Mako NETWORKS

Guardian Manual

For General Operation

Quick Reference

Guardian is Mako Networks' Web Access Control (WAC) solution, allowing your business to block access to unwanted content and allow access to business-relevant information.

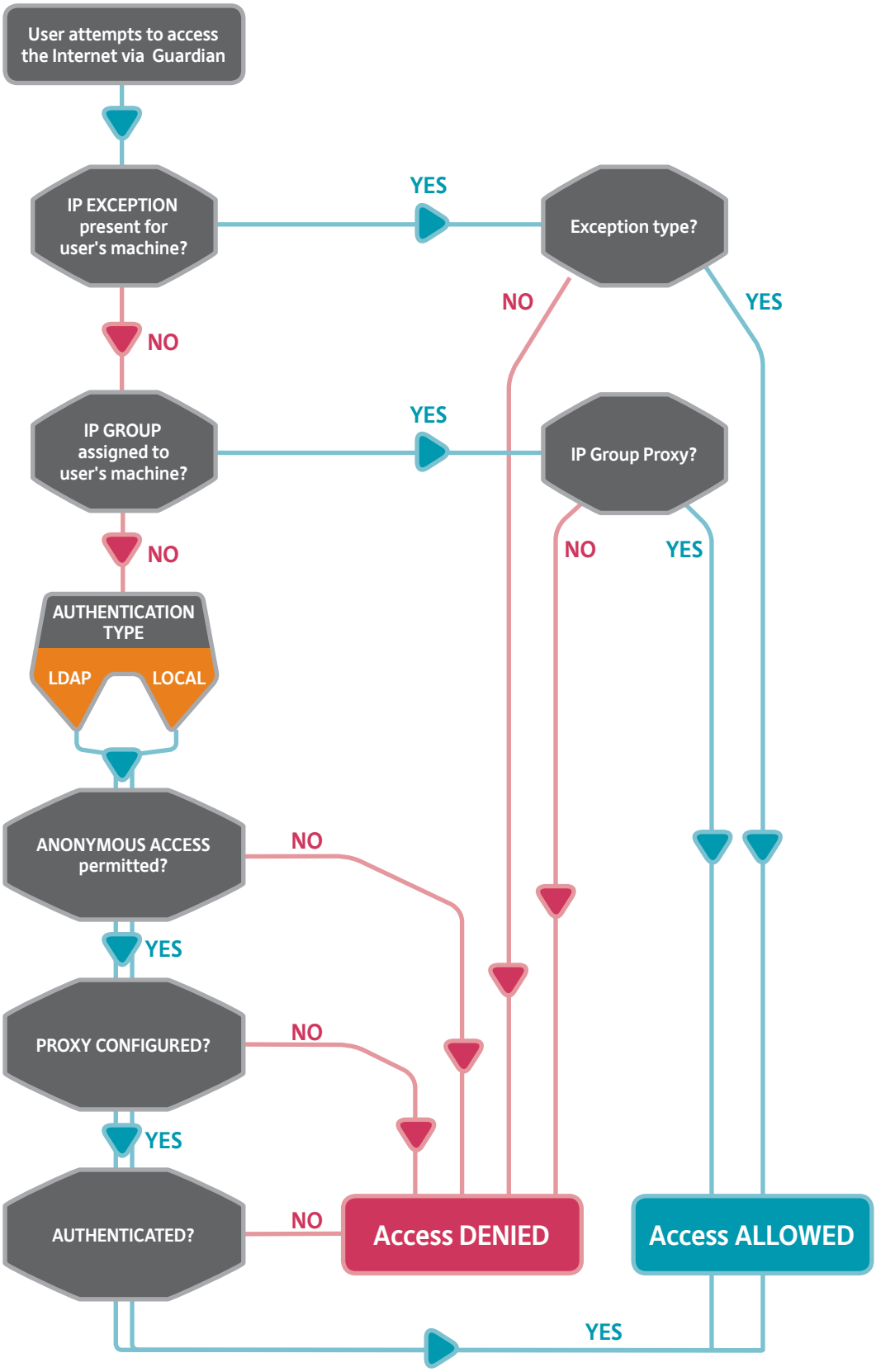
Guardian lets you filter by:

1. **Mako-provided Blacklists** — Select from pre-defined, automatically updated site categories to block or allow.
2. **User-created Blacklists** — Upload your own blacklists which you can use to block or allow.
3. **Custom sites** — Enter your own URLs.
4. **Phrases** — Select different pre-defined phrase types or groups to block.
5. **Custom Phrases** — Create your own phrase categories.
6. **User-based Rules** — Filter by individual users who authenticate via the Mako or your own LDAP directory server.
7. **Time-based Rules** — Specify different times for different rule sets.

This reference is an overview. Read this guide fully for details.

1 Guardian Web Access Flowchart

The following diagram illustrates the flow of decision making that goes on through Guardian, once IP and group filters are set up, when a web page is asked to be seen by a user.



Contents

2 Introduction

2.1 Guardian Service

Guardian is an active web content filtering service that gives you comprehensive control over the web content you allow on your network. With Guardian you can meet the legal requirements to control access to objectionable or inappropriate web sites.

Guardian runs on all our 6000 and 7000 series appliances, which we call the Customer Premise Equipment (CPE), but in this manual, any Mako appliance will be called a **Mako**. Guardian restores employee productivity lost through non-business related web browsing. Guardian empowers you to quickly and easily manage access to web content from anywhere in the world using the **Content Management System, or CMS**.

Guardian enforces your acceptable use policy and protects your business from legal liabilities that could arise from Internet misuse.

Guardian lets you filter by:

Mako-provided Blacklists	Select from pre-defined, automatically updated site categories to block or allow.
User-created Blacklists	Upload your own blacklists which you can use to block or allow.
Custom sites	Enter your own URLs.
Phrases	Select different pre-defined phrase types or groups to block.
Custom Phrases	Create your own phrase categories.
User-based Rules	Filter by individual users who authenticate via the Mako or your own LDAP directory server.
Time-based Rules	Specify different times for different rule sets.

2.2 Guardian Management

Once setup is completed, Guardian controls access to Internet content without any user interaction required. Guardian is managed through the CMS, accessible through a web browser from anywhere in the world. The CMS provides the flexibility to tailor your policies on demand. Blacklists are automatically kept up to date for you. You choose exactly what you want to allow and what you want to deny on your network.

2.3 Content Management System (CMS)

This manual is to be used in conjunction with the CMS Manual. The CMS Manual provides you everything you need to know about setting up a Mako appropriately for your system, and a copy is available on our web site.

2.4 Manual Conventions

"Sub-tab > Function"

The above shorthand assumes you've selected a Mako to configure, then navigated your way through **Configure > Services > Guardian** pages.

An explanatory note. Usually not critical for the normal operation of the system.

A settings note. The note requires your attention, but due to the difference in browsers or configuration might not apply for the operation or configuration of the system.

A warning note. The note requires your attention and will affect the way you and other approved users will use your system.

A danger note. The note requires your full attention and may significantly affect your system's integrity, cause electrical damage, data corruption or even a health and safety-related injury.

3 Starting Guardian

3.1 Considerations

Before you begin, give some consideration to how you will govern access to online content. You can choose to create a single set of rules that apply to every computer on your network. You can also create exceptions to these rules by IP Address and separate rules for different groups of users. If you decide to create rules for groups of users, you can choose from the following types of user authentication:

- **LDAP** -Users authenticate from a correctly configured LDAP server located on their network.
- **Local** - Users authenticate from a user-configured list of users on the Mako system.
- If you decide to have user-based rules, you cannot have both LDAP and Local authentication configured at the same time -you may choose one only. If you choose to have user-authentication you can also allow Anonymous connections; users who do not authenticate will be subject to a default set of rules of your choosing. Anonymous connections may be used at the same time as LDAP and Local as a fall-back.

Users must be placed into groups of your choosing; such as "Students" and "Teachers", or "Warehouse", "Admin", and "Management". Users can belong to multiple groups and the rules you setup are tied to the groups rather than individual users to make configuration easier and quicker.

In addition, you can choose to setup IP-based rules for computers that will override the user-based and anonymous authentication settings. These IP-based rules are useful for kiosks or other shared computers.

3.2 Licencing

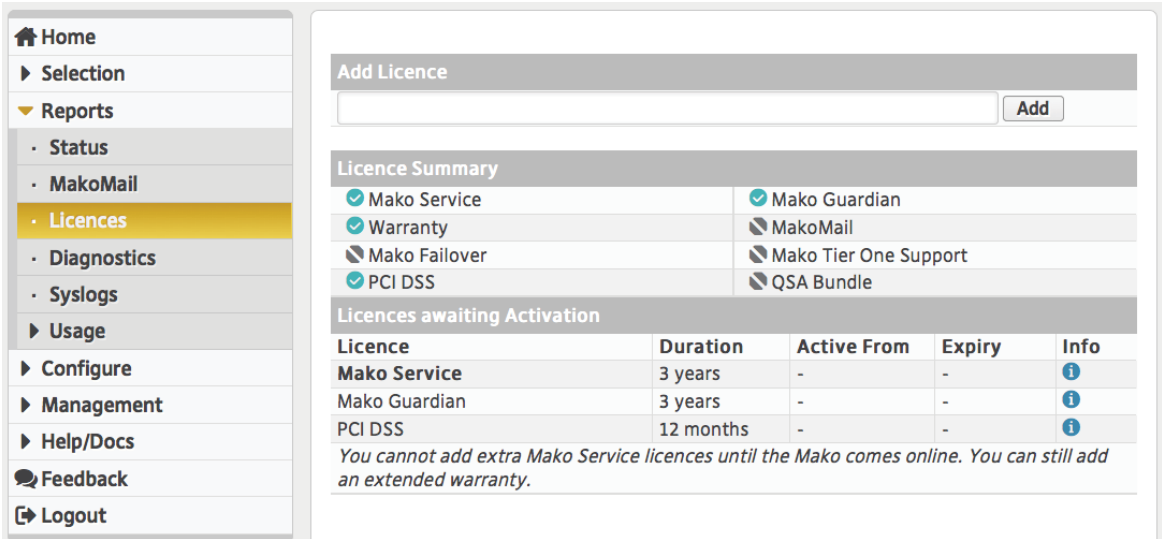
To be able to use Guardian, you must first purchase a licence from your Reseller. Guardian licences are available in a variety of terms – Contact Mako for more information.

We may have already entered your licence for you. Adding a Guardian licence automatically enables it on your profile, so you might be able to skip this step.

The licence code must be entered into the CMS website against your Mako. To do this:

- Go to your security service provider's website.
- Login using your designated username and password.
- Select the Mako on which you will install Guardian.
- Click on Reports > **Licences**
- In the **Add Licence** field, enter your Guardian Licence Code. Click **Add**.

  The licence summary will change to indicate a valid Guardian licence.


Home
Selection
Reports
Status
MakoMail
Licences
Diagnostics
Syslogs
Usage
Configure
Management
Help/Docs
Feedback
Logout
Add Licence
Add
Licence Summary
Mako Service
Mako Guardian
Warranty
MakoMail
Mako Failover
Mako Tier One Support
PCI DSS
QSA Bundle
Licences awaiting Activation
Licence
Duration
Active From
Expiry
Info
Mako Service
3 years
-
-
Mako Guardian
3 years
-
-
PCI DSS
12 months
-
-
You cannot add extra Mako Service licences until the Mako comes online. You can still add an extended warranty.

4 Enabling Guardian

4.1 Sites > Categories

- Check **Enable Guardian.**

4.1.1 Enable Mako Spyware Protection

Guardian has an option to help protect your computers from spyware.

- Check **Enable Mako Spyware Protection**.

Mako's spyware protection is designed to complement existing anti-virus and anti-spyware software, and should be used in conjunction with these for maximum protection.

4.1.2 Enable Secure Website Protection

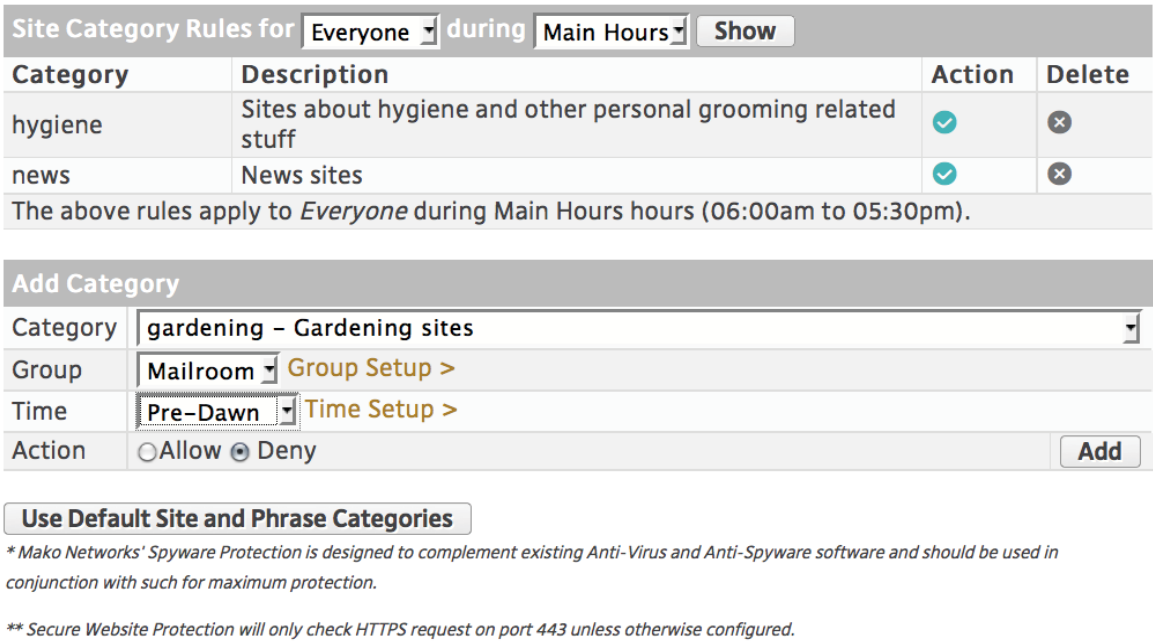
- Check **Enable Secure Website Protection**.

While most websites use the http prefix, some use the secure https prefix, and can slip through normal content filtering. Enabling Secure Website Protection ensures that Guardian will include https websites in its filtering protocol. While the default setting for this is unchecked, it's highly recommended to enable this option: end users could use the https prefix to circumvent the standard http blacklist sites.

Configuration of local machines is required for Secure Website Protection to work. If configured incorrectly no HTTPS websites will be accessible.

This will only check HTTPS requests on default port 443.

4.1.3 Adding Rules based on Categories



Rules allow or deny web content based on the type of web content, a group you define, in a timeframe you define. To define Categories, Groups and Times, see the relevant sections in this manual.

The **Add Category** section is where you create rules for certain web-content categories. These site categories are regularly refreshed through automated updates provided by the CMS.

To create a rule:

- In the **Add Category** drop down menu, select a category.
- Select the group the rule is for.
- Select when the rule will apply.
- Select whether this rule will **Allow** web traffic in this category, or **Deny** it.
- **Add** when finished.

  When the page is refreshed, your new rule will be listed in the top section.

  A good place to start is to click on the **Use Default Site** and **Phrase Categories** button. This will assign the default settings.

Allow rules take precedence over Deny rules. So if a user belongs to a group that allows access to hacking sites, this will override the default Everyone, Anytime rule.

Regularly updated lists of sites associated with the enabled rules are blocked by default. Alternatively, you can allow the blocked category. This may be useful when Phrase Categories block a particular category of site that you would rather allow.

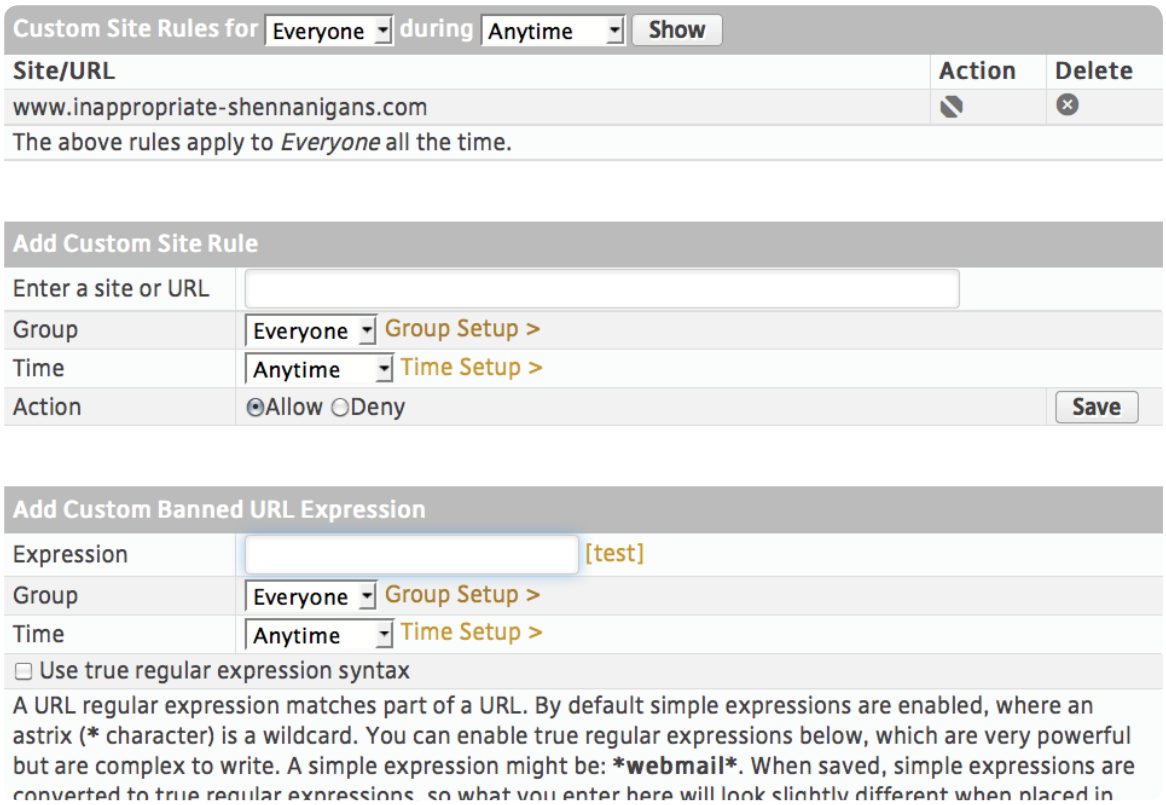
To delete a rule from the list:

- Click the delete button .

  By default, the rules you add on this page will apply to Everyone, Anytime.

4.2 Sites > Custom Sites

The Custom Sites screen allows you to either allow or deny access to specific websites.



» **To allow or deny access to a specific website:**

- Type its URL in the **Add Custom Site Rule** field.
- Click **Allow/Deny**.
- **Save** when finished.

You may want to allow a site if one of the other Guardian configuration options is blocking it. For example you may have blocked access to Drug related sites in the Site Categories section but want to allow users to visit a chemist site.

4.2.1 Add Custom Banned URL Expression

This field enables you to block URLs that contain a string of letters or numbers. For example, you may wish to block all URLs that contain the word "mail". If so, enter the word "mail" in the Add Custom Banned URL Expression field. If you wanted to block all .com sites with the word "mail" you would enter "*mail*.com".

By default, the categories you add on this page will apply to Everyone, Anytime.

4.3 Sites > Custom Categories

The Custom Categories screen lets you create your own blacklists (or whitelists if you choose to allow them).

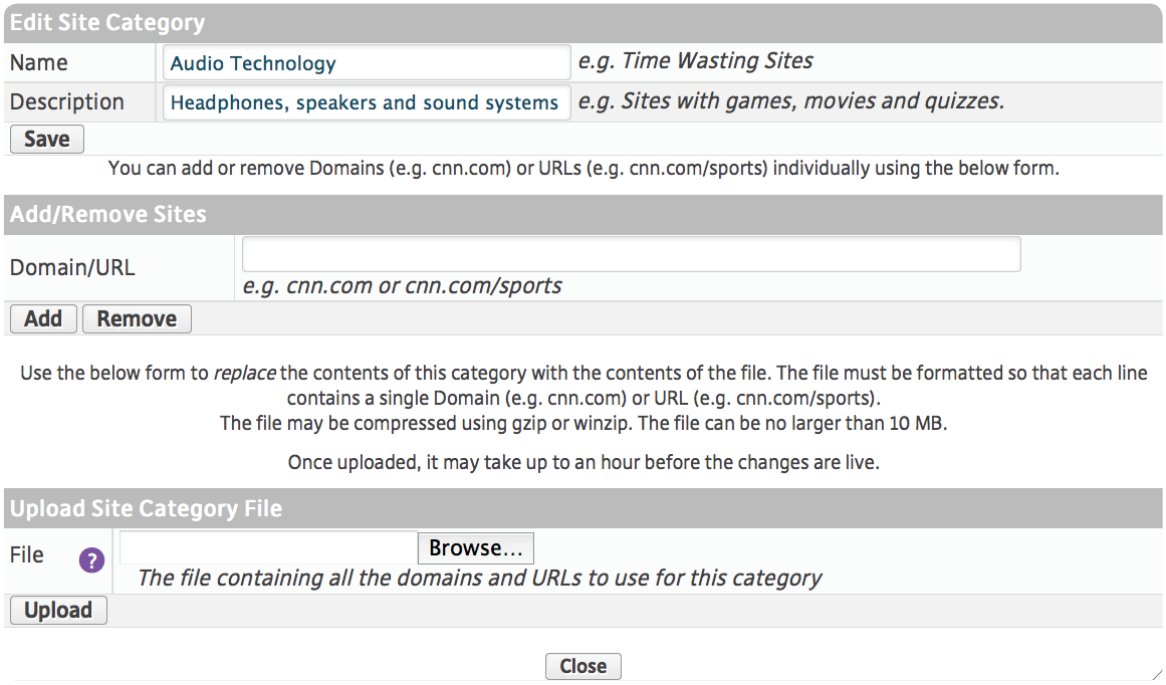
» **To create a customised category list:**

- Enter a category name (this will appear in future drop-down selections).
- Enter a brief description for your category.

Add when finished.

To add URLs to your category:

Click the edit icon, . This pop-up will appear.



Here, you could edit your Category's name and description, add or remove a single URL, or add a batch of URLs in a text file.

To Add/Remove single a URL to a category:

- Enter the URL in the Add/Remove Sites field.
- **Add/Remove** when finished.

  To upload a batch of URLs:

- Click **Browse...** in the Upload Site Category File section.
- Navigate your way to attach the appropriate list of URLs.
- **Upload** when finished.

  The batch text file should follow the following format:

- The file should be a plain text file (i.e. something that can be opened in Notepad. Not a Word document or a Rich Text file).
- File size limit is 10MB.
- The file should contain one URL or Domain per line.
- Lines that start with a hash (#) are ignored.
- The file can be ZIPped or GZIPped. Or, it can be uploaded as-is.
- The domain portion of the file can only be: letters (A-Z), numbers (0-9), full stops (.), and hyphens (-).
- Sample file:

  http://cnn.com/

http://bbc.co.uk

seek.co.nz

microsoft.com/support

apple.com/

4.3.1 Batch file Considerations

- It may take up to an hour before your uploaded file is parsed and loaded into the system.
- If there is an error with any URL or Domain in that file, then the entire update is aborted.
- If the URL has a question mark (?), then any content after (and including) the ? is ignored. For example, http://www.cnn.com/search?query=election becomes: http://www.cnn.com/search

4.4 Phrases > Categories

Phrase blocking checks the actual text content of a website for undesirable phrases and wording. From the Categories page you can create rules to block web content using the terms you define in the Custom Phrases page.

» **To add a category rule:**

- In the **Add Phrase Category** drop down menu, select a category.
- Select the group the rule is for. (Click **Group Setup** to create a new group.)
- Select when the rule will apply. (Click **Time Setup** to create a new time range.)
- **Add** when finished.

  When the page is refreshed, your new rule will be listed in the top section.

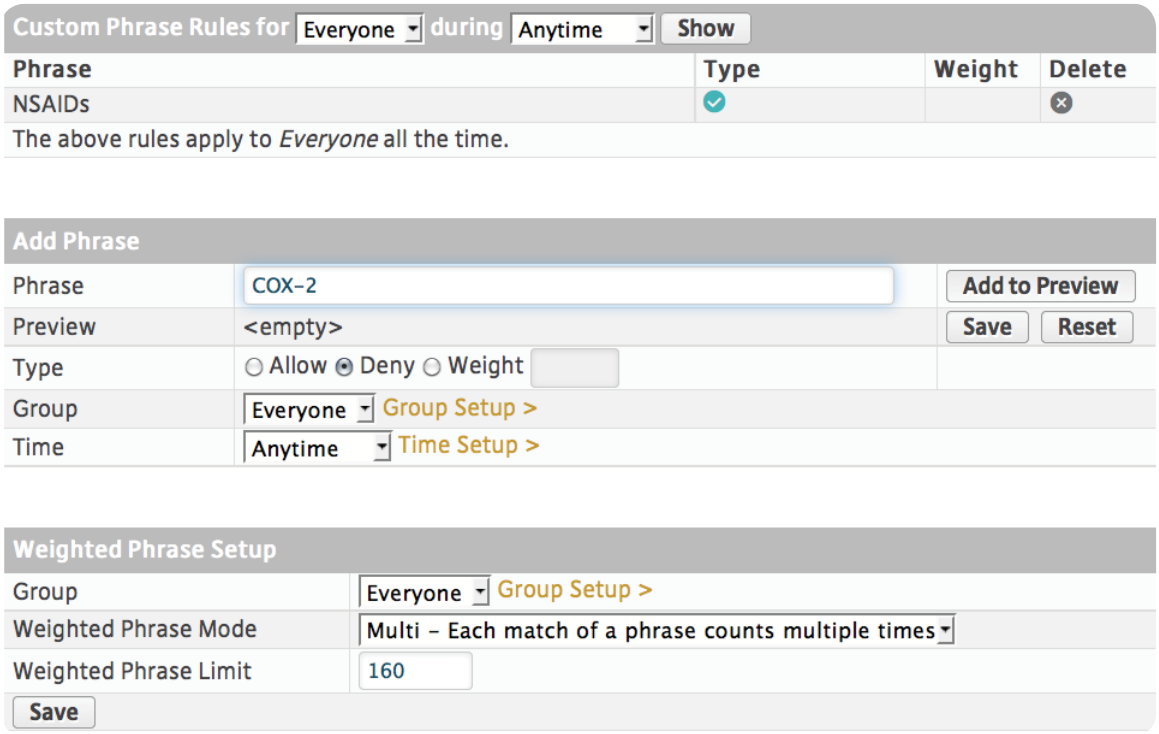
» **To add a Phrase Category:**

- Select the category from the drop down menu and click the Add button
- To remove, click  .

  By default, the categories you add on this page will apply to Everyone, Anytime.

4.5 Phrases > Custom Phrases

Custom Phrases are used to block, or allow, access to websites based upon their actual text content.



You can choose to specifically allow or deny sites that contain words or groups of words. You can also allocate points to a number of words and when a site contains enough words to add up to your point limit, then block or allow access to the site. This is called **weighting**.

Custom phrases and Blocking are only supported on HTTP traffic types – not HTTPS.

4.5.1 Blocking or Allowing Without Weighting

In these instructions, we use "word1" as our phrase example.

To Allow/Deny all sites that contain the Phrase "word1":

- In the **Add Phrase** section Enter 'word1' in the Phrase field.
- Choose **Allow** or **Deny**, for pages that contain "word1"
- Select the appropriate Group for this phrase.
- Select the appropriate Time range for this phrase.
- **Save** when finished.

  All sites that contain the word "word1" will be blocked for the selected Group within the selected Time range.

  Alternatively, you could type a sentence in the Phrase field and all sites containing that sentence will be blocked.

4.5.2 Blocking or Allowing With Weighting

With weighting you assign a score to your phrase, a score limit for a page, and if the page score is exceeded by the total phrase score, it's blocked.

Here's an example, using arbitrarily assigned scores.

Based on the experience in our ficticious business, if the page contains the phrase "wood", it's likely to be relevant information, but the phrase "woodchuck" indicates it's likely to be irrelevant.

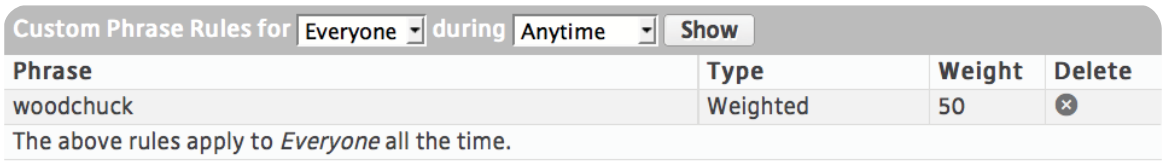
Then we hit this page:

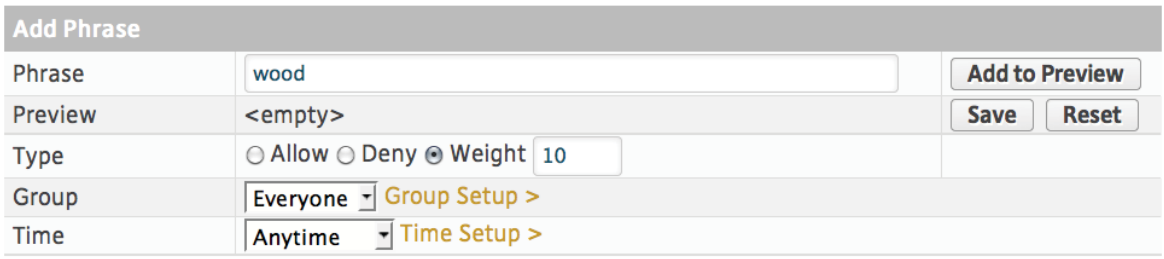
How much wood
Would a woodchuck chuck
If a woodchuck could chuck wood?
As much wood
As a woodchuck could
If a woodchuck could chuck wood.

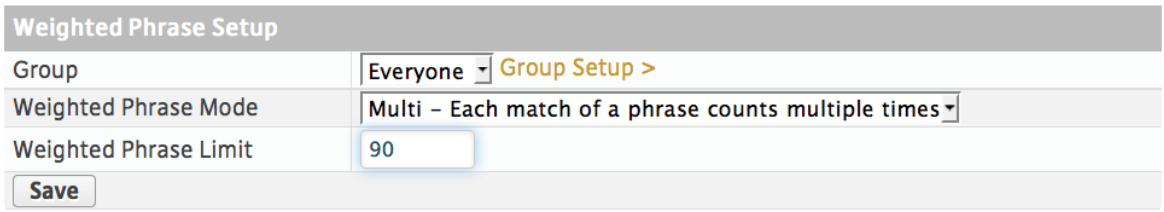
Phrase	Phrase score	Phrase Score Total
"wood"	10	40
"woodchuck"	50	200

As we can see by the scoring we've chosen, we don't mind pages with the word "wood", as we've given it a low score, but we're not keen on pages with the word "woodchuck".

Weighted Phrase limits can be used to set upper and lower limits for relevance, or range limits. For example, if the "wood" Phrase score was 10, but the Weighted Phrase Limit was 30, this page would be denied, as it has a 'wood' score total of 40. If the "wood" Weighted Phrase Limit was 110, the page would be allowed... So long as the "woodchuck" Weighted Phrase Limit wasn't exceed by whatever limit we set (in this case, any score over 200).







To use Weighting:

- Enter the word to be weighted in the Phrase field.
- Choose Weight, and enter a score of your choosing. (Your scoring scale is entirely up to you.)
- Select the appropriate Group for this phrase.
- Select the appropriate Time range for this phrase.
- **Save** when finished.

Weighting may need a period of fine-tuning for your particular purpose. If you choose to use weighting, consider re-evaluating your weighting from time-to-time. You may be missing out on relevant information through a change in language that the source sites are using.

By default, the categories you add on this page will apply to Everyone, Anytime.

4.5.3 Phrase building

Phrase building is a function that allows you to define keywords for an exact match of a word or phrase.

For example, if you wanted to match web pages that had the phrase "star wars general", a successful match must contain *that exact phrase, words in that order, with spaces,* before Guardian can decide whether to allow it or not.

To build a basic exact match phrase:

- Enter the phrase to be targeted in the Phrase field.
- Select the appropriate Type: Allow, Deny, Weight (score).
- Select the appropriate Group for this phrase.
- Select the appropriate Time range for this phrase.
- **Save** when finished.

4.6 Users and Groups > Options

Guardian allows you to report on and control web access by user.

For LDAP authentication you must have an appropriately configured LDAP server installed on your network. Alternatively you can create Local Users on this management website. You cannot use both LDAP User and Local User Authentication at the same time.

To choose which method of user authentication to use:

- Select:

Anonymous (None): No user-based authentication. All users will be filtered according to the Everyone rules. You may still create IP Exemptions in the Advanced section.

LDAP User Authentication: Users are authenticated via a local LDAP server.

Local User Authentication: Users are authenticated via the CMS.

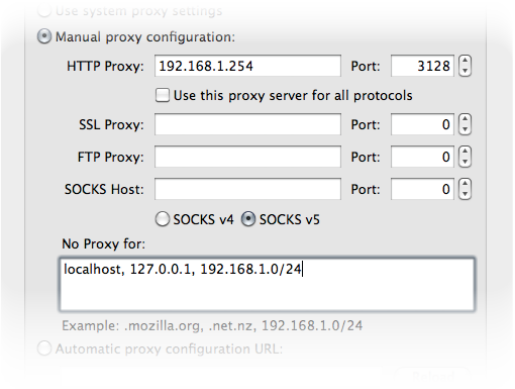
When you select either LDAP or Local User Authentication you also have the option to allow anonymous/unauthenticated web access. If selected, computers that do not authenticate their user will have the Everyone rules applied to them. If you choose not to allow anonymous/ unauthenticated web access, users who do not authenticate will be blocked from accessing web sites.

IP Exceptions established in the Advanced section take precedence over these rules.

All computers with users who wish to authenticate must be aware of the Mako's proxy settings. The Mako will issue proxy information to computers on its network automatically if it is being used to issue DHCP information. If your Mako is not being used for DHCP or your Operating System does not support proxy information being issued via DHCP, you must enter the proxy settings manually.

The proxy information will be shown at the bottom of the **Users and Groups > Options** screen if you have selected LDAP or Local authentication as shown below. One line will be shown for each of the LAN ports on your Mako.

If any of the browsers on your network do not support pac files you must set up proxy bypass for the local network. Otherwise the web pages informing the user a page has been blocked will not work. i.e. localhost, 127.0.0.1, 192.168.1.0/24, 192.168.2.0/24, ... for all the local LANs.



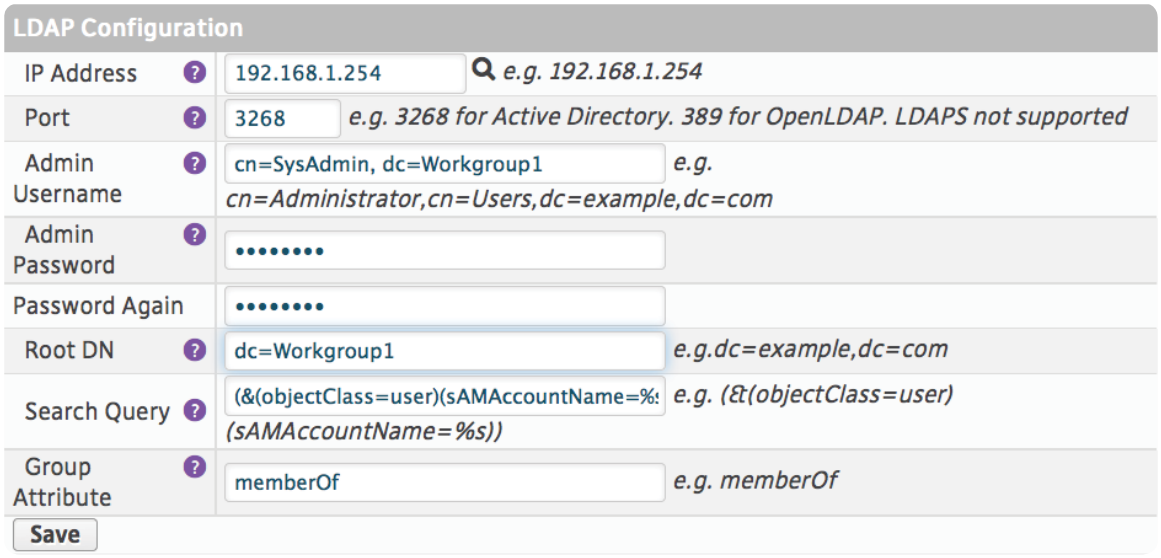
4.7 Users and Groups > LDAP

The LDAP page provides the fields for you to enter the appropriate data for Guardian to communicate with your correctly configured LDAP server.

The Lightweight Directory Access Protocol is an application protocol for querying and modifying directory services running over TCP/IP.

A directory is a set of objects with similar attributes organised in a logical and hierarchical manner. LDAP can be used to access many different types of directory services including Microsoft Active Directory.

If your business already uses an LDAP-accessible application to store usernames and passwords, you can continue to use this central repository with Guardian.

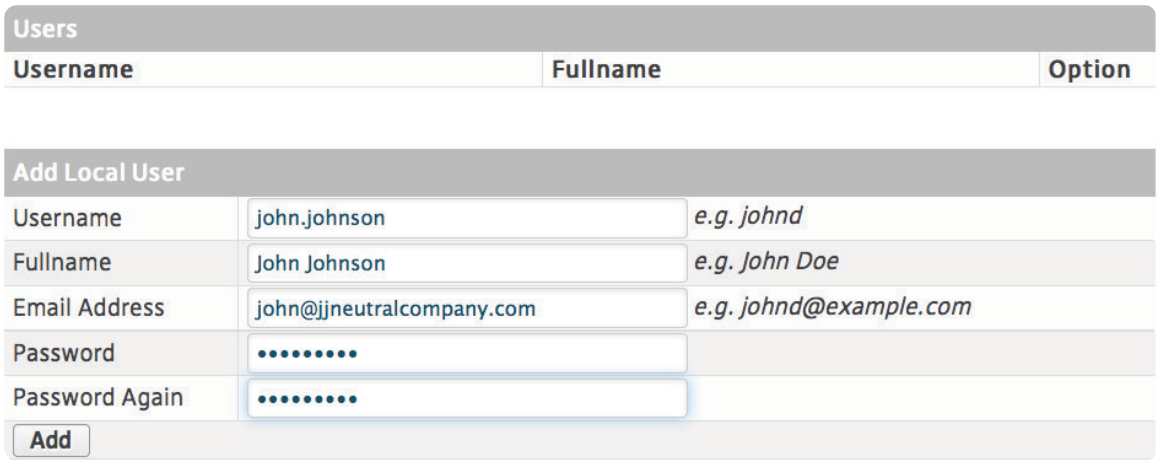


In order to enter the relevant information, you should consult with the System Administrator for your LDAP server. Each server is different and can be configured in many ways.

Guardian requires Simple Authentication enabled to be able to communicate with an LDAP server.

4.8 Users and Groups > Local Users

Guardian allows you to force users to authenticate themselves before accessing the web. You can create a list of users with their respective usernames and passwords in this section. You do not need an external LDAP server in order to use this local authentication, your Mako will identify the users and control their web browsing according to the rules you choose.



4.9 Users and Groups > Groups

In order to create separate filtering rules for users, you will need to place your users into groups. If you have chosen to have no user-based authentication, you can create IP-based groups and group machines instead of users.

If you have chosen to have LDAP or Local user-based authentication, you may also create IP-based groups which will take preference over the user-based rules.

The screen depicted below shows group setup for Local authentication but the process is the same if you have chosen LDAP or IP from the **Users and Groups** > **Options** section.

To create a group:

- Enter a name for the group.
- Add when finished.

  Your Group will then appear in the Groups list. You can continue adding as many Groups as you need.

To add users (or IP addresses if you have created an IP Group):

- Click the Group's icon.
- In the resulting pop-up window, select the User from the drop down list under **Add Group Member**.
- Close when finished.

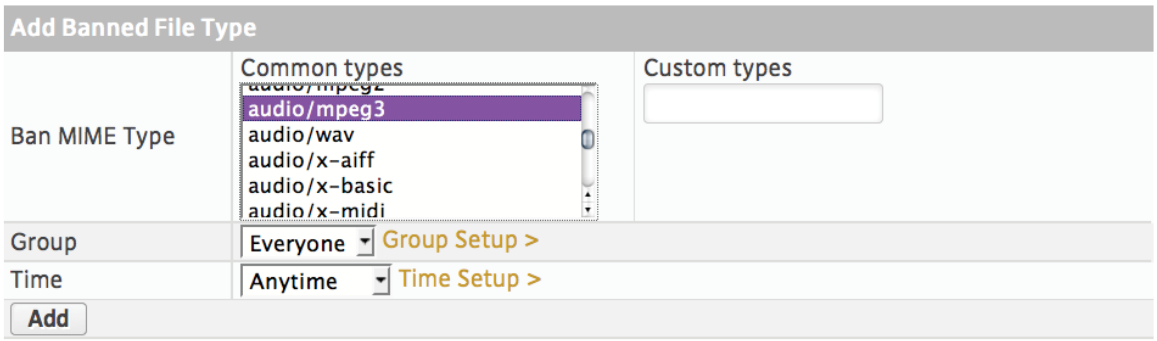
  Users can belong to more than one group.

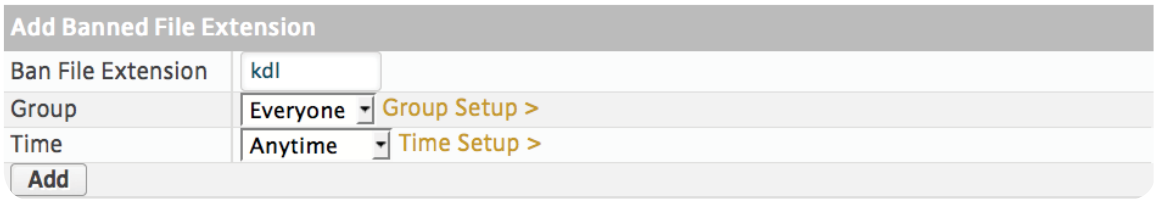
  Once you have created groups that contain one or more users you can use them on the Sites, Phrases and Advanced pages to create rules that apply to that group.

4.10 Advanced > File Types

The File Types section allows you to block users from downloading certain files by their extension or MIME type.

The top section only displays rules relevant to the Group and Time range specified. You may wish to show your Group and Time settings before you set a rule for them.





To add a Banned File Type:

- Select the appropriate existing common (MIME) type, or enter a custom type.
- Select the relevant Group and Time for the ban.
- **Add** when finished.

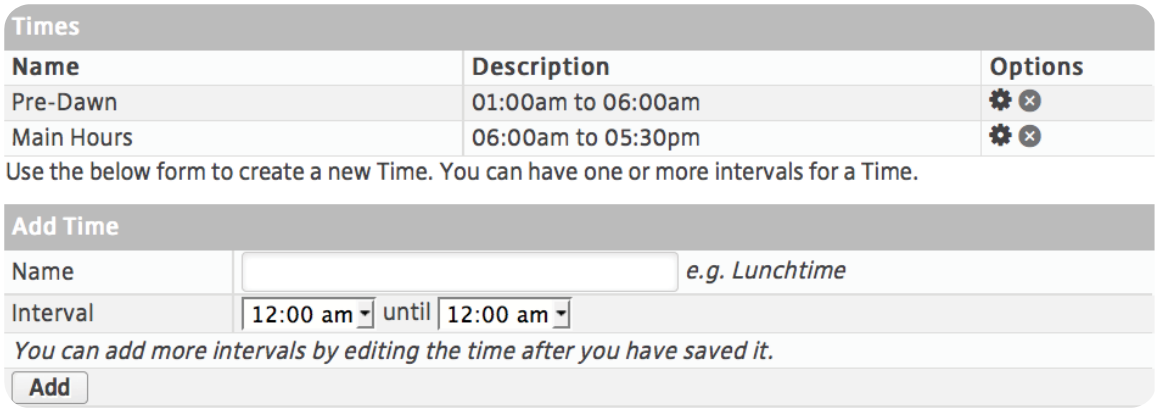
To add a Banned File Extension:

- Enter the file type suffix.
- Select the relevant Group and Time for the ban.
- **Add** when finished.

By default, the categories you add on this page will apply to Everyone, Anytime. Should you wish to integrate user and time-based restrictions, you will need to create some groups and time periods you wish to establish separate rules for.

4.11 Advanced > Times

You may wish to have different rules that apply at different times of the day.



To add Time ranges:

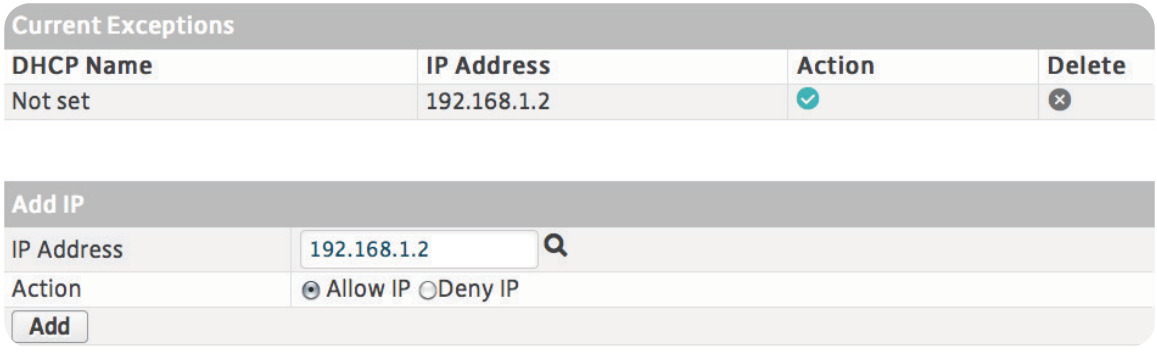
- In the Add Time section, enter a Time range name.
- Select the times in which rules will be applied.
- **Add** when finished.
  You can edit the time by clicking .

4.12 Advanced > Exceptions

You might wish to have certain computers on your network exempt from the Guardian rules.

To make an IP Address exempt from Guardian:

- Enter an IP Address.
- Click **Allow IP** (to be exempt) and they will not have any Guardian rules applied to them when accessing the Internet, OR:
- Click **Deny IP** and that machine will not be able to access websites at all.
- **Add** when finished.



Computers with IP Exceptions will override any user-based rules.

4.13 Configure > Advanced > Site Bypass

Some websites are coded in such a way that they do not work properly when viewed through the Guardian proxy.

Bypassed Website IP Addresses

IP Address / Network	Comments	Option
64.62.243.92	Shortcut web adddress	⊗
64.62.243.91	Shortcut web adddress	⊗
202.162.73.0/24	Demo site	⊗

Add Website IP Address Bypass

IP/Network of Website	202.162.73.0/24	*e.g. 202.162.73.0/24*
Comments	Demo site	
Add		

To force an IP Address to bypass the Guardian proxy:

- Enter the IP/Network of the website in the field below (preferably in CDIR notation).
- Add a comment to identify the exempted IP address.
- **Add** when finished.

A website may use more than one IP Address, and more than one Network, so multiple entries may be required. A website may change its IP Address(es) over time.

4.14 Configure > Advanced > Landing Page

If you would like to present users with a specific web page the first time they connect to your network, enter the URL on this page.

To create a landing page re-direct:

- Enter the address of the page in the website field.
- Enter a timeout duration. If a web browser is inactive for this period on your network, it will be redirected to the landing page after this duration.
- **Save** when finished.

5 Finishing Up

Once you have set up Guardian to your liking, go back to the **Guardian > Sites > Categories** page and ensure there is a tick in the **Enable Guardian** check box.

Your Mako will then start Guardian. This process can take up to five minutes for the first time. Once active, Guardian will display a block message like the one below for all web pages that are blocked.

5.1 Blocked site

That's it! You now have control over what type of content your network has access to.

11 Warranty

1) **Standard Limited Warranty.** If the products purchased hereunder are resold by a distributor or reseller to an end-user (customer) pursuant to the terms hereof in their original, unmodified, unused condition, Purchaser shall pass on to its customers, or keep as applicable for internal use, the MAKO NETWORKS LTD. standard limited warranty for the products, as summarized in documentation supplied with the product and including provisions and limitations set forth below. The Manufacturer warrants the Mako Appliance for one (1) year. The Warranty begins on the date of purchase as shown on your providers invoice.

2) **Express End-user Limited Warranty.** Each MAKO NETWORKS LTD. product purchased hereunder is warranted against defect in material and workmanship and will substantially conform to MAKO NETWORKS LTD. product documentation for the period set forth in the documentation supplied with the product following delivery to end-user (the "Warranty Period"). This warranty extends only to end-user and will not extend to, nor may it be assigned to, any subsequent user, Purchaser or user of a MAKO NETWORKS LTD. product, whether such MAKO NETWORKS LTD. product is alone or incorporated into end-user's product.

3) **Exclusions.** The express warranty set forth above is contingent upon the proper use of a MAKO NETWORKS LTD. product in the application for which it was intended and will not apply to any MAKO NETWORKS LTD. product that has been (i) damaged during shipping, (ii) modified or improperly maintained or repaired by a party other than MAKO NETWORKS LTD. or its designees, or (iii) subjected to unusual physical or electrical stress. This includes operation of the product outside the Operating Specifications of the product.

4) **Limitation of Remedy.** In the event a MAKO NETWORKS LTD. product fails to perform as warranted, MAKO NETWORKS LTD. sole and exclusive liability and end-user's only remedies for breach of this warranty shall be, at MAKO NETWORKS LTD.'s option to repair, replace or credit an amount not exceeding the Purchaser's purchase price of each product found to be defective, provided that:

   4.1) **End-user complies with the rejection and warranty procedures contained in Section 5 below and returns the MAKO NETWORKS LTD.** product that the end-user considers defective for examination and testing.

   4.2) **MAKO NETWORKS LTD.** shall not be liable under this warranty if testing and examination by MAKO NETWORKS LTD. discloses that the MAKO NETWORKS LTD. product has been modified or altered in any manner after it was shipped by MAKO NETWORKS LTD.

   4.3) **MAKO NETWORKS LTD.** shall not be liable under this warranty if testing and examination by MAKO NETWORKS LTD. discloses that the alleged defect in the MAKO NETWORKS LTD. product does not exist or was caused by end-user or any third person's misuse, neglect, improper installation or testing, unauthorized attempts to repair or any other cause beyond the range of intended user, or by accident, fire or other hazard.

   4.4) **MAKO NETWORKS LTD.** shall not be liable under any warranty under this Agreement with respect to any MAKO NETWORKS LTD. product that is not returned in its original shipping container or a functionally equivalent container.

   4.5) **If MAKO NETWORKS LTD.** testing and examination does not disclose a defect warranted under this Agreement: MAKO NETWORKS LTD. shall so advise Purchaser and dispose of such MAKO NETWORKS LTD. product in accordance with Purchaser's instructions on behalf of end-user and at Purchaser's cost.

Support
support@makonetworks.com

Web site
www.makonetworks.com