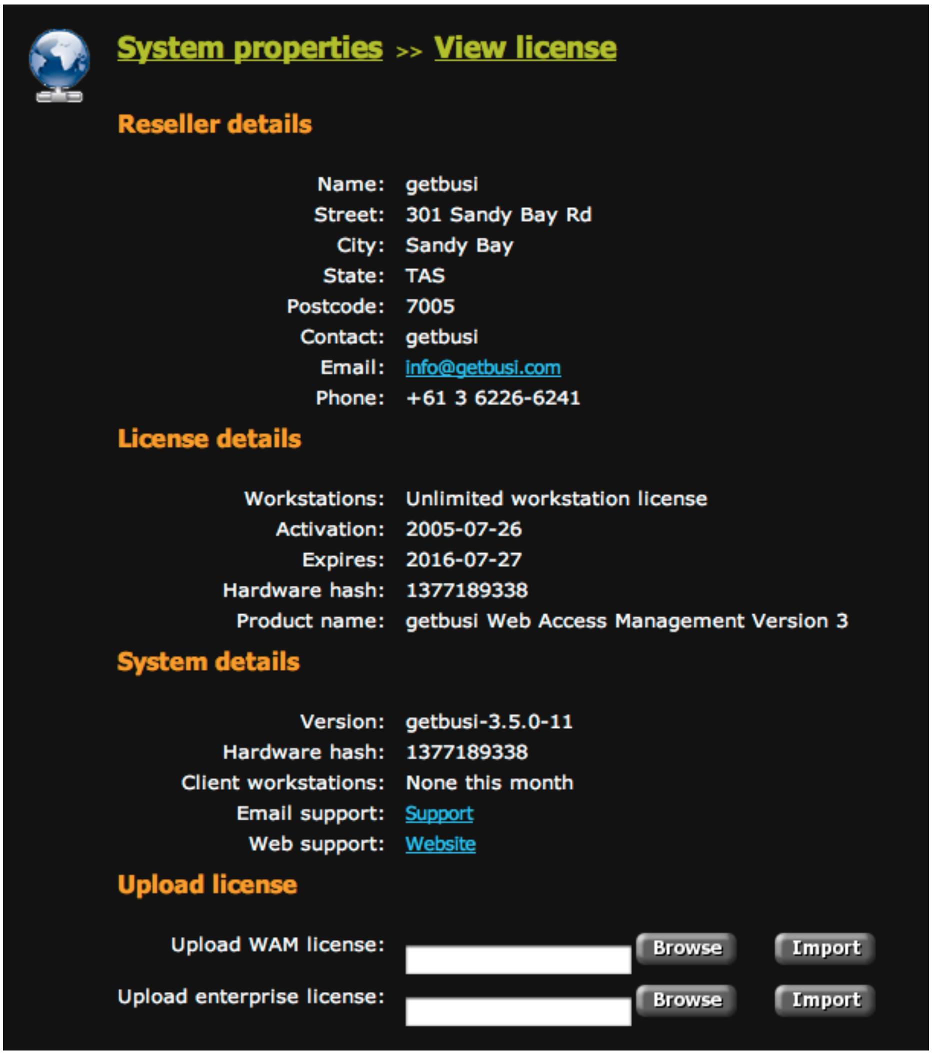
The **Enterprise** section allows you to configure your Getbusi system for a distributed network. These settings are only available if you have uploaded a valid enterprise license. For information on how to install an enterprise license, see section 12.8.4.2: Installing Your Enterprise License.

Please refer to the Enterprise Guide for more information about configuring Getbusi for a distributed system.

Please proceed to section 12.8 License

12.8 License

The **License** page displays the vendor from whom you purchased Getbusi, your current license details and your system details. From the license page, you can also install a new Getbusi license.



System properties >> View license

Reseller details

Name: getbusi
Street: 301 Sandy Bay Rd
City: Sandy Bay
State: TAS
Postcode: 7005
Contact: getbusi
Email: info@getbusi.com
Phone: +61 3 6226-6241

License details

Workstations: Unlimited workstation license
Activation: 2005-07-26
Expires: 2016-07-27
Hardware hash: 1377189338
Product name: getbusi Web Access Management Version 3

System details

Version: getbusi-3.5.0-11
Hardware hash: 1377189338
Client workstations: None this month
Email support: Support
Web support: Website

Upload license

Upload WAM license:
Upload enterprise license:

Figure 71

12.8.1 Reseller Details

The *Reseller details* section displays the contact information of your vendor (either Getbusi, or a licensed distributor of Getbusi). If you wish to renew your license, you should contact the vendor displayed in the *Reseller details* section.

12.8.1.1 Obtaining your License

You will need to contact either Getbusi support, or your Getbusi reseller to obtain a license. Once you have requested a license, a license will be generated for you. You will receive an email with instructions on how to retrieve your license from the Getbusi website. If you purchased Getbusi through a reseller, you should receive directions from them on how to obtain your Getbusi license from the Getbusi website.

You should download your license from the website and save it to a known location on your workstation.

12.8.2 License Details

The *License details* section displays information pertaining to your currently installed license. It shows the number of workstations you are currently licensed for, the date of license activation, the date when your current license expires, the hardware hash you provided when requesting your current license, and the version of the Getbusi software you are licensed for.

If you have purchased an enterprise license and have uploaded that license onto your Getbusi server, then the enterprise license details will also be displayed. The system will show the date of the enterprise license activation, the expiration date of the enterprise license and the hardware hash in the enterprise license.

12.8.3 System Details

The *System details* section displays information pertaining to your actual system. This information includes the version of the Getbusi software running on your system, the hardware hash of your system, the number of unique client workstations that used the Getbusi system in the current month, an email link to Getbusi support, and a web link to Getbusi's website.

When requesting a license, you will be asked to provide the hardware hash displayed in the *System details* section. This hardware hash must match the hardware hash encoded in your license.

Please note that if any hardware changes on your system, it is likely that the hardware hash for your system will also change, causing a mismatch with the hardware hash in your license. If after altering your system's hardware, you find that your license is no longer valid, check to see if the system's hardware hash and the license hardware hash match. If they do not, you will have to contact Getbusi for a new license.

12.8.4 Upload License

When you have retrieved your license, you may upload it into the system. There are two valid license types: a WAM License and an Enterprise License. When loading your license into the Getbusi system, you must load the license into the area that corresponds with your license type.

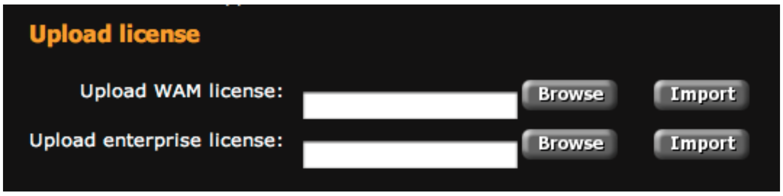


Figure 72

12.8.4.1 Installing Your WAM License

The WAM license is a license to run a single, independent Getbusi system. To upload a WAM license, click on the grey **Browse** button in the *Upload WAM license* section and locate the license that has been saved on your workstation. Click on the grey **Import** button to load the license into your Getbusi system.

12.8.4.2 Installing Your Enterprise License

The Enterprise license is a license that allows you to run multiple Getbusi systems in a master/slave configuration. To upload an Enterprise license, click on the grey **Browse** button in the *Upload enterprise license* section and locate the enterprise license that you saved on your workstation. Click on the grey **Import** button to load the enterprise license into your Getbusi system.

12.9 Messages

Certain events like users being over quota, or pages getting blocked by filters, will generate redirection error messages informing the user of the event. You may customise these messages to your preference. On the **Messages** page, a list of all of the redirection error messages are displayed, each with a corresponding text box containing the default message (if any).

The following list describes the name of the error message, and the event that would trigger it:

- **Filtered Message**: This message appears if there is an attempt to view a site that is being blocked by any of the filters applied to a policy.
- **Whitelist Message**: For policies being implemented to only allow access to sites in a local good list, this message appears when there is an attempt to view a site not specifically approved by the local good list.
- **Banned File Type Message**: This message appears if there is an attempt to download a file that has been banned by a policy.
- **Over Quota Message**: For policies that implement quotas, this message appears when a user exceeds either their daily, weekly or monthly quota.
- **Computer Denied Message**: For machine-based policies, this message appears when a machine has been denied access to Internet resources.
- **Computer Over Quota Message**: For machine-based policies, this message appears when a machine has exceeded its daily, weekly or monthly quota.

To customise any of the aforementioned errors, type the message you wish to be displayed when that error is triggered in the error's corresponding text box. Click on the grey **Apply** button that corresponds to the error and text box. You may also click on the corresponding grey **Test** button, to generate a test of the message. When you click the **Test** button, a new browser window will appear with the text for that error.

12.10 Miscellaneous Settings

This page allows you to set some general settings for your Getbusi system.

12.10.1 General Details

- The **Site Name** field allows you to set a name for your Getbusi system that will appear on email feedback reports. Although you may simply set this to the hostname of your Getbusi server, you may also set this to any name you wish.
- The **Report Email Address** field allows you to designate an email address to which you deliver email reports. You should set this to a valid email address that you check regularly, as your Getbusi system will email you reports about its health and other status updates.
- The **SMTP (Email) Server** field allows you to set the IP address of your email server. This is the email server that the Getbusi will deliver email through. This could be your internal email server, or that of your ISP.
- The **Process reporting data when the system load is** allows you to customise the load threshold for processing data. If the load threshold is exceeded, your system will delay writing Internet usage and quota usage to the database until the system load drops back below the threshold. This feature allows the system to cope with temporary spikes in load during periods of high usage.
- The **System Scale** drop-down list allows you to customise which unit of measurement you wish to use for reporting. The scale may be set to either *Kilobytes* (KB), or *Megabytes* (MB).
- The **Default Price** field allows you to set a price per megabyte for data being downloaded through your Getbusi system. By default, this price is set to $0.00. This setting allows you to bill and credit your users, as well as issue tickets for users wishing to purchase bandwidth.

To apply your settings, click the corresponding grey **Apply** button at the end of the **General Details** section.

12.10.2 Filtering

This section allows Getbusi Advance customers to select a Filtering Type. If you are not using Getbusi Advance please proceed to section 12.10.2.1: Getbusi Managed Filters.

The drop-down list allows you to select from three filtering types, each incorporating real-time website classification. You also have the option of using the Managed Filters maintained by Getbusi (detailed in the following section).

1. The **Getbusi Advance** option will utilise a local cache of previously classified websites in conjunction with your locally managed Good / Bad / Expression lists. When an unclassified website is accessed your Getbusi machine will automatically seek a category from an upstream Category Name Server, this action is seamless within the request.
2. The **On-demand Filters** option will ignore the local cache of previously classified websites as well as the locally managed Good / Bad / Expression lists and categorise all websites on-the-fly. Each time a request is made through the Getbusi proxy, the website will be seamlessly categorised against an upstream Category Name Server.
3. The **URL Classification Only** option will disable the redirection of Users. Instead, every request using the Getbusi proxy will be categorised and listed in the Prohibited Attempts report. This option is for those that wish to sacrifice access control for classification of all traffic.

12.10.2.1 Getbusi Managed Filters

In order to keep your filter lists up-to-date, your Getbusi system can automatically download managed filters from the Getbusi website. These filter lists are constantly being updated by Getbusi, so it is highly recommended that you do not disable this feature.

- The **Update Time** drop-down menus allow you to set the time of day that you want your Getbusi system to retrieve managed filters. Your Getbusi system will download the latest managed filters every day at the time you set.
- The **Do not update manage filters** check-box allows you to disable the automatic managed filters update feature. This is not recommended.
- The **Update managed filters now** button allows you to perform a one-off, unscheduled update of managed filters.
- The **Allow Getbusi to classify the sites visited (beta)** drop-down menu enables a feature (currently in beta) that periodically Emails a report to Getbusi. The report contains a full listing of all visited domains and a listing of all of the manually blocked and unblocked sites on your system. If any of the domains your users have visited have not been classified, Getbusi staff will categorise the domains. Getbusi does not record where the domain information was sent from or which user made the request. This feature helps us improve our domain classification and filter lists. The collective gathering of domain information provides a greater level of domain classification and improved reports on Internet usage for our clients on their Getbusi systems. To enable this feature, select either the 'Daily' or 'Weekly' options. This feature is disabled by default.

To apply your settings, click the corresponding grey Apply button at the end of the **Filtering** section.

12.10.2.2 Redirection Processes

The Redirection processes field allows you to set the number of redirection processes. These processes are used to check client requests against filtering policies. You should configure one redirection process for every 10 workstations simultaneously using the Getbusi system. The minimum recommended number of redirection processes is *5*, and the maximum is *80*.

Note: Getbusi Advance's real-time filtering will increase the load on the Redirection Processes. If you are using Getbusi Advance you should configure 1 process for every 5 workstations simultaneously using the Getbusi system.

12.10.3 Changing Your Administrative Password

Your default Getbusi admin password is *test*. We highly recommend you change this password, since anyone with the admin password can reconfigure your Getbusi system.

1. In the **Old Password** field, enter the existing admin password. By default, this is *test*.
2. In the **New Password** field, enter a secure password for your admin user.
3. In the **Confirm Password** field, re-enter the password from step 2.

To apply your settings, click the corresponding grey Apply button at the end of the **Admin Password** section.

Please proceed to the section 12.11: Status.

12.11 Status

The **Status** page allows you to check the server's health and ensure that the network and system services are running as expected. The status page contains a number of sections, network checks, file system checks, system load checks and authentication checks.

12.11.1 Network Checks

The network check section contains an area to add network checks, and an area to view the status of the configured network checks. By default, there are no network checks configured in the system. Network checks allow you to check to make sure that your Getbusi server is properly connected to your network. It can also help you determine if your network is functioning properly.

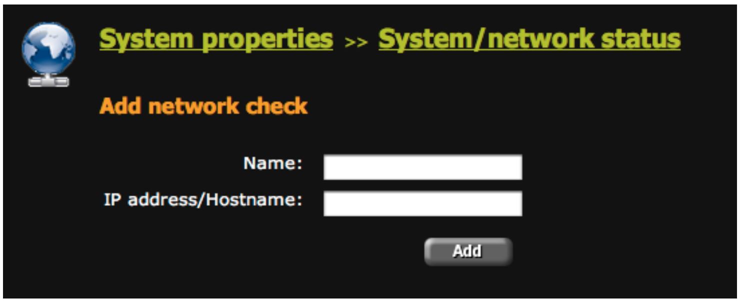
12.11.1.1 Add Network Check

Network checks utilise the ping utility to see if there is network access to the configured target host. You can add as many network checks as you wish, but there are three recommended ones.

The first recommended network check is to identify a known, fixed-ip host on your local area network, like your default gateway, a mail server or a file server. This test tells you if your Getbusi machine has access to your local area network.

The second recommended network check is to identify a known, fixed-ip host outside of your network. A good candidate might be your next-hop router outside of your network, like your ISP's router. In order for this to work, your firewall will need to allow outbound ICMP packets.

The third recommended network check is to identify a known website, like google, which will respond to ping requests. This not only tests your external Internet access, but also tests to ensure that DNS is working properly.



System properties >> System/network status

Add network check

Name:

IP address/Hostname:

Figure 73

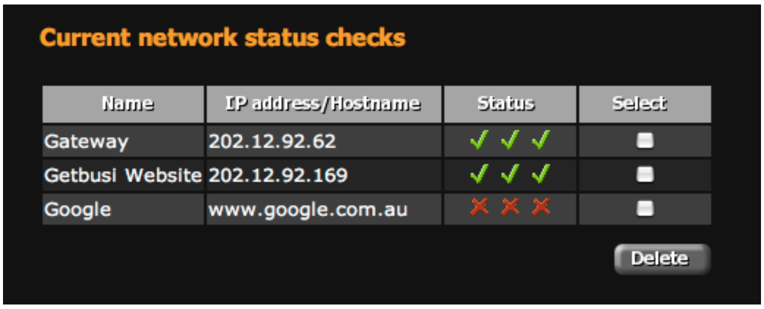
1. Enter a unique name for the network check in the **Name** field.

2. Enter either an IP address, a fully-qualified hostname, or a URL in the **IP address/Hostname** field.

3. Click the grey **Add** button to add your network check. Repeat steps 1 - 3 to add additional network checks.

12.11.1.2 Viewing the Status of Network Checks

The **Current network status checks** area shows you the status of all configured network checks in your Getbusi system. Green checks indicate a successful check. Red x's indicate a failed network check.



Current network status checks

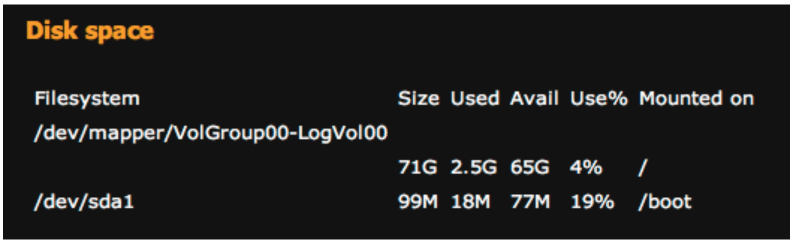
Name	IP address/Hostname	Status	Select
Gateway	202.12.92.62	✓ ✓ ✓	□
Getbusi Website	202.12.92.169	✓ ✓ ✓	□
Google	www.google.com.au	✗ ✗ ✗	□

Figure 74

To delete a configured network check, click in the check-box that corresponds with the network check you wish to delete from the system and click the grey **Delete** button. You may delete more than one network check at a time. When the page refreshes, the **Current network status checks** status area should no longer show the deleted network check(s).

12.11.2 Disk Space

The **Disk space** section provides you with information about the amount of space being used on your hard disk(s). This information can help with decisions determining your data retention policy or how much disk space to configure for your cache. We recommend never allowing your partitions to fill beyond 90% of their capacity.



Disk space

```
Filesystem                       Size  Used  Avail  Use%  Mounted on
/dev/mapper/VolGroup00-LogVol00
                                 71G   2.5G  65G    4%    /
/dev/sda1                        99M   18M   77M    19%   /boot
```

Figure 75

Figure 75 shows a sample of a disk space check. The only partition of interest is the root, or "/" partition. This is the partition that would contain the proxy cache and the database. If you configured your system to have the database on a separate partition, it would appear on a separate line.

12.11.3 System Load

The **System Load** section displays the number of waiting processes for the last minute, 5 minutes and 15 minutes. Under normal conditions, the 5 and 15 minute values should remain under 3. If you have a dual processor or Hyper-Threading processor, this value should remain under 6. If you are running reports, or are in the process of reconfiguring the system, these values may rise above recommended levels for short periods of time. You will also see short bursts of high load in times of high usage.

12.11.4 Authentication Groups

The **Authentication Groups** section allows you to see if the system can retrieve group information from the authentication system being used. An empty table is indicative of communication problems between your Getbusi server and the authentication system.

12.11.5 External Network Connections

The **External Network Connections** section allows you to test various external connections. These checks not only test that external connections are available, but that they're allowed through your firewall. To run external network connection tests, click on the grey **Test** button. It can often take a short amount of time to return the results of the tests. The returned values show the result of testing:

- DNS resolution: DNS is required to resolve names (like www.google.com) to IP addresses. Without DNS, you will not be able to access external websites by commonly known names.
- RSYNC access: RSYNC is required if you wish to receive managed list updates from Getbusi.
- FTP access: FTP is required if you wish to be able to automatically update your system software.
- HTTP access: HTTP is required for access to regular web sites on the Internet
- HTTPS access: HTTPS is required for access to secure web sites on the Internet
- SSH access (only outbound is required): SSH access is used by Getbusi support to help you troubleshoot problems.
- FILTERING access: This protocol is required for Getbusi Advance systems to communicate with the upstream Category Name Servers which provide on-the-fly classification of uncategorised websites.
- SMTP access: SMTP is required to allow your Getbusi server to send email reports.
- NTP access: NTP is required to keep your system's clock properly synchronised. Disallowing NTP access will adversely affect Time-based Policies because your system's clock can become increasingly inaccurate over time.

12.12 Support

The **Support** page allows you to initiate up a secure shell connection to Getbusi's support server. Using this connection, Getbusi technical support can log into your system to provide in-depth troubleshooting. This connection is secure and does not pose a security risk to your system.

Since you initiate the support session, Getbusi staff only have access to your Getbusi server only when you wish. The only requirement for a secure shell connection is for you to have ssh port 22 outbound allowed through your organisation's firewall. To see if you have your firewall to allow ssh outbound, see section 12.11.5: External Network Connections.

To enable a support connection, contact Getbusi support at:

Telephone (Australia):	(03) 6226 6241
Telephone (International):	+61 3 6226 6241

The Getbusi staff will instruct you on how to initiate a secure shell connection.

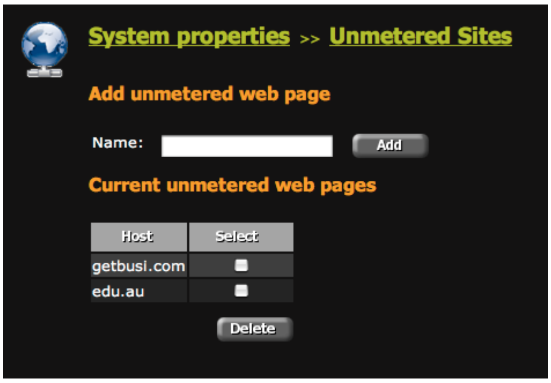
12.13 Unmetered Sites

The **Unmetered sites** page allows you to designate certain Internet resources that when accessed, will not count against a download quota. The activity from the site will still be logged against the user, group or computer group.

Unmetered sites may only be configured for domains. You may not configure an unmetered URL. This means that when you add an unmetered site to your Getbusi system, all pages hosted on that site, and any subdomains of that site will not count against quotas.

For example, if you employ Getbusi at a school and you wish do not wish for access any other educational institution in Australia to count towards your student quotas. In this case, you could add the domain ***edu.au*** to unmetered sites. Any access to any website ending in *edu.au* will then not count against download quotas.

This example highlights the care you should take in configuring unmetered sites. For information about domain hierarchies, please see section 7.1.1: Domain Names.


System properties >> Unmetered Sites
Add unmetered web page
Name:
Add
Current unmetered web pages
Delete

Host	Select
getbusi.com	□
edu.au	□

Figure 76

12.13.1 Adding and Removing Unmetered Sites

- To add an unmetered site, enter the domain of the site in the *name* text box and click on the grey **Add** button. The *Current unmetered web pages* table will display your newly added site when the page refreshes.
- To remove an unmetered site from your system, click on the site's corresponding check box and click on the grey **Delete** button. The *Current unmetered web pages* table will update to reflect your changes when the page refreshes.

12.14 Updates

The **Updates** page allows you to view and install available updates for your Getbusi system and kernel.

To check for updates, click the grey **View** button. If there are system updates available, they will be listed under the **System updates** section. If there are kernel updates available, they will be listed under the **Kernel updates** section.

If there are available updates, you may configure your system to update itself at night. In the drop-down menu that corresponds with *Update system tonight*, select *yes* if you wish to have your system update overnight and click the grey **Apply** button. If you select *no*, then your system will not update itself.

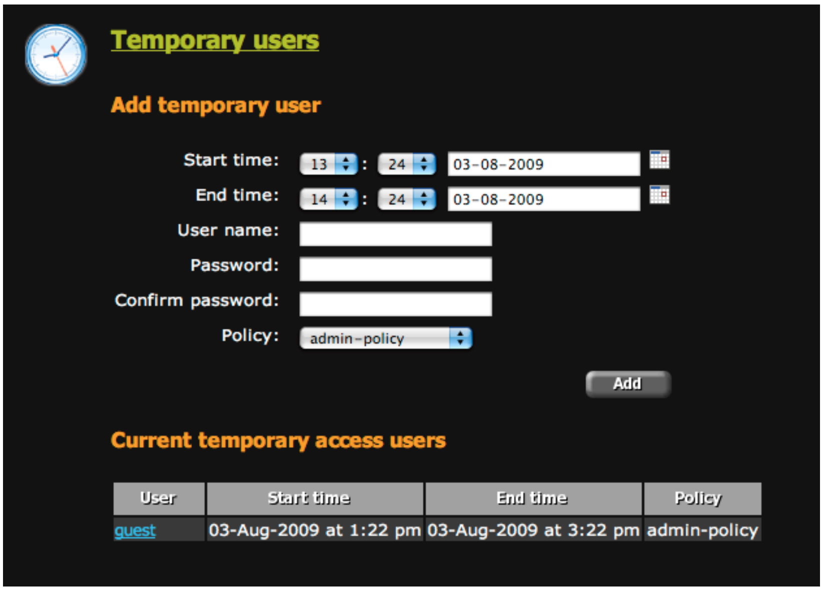
You may choose to manually update your system by clicking on the grey **Update** button. It is generally recommended that you choose to update your system overnight. If you want to update your system immediately, then you should choose a time when your system is not experiencing high load.

13 Temporary Users

The Getbusi system allows you to create temporary users if a person needs access to Internet resources through your system for a short period of time and you do not wish to add a new user to your authentication system. **Temporary users will not operate with a system that implements Seamless Windows/NT/2000/2003 authentication.** The following table shows which authentication systems and browsers work with temporary users:

Authentication System	**Firefox/Safari**	**Opera**	**Internet Explorer**
Windows Seamless	No	Yes	No
Windows Basic	Yes	Yes	Yes
LDAP - Posix	Yes	Yes	Yes
LDAP – Mac OS X Open Directory	Yes	Yes	Yes
LDAP – Novell eDirectory	Yes	Yes	Yes
LDAP – Other	Yes	Yes	Yes
LDAP – getbusi	Yes	Yes	Yes

Please note that temporary users are not affected by any quota restrictions for their configured policies, and will not be reflected in many of the Getbusi reports.



Temporary users

Add temporary user

Start time: 13 : 24 03-08-2009

End time: 14 : 24 03-08-2009

User name:

Password:

Confirm password:

Policy: admin-policy

Current temporary access users

User	Start time	End time	Policy
guest	03-Aug-2009 at 1:22 pm	03-Aug-2009 at 3:22 pm	admin-policy

Figure 77

13.1 Adding Temporary Users

1. To add a temporary user to your Getbusi system, first select the allowed time range for the temporary user's access. You may use the calendar icons to help select the allowed range.

2. Enter the temporary user's name in the *User name* field. This will be the name the user will use when prompted for a username by their browser.

3. Enter the temporary user's password in the *Password* field. Type the same password in the *Confirm password* field. This will be the password the user will use when prompted by their browser.

4. Select the policy to apply for the temporary user.

5. Click on the grey **Add** button to add the temporary user to the system. Access will be granted to the user immediately.

13.2 Modifying and Deleting Temporary Users

To modify an existing temporary user in your Getbusi system, click on the user's name in the *Current temporary access users* table. The form above the table will refresh to reflect that user's settings. Make the necessary modifications and click on the grey **Apply** button.

If you wish to delete the user, click on the grey **Delete** button. All changes will be immediately effective.

14 Server Configuration

The server configuration link opens a new browser window and allows you to modify server configuration parameters. For information about server configuration, please read the Installation Guide.

15 Additional Links

Links to the Installation Guide, the User Guide, and if an enterprise license is installed, the Enterprise System Guide are provided as shortcuts to those documents and will open if clicked. These documents are in PDF format and require a PDF reader to view.

Please proceed to section 16: Client Proxy Settings

16 Client Proxy Settings

Once your Getbusi system has been installed and configured, client workstations need to be set up to request web data (HTTP, HTTPS and FTP) through the Getbusi server. This is most commonly done by setting the proxy settings in the client browsers.

This step is important as it forces client workstations to use the Getbusi server to access Internet resources. Without this step, client workstations may access Internet resources independently, bypassing your Getbusi server and any policies you've configured.

There are a number of methods that can be used to set proxy settings in client web browsers. Three techniques are identified below, with their merits and disadvantages.

16.1 Manual Browser Configuration

Web browsers and other HTTP-based user agents have methods for explicitly setting a proxy address and port. This method is reliable and easy to implement on smaller sites but is not necessarily suitable for larger organizations because manually setting all web browsers proxy settings in a large environment may be very time-consuming. This approach does not provide much flexibility, especially if you need to quickly change all of your clients' web browser proxy settings.

You will need to check your specific web browser's documentation for information on how to set the browser's manual proxy configuration. The settings you will need for manual proxy configuration are:

- The proxy URL: http://<Your Getbusi server's IP address>
- The proxy port: by default, it is port **3128*.*** If you have changed the proxy port (section 12.3.1: Cache Settings to see what port your Getbusi server is listening on)

Ensure that the browser is configured to use your Getbusi server for all protocols. Some browsers allow you to set the proxy URL and port for all protocols, and others require you to configure the proxy URL and port for each protocol.

16.2 Automatic Proxy Configuration Using auto.pac

Proxy auto-configuration is more flexible than manually entering your proxy settings. The configuration file that contains your proxy settings is simply a text file that contains JavaScript functions. When you start your web browser it downloads the configuration file and then evaluates the JavaScript before each request. What the JavaScript returns determines if the request is sent to the Getbusi server or not.

The auto-configuration technique gives you more control. You can temporarily disable your Getbusi service, implement load balancing or migrate users to a new system. You can also instruct the web browser to try a list of Getbusi addresses which the browser tries in sequence. If the first Getbusi system is unavailable, it tries each entry sequentially in the list until it finds an available service.

Note: If your web browser has local caching enabled, it may cache the auto-configuration file. If you make changes to your auto-configuration file, you may need to clear your web browser’s local cache or do a forced refresh to load the new settings. Internet Explorer, Mozilla Firefox, Google Chrome and Opera all support proxy auto-configuration.

16.3 Web Proxy Auto Discovery (WPAD)

The Web Proxy Auto Discovery (WPAD) protocol allows web browsers to automatically discover a proxy server. Browser support for WPAD varies greatly. You must check to ensure that the browsers deployed in your organisation support WPAD. Internet Explorer (version 5 and higher) supports WPAD by default. The most recent versions of gecko-based browsers (Mozilla, Netscape and Firefox) support WPAD, but earlier versions do not.

WPAD is not a Getbusi technology and the following examples are provided for convenience. Get*busi* does not provide advice beyond the following examples for configuring WPAD due to the variability of settings and network configurations. Get*busi* also does not support hosting the wpad.dat file on the appliance. If you require support beyond the following examples, Getbusi recommends you contact Microsoft, or a Microsoft Solutions Provider.

There are two methods which allow a URL to be generated that refers to a proxy auto-configuration file: DHCP and DNS Lookup.

16.3.1 DHCP for WPAD

We do not recommend implementing DHCP for WPAD, even though it is the Microsoft preferred method. This method does not work in all situations. The best method to use is the DNS method, described in the next section.

The DHCP implementation sends a query from your browser for 'option 252' to your configured DHCP server. The response received is a string which contains the proxy URL.

To configure DHCP for WPAD, you must add the following entries:

- option wpad code 252 = text;
- option wpad “http://<WEB-SERVER>/auto.pac”;

(Where <WEB-SERVER> is the IP address of the web server serving the auto-configuration file and auto.pac is the name of the auto-configuration file.)

If serving this file from an Apache web server on Linux, add the following MIME type to the /*etc/mime.types* file:

- application/x-ns-proxy-autoconfig pac

16.3.2 DNS for WPAD

The DNS for WPAD is the recommended WPAD configuration. When configured, the client machine running the web browser performs an address lookup for the host name *wpad* in the local domain. For example, if your local domain is: *mysite.com*, the client machine requests the IP address for *wpad.mysite.com* from your DNS server. If this lookup is successful, the client machine makes a TCP connection on port 80 and requests the file: *wpad.dat*.

If you are serving the *wpad.dat* file from an Apache web server, you will need to not only serve the file, but add the entry: *application/x-ns-proxy-autoconfig pac dat* to the */etc/mime.types* file, and restart Apache.

An example WPAD file follows on Page 94

16.3.3 WPAD File Example

The following is only an example of the *wpad.dat* file that may to be served from your web server. Please note that Getbusi does not provide advice beyond this example on how to configure a *wpad.dat* file for your network due to the variable nature of client networks and settings. Get*busi* also does not support serving the wpad.dat file from your Getbusi appliance. If this example does not suit your needs, Getbusi suggests you contact Microsoft for support.

Example wpad.dat file:

```
function FindProxyForURL(url, host) {
//If they have only specified a hostname of a local machine (ie, no dots), go
directly.
if (isPlainHostName(host))
return "DIRECT";

// inside the network
if (dnsDomainIs( host,"my.domain.com.au") || shExpMatch(host, "192.168.*"))
return "DIRECT";

// we only cache http, ftp and gopher
if ( url.substring(0, 5) == "http:" || url.substring(0, 6) == "https:" ||
url.substring(0, 4) == "ftp:"|| url.substring(0, 7) == "gopher:" )
return "PROXY 192.168.0.1:8080;PROXY 192.168.0.2:3128";

// control specific subnets
if (isInNet(myIpAddress(), "192.168.1.0", "255.255.255.0"))
return "PROXY 192.168.1.1:3128";

return "DIRECT";
}
```