Z1 GEM Administration Guide

Copyright © ZYBERT Computing Ltd 2001-2010

1 Introduction

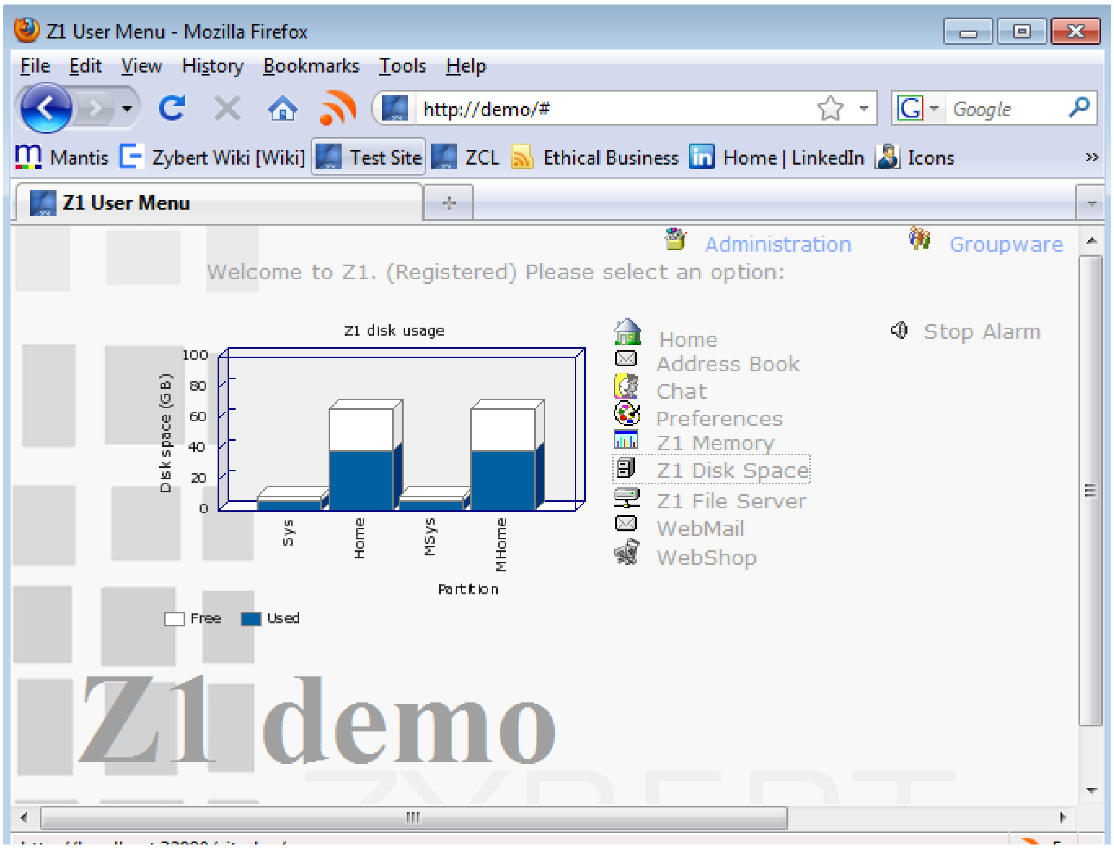
Z1 requires very little administration. However, certain parameters have to be set in order to use the services Z1 provides.

Every user of your network should have a username and password in order to use file sharing services and email.

Downloading of external mailboxes requires the user names, passwords and addresses. Additionally you have to tell Z1 how to distribute mail messages received from external mailboxes.

2 Admin functions

2.1 Home page



Welcome to Z1. (Registered) Please select an option:

This is a prototype home page of Z1. You may edit and modify this page add more pages or CGI scripts. You may use PHP in your html pages or may write CGI script in most languages.

Z1 home page is stored in \\www\www\htdocs\Z1\Z1_HomePage.php. You may edit this page (if you have Z1 Admin rights). There is a link (shortcut) to this page in \\www\www\htdocs\index.html.

CGI scripts and programs may be stored in \\www\www\cgi-bin directory and will then be accessible from local network as http://www/cgi-bin/[filename].

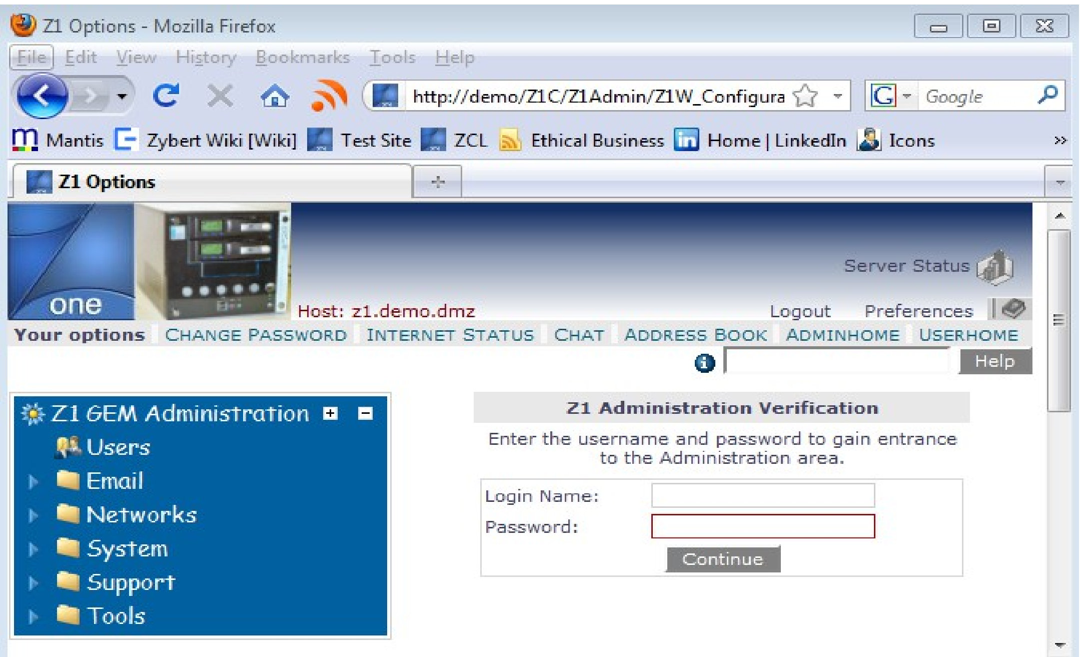
Users may store their html files in \\www\[username]\public_html folder. They will then be accessible from LAN as http://www/~[username]/[filename]. The default file name is index.html. Each user is provided with an empty index.html file that they may edit.

2.2 Administrator page

Click on *Login*. This will lead you through administration menu of Z1. You will have to login with a password (username and password is supplied on your license card):

Note: Login procedure here provides your browser with a KEY that gives you access to system tools, depending on your rights on Z1. For security reasons this key expires after two hours.

In an unlikely even that you spend more than two hours on administration the system may ask you to login again. Nevertheless – if you are a system administrator it is better to logout after finishing your administration tasks. Exiting from the browser will have the same effect as logging out.



Host: z1.demo.dmz

Z1 Administration Verification

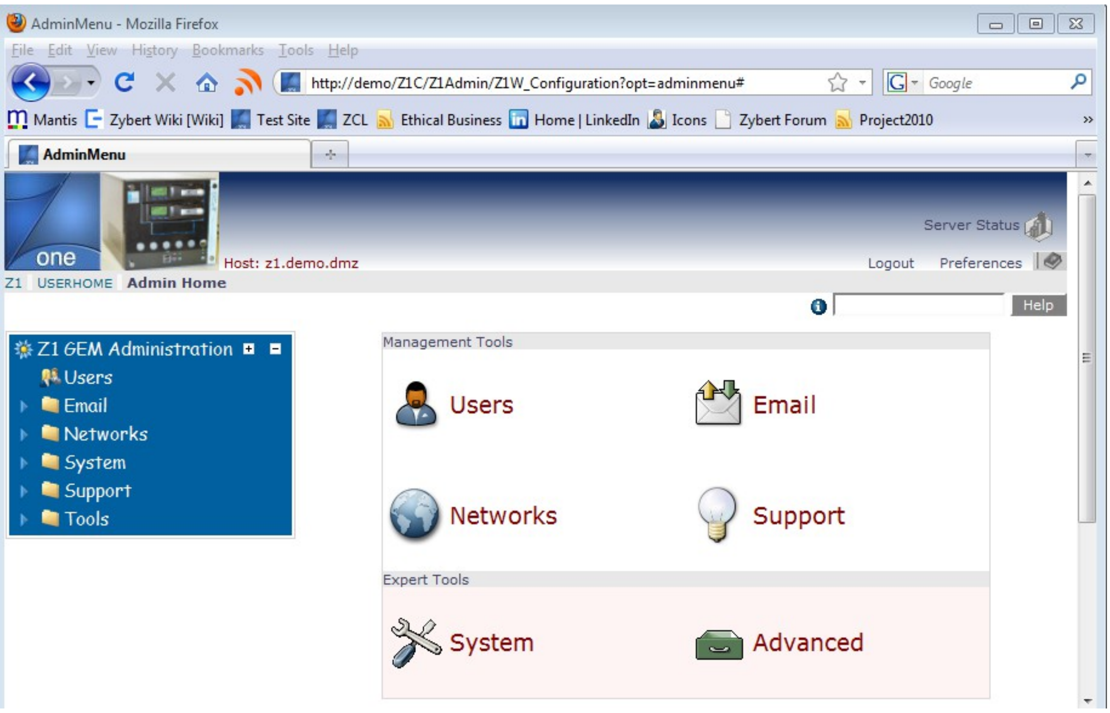
Enter the username and password to gain entrance to the Administration area.

Login Name:

Password:

Enter username and password and click *Continue.*

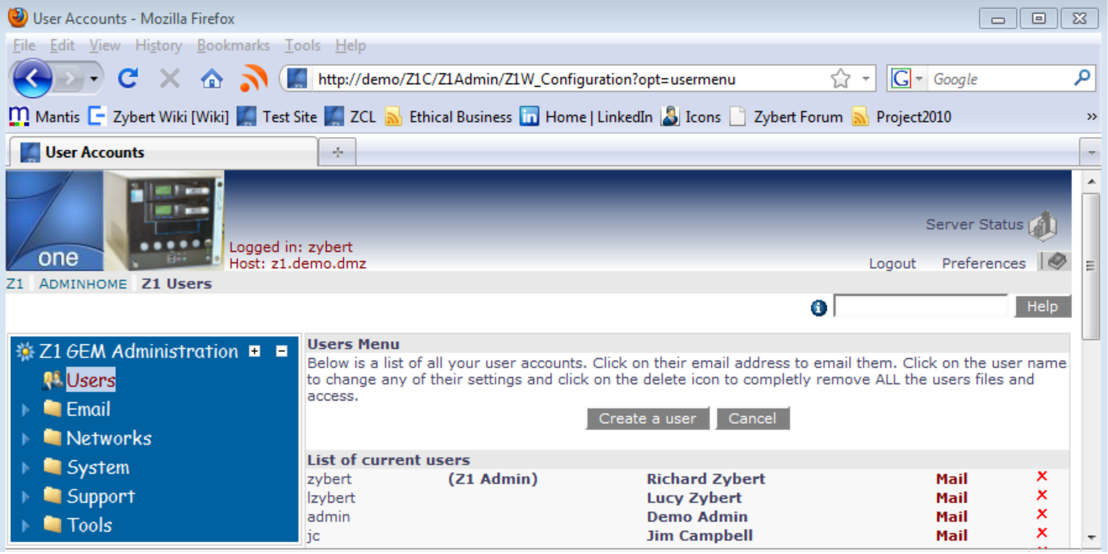
You will see the main Admin page:



Host: z1.demo.dmz

Select *User Accounts*

2.3 User administration



Logged in: zybert
Host: z1.demo.dmz

Users Menu

Below is a list of all your user accounts. Click on their email address to email them. Click on the user name to change any of their settings and click on the delete icon to completly remove ALL the users files and access.

Create a user | Cancel

List of current users

zybert	**(Z1 Admin)**	**Richard Zybert**	**Mail**	✕
lzybert		**Lucy Zybert**	**Mail**	✕
admin		**Demo Admin**	**Mail**	✕
jc		**Jim Campbell**	**Mail**	✕

You will be able to create user accounts. You should make an account for each user. The username and password should be the same as the pair they use to login to their Windows workstations. This simplifies file sharing process. If you create new user names, we recommend that you use simple, short names in lower case (like *john*). Please, note that all user names and passwords are case sensitive on Z1. Passwords should be between 6 and 8 characters long. Ideally they should be easy to remember and hard to guess. First names, names of pets etc are notoriously easy to crack. Most 'dictionary' words are too. Mixing letters and digits makes better passwords.

User passwords, once set cannot be read – even by the administrator. If you are an administrator, you can change any password but you cannot read the existing one. Therefore, administrator password should be well protected – you will need at least one admin password to access the system.

When creating a user you can give them 'Admin rights' – this user becomes an administrator and is allowed to change system settings. Administrators have read/write access to all user files, including mail. You should not need more than 2-3 administrators and it is a good practice to limit the number of administrators. Users without administrator privileges may fully use the system and their mistakes should not cause problems for other users. Mistakes of administrators may be more dangerous.

When you create a user account the system creates an email account for this user, users home directory with a subdirectories **mbox, public_html, shared**.

- **mbox** is a directory that keeps email folders of the user if *IMAP* protocol is used. Otherwise, it will stay empty. It should not be removed to allow the user to switch to IMAP protocol later.
- **public_html** is where user's personal WEB pages are kept. Each user may construct their own web pages and store them in this directory. They can then be accessed by everybody on the local network as **http://www/~username/filename**. HTML files should have extensions .html or .htm. Users are not allowed to create CGI scripts. When the account is created an empty html file called **index.html** is stored in public_html directory. This is the file the user should edit first in order to construct his/her personal web pages.
- **shared** is a special folder (actually a shortcut) where the user may keep files that should be available to others. This shortcut points to \\z1\shared\user - it will be visible by all users and files stored there are accessible to everybody.

User home directory will be visible to the user after logging into windows computer on the LAN – as \\z1\user. Except for the files stored in folder *shared* new files created by the user are not accessible to others (well… except for system administrator who can see everything)

In the names of shares above it is assumed that the network name of your Z1 is z1 – if you change this name in the initial configuration, you should use the new name. However, you may always use a name \\www\share - www is an alias for Z1 that is independent of the name you give it.

Please see chapter on File Sharing for more details.

After an account was created you may modify it or delete it. Please note that deleting the user account will remove all users files from the system. It may be a good idea to backup user files before deleting an account. (More on this in file sharing)

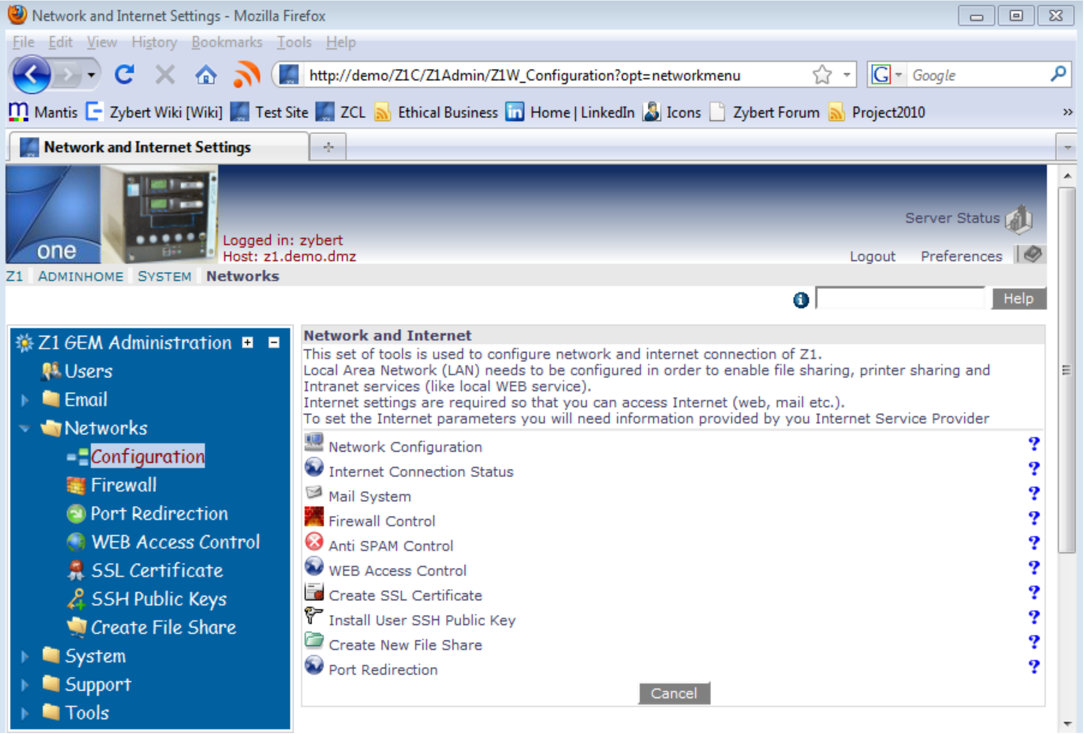
There is no limit on the number of accounts you may create. However – for ease of long term administration you should not keep idle accounts forever – accounts of users who left the company – it is best to backup the files to a permanent medium and remove the accounts.

When you created accounts you need, click *Cancel*.

2.3.1 Network and Internet administration

Click on *Network and Internet configuration* on the main admin page. You should see the new menu with the list of networking subsystems.

Configuration of the Local Network should not be necessary at that moment – this simply allows you to modify parameters you set in the initial configuration.



Network and Internet

This set of tools is used to configure network and internet connection of Z1.
Local Area Network (LAN) needs to be configured in order to enable file sharing, printer sharing and Intranet services (like local WEB service).
Internet settings are required so that you can access Internet (web, mail etc.).
To set the Internet parameters you will need information provided by you Internet Service Provider

- Network Configuration ?
- Internet Connection Status ?
- Mail System ?
- Firewall Control ?
- Anti SPAM Control ?
- WEB Access Control ?
- Create SSL Certificate ?
- Install User SSH Public Key ?
- Create New File Share ?
- Port Redirection ?

Cancel

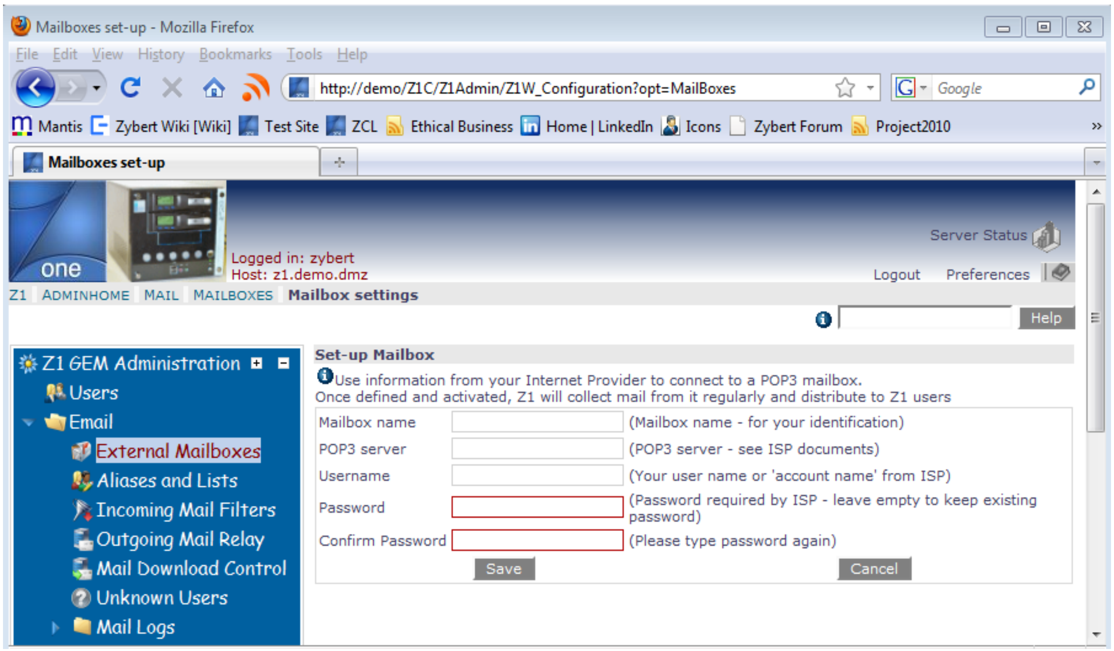
2.3.2 Mail System

Z1 may be set-up to collect mail from a number of external mailboxes and distribute it locally. You should specify here all POP3 mail accounts you want Z1 to handle. At specified intervals (selected at the bottom of this page) Z1 will attempt to collect mail for all mailboxes and distribute to local users.

The specific rules how to distribute mail to users should be specified on Mail Alias page, the default behaviour is that mail addressed to 'fred@anyaddress.com' will be sent to a local user **fred**. Mail aliases allow you to change this and distribute mail to users or group of users depending on addressee, sender or subject.

You can specify here when and how often Z1 should collect your mail.

All mail is delivered immediately.



Logged in: zybert
Host: z1.demo.dmz

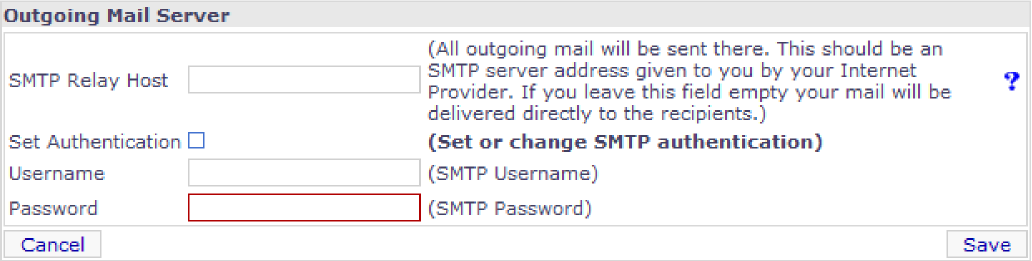
Set-up Mailbox

Use information from your Internet Provider to connect to a POP3 mailbox.
Once defined and activated, Z1 will collect mail from it regularly and distribute to Z1 users

Mailbox name		(Mailbox name - for your identification)
POP3 server		(POP3 server - see ISP documents)
Username		(Your user name or 'account name' from ISP)
Password		(Password required by ISP - leave empty to keep existing password)
Confirm Password		(Please type password again)

You must enter your real company mail address. This is the address you were given by the ISP with the POP3 mailbox. This is how the system will recognize mail addresses that are local when downloading mail. You may have more than one address that your company uses – you can specify other addresses in the Mail Alias page.

Click Save.



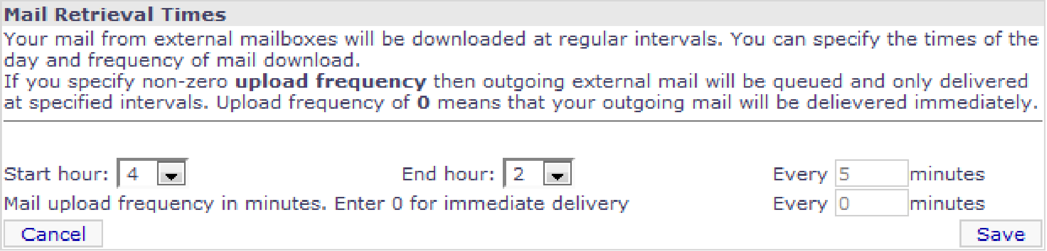
Outgoing Mail Server

SMTP Relay Host		(All outgoing mail will be sent there. This should be an SMTP server address given to you by your Internet Provider. If you leave this field empty your mail will be delivered directly to the recipients.) ?
Set Authentication □		**(Set or change SMTP authentication)**
Username		(SMTP Username)
Password		(SMTP Password)

If you specify the SMTP Relay Host (again – provided by your ISP) then all outgoing mail will be passed there for delivery. This may be an efficient way of handling mail, especially if your Internet access contract uses dynamic IP address – check the ISP documentation. If you leave this field empty all outgoing mail will be delivered directly to the recipient mailbox.

If you are unsure, leave this field empty.

Click Save.



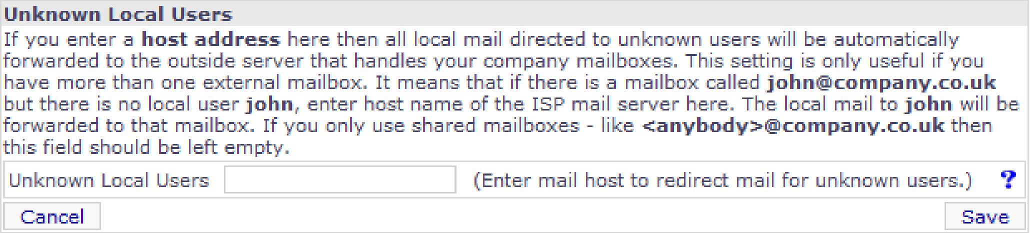
Mail Retrieval Times

Your mail from external mailboxes will be downloaded at regular intervals. You can specify the times of the day and frequency of mail download.
If you specify non-zero **upload frequency** then outgoing external mail will be queued and only delivered at specified intervals. Upload frequency of **0** means that your outgoing mail will be delievered immediately.

Start hour: 4 End hour: 2 Every 5 minutes

Mail upload frequency in minutes. Enter 0 for immediate delivery Every 0 minutes

Set the period and frequency of POP3 mail download. We recommend that mail download is stopped between 2am and 4am – at that time GEM is performing its daily backup and it is better not to change files at that time. Upload frequency (usually set to 0) allows you to queue outgoing messages and then send them in batches. It is not really required if you have a broadband connection.



Unknown Local Users

If you enter a **host address** here then all local mail directed to unknown users will be automatically forwarded to the outside server that handles your company mailboxes. This setting is only useful if you have more than one external mailbox. It means that if there is a mailbox called **john@company.co.uk** but there is no local user **john**, enter host name of the ISP mail server here. The local mail to **john** will be forwarded to that mailbox. If you only use shared mailboxes - like **<anybody>@company.co.uk** then this field should be left empty.

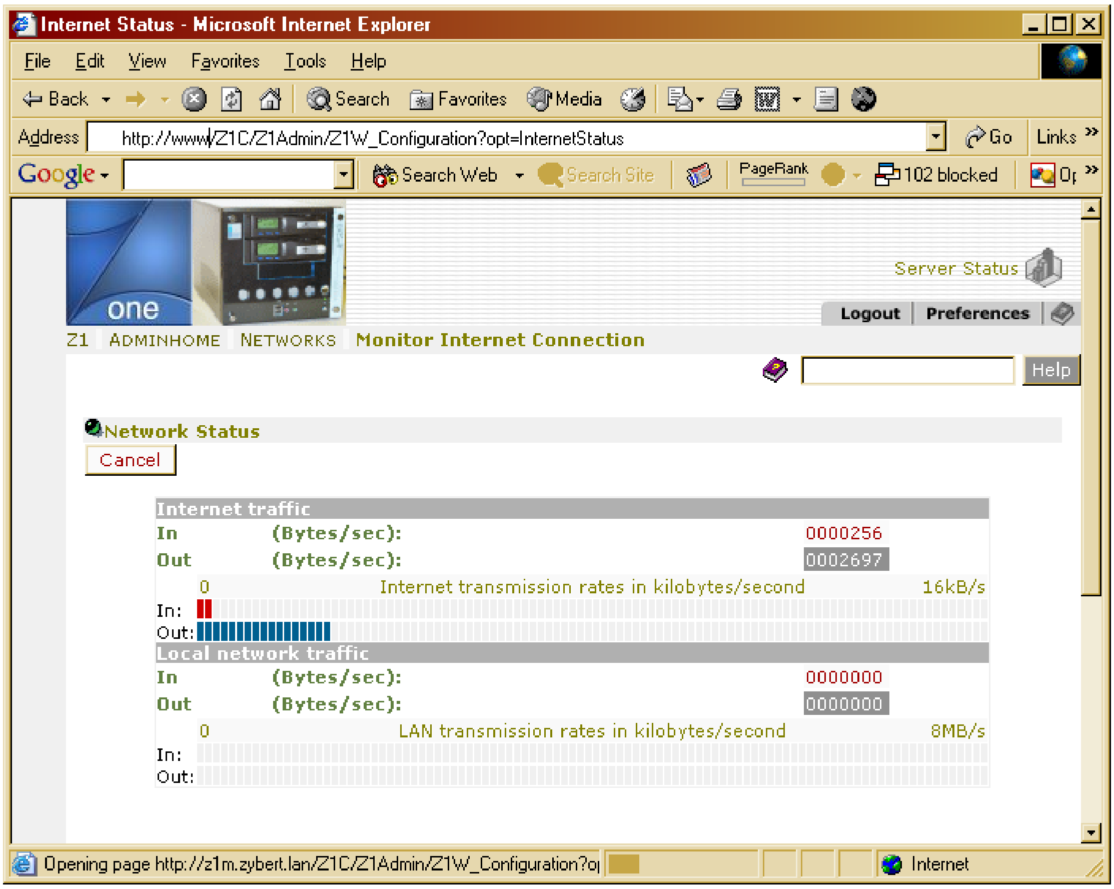
Unknown Local Users (Enter mail host to redirect mail for unknown users.)

Unknown Local Users setting is a special device to allow you to use multiple ISP mailboxes efficiently. If you have multiple mailboxes and some of them are used by external users then it is important that you should be able to send mail to them using your company mail address. Z1 will assume that all mail to company mail address is local. However – with this field set (it should be tha name of the ISP mail server) – if you send mail to a user at company mail address and that user (or alias) does not exist – the mail will be automatically passed to the ISP for delivery to their mailbox – if it exist – if there is no such mailbox then in all probability the mail will return to Z1 and will be handled following the normal rules you set up in the Mail Alias page.

If you are unsure, leave this field empty.

2.3.3 Monitoring Internet Connection

Click on Internet connection status. Because this page uses system resources, it does not refresh forever. Depending on your browser, it may ask you to refresh it from time to time or your browser may report a time-out. Refreshing the page will start the count again. (Please, note that this page may not work in some browsers)


Internet Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Google Search Web Search Site PageRank 102 blocked
one
Server Status
Logout Preferences
Z1 ADMINHOME NETWORKS Monitor Internet Connection
Help
Network Status
Cancel
Internet

Address: http://www/Z1C/Z1Admin/Z1W_Configuration?opt=InternetStatus

```
Internet traffic
In      (Bytes/sec):                              0000256
Out     (Bytes/sec):                              0002697
  0        Internet transmission rates in kilobytes/second       16kB/s
In:
Out:
Local network traffic
In      (Bytes/sec):                              0000000
Out     (Bytes/sec):                              0000000
  0          LAN transmission rates in kilobytes/second          8MB/s
In:
Out:
```

Opening page http://z1m.zybert.lan/Z1C/Z1Admin/Z1W_Configuration?o|

2.3.4 Firewall

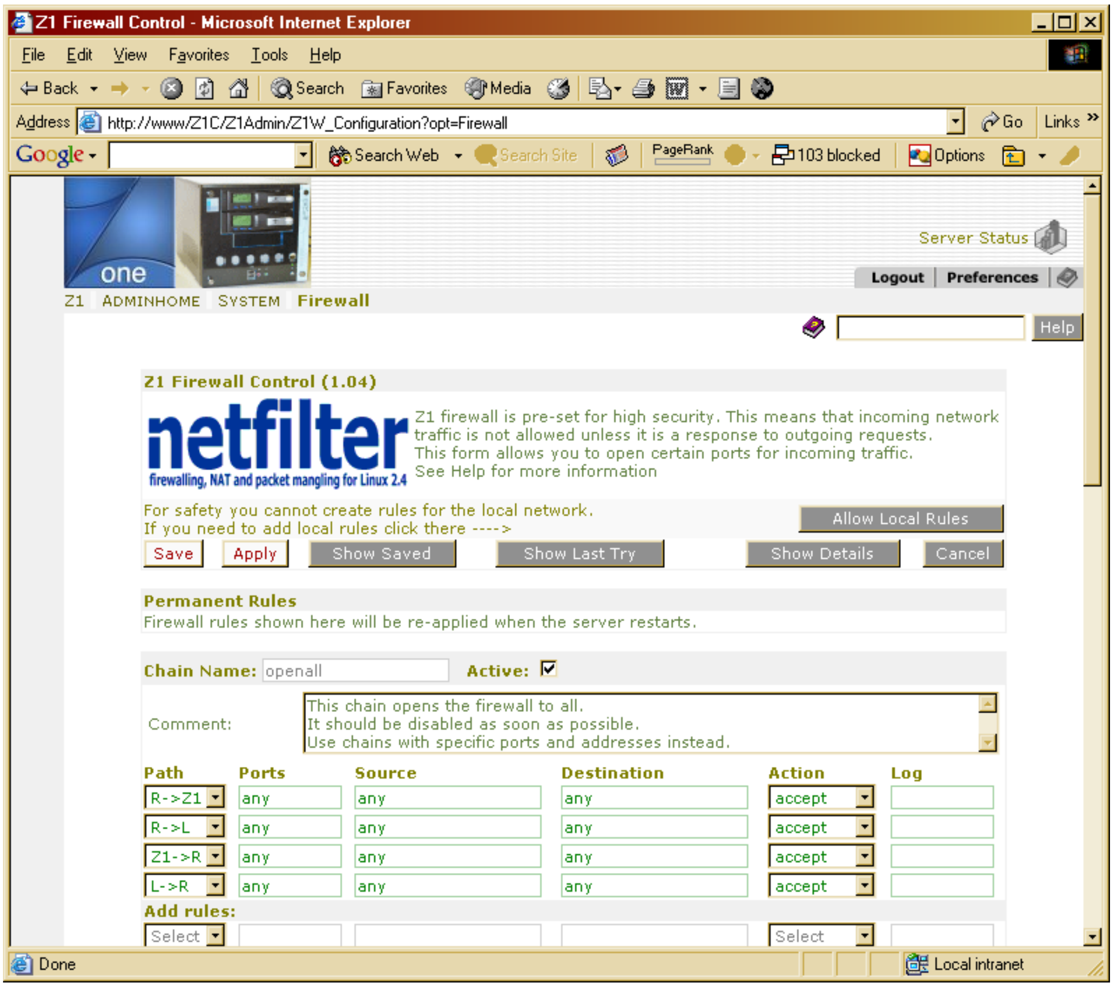
Z1 operates NETFILTER firewall built into the linux kernel. A basic set of rules is pre-set to ensure secure operation. You can add new rules to add or replace existing rules. All rules are grouped into **chains** to make the firewall administration easier you can set-up your own chains to control access to your network.

If during the initial set-up process you requested that the firewall stays open then one active chain **openall** will show up here. This opens all ports and should be deactivated as soon as possible.

The default firewall configuration allows unlimited traffic from LAN to Z1 and from LAN to Internet. Most of the incoming Internet traffic is blocked and logged. As NETFILTER is a '*stateful*' firewall packets that are sent from Internet as replies to outgoing packets are accepted.

Please, read the on-line HELP carefully. Firewall set-up may get complicated and there is a theoretical possibility of setting the firewall in such a way that all access to Z1 will be blocked (which makes it difficult to change it back). Therefore an **APPLY** button is provided for 'temporary' firewall set-up. If you modify your firewall settings and press **APPLY** without pressing **SAVE** – the firewall settings will return to their previous values at the reboot. If you are working from LAN then not enabling **LOCAL** rules is a good practice (they are disabled in the configuration tool be default). This guarantees that you cannot enter rules that would 'lock' you out from the server.

Copyright © ZYBERT Computing Ltd 2001-2010


Z1 Firewall Control - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www/Z1C/Z1Admin/Z1W_Configuration?opt=Firewall
Go Links
Google Search Web Search Site PageRank 103 blocked Options
one
Server Status
Logout Preferences
Z1 ADMINHOME SYSTEM Firewall
Help
Save Apply Show Saved Show Last Try Show Details Cancel
Allow Local Rules
Done
Local intranet

Z1 Firewall Control (1.04)

netfilter
firewalling, NAT and packet mangling for Linux 2.4

Z1 firewall is pre-set for high security. This means that incoming network traffic is not allowed unless it is a response to outgoing requests.
This form allows you to open certain ports for incoming traffic.
See Help for more information

For safety you cannot create rules for the local network.
If you need to add local rules click there ---->

Permanent Rules

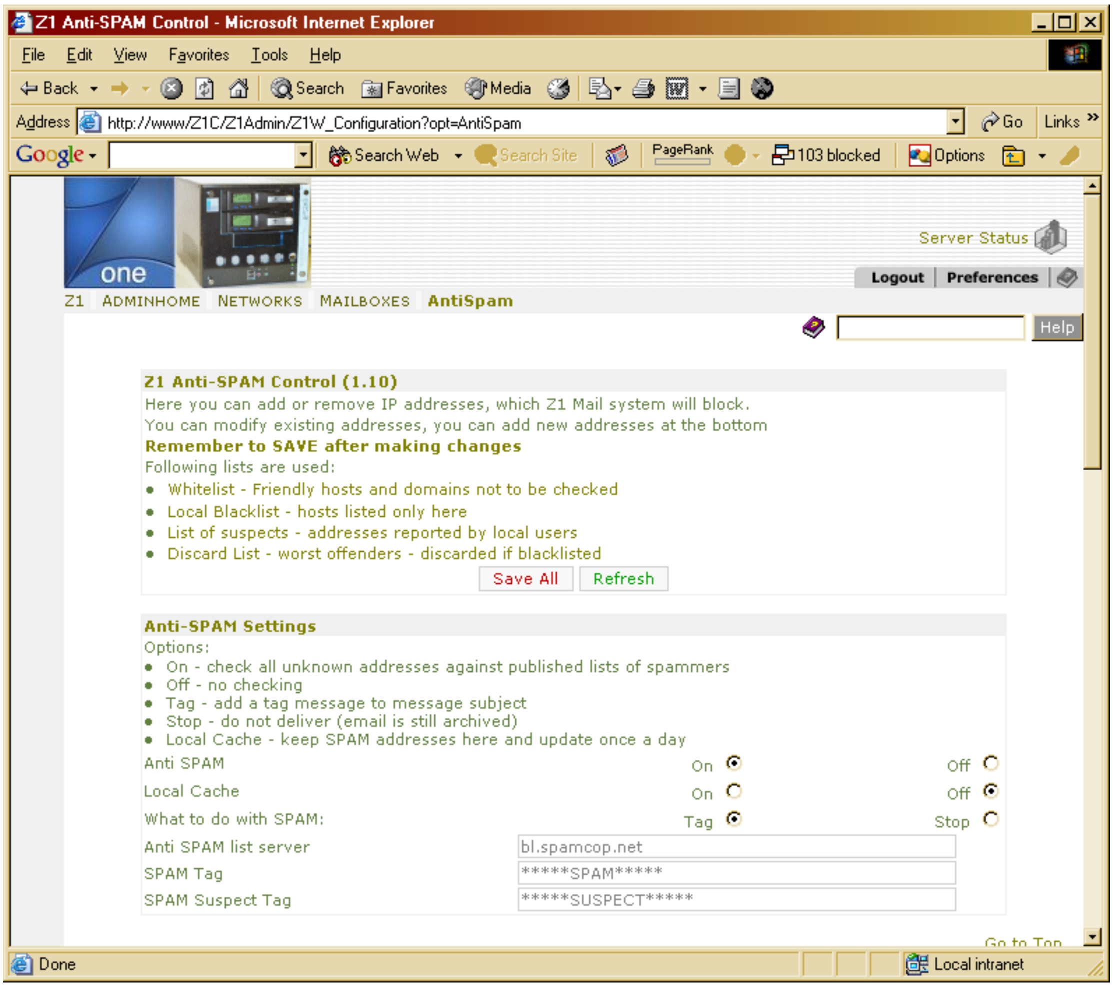
Firewall rules shown here will be re-applied when the server restarts.

Chain Name: openall Active: ☑

Comment: This chain opens the firewall to all.
It should be disabled as soon as possible.
Use chains with specific ports and addresses instead.

Path	Ports	Source	Destination	Action	Log
R->Z1	any	any	any	accept	
R->L	any	any	any	accept	
Z1->R	any	any	any	accept	
L->R	any	any	any	accept	
Add rules:					
Select				Select	

2.3.5 Anti-SPAM Control


Z1 Anti-SPAM Control - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www/Z1C/Z1Admin/Z1W_Configuration?opt=AntiSpam
Go Links
Google Search Web Search Site PageRank 103 blocked Options
one
Server Status
Logout Preferences
Z1 ADMINHOME NETWORKS MAILBOXES AntiSpam
Help
Save All Refresh
Go to Top
Done
Local intranet

Z1 Anti-SPAM Control (1.10)

Here you can add or remove IP addresses, which Z1 Mail system will block.
You can modify existing addresses, you can add new addresses at the bottom
Remember to SAVE after making changes
Following lists are used:

- Whitelist - Friendly hosts and domains not to be checked
- Local Blacklist - hosts listed only here
- List of suspects - addresses reported by local users
- Discard List - worst offenders - discarded if blacklisted

Anti-SPAM Settings

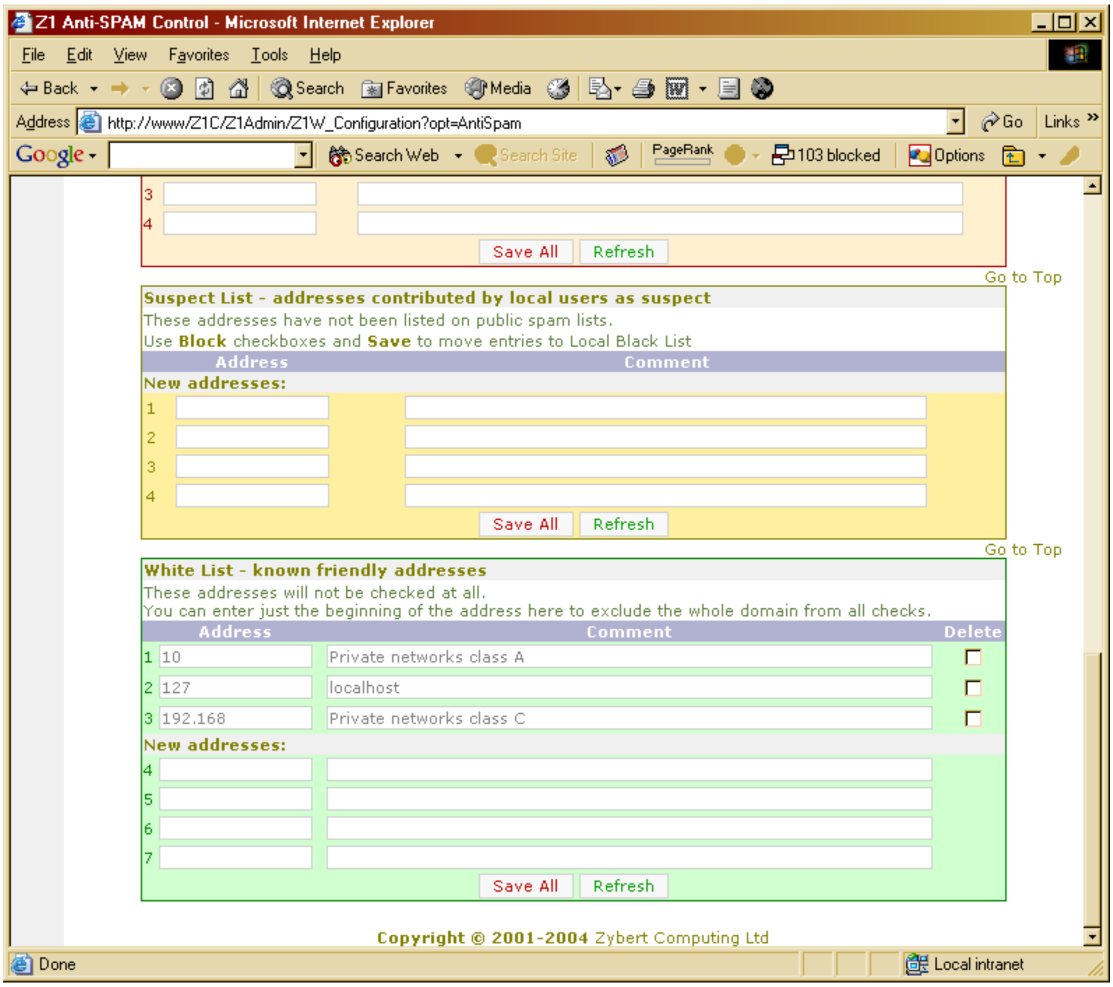
Options:

- On - check all unknown addresses against published lists of spammers
- Off - no checking
- Tag - add a tag message to message subject
- Stop - do not deliver (email is still archived)
- Local Cache - keep SPAM addresses here and update once a day

Anti SPAM	On ●	Off ○
Local Cache	On ○	Off ●
What to do with SPAM:	Tag ●	Stop ○
Anti SPAM list server	bl.spamcop.net	
SPAM Tag	*****SPAM*****	
SPAM Suspect Tag	*****SUSPECT*****	

Z1 uses **SpamAssassin** program to detect SPAM mail. SpamAssassing configuration may be modified by each user with the SpamAssassing module of **Usermin**. Usermin can be accessed on port 20000 (http:://www:20000). It contains a number of useful tools. SpamAssassin module is in the **MAIL** section of Usermin.

Additionally Z1 checks addresses in the headers of incoming mail against public '**Black Lists**'. This service can be controlled here – you may decide what should happen to black-listed email, you can build your own black and white lists. There is also a 'grey' list – a list of suspect addresses – mails that match this list will not be stopped but their subject field will be modified to warn the recipients. There is a mechanism of users contributing to your grey list as well as a mechanism for the administrator to 'upgrade' grey list addresses to the black list. It is a good idea to place the address of your Internet provider (where your mailbox is kept) into your White list. This protects you from the situation where your provider finds itself on a Black list and that causes all your mail being treated as SPAM.


Z1 Anti-SPAM Control - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Google Search Web Search Site PageRank 103 blocked Options
Save All Refresh
Go to Top
Save All Refresh
Go to Top
Save All Refresh
Done
Local intranet

Address http://www/Z1C/Z1Admin/Z1W_Configuration?opt=AntiSpam

3		
4		

Suspect List - addresses contributed by local users as suspect

These addresses have not been listed on public spam lists.

Use **Block** checkboxes and **Save** to move entries to Local Black List

	Address	Comment
New addresses:		
1		
2		
3		
4		

White List - known friendly addresses

These addresses will not be checked at all.

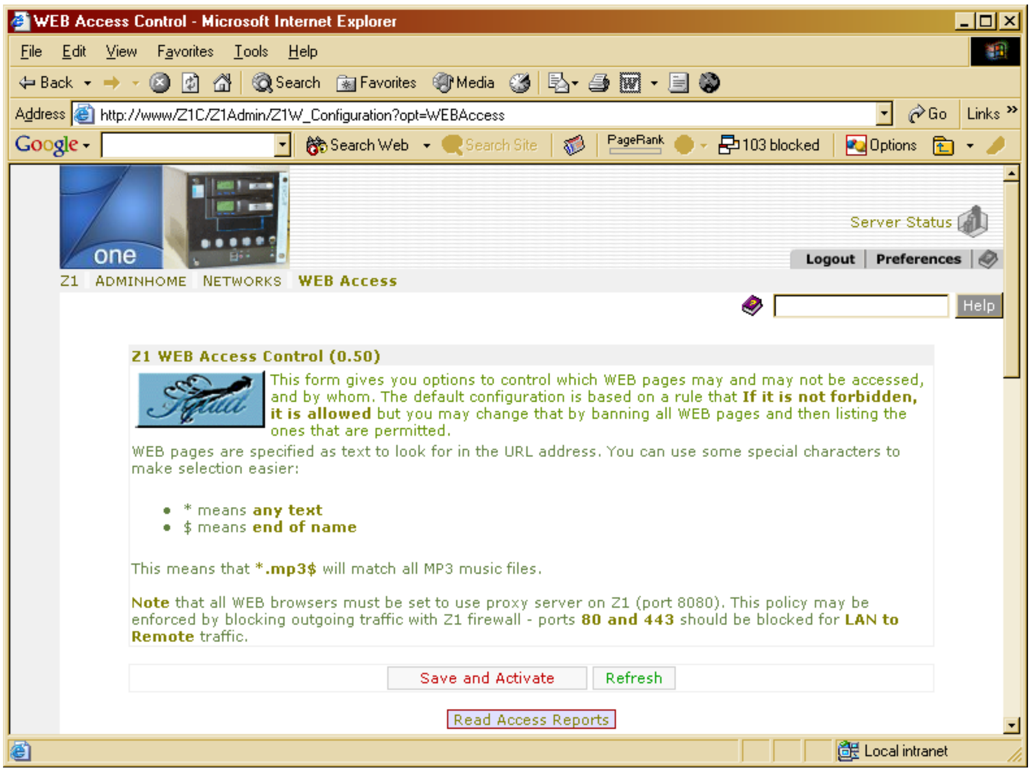
You can enter just the beginning of the address here to exclude the whole domain from all checks.

	Address	Comment	Delete
1	10	Private networks class A	□
2	127	localhost	□
3	192.168	Private networks class C	□
New addresses:			
4			
5			
6			
7			

Copyright © 2001-2004 Zybert Computing Ltd

See on-line help for more information.

2.3.6 WEB Access Control


WEB Access Control - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www/Z1C/Z1Admin/Z1W_Configuration?opt=WEBAccess
Go Links
Google Search Web Search Site PageRank 103 blocked Options
one
Server Status
Logout Preferences
Z1 ADMINHOME NETWORKS WEB Access
Help
Save and Activate
Refresh
Read Access Reports
Local intranet

Z1 WEB Access Control (0.50)

This form gives you options to control which WEB pages may and may not be accessed, and by whom. The default configuration is based on a rule that **If it is not forbidden, it is allowed** but you may change that by banning all WEB pages and then listing the ones that are permitted.

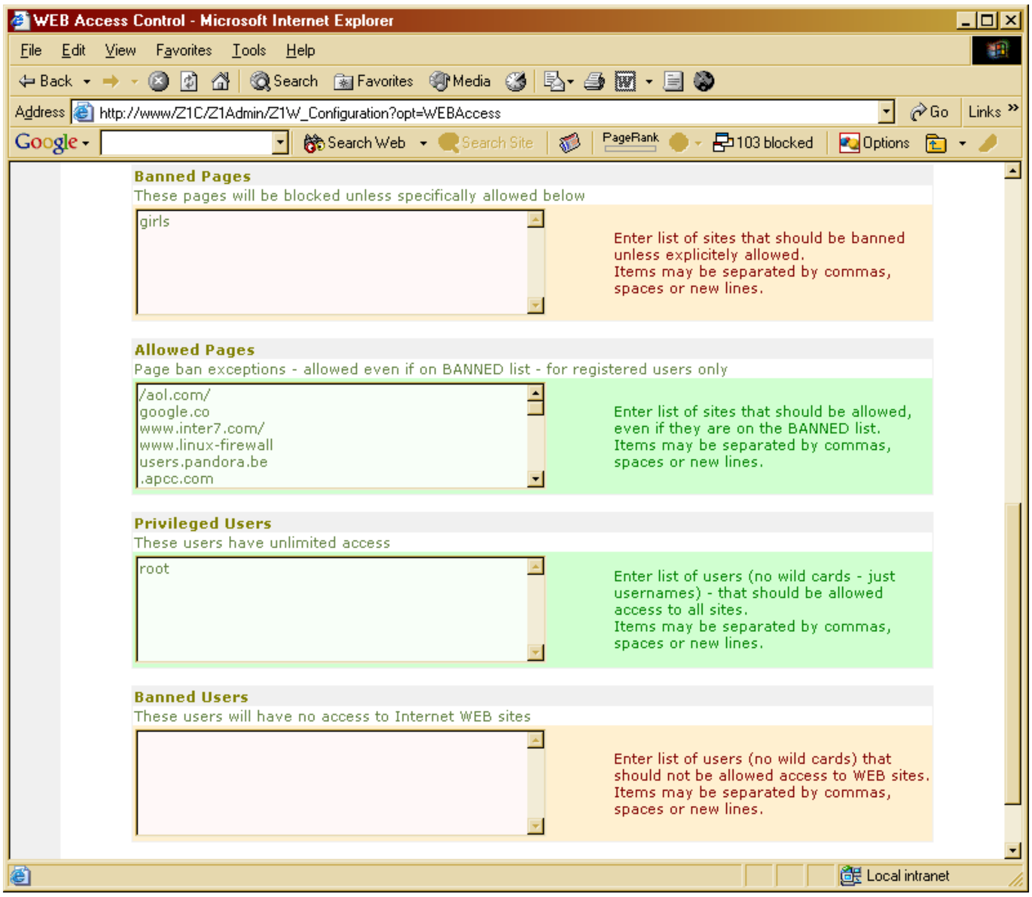
WEB pages are specified as text to look for in the URL address. You can use some special characters to make selection easier:

- * means **any text**
- $ means **end of name**

This means that ***.mp3$** will match all MP3 music files.

Note that all WEB browsers must be set to use proxy server on Z1 (port 8080). This policy may be enforced by blocking outgoing traffic with Z1 firewall - ports **80 and 443** should be blocked for **LAN to Remote** traffic.

Z1 uses **SQUID** proxy server to provide WEB access control and monitoring. This page provides a minimal control of who can access WEB sites and allows administrator to block certain WEB sites alltogether.


WEB Access Control - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www/Z1C/Z1Admin/Z1W_Configuration?opt=WEBAccess
Go Links
Google Search Web Search Site PageRank 103 blocked Options
Local intranet

Banned Pages

These pages will be blocked unless specifically allowed below

```
girls
```

Enter list of sites that should be banned unless explicitely allowed.
Items may be separated by commas, spaces or new lines.

Allowed Pages

Page ban exceptions - allowed even if on BANNED list - for registered users only

```
/aol.com/
google.co
www.inter7.com/
www.linux-firewall
users.pandora.be
.apcc.com
```

Enter list of sites that should be allowed, even if they are on the BANNED list.
Items may be separated by commas, spaces or new lines.

Privileged Users

These users have unlimited access

```
root
```

Enter list of users (no wild cards - just usernames) - that should be allowed access to all sites.
Items may be separated by commas, spaces or new lines.

Banned Users

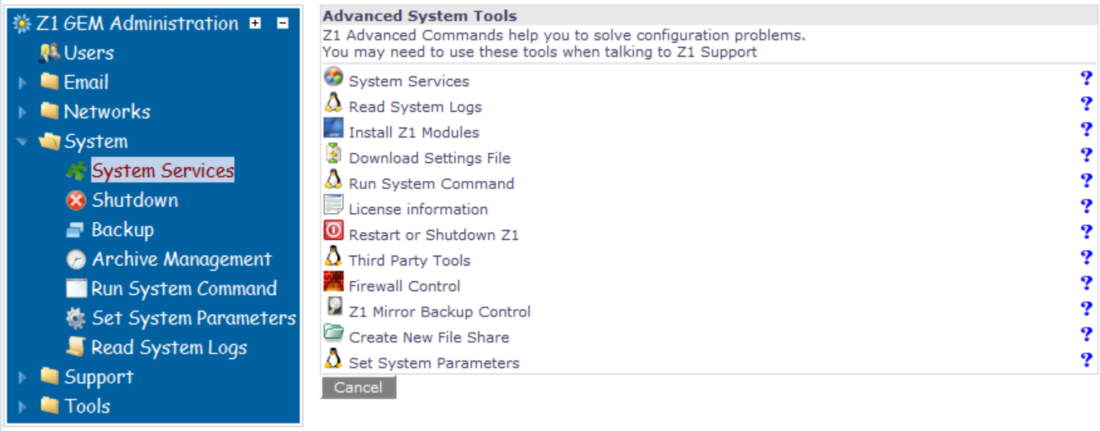
These users will have no access to Internet WEB sites

Enter list of users (no wild cards) that should not be allowed access to WEB sites.
Items may be separated by commas, spaces or new lines.

Copyright © ZYBERT Computing Ltd 2001-2010

2.4 Expert menu

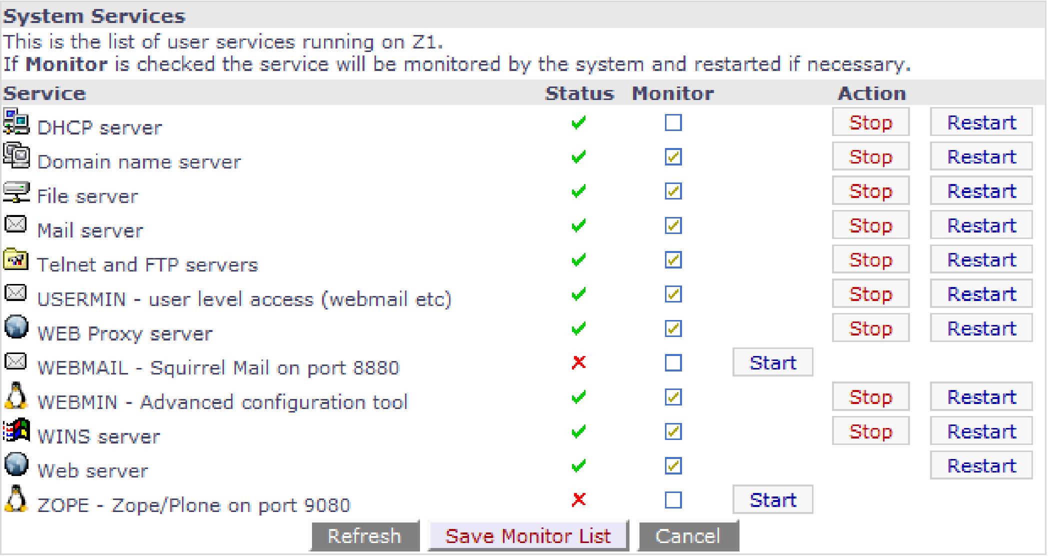
This is a collection of tools that go beyond the simple administration of the system. They help you to diagnose problems, intervene when things do not work as intended. These tools are also very helpful when you talk to Z1 Support.



Advanced System Tools

Z1 Advanced Commands help you to solve configuration problems.
You may need to use these tools when talking to Z1 Support

2.4.1 System Services



System Services

This is the list of user services running on Z1.
If **Monitor** is checked the service will be monitored by the system and restarted if necessary.

Service	Status	Monitor	Action	
DHCP server	✓	□	Stop	Restart
Domain name server	✓	☑	Stop	Restart
File server	✓	☑	Stop	Restart
Mail server	✓	☑	Stop	Restart
Telnet and FTP servers	✓	☑	Stop	Restart
USERMIN - user level access (webmail etc)	✓	☑	Stop	Restart
WEB Proxy server	✓	☑	Stop	Restart
WEBMAIL - Squirrel Mail on port 8880	✗	□	Start	
WEBMIN - Advanced configuration tool	✓	☑	Stop	Restart
WINS server	✓	☑	Stop	Restart
Web server	✓	☑		Restart
ZOPE - Zope/Plone on port 9080	✗	□	Start	

This page shows status of basic system services. It also allows you to start/stop/restart selected services.

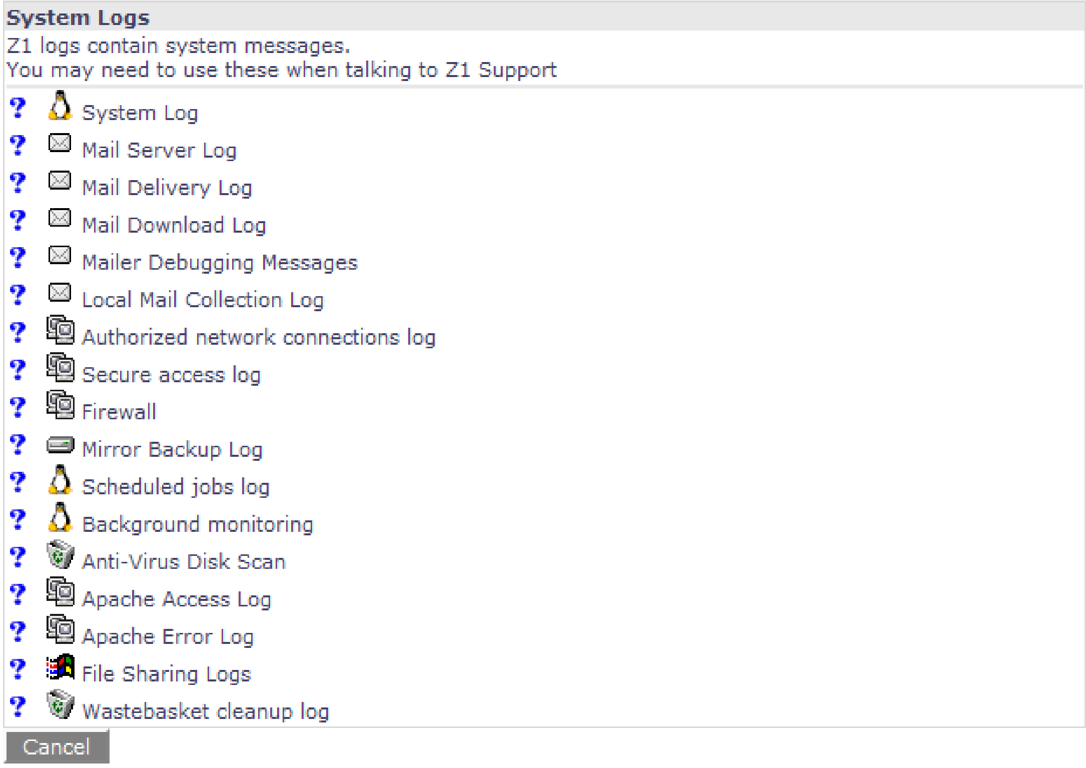
Note that stopping services may interrupt users and sometimes lead to data loss. You should not do it unless there is a real problem.

You may ask the system to monitor selected services and restart them if a problem is detected. The system check the selected services every two minutes.

Note that if a service is being monitored and is not started automatically on a system start then it will be started by the system monitor. Therefore – if you disable DHCP server in the Network Settings, make sure that the monitor for DHCP is off.

2.4.2 System logs

This page gives you access to Z1 logging information. Some of the system logs are difficult to read but they may contain important information to help system diagnostics. Z1 Support personnel may ask you to look into these files when you call them with a problem.

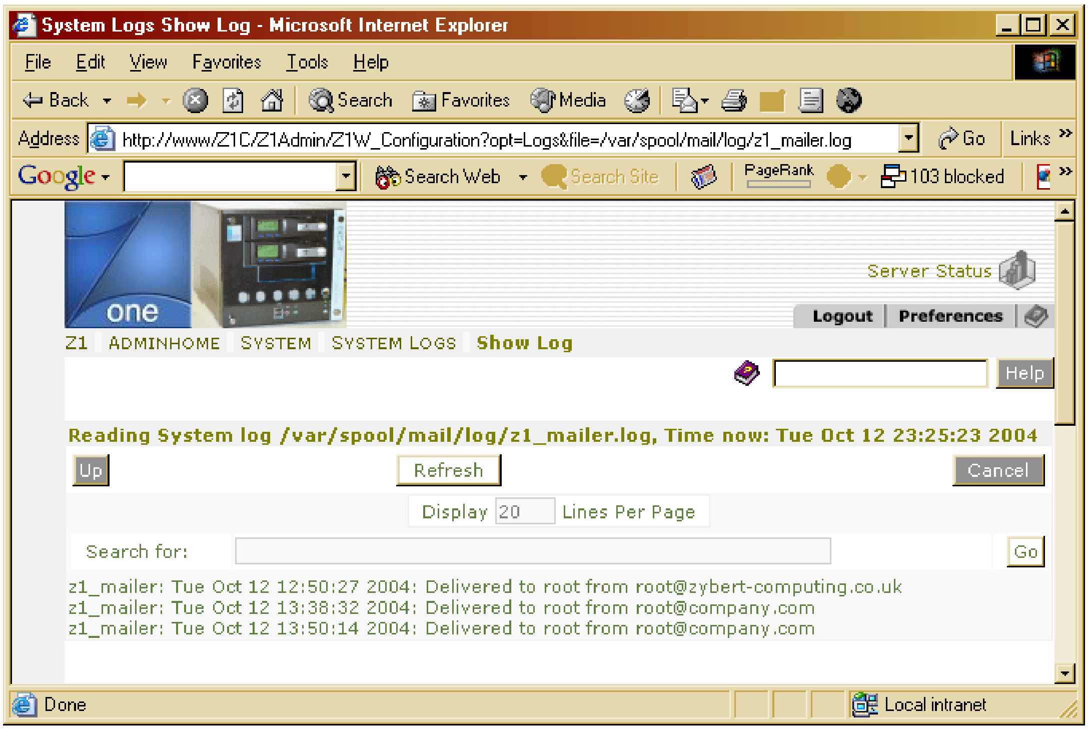


System Logs

Z1 logs contain system messages.
You may need to use these when talking to Z1 Support

- System Log
- Mail Server Log
- Mail Delivery Log
- Mail Download Log
- Mailer Debugging Messages
- Local Mail Collection Log
- Authorized network connections log
- Secure access log
- Firewall
- Mirror Backup Log
- Scheduled jobs log
- Background monitoring
- Anti-Virus Disk Scan
- Apache Access Log
- Apache Error Log
- File Sharing Logs
- Wastebasket cleanup log

Here is an example of log file display:



System Logs Show Log - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google
Search Web
Search Site
PageRank
103 blocked
one
Server Status
Logout
Preferences
Z1 ADMINHOME SYSTEM SYSTEM LOGS Show Log
Help
Up
Refresh
Cancel
Go
Done
Local intranet

Address: http://www/Z1C/Z1Admin/Z1W_Configuration?opt=Logs&file=/var/spool/mail/log/z1_mailer.log

Reading System log /var/spool/mail/log/z1_mailer.log, Time now: Tue Oct 12 23:25:23 2004

Display 20 Lines Per Page

Search for:

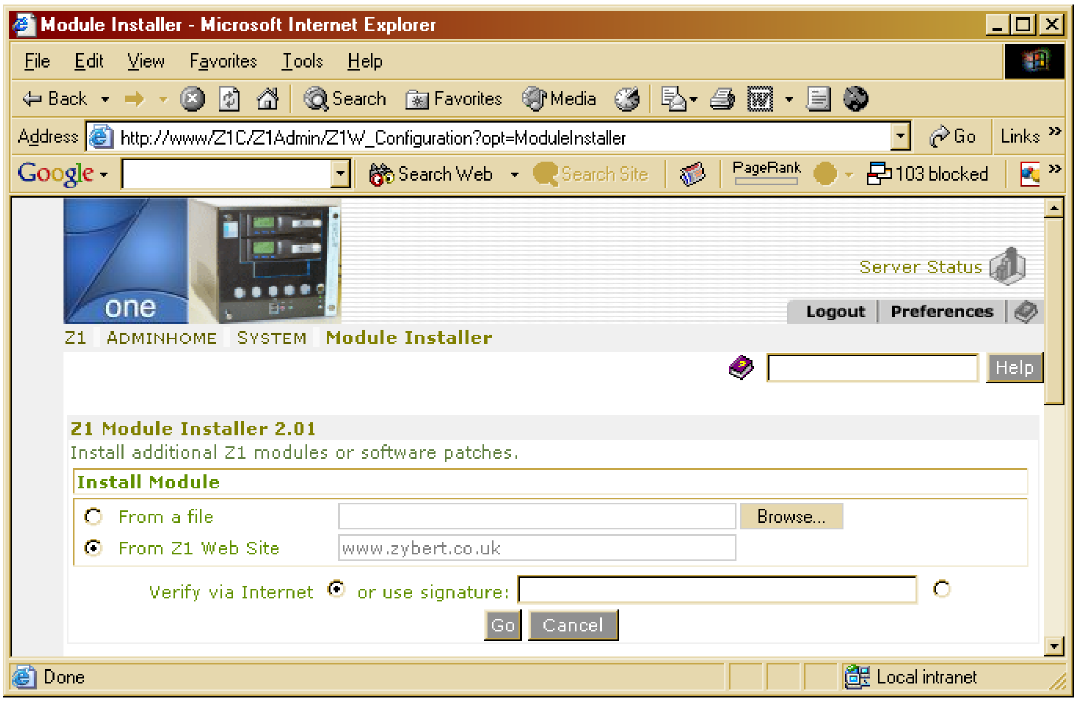
```
z1_mailer: Tue Oct 12 12:50:27 2004: Delivered to root from root@zybert-computing.co.uk
z1_mailer: Tue Oct 12 13:38:32 2004: Delivered to root from root@company.com
z1_mailer: Tue Oct 12 13:50:14 2004: Delivered to root from root@company.com
```

2.4.3 Module installer

From time to time Z1 software team releases patches, bug fixes and upgrades to existing software. There may also be new, optional elements of Z1 software, extras etc.

Depending on your service contract all these may be mailed to you or you may install them from ZYBERT web server.

The installation process makes this easy by communicating with the web server directly, selecting modules that should be installed in your system and then installing them directly from the web server.


Module Installer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www/Z1C/Z1Admin/Z1W_Configuration?opt=ModuleInstaller
Go Links
Google Search Web Search Site PageRank 103 blocked
one
Server Status
Logout Preferences
Z1 ADMINHOME SYSTEM Module Installer
Help

Z1 Module Installer 2.01

Install additional Z1 modules or software patches.

Install Module

○ From a file Browse...

● From Z1 Web Site www.zybert.co.uk

Verify via Internet ● or use signature: ○

Go Cancel

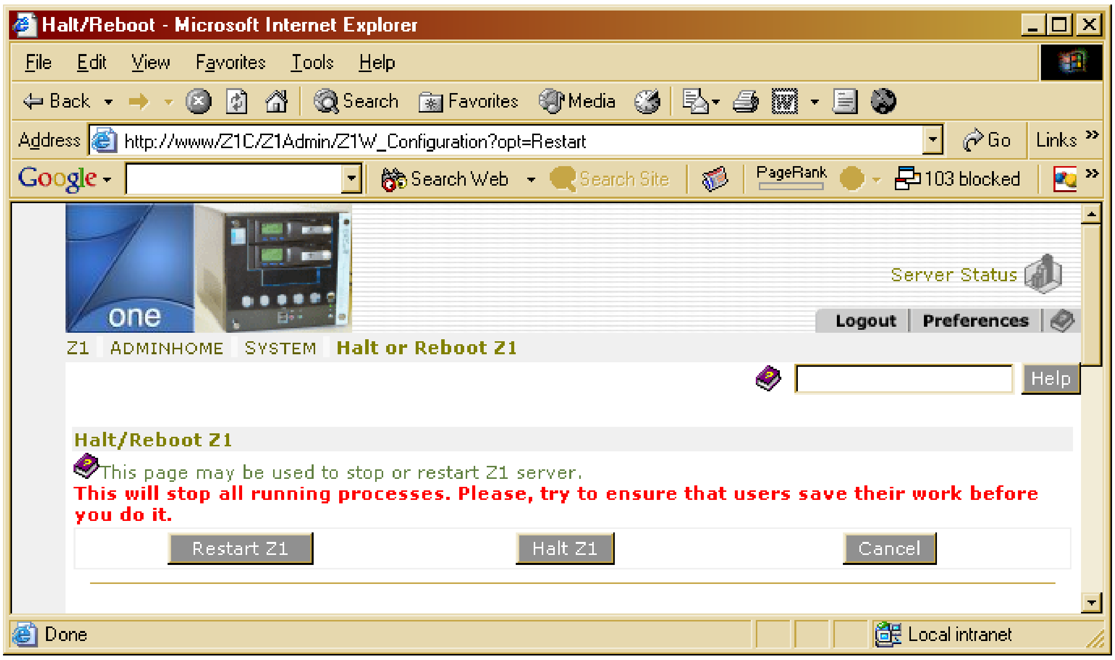
For security reasons all modules have a signature that can be checked against Z1 module database. The system will refuse to install a module that cannot be verified. Usually this is done via your Internet connection but in exceptional situations the correct signature may be pasted into text box here.

If a module is supplied to you via email you should always allow Z1 to verify the module via Internet. Additional instructions concerning installation of a specific module may be provided with the module.

Click *Go* to start installation.

2.4.4 Rebooting Z1

If you need to stop or reboot Z1 it should be done here – click on *Restart or Shutdown Z1*. You will see the confirmation page:


Halt/Reboot - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www/Z1C/Z1Admin/Z1W_Configuration?opt=Restart
Go Links
Google Search Web Search Site PageRank 103 blocked
one
Server Status
Logout Preferences
Z1 ADMINHOME SYSTEM Halt or Reboot Z1
Help
Done
Local intranet

Halt/Reboot Z1

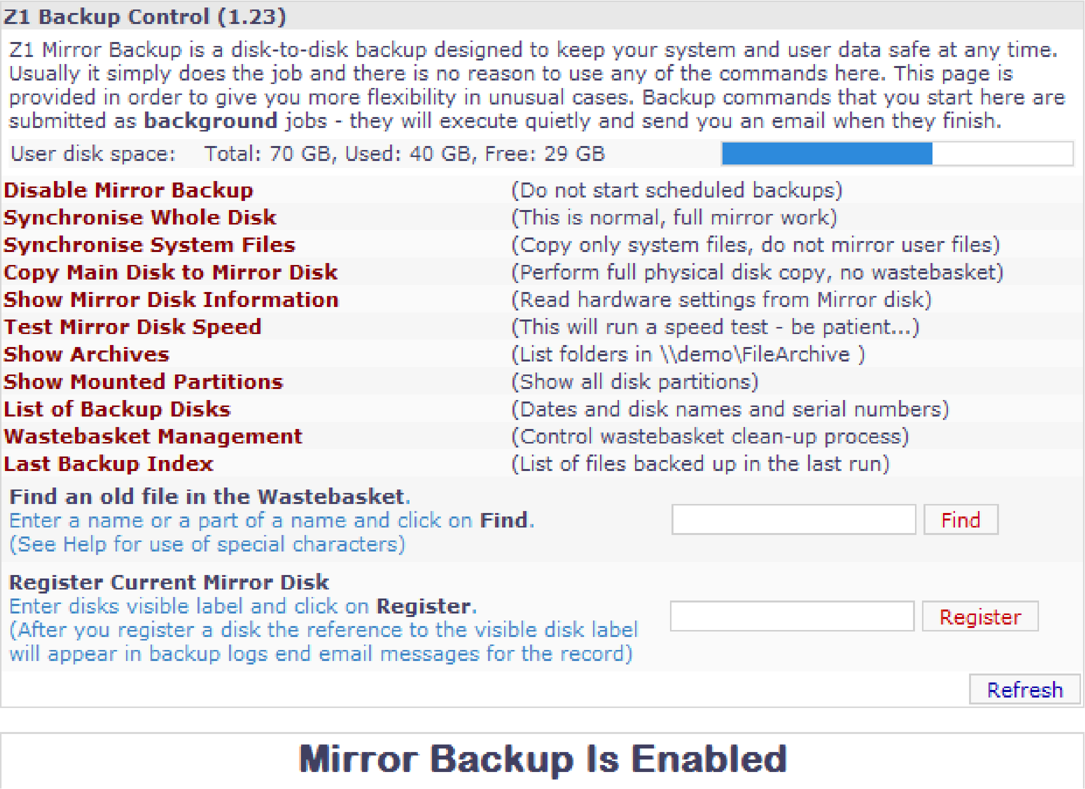
This page may be used to stop or restart Z1 server.

This will stop all running processes. Please, try to ensure that users save their work before you do it.

Restart Z1
Halt Z1
Cancel

Z1 should only take few minutes to restart. If you press *Halt Z1* please, GEM should turn itself off after stopping all processes.

2.4.5 Backup Control



Z1 Backup Control (1.23)

Z1 Mirror Backup is a disk-to-disk backup designed to keep your system and user data safe at any time. Usually it simply does the job and there is no reason to use any of the commands here. This page is provided in order to give you more flexibility in unusual cases. Backup commands that you start here are submitted as **background** jobs - they will execute quietly and send you an email when they finish.

User disk space: Total: 70 GB, Used: 40 GB, Free: 29 GB

Disable Mirror Backup	(Do not start scheduled backups)
Synchronise Whole Disk	(This is normal, full mirror work)
Synchronise System Files	(Copy only system files, do not mirror user files)
Copy Main Disk to Mirror Disk	(Perform full physical disk copy, no wastebasket)
Show Mirror Disk Information	(Read hardware settings from Mirror disk)
Test Mirror Disk Speed	(This will run a speed test - be patient...)
Show Archives	(List folders in \\demo\FileArchive)
Show Mounted Partitions	(Show all disk partitions)
List of Backup Disks	(Dates and disk names and serial numbers)
Wastebasket Management	(Control wastebasket clean-up process)
Last Backup Index	(List of files backed up in the last run)

Find an old file in the Wastebasket.
Enter a name or a part of a name and click on **Find**.
(See Help for use of special characters)

Register Current Mirror Disk
Enter disks visible label and click on **Register**.
(After you register a disk the reference to the visible disk label will appear in backup logs end email messages for the record)

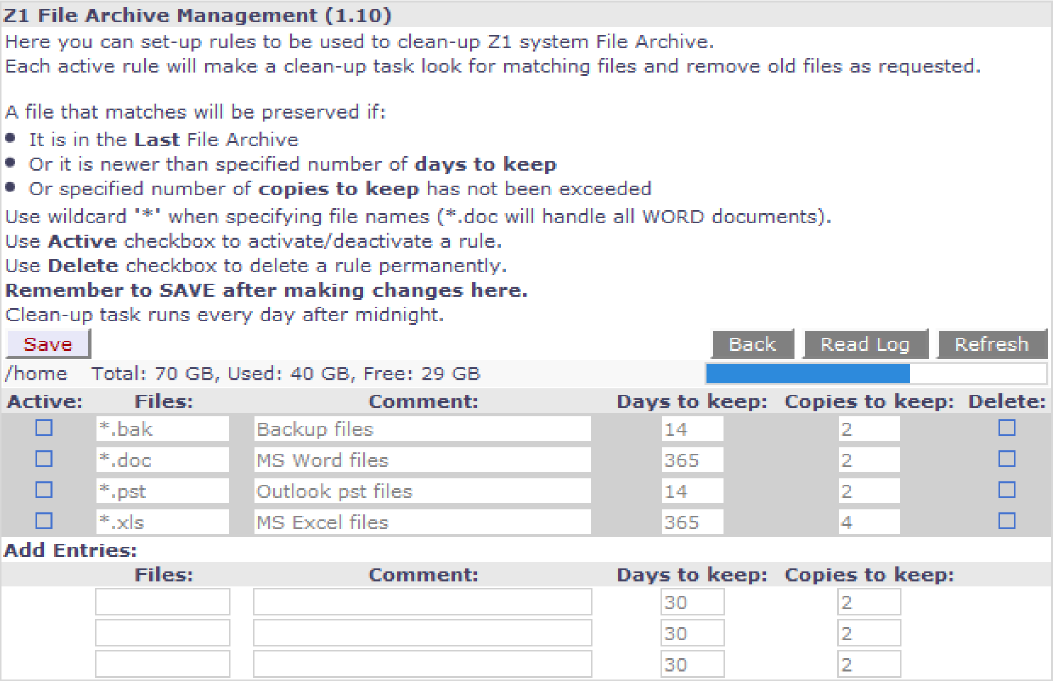
Mirror Backup Is Enabled

Z1 disk-to-disk backup system is designed to work automatically, with no need of intervention. Every night the backup disk is synchronized with the main disk, all changed files on the backup disk are archived first. The backup disk is prepared to be bootable if necessary. An short email is sent to **root** with basic backup statistics. It is important that you set-up a mail alias to redirect root mail to a real administrator.

This page gives you a possiblity of forcing immediate backup, disabling and enabling backup, checking the status of the backup disk etc.

The items are explained on the screen and in the on-line help file.

If your disk is getting full you should try to introduce some rules on the Archive (wastebasket) system. Click on **Archive Management**.



Z1 File Archive Management (1.10)

Here you can set-up rules to be used to clean-up Z1 system File Archive.
Each active rule will make a clean-up task look for matching files and remove old files as requested.

A file that matches will be preserved if:

- It is in the **Last** File Archive
- Or it is newer than specified number of **days to keep**
- Or specified number of **copies to keep** has not been exceeded

Use wildcard '*' when specifying file names (*.doc will handle all WORD documents).
Use **Active** checkbox to activate/deactivate a rule.
Use **Delete** checkbox to delete a rule permanently.
Remember to SAVE after making changes here.
Clean-up task runs every day after midnight.

/home Total: 70 GB, Used: 40 GB, Free: 29 GB

Active:	Files:	Comment:	Days to keep:	Copies to keep:	Delete:
□	*.bak	Backup files	14	2	□
□	*.doc	MS Word files	365	2	□
□	*.pst	Outlook pst files	14	2	□
□	*.xls	MS Excel files	365	4	□

Add Entries:

Files:	Comment:	Days to keep:	Copies to keep:
		30	2
		30	2
		30	2

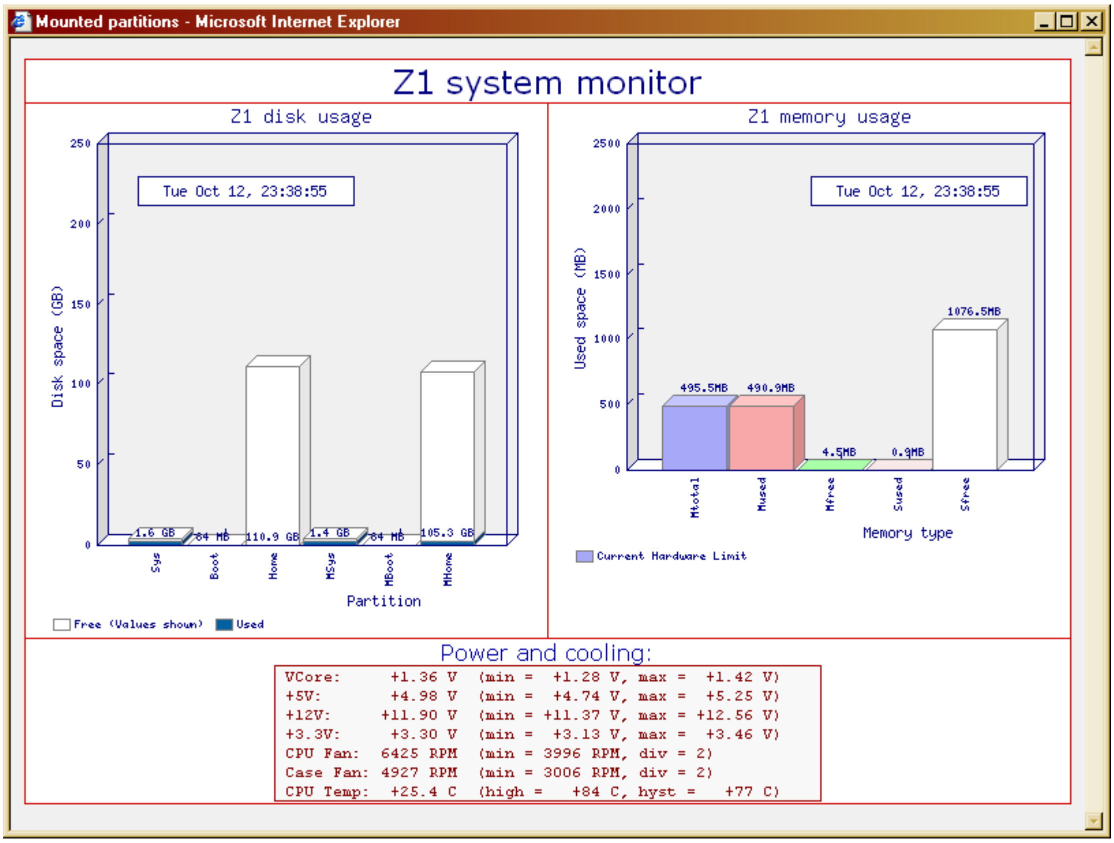
Here you can set limits on how long you need to keep files for, or how many versions. If you set a limit for some type of files to 14 days and 2 copies then all files of that type will be kept for 14 days at least but at least two latest versions will be preserved, even if they are older than 14 days.

Note – these settings are for **ARCHIVE ONLY**. Nothing interferes with files you are using. Archive contains only old files that have been changed or deleted by users.

If no rules are active then all old files are kept forever.

3 System status

To see disk and memory usage of Z1 click on *Server Status*. New browser window will open with the display more or less like this:



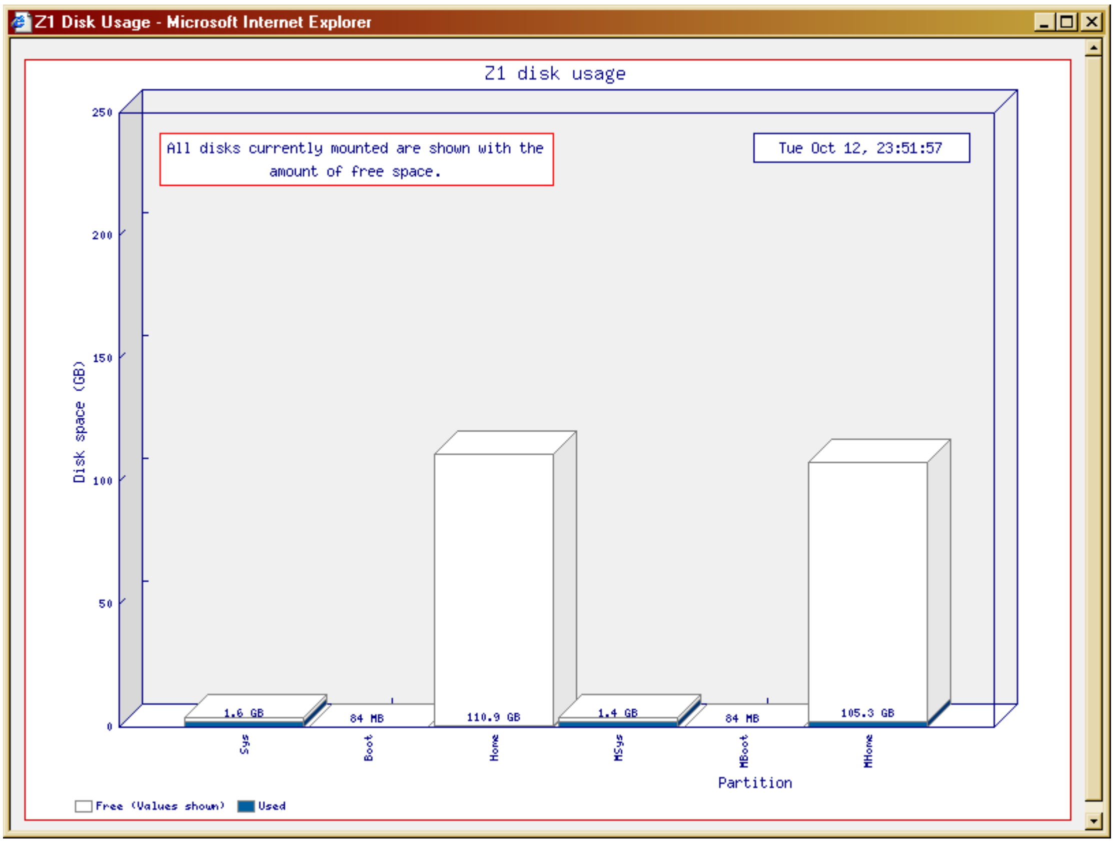
Power and cooling:

```
VCore:      +1.36 V  (min =  +1.28 V, max =  +1.42 V)
+5V:        +4.98 V  (min =  +4.74 V, max =  +5.25 V)
+12V:      +11.90 V  (min = +11.37 V, max = +12.56 V)
+3.3V:      +3.30 V  (min =  +3.13 V, max =  +3.46 V)
CPU Fan:   6425 RPM  (min = 3996 RPM, div = 2)
Case Fan:  4927 RPM  (min = 3006 RPM, div = 2)
CPU Temp:   +25.4 C  (high =   +84 C, hyst =   +77 C)
```

The plots will automatically refresh (memory every 20 seconds, disk every 5 minutes). These graphs give you a general idea about the load of the system and usage of resources.

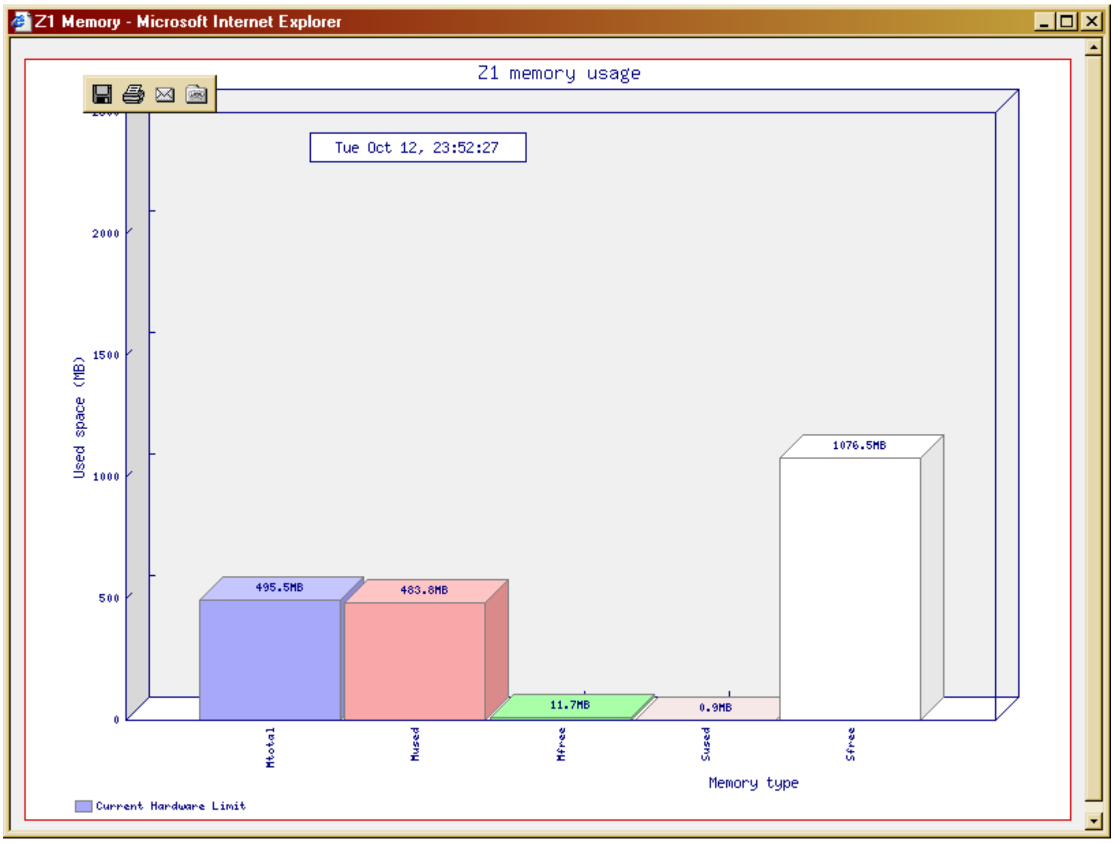
Additionally main voltages, CPU temperature and speed of two main fans is shown together with allowed limits. If you click on this text the display will refresh.

If you click on a graph you will get an enlarged version with more details. In the case of memory display the enlarged version also refreshes quickly (every 2 seconds):



All disks currently mounted are shown with the amount of free space.

Tue Oct 12, 23:51:57

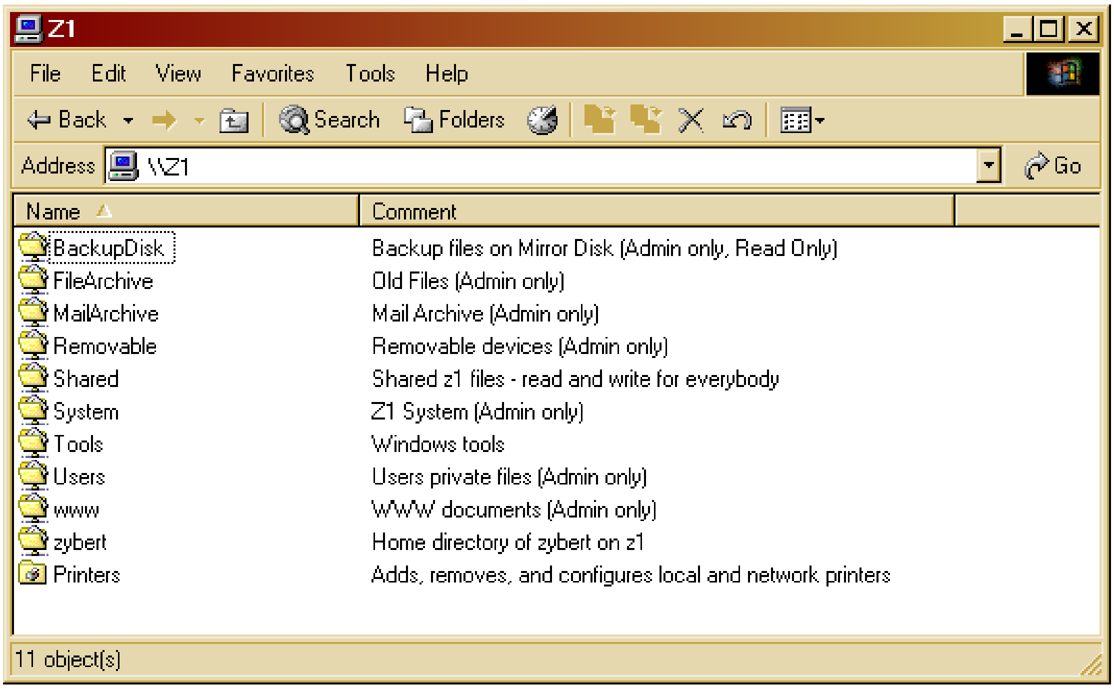


Tue Oct 12, 23:52:27

Click on the graph to return to previous display.

4 File system

Z1 provides several *Shares* to ensure a logical separation of different regions and to provide security. Every user will see the following structure:



Name	Comment
BackupDisk	Backup files on Mirror Disk (Admin only, Read Only)
FileArchive	Old Files (Admin only)
MailArchive	Mail Archive (Admin only)
Removable	Removable devices (Admin only)
Shared	Shared z1 files - read and write for everybody
System	Z1 System (Admin only)
Tools	Windows tools
Users	Users private files (Admin only)
www	WWW documents (Admin only)
zybert	Home directory of zybert on z1
Printers	Adds, removes, and configures local and network printers

Home directory of each user – visible only to this user (and administrator) is labelled with the user login name.

Permission on different shares are set-up for high security. These permissions can be changed with SWAT tool (in Third-Party-Tools).

As an administrator, you have a read/write access to all files. (This is a very good reason to limit the number of users with administrator rights).

The individual shares have following functions:

- [username] – private user files, not accessible to other users
- Shared – shared files. Each user has a folder there but all files are accessible to other users.
- BackupDisk – Read-Only access to backup disk. It usually contains the last nights ‘snapshot’ of the main disk so it can be used to recover files accidentally lost or damaged.
- FileArchive – before each nightly snapshot backup all files that are to be deleted or changed on the backup disk are first copied into an archive structure on both disks. There is one such structure for every day. This system allows you to recover old files.
- MailArchive – all incoming and outgoing email is archived. This share contains a structure of folders – one per day – with old, archived mail. These files have a standard text (mbox) format and may be read with any text editor. Do not modify these files, as this may make then unreadable by your mail client.
- Removable – used for accessing USB storage devices that can be plugged into Z1 USB sockets.
- System – the whole Z1 disk
- Tools – A collection of tools that can be installed on your Windows Workstation.
- Users – all users private folders

A file for the previous day is created at 1:00 in the morning. Messages for the current day cannot be viewed this way – they are still in the Inbox of the mailbackup mail account and you will need to access them using a mail program. In order to save disk space and to limit security risks we recommend that you remove old messages from mail backup from time to time (you may back them up first to a CD Writer or tape or something)

5 Backup and Recovery

Z1 Gem is delivered with three identical disks. Two of the disks are mounted in the GEM case.

The disk mounted in the top shelf of the GEM body is the main disk. This is the disk where all data files are kept. This disk also contains all system files and is in constant use.

The second disk is the current backup disk.

Every night (currently at 2am) the the backup disk is synchronized with the main disk. All user and system files that changed on the main disk since the last backup are copied over to the backup disk. Before any file on the backup disk is modified or deleted, it is copied to file archive. This way all your old files are stored and can be recovered later. At the end of the backup run the two disks in the machine are identical.

The backup disk is available READ-ONLY during the day. So – if you delete or damage an important file you can restore the previous day copy from the backup disk. (This is at initially only available to administrators but this setting can be easily changed).

If your main disk gets corrupted, or damaged you can turn it off using the supplied key and press reset button. GEM will reboot from your backup disk. This should be only a temporary, quick solution – in this configuration there is no backup. GEM will always boot from the first disk it finds – counting from the top – and use the next disk as a backup disk.

It is important that the Backup disk is in place when GEM starts. The system allows for a 'hot-swap' of the backup disk but you cannot ADD a disk to the system if it was not there during the boot process.

A more permanent solution of a corruption of the main disk is to turn the GEM off, swap the two disks – backup disk to the top shelf, main disk to the bottom shelf – and start again. The system will boot from the top disk and the bottom disk is now treated as a backup disk. Any corruption of data or system files can be now corrected, you can even tell the system to re-format the backup disk and copy the main disk to it.

The third supplied disk should be kept permanently off site in a safe place. Usually once a week (but you may choose your own frequency) the backup disk should be removed from GEM and the third disk should be put in. You can do this without stopping the server and even while users are connected to the system. GEM will recognize the disk and will continue. The disk removed from GEM should be taken off site. This procedure ensures that you can survive major disasters – like fire, flood or simply your computers being stolen. Your off-site disk can be plugged into a replacement server and you can continue working. How much data you loose in a case like this depends on how long the disk was away from GEM.

This may lead to a conclusion that it is best to do the 'swap' every day. It might be so if you also have a procedure to remove the third disk from the premises. Otherwise all your three disks are in one place most of the time and this increases the risk.

Most small businesses choose the following procedure:

The third disk is kept away from the office most of the week. It is swapped at 5pm every Friday and the removed disk is taken away.

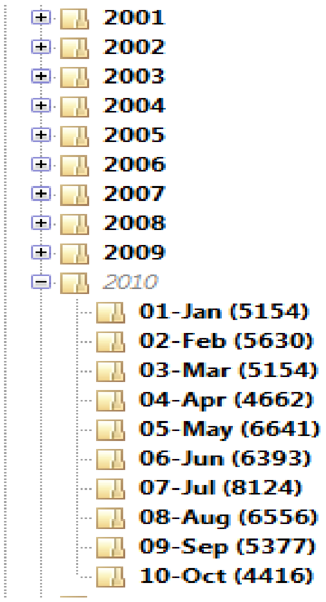
If it is essential that the backup disk is swapped every day you should consider purchasing a forth disk and do the swap every day, still keeping one of the disks away from the rest. You should then set-up a ‘rotation’ procedure to minimize risk to your data.

Please note that hard disks are delicate. The spare disk should not be dropped, liquids should not be spilled at it, it should be stored in a dry place away from direct sunlight or sources of heat.

6 Mail Archive

All mail is archived into a tree of IMAP folders. You may access them by with any IMAP mail client if your user account has correct privileges. This will allow you to see all mail messages sorted into separate mail folders for each month.

If you do not want to use IMAP in your usual mail program (Some version of Outlook may disable some useful functionalities if IMAP is in use) then we recommend that you use a different mail program – like Outlook Express that probably exists on your computer anyway - specifically to access mail archive.



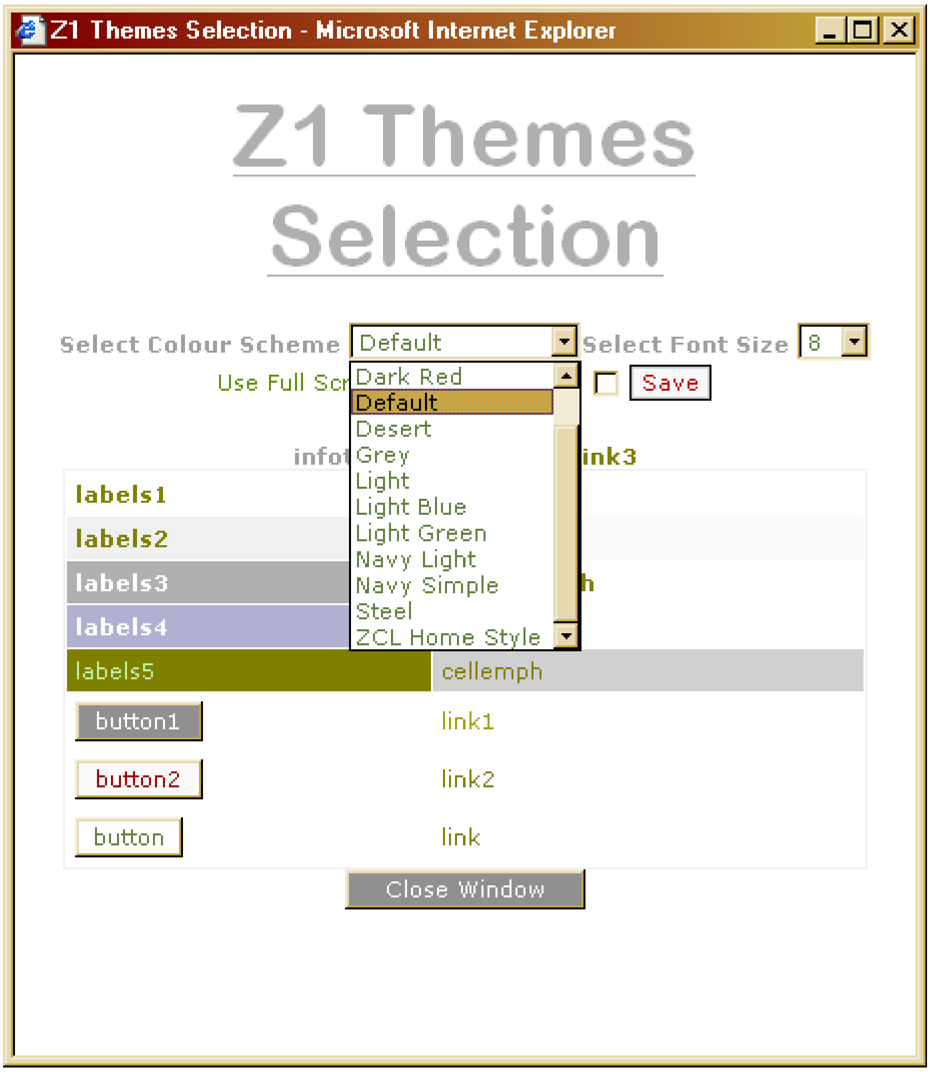
- 2001
- 2002
- 2003
- 2004
- 2005
- 2006
- 2007
- 2008
- 2009
- 2010
  - 01-Jan (5154)
  - 02-Feb (5630)
  - 03-Mar (5154)
  - 04-Apr (4662)
  - 05-May (6641)
  - 06-Jun (6393)
  - 07-Jul (8124)
  - 08-Aug (6556)
  - 09-Sep (5377)
  - 10-Oct (4416)

Also, remember that you have read access to these messages with the file sharing system – if you have enough privileges.

7 Colour Themes

Your monitor, lighting conditions (or your personal taste) may cause not be suitable for the default style of the administration displays. Z1 uses Dynamic Style System, which allows you to select from a range of colour combinations to suit your preferences.

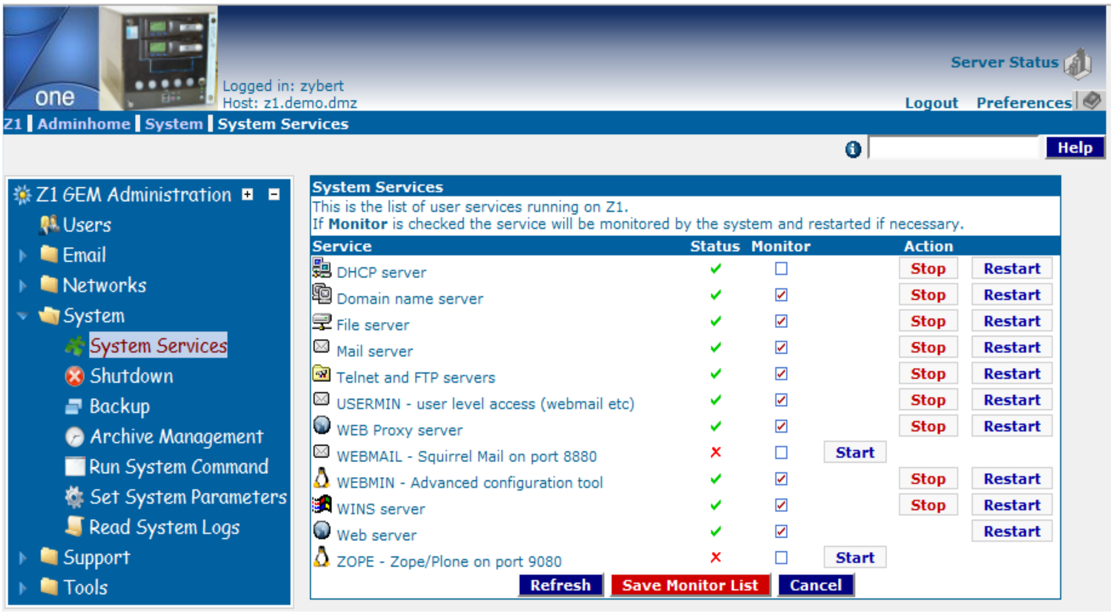
Click on *Preferences*. A new window will open:



If you select a theme and close the window all subsequent pages will use the new colour scheme (and font size). The information is kept as a cookie in your browser and will remember your selection until you change it.

Copyright © ZYBERT Computing Ltd 2001-2010

So – if you select *Navy Light* theme your typical display will look like this:



Logged in: zybert
Host: z1.demo.dmz

Z1 | Adminhome | System | System Services

System Services

This is the list of user services running on Z1.
If **Monitor** is checked the service will be monitored by the system and restarted if necessary.

Service	Status	Monitor		Action	
DHCP server	✓	□		Stop	Restart
Domain name server	✓	☑		Stop	Restart
File server	✓	☑		Stop	Restart
Mail server	✓	☑		Stop	Restart
Telnet and FTP servers	✓	☑		Stop	Restart
USERMIN - user level access (webmail etc)	✓	☑		Stop	Restart
WEB Proxy server	✓	☑		Stop	Restart
WEBMAIL - Squirrel Mail on port 8880	✗	□	Start		
WEBMIN - Advanced configuration tool	✓	☑		Stop	Restart
WINS server	✓	☑		Stop	Restart
Web server	✓	☑			Restart
ZOPE - Zope/Plone on port 9080	✗	□	Start		

8 Alarms

Z1 GEM continuously monitors its status. Most problems are automatically resolved, sometimes a mail message will be sent to **root** (remember to alias root to a real user!). These messages will contain information about the problem and instructions for remedial action.

In some extreme cases GEM may generate an audible alarm. Usually it follows an email to root and it is only used if an action is urgently required in order for the system to operate.

The alarm sound may be cancelled by clicking on **Stop Alarm** on the main WEB page of GEM (http://www).

An example if the alarm is when the backup disk is removed and the replacement disk is not inserted (or not turned on). The alarm will sound and it can be stopped manually or it will stop automatically when the replacement disk is in place and is detected.

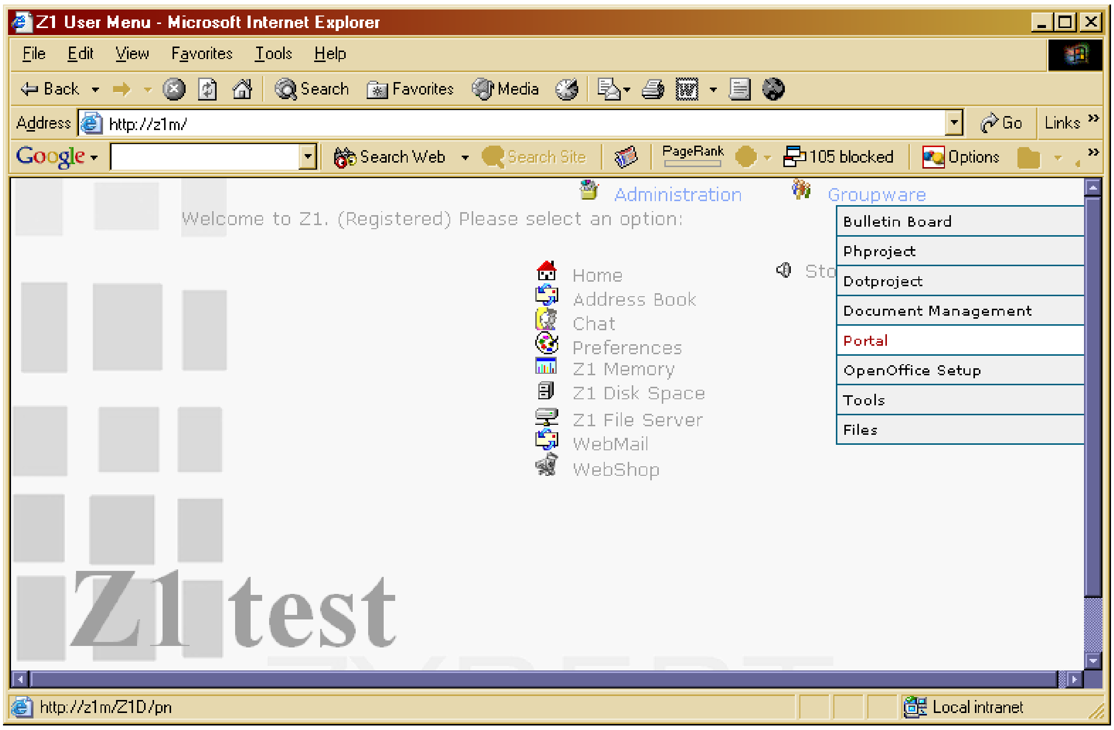
Disk enclosures have their independent alarm and monitoring system. They check disk temperatures and disk fan operation. If a problem is detected the alarm sounds and the information is displayed on the front panel. The alarms must be cleared using front panel controls of disk enclosures.

9 Additional Open Source Tools

Note: All open source software is governed by GNU Public License (GPL) or a similar license. Please read the terms of GNU license (in Administration Menu). One effect of this is that there is absolutely no guarantee attached to the distribution. Zybert Computing as well as Zybert resellers will make an affort to help you with problems but if a support of these programs is required it falls outside of the scope of our support programmes.

A selected collection of Open Source tools is installed on the Z1. There is a group of tools to run on the client (Windows PC) computers. These are in \\z1\Tools folder. Most of them are kept in an installer form and need to be installed on each PC.

Another collection are tools that are installed on Z1 and accessible via WEB interface.



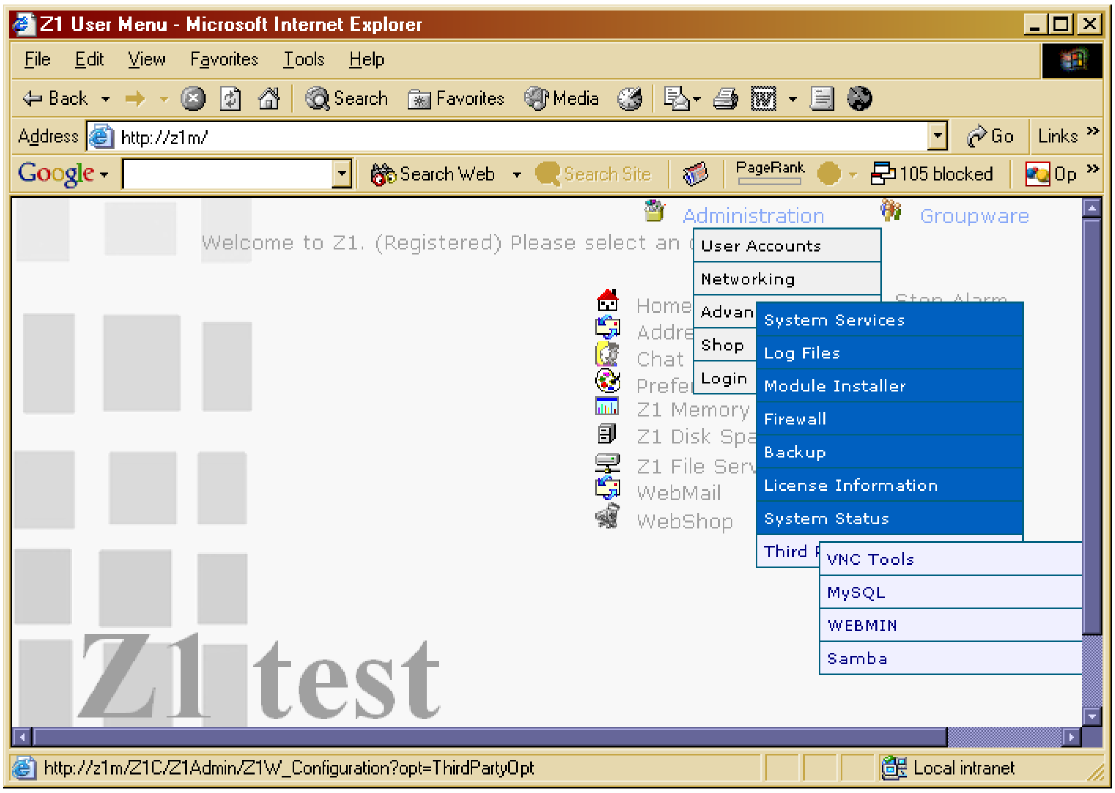
Welcome to Z1. (Registered) Please select an option:

Bulletin Board (YaBB), Phproject, Dotproject, Document Management (MyDMS) and Portal (PostNuke) are all WEB based 'groupware' tools. Administration account in each of these tools is independent of Z1 user account – use user **admin** password **admin** to access the administration for the first time.

OpenOffice is a fully functional Open Source office system, compatible with Microsoft Office (it can read and save Microsoft Office documents). OpenOffice can be either installed fully on each workstation (about 100MB) or it can be left in place – each user runs a Setup that configures their PC to use OpenOffice from the shared disk. Full – stand alone installation may be useful for laptops and other computer that may have to be used independently of the network. For stationary workstations the server/client installation is faster and requires very little disk space.

WebShop is a *'out of the box'* installation of Open Source Internet Shop from osCommerce.com. Before it can be used you need to run the Install procedure – this has to be done after the initial network setting. (Install as well as shop administration can be selected from the Administration Menu)

The third collection of Open Source tools can be found in Administration/Third Party Tools:



MySQL (phpMyAdmin), WEBMIN and Samba (SWAT) are well known server configuration/administration tools. They all require **root** username and password to be accessed first time.

Please note that some of the WEBMIN tools may be in conflict with the normal Z1 administration. They should be used only with full understanding of the system.

VNC Tools points to a varying collection of graphical (X) administration/monitoring programs running under a VNC system on Z1 and accessible to WEB browsers with Java support.

Additionally Usermin is running on Z1 and can be accessed on port 20000 (http://www:20000). Usermin is a collection of useful programs helping users to change their personal settings on the server. Any user registered on Z1 can access Usermin. In particular Usermin allows users to add extra rules to SpamAssassin Anti-SPAM program to control their own mail.

WebMail points to an installation of **SquirrelMail** that allows every user to access and send their mail.

10 Notes