

Guardian Digital Internet Acceleration and Management Server

IAM Guide

Copyright ©2000 - 2003 Guardian Digital, Inc.

Contents

1	INTRODUCTION	1
2	CONTACTING GUARDIAN DIGITAL	2
3	TECHNICAL SUPPORT	3

4	Internet Acceleration and Management Server	5
4.1	Setting up a basic server	5
4.1.1	Installation of the IAM Server	5
4.1.2	Accessing the newly installed IAM Server . .	6
4.1.3	IAM Server configuration	6
4.2	Viewing Proxy Reports & Graphs	30
4.2.1	Reports	30
4.2.2	Graphs	32
5	VIRUS DETECTION	34
5.1	Configuring virus scanning	34
5.1.1	Defining Abort Sites	35
5.1.2	Defining Abort Patterns	36
5.1.3	Defining Scan Patterns	36
5.1.4	Scheduling Virus Updates	37

1 INTRODUCTION

Welcome to the Guardian Digital Internet Acceleration and Management (2

) Server! This QuickStart Guide provides information about the IAM Server and describes the steps necessary to successfully install and configure it.

For more detailed information about how to use EnGarde Secure Professional, be sure to refer to the complete EnGarde Secure Professional Users Guide.

2 CONTACTING GUARDIAN DIGITAL

Guardian Digital welcomes your input and feedback. You may direct all questions, commands, or requests concerning the software you purchased, your registration status, or similar issues to the Guardian Digital Customer Service department at the following address:

Guardian Digital Customer Service
165 Chestnut Street
Allendale, New Jersey 07401
United States

Phone:	+1-201-934-9230
E-Mail:	customer.service@guardiandigital.com
World Wide Web:	http://www.guardiandigital.com
Online Store:	http://store.guardiandigital.com

The department's hours of operation are 9:00 AM to 7:00 PM Eastern Time, Monday through Friday.

3 TECHNICAL SUPPORT

Guardian Digital provides comprehensive support for your enterprise. Guardian Digital can help bridge the gap between the fast-paced nature of the Internet, security, and the latest open source technologies available in EnGarde. Guardian Digital can provide you with the information necessary to develop unique customizations of EnGarde products to achieve the fastest time to market with the most cost-effective solutions.

Included with your purchase is 60 days of e-mail, telephone, and Web installation and configuration support beginning at the time of purchase. This includes up to four incidents of installation and configuration support within that 60 day period.

Guardian Digital encourages you to visit us on the Web for the answers to many commonly asked questions and system documentation. Contact Guardian Digital Technical Support between the hours of 9:00 AM and 7:00 PM Eastern time.

To provide the answers you need quickly and efficiently, the Guardian Digital Technical Support staff needs some information about your computer and software. Please include this information in your correspondence:

- Program name and version number
- Product registration number
- Any additional hardware or peripherals connected to your computer
- How to reproduce your problem: when it occurs, whether you can reproduce it regularly, and under what conditions

- Information needed to contact you by voice, fax, or e-mail
- Steps you have taken thus far to try to resolve the problem
- Any additional software installed

Please contact us using one of the following methods:

Phone: +1-201-934-9230
E-Mail: support@guardiandigital.com
World Wide Web: <http://www.guardiandigital.com>

To avoid delay in processing your request, be sure to include your account number in the subject of the e-mail.

4 Internet Acceleration and Management Server

The Guardian Digital IAM Server combines user authentication, web caching, virus scanning, and Internet security functions into a single product typically installed at the Internet gateway.

The IAM Server provides caching to conserve network bandwidth and reduce client response times. Control over users and the destinations they visit on the Internet provides a single point at which all users access Internet resources, narrowing the concentration of security efforts.

4.1 Setting up a basic server

4.1.1 Installation of the IAM Server

The Guardian Digital Internet Acceleration and Management Server is installed via the Guardian Digital Secure Network (GDSN). To install the IAM Server insert the CD-ROM disk that was included with Guardian Digital IAM Server purchase into the CD-ROM drive of the EnGarde server you will be installing the IAM Server on.

Selecting *Install from Local Media* in the GDSN will perform the installation. Instructions on how to use the GDSN can be found in *Section 5* on page 166 of EnGarde Secure Professional User Manual. Additionally the *Install from Local Media* portion can be located on page 168 under *Section 5.1.2 Install from Local Media*.

4.1.2 Accessing the newly installed IAM Server

Once the GDSN finishes installing all of the IAM Server packages, you will be able to access the *Proxy Management* section from the *System Management* screen.

Service Configuration	
Below you can configure the services this machine is offering.	
FTP Server Configuration	Edit global options, chroot list, and blacklist.
Secure Shell Management	Edit your system-wide secure shell configuration and generate keys.
Mail Server Management	Set up virtual domains, transport maps, and global options.
DNS Management	Create forward and reverse zones and edit the global options.
Proxy Management	Configure and setup ACL's for your local caching proxy.

4.1.3 IAM Server configuration

All functions of the IAM Server can be configured using the WebTool. To start configuration of the IAM Server select *General Configuration* from the *Proxy Management* menu.

Proxy Management
Below you can configure various aspects of the proxy server.

General Configuration
Setup basic proxy configuration parameters.

Schedule Virus Updates
Define how often virus updates should take place.

SOCKS Configuration
Enable, disable, and configure the SOCKS subsystem.

Proxy Authentication
Enable or disable different methods of proxy authentication.

Proxy Privacy Settings
Enable or disable certain levels of concealment.

Standard ACL Management
Create, edit, and delete standard ACLs.

Restricted ACL Management
Create, edit, and delete restricted users and ACLs.

Virus Scanner Configuration
Set up patterns you would like to have scanned for viruses.

Cache Peering
Configure 'peer' caches this cache can query for requested pages.

Autoconfiguration
Configure a script browsers may download to configure their proxy settings.

Reports
View daily and weekly user usage statistics.

Graphs
View graphs representing cache performance.

[\[Stop Proxy \]](#)[\[Restart Proxy \]](#)

General Configuration

The *General Configuration* section sets up the basic proxy services and also has a few options to add some mandated policies such as virus scanning and user authentication.

General Configuration

Proxy Administrator proxy@guardiandigital.com

Address To Listen On 192.168.1.2

Port To Listen On 8080

Permitted Ports 1022-1023 554

Permitted SSL Ports 1022-1023

Cache Peering? Enabled

Transparent Proxy? Disabled

Mandate Proxy? Enabled

Traffic Shaping?
☒ No Traffic Shaping
☐ Limit To --- Please Select ---

Virus Scanning Host
☒ No Virus Scanning
☐ Use This Host http://bluehen.inside.guardiandigital.com

To configure the proxy all the options on this screen must be completed. A description of each item can be found by clicking on the name of the item.

Proxy Administrator The Proxy Administrator field requires an e-mail address. This e-mail address will be displayed when end-users receive errors from the proxy.

Address To Listen On This is the address you want the proxy server to answer requests on. Generally you want this to be the internal address so users on the inside can access the proxy server to the outside. On a non-gateway, this is the IP of the only interface.

Port To Listen On The proxy server by default will use port 8080. Port 3128 is also a common proxy port. If you are uncertain what to enter leave the default of 8080.

Transparent Proxy? The *Transparent Proxy* option forces user traffic to be redirected through the proxy regardless of their web

browser configuration. *Proxy Authentication* can not be enabled if *Transparent Proxy* is enabled.

Mandate Proxy? Enabling the *Mandate Proxy* option will force the users to use the proxy by denying them access to the web via port 80. However, this requires the user configured their web browser for the proxy and in turn allows *Proxy Authentication* to be enabled.

Traffic Shaping? Traffic Shaping allows the proxy server to control the amount of bandwidth the proxy server will allow each user to use. You can select the amount of bandwidth usage from the pull-down menu. Each rate shows the actual throughput in parenthesis.

For example 56kbit is about the speed of a 56k modem while, 512kbit is about equivalent to a standard DSL connection and 1.544Mbit is the equivalent of a T1 line.

Each user will receive a percentage of the overall available bandwidth based on the number of concurrent users versus the total bandwidth selected.

Virus Scanning Host Enabling Virus Scanning will allow the En-Garde Proxy Server to scan specific files with defined file extensions for viruses. For example, all '.EXE' and '.ZIP' files. Enabling Virus Scanning here will add the Virus Scanner Configuration menu to the Proxy Management section allowing the Virus Scanner to be configured in detail. There is a separate section dedicated to the Virus Scanner Configuration in *Section 5* on page 34.

NOTE: Transparent Proxy, Mandate Proxy and Traffic Shaping are only valid if the proxy server is located between the internal and external networks.

SOCKS Configuration Guide

What is SOCKS?

SOCKS is a networking proxy protocol that enables hosts on one side of a SOCKS server to gain full access to hosts on the other side of the SOCKS server without requiring direct IP-reachability. SOCKS is often used as a network firewall, redirecting connection requests from hosts on opposite sides of a SOCKS server. The SOCKS server authenticates and authorizes requests, establishes a proxy connection, and relays data between hosts.

Configuration Outline

Configuration is broken down into three sections: *General Configuration*, *Client Rules*, and *SOCKS Rules*. *General Configuration* sets up global properties of the SOCKS server (interfaces, etc).

Client and *SOCKS Rules* are the core of the SOCKS access control system. These rules operate on different layers of the connection. *Client* rules operate at the TCP/IP layer and *SOCKS* rules operate at the application layer.

Before a client can even establish a connection with the SOCKS server they need a Client rule allowing them. Once the user has a TCP/IP session established the SOCKS rules are consulted.

Rules come in two configurations: *pass* and *deny*. As you'd expect, *pass* rules permit the connection to continue while *deny* rules do not.

Next comes the issue of Authentication. If Authentication is enabled then the client must send a valid (local) username/password along with their initial SOCKS request. In order for the user to be authenticated, they must have a valid account on the EnGarde Server.

An Example SOCKS Configuration Guide

Begin by choosing your Internal and External interfaces. This must be properly configured for the SOCKS proxy to work correctly. Click the *Save Settings* button to update the configuration.

Rules are evaluated in a top-down manner. In other words, when a connection is requested the SOCKS server will walk through all the Access Control Lists (ACL's) (in a top-down fashion) and allow/deny the connection as soon as it hits a matching rule.

A sensible configuration is to have a block rule at the bottom of the evaluation chain so that access is denied if there is not a rule explicitly allowing it. Enter pass rules for subnets above this. Finally, you would add block rules above these for specific clients or ports to be blocked.

The following configuration uses CIDR notation to represent the networks. For a explanation of what CIDR notation is refer to page ??.

Consider the following setup. 1.2.3.0/24 is our local subnet (the one we want to grant access to), and 1.2.3.200/32 is a specific host we wish to block:

Action	From	To	Port
block	1.2.3.200/32	Any	Any
pass	1.2.3.0/24	Any	Any
block	Any	Any	Any

When a connection is established the SOCKS daemon will look at the first ACL. If the client making the request is 1.2.3.200 then access will be denied. If it is not then the SOCKS daemon will move to the next rule. If the client is on the subnet 1.2.3.0/24 then access is granted. Finally access is denied if the client making the request does not match any other rules.

Important note! As stated above there are two types of access control rules: Client Rules and SOCKS Rules. The example above applies to both rule types; they are logically the same except for the point of the connection where the access control mechanism is used.

This WebTool module is designed to provide the capability for a very broad Client rule allowing everybody on your LAN and very specific SOCKS rules blocking abusers/sites/ports.

The following is a slightly more advanced configuration.

Client Rules

	Action	From	To	Port	Auth?
[1]	pass	1.2.3.0/24	Any	Any	-
[2]	pass	1.2.4.0/24	Any	Any	-
[3]	block	Any	Any	Any	-

SOCKS Rules

	Action	From	To	Port	Auth?
[4]	block	1.2.3.20/32	209.11.107.14/32	Any	-
[5]	block	1.2.3.10/32	Any	Any	-
[6]	pass	1.2.3.0/32	Any	Any	Yes
[7]	pass	1.2.4.0/24	Any	Any	-
[8]	block	Any	Any	Any	-

Rules 1 - 3 are Client rules and client 4 - 8 are SOCKS rules. Below is a narrative explaining how these rules would be evaluated.

- When a connection is first established...

- If the client is on either the 1.2.3.0/24 or the 1.2.4.0/24 subnet, access will be granted.
 - Otherwise the connection will be dropped immediately (the client will get a 'Connection refused' message).
- Once the connection is established the SOCKS server processes the SOCKS rules.
 - If the client is 1.2.3.20 and she is trying to access 209.11.107.14, access is denied.
 - If the client is 1.2.3.10, access is denied.
 - If the client is on the 1.2.3.0/24 subnet then access is denied unless authentication credentials are sent by the client and they are successfully validated.
 - If the client is on the 1.2.4.0/24 subnet then access is granted.
 - Otherwise the connection will be dropped gracefully.

I hope this guide has been helpful for you. If you still have questions on how to configure SOCKS access control rules after you have read this (and your user's manual), please contact Guardian Digital Support.

SOCKS Configuration

All of the SOCKS configuration is done at this main menu. The ability to enable and disable socks, configure internal/external interfaces and add/remove client and socks rules are all here.

The main SOCKS menu is broken down into four sections including the socks current status, the *General Configuration*, *Client Rules* and *SOCKS Rules*.

Proxy Management :: SOCKS Configuration

Below you may configure your local SOCKS proxy. SOCKS is a protocol which allows machines behind a firewall (without direct access to the internet).

This is different from the Caching Proxy used for web services in that the Caching Proxy provides acceleration services by storing local copies of the pages it retrieves.



Current Status: [Running] (Click to toggle)
Boot Status: [Enabled]

General Configuration

Internal Interface eth1 (192.168.1.2) Save Settings
External Interface eth0 (209.10.240.68)



Below you may configure access control rules. These rules define what addresses may use the SOCKS proxy for what purpose. For more information on what these rules are and how they should be properly configured, [\[Click Here \]](#).

Client Rules

Action	From	To	Port	Auth?	
pass	192.168.1.0/24	Any	Any	---	 
block	Any	Any	Any	---	

[\[New Client Rule \]](#)

SOCKS Rules

Action	From	To	Port	Auth?	
block	Any	127.0.0.0/8	Any	---	 
pass	192.168.1.0/24	Any	Any	Yes	
block	Any	Any	Any	---	

[\[New SOCKS Rule \]](#)

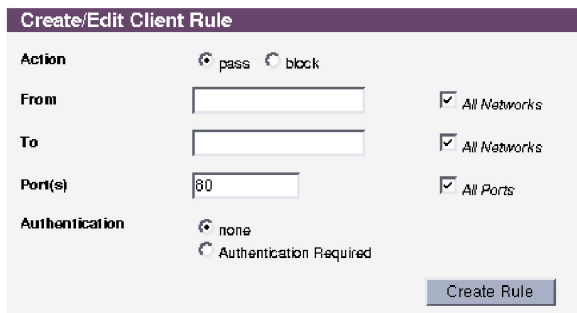
The running status allows the server to be turned on or off by clicking the *Stopped* or *Running* option from *Current Status*. To determine if this server is started at system boot time the option to *Enable/Disable* is located next to the *Boot Status*. Click on the link to enable or disable it.

Following that section is the *General Configuration*. The internal and external interfaces must be configured for proper operation. The pull down menus have a list of all IP addresses and interfaces located on the EnGarde system.

The last two sections are the Client and SOCKS rules. When a rule is added it will be displayed under its proper section. To change the order of the rules click on the up/down arrow associated with it and it will be moved. For more information concerning these rules refer to the *SOCKS Configuration Guide* on page 10.

New Client Rule

Located at the lower right corner of the *Client Rules* section of the main menu is the *New Client Rule* link. Selecting this allows a new client rule to be created. The following menu will appear allowing you to do so.



The screenshot shows a dialog box titled "Create/Edit Client Rule" with a purple header. It contains several configuration options:

- Action:** Two radio buttons, "pass" (selected) and "block".
- From:** A text input field, currently empty, with a checkbox "All Networks" checked to its right.
- To:** A text input field, currently empty, with a checkbox "All Networks" checked to its right.
- Port(s):** A text input field containing "80", with a checkbox "All Ports" checked to its right.
- Authentication:** Two radio buttons, "none" (selected) and "Authentication Required".
- Create Rule:** A button located at the bottom right of the dialog.

This menu has all the option needed to configure a client rule. Leaving the *From*, *To* and *Port(s)* fields blank will apply a default of *Any* for the appropriate category. When the rule has been configured click the *Create Rule* button to save it.

The new rule will appear on the main menu.

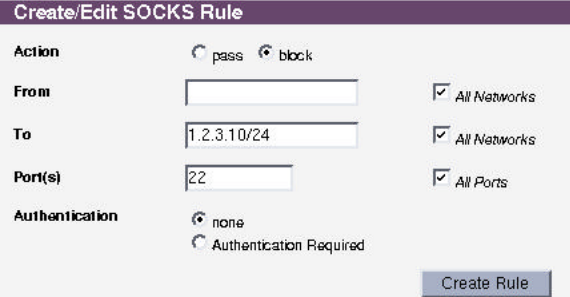
To edit or delete a rule click on the pass/block under *Action* that is associated with that rule. A new menu will appear similar to the *Create Client Rule* window.

Here changes can be made and updated by select the *Update Rule* option or the rule can be deleted by selected the *Delete Rule* option.

When changes are made here they will be reflected on the main menu as well.

New SOCKS Rule

Creating a new SOCKS rule works the same as creating a *Client Rule*, as discussed above.



The screenshot shows a dialog box titled "Create/Edit SOCKS Rule". It contains several fields and checkboxes:

- Action:** Two radio buttons, "pass" (unselected) and "block" (selected).
- From:** A text input field (empty) with a checkbox "All Networks" (checked) to its right.
- To:** A text input field containing "1.2.3.10/24" with a checkbox "All Networks" (checked) to its right.
- Port(s):** A text input field containing "22" with a checkbox "All Ports" (checked) to its right.
- Authentication:** Two radio buttons, "none" (selected) and "Authentication Required" (unselected).
- Create Rule:** A button at the bottom right.

Proxy Authentication

Enabling the *Proxy Authentication* option will require each user to enter in a user name and password before they will be allowed to access the web. If Proxy Authentication is enabled there are four options to choose from.



The screenshot shows a section titled "No Authentication" with the text "Users do not have to authenticate themselves to use the proxy." Below this is a radio button labeled "Enable No Authentication", which is selected.

No Authentication disables all proxy authentication and allows any internal user to use the proxy server.

NTLM Authentication

Users must authenticate themselves against a remote Windows PDC. You must enter the name of your Windows domain, and optionally the name of a Windows group to which the users must be a member in order to be authenticated.

Please note that you must have Winbind (in the *Windows File Sharing* module) enabled and configured before this scheme is usable.

☒ Enable NTLM Authentication

Windows Group Name

NTLM Authentication Users must authenticate themselves against a remote Windows PDC. You must enter the name of your Windows domain, and optionally the name of a Windows group of which the users must be a member in order to be authenticated.

NOTE: Please note that you must have Winbind (in the Windows File Sharing module) enabled and configured before this scheme is usable.

Basic Windows Authentication

Basic Windows Authentication does not require Winbind to function. Users must still authenticate themselves against a remote Windows PDC. Users are always challenged with a username/password prompt.

☒ Enable Basic Windows Authentication

Windows Domain Name

Basic Windows Authentication attempts to authenticate against the SMB domain you enter in the text box. To configure this on the Windows end you must create a file named 'proxyauth' and store it in the login share which contains the word "allow." If a user is authorized to log into this domain then they will be able to read this file and access will be granted. If they are unauthorized then the login will fail and proxy access will be denied.

Local Authentication

Users must authenticate themselves against the local Linux password database. This means your users must all have accounts set up on this machine.

☒ **Enable Local Authentication**

Local Authentication uses the local username/password database to perform authentication. This is nice because users can change their proxy passwords via WebTool User Manager.

LDAP Authentication

Users must authenticate themselves against a remote LDAP database. You must enter several LDAP parameters below.

☒ **Enable LDAP Authentication**

LDAP Server

ldap.guardiandigital.com

Base DN

o=dc=guardiandigital,dc=com

DN to Bind To

o=dc=guardiandigital,dc=com

Username DN Attribute

cn

DN Password

y%r2cf1d&2

LDAP Authentication allows the proxy server to authenticate a user by accessing an LDAP server. An LDAP server must be already configured. For the proxy server to authenticate with LDAP each user's LDAP entry must contain a username, either defined by 'cn' or 'uid' and a 'userPassword' must be set.

LDAP Server This will contain the address of the LDAP server.

Username DN Attribute The username attribute is defined here. Generally the username will be defined by either 'cn' (CommonName) or 'uid' (UserID).

Base DN This is the top level Distinguished Name the proxy server will use to start it's searches at when looking up user entries.

DN to Bind to The proxy server requires a Distinguished Name to bind to regardless if a password is required.

DN Password This is the password associated with the DN that is being bound to.

Proxy Privacy Settings

The Proxy Privacy Settings allows the type of concealment to be configured for the proxy server to perform. Concealment lets you strip certain HTTP headers from requests as they pass through the proxy, protecting the privacy of the users.

The four settings provide the choice for none, standard, paranoid and custom concealment.

NOTE: Certain headers are required as per the HTTP specification, and stripping some of the headers below may cause connection difficulties for the users. If users complain about connection problems you are advised to lower the concealment setting as a higher settings can cause more problems with certain sites.

No Concealment

No header cleansing is performed and requests are passed through the proxy unmodified. This is the default behavior and should be chosen if there is trouble reaching certain sites.

Standard Concealment

From, *Referer*, *Server*, *User-Agent*, *WWW-Authenticate*, and *Link*, headers are all stripped from the request before it leaves the proxy.

Paranoid Concealments

All headers are stripped except for *Allow*, *Authorization*, *Cache-Control*, *Content-Encoding*, *Content-Length*, *Content-Type*, *Date*, *Expires*, *Host*, *If-Modified-Since*, *Last-Modified*, *Location*, *Pragma*, *Accept*, *Accept-Charset*, *Accept-Encoding*, *Accept-Language*, *Content-Language*, *Mime-Version*, *Retry-After*, *Title*, *Connection*, and *Proxy-Connection*. This is the most "paranoid" option.

NOTE: Problems may be experienced trying to connect to some sites with this setting.

Custom Concealment

This option lets you choose what headers to cleanse at the proxy. Any headers not checked will be permitted through as-is.

ACL Management

ACL Management allows you to configure what users are permitted to access the Internet.

There are two ACL Management options, *Standard* and *Restricted*.

Standard ACL Management

General ACL rules are defined in the *Standard ACL Management* section. There are four sections, *Non-Internet Users*, *Unrestricted Users*, *Allow Rules* and *Deny Rules*. When you define an ACL it will appear in its associated category. By clicking on a user or rule

in these categories a window will be displayed with the options to edit or delete the current user or rule that was selected.

Non-Internet Users	
eric	root
[New Non-Internet User]	
Unrestricted Users	
[New Unrestricted User]	
Allow Rules	
middlesex	
[New Allow Rule]	
Deny Rules	
www.xsex.dk	sex
[New Deny Rule]	

Non-Internet Users are users that have an account on the local system but should not be allowed any access to the IAM server.

For example, let's say user Eric has a local account on the EnGarde system and the IAM server authentication is set to *Local Authentication*. The system administrator has determined that Eric should not be allowed access to the Internet through the Guardian Digital IAM server.

Eric has a local account so by default he is allowed to use the IAM server. Selecting *New Non-Internet User* and entering *eric* into the *Value* field entry box will deny Eric the ability to use the IAM server but still allow him access to the EnGarde box.

Unrestricted Users are special users that can use the proxy and have unrestricted access. For example if you define a rule that denies access to a certain website (allow/deny rules will be discussed shortly) but you want the system administrator

to have access you would add that system administrators user name here from the *New Unrestricted User* option.

Allow and Deny Rules are directives that are used to control or restrict access to individual Internet sites. All “normal” users are affected by these rules. A normal user is a proxy user that is not defined in any of the previous categories.

Allow and Deny rules work by checking the URL against their rule set to determine if the user can access a particular web page. The proxy server processes the URL by first checking it against any Allow Rules. If it finds it in an allow rule it will process the request. If it does not, it will check the Deny Rules. If it finds it in a deny rule then the request will be denied. Finally if it doesn't match either of the rules then the request is processed.

For example if you make a deny rule and use the value “sex”, then whenever a user tries to access a URL with the word ‘sex’ in it they will be denied. However, there may be situations where there is a valid web page with the word “sex” in the name, for example, “middlesex”. An allow rule for the “middlesex” site would permit access to specifically that site. This will take precedence over the “sex” deny rule.

The Allow and Deny rules do not need to be full URLs. The proxy server can do pattern matching and use regular expressions to match rules to URLs.

Restricted ACL Management

The *Restricted ACL Management* section allows for the ability to define users that have very restrictive access. The interface is similar to the *Standard ACL Management* interface mentioned above.

Restricted Users	
eric	[New Restricted User]
Restricted URLs	
slashdot.org	freshmeat.net [New Restricted URL]

Restricted Users have access to restricted URLs and *only* those URLs. To define a new restricted user select *New Restricted User* and enter in the user name in the *Value* field of the entry box.

Restricted URLs are defined here by selecting *New Restricted URL* and entering the URL into the *Value* field of the entry box.

Virus Scanner Configuration

Please see *Section 5* on page 34 for virus configuration info.

Cache Peering

Cache Peering allows web page caches to be shared among more than one server. This will improve performance and decrease bandwidth usage to the web. Cache Peering works between two EnGarde servers, but may work with other proxy servers that use ICP.

Cache Peering allows a server to handle a users request, check to see if it has the request URL cached and if not pass it on to the next peered server. If the next peered server has what the user is asking for it will return the response back to the original peered server. Then the original peered server will hand the results over to the user.

Only if the page isn't cached among those servers will it be retrieved from the web. This method greatly increases the speed at which pages can be displayed to the user while reducing the overall bandwidth.

To define a peer server select *Cache Peering* from the *Proxy Management* screen.

Proxy Management :: Cache Peers			
Below is a listing of the currently defined cache peers. To edit or delete a peer, simply click on its name below. To define a new peer click the [New Peer] link.			
Hostname	IP Address	Proxy Port	ICP Port
proxy.guardiandigital.com	192.168.1.2	8080	3130
[New Peer]			

Select *New Peer* to define the peer. You will need to know the server's IP address, hostname and the ports it runs its proxy server and ICP on so that you can properly define the server.

When all entries have been filled in selecting *Define Peer* will create the peer and it will appear on the main *Cache Peering* section. You can edit or delete your defined peer(s) by clicking on the highlighted name.

If the other server is also running the Guardian Digital IAM server user the default *Proxy Port* (8080) and *ICP Port* (3130) when configuring it.

Assuming the peer you defined is configured correctly cache peering will now work between the EnGarde server and the defined peer.

NOTE: Both proxy servers need to have cache peering turned on and define the other server as its peer.

Autoconfiguration

Autoconfiguration of the proxy server allows the system administrator to configure everything then supply the users with a file they import into their browser to configure the proxy information automatically. Browsers that support this feature are Internet Explorer, Netscape Navigator and Mozilla.



There are three items that need to be configured before a PAC file can be generated. You need to configure the following:

Hosting Website is the virtual host located on the local EnGarde machine that will host the PAC file for internal users to download. The virtual host must exist prior to this point or autoconfiguration can not be completed. Refer to *Virtual Host Management* of your EnGarde Secure Professional User Manual for information concerning virtual hosts.

PAC Filename is the filename that stores the auto configuration information. This file must end in '.pac'. For example, "proxy.pac" or "internal.pac".

Non-Proxy Domains are a list of domains in which the user should not be going through the proxy to access. These are generally

intranets and internal sites that are on the local side of the proxy server.

Enter one site on each line in the following form:

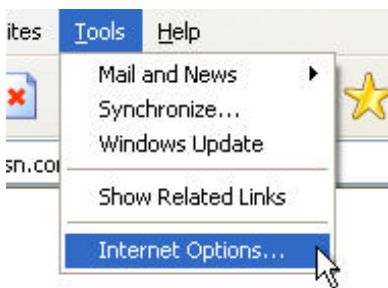
- `www.domain.com` – skip a particular site
- `.domain.com` – skip an entire domain
- `1.2.3.4` – skip a particular IP address
- `1.2.3.` – skip an entire network block

Importing a PAC file

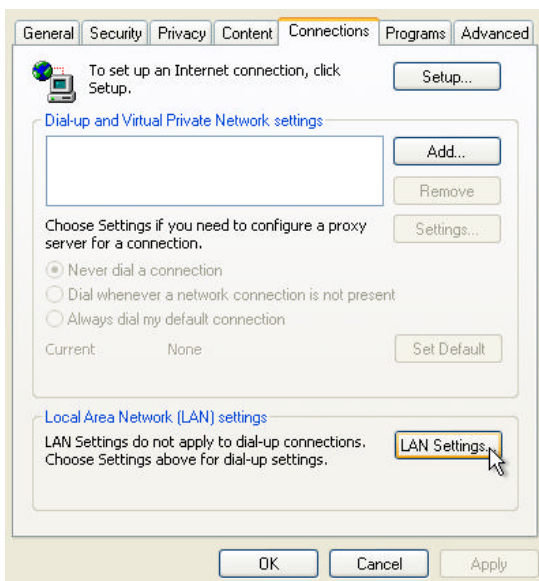
Once the PAC file has been created it can be downloaded from the provided URL. The user must configure their browser to point to the PAC file. Instructions for supported browsers is in the sections that follow.

Internet Explorer

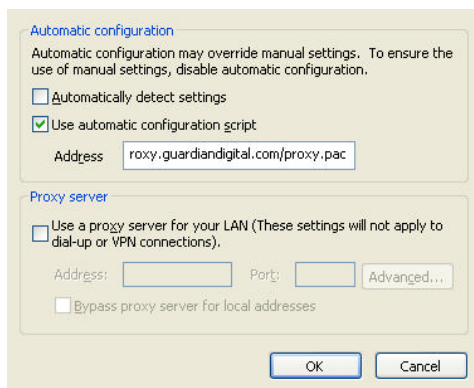
To configure Internet Explorer to use a PAC file, select *Internet Options* from the *Tools* menu in Internet Explorer.



This will bring up a tabbed menu. From the top tabs select the tab labeled *Connections*. This will display a fresh menu. From that menu select the last option, *LAN Settings*.



A new window will open and the first set of options are labeled *Automatic* configuration. In there select the check-box for *Use automatic configuration script* and enter in the address that was displayed in the WebTool.

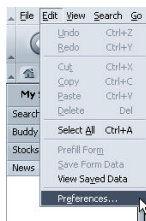


Once changes have been made select the *OK* button, then *OK* again from the tabbed menu screen. The proxy is now configured for Internet Explorer.

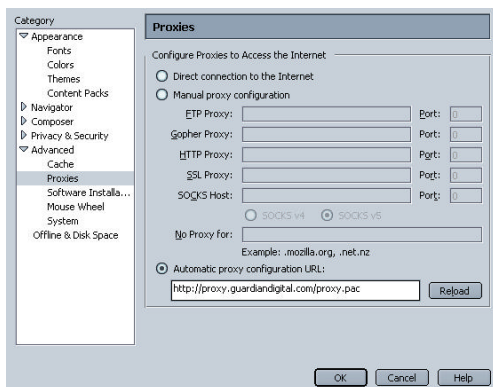
NOTE: The URL must begin with HTTP://

Netscape Navigator

To configure Netscape Navigator to use a PAC file, select *Preferences* from the *Edit* menu.



This will display the following screen. Using the expanding tree on the left of the screen select *Privacy->Proxy*.



At the bottom of that screen select the option for *Automatic proxy configuration URL* and enter in the URL provided in the WebTool.

After selecting *OK* from here the automatic proxy is configured in Netscape Navigator.

4.2 Viewing Proxy Reports & Graphs

The proxy reports and graphs are broken down into two separate sections, *Reports* and *Graphs*.

4.2.1 Reports

The reports section gives detailed reports on a daily and weekly basis of proxy activity, per user usage and details on a per user basis.

These logs are archived for 8 weeks. When selecting *Reports* from the *Proxy Management* menu a screen displaying all the recent reports will be displayed.

Daily Reports		
* Jul 22, 2002	* Jul 23, 2002	* Jul 24, 2002
* Jul 25, 2002	* Jul 26, 2002	* Jul 27, 2002
* Jul 29, 2002	* Jul 30, 2002	* Jul 31, 2002
* Aug 01, 2002	* Aug 02, 2002	* Aug 04, 2002
* Aug 05, 2002	* Aug 06, 2002	
Weekly Reports		
* Week of Jul 29, 2002		

By clicking on a report the details for that report will be broken down by user, connections, Kb/Mb/Gb transfered and time used.

User / Address	Connections	Bytes (%)	Time (%)
nwm	1,403	18.7 MB (99.26%)	00:06:10 (99.90%)
192.168.1.1	61	142.0 KB (0.74%)	00:00:11 (3.10%)
192.168.1.2	1	1.5 KB (0.01%)	00:00:00 (0.00%)
TOTAL	1,465	18.8 MB (100.00%)	00:06:21 (100.00%)

The user is represented either by their user name if proxy authentication was used or by their IP address if there was no authentication. **Connections** is the total number of connections that were made by that user/IP on the given day. **Bytes(%)** represents the amount of data transfered followed by the percent of the total amount transfered for the day in parenthesis. Lastly **Time** represent the hours, minutes and seconds followed by the percentage of time used.

Clicking on a user or IP will display detailed statistics.

User/Address: **nwm**
Report Date: **Jul 26, 2002**

Click on a username or an address to see what sites that user visited.

	Website	Connections	Bytes (%Total)	Time (%Total)
[DENY]	209.10.240.70	30	5.4 MB (28.85%)	00:00:19 (5.28%)
[DENY]	usa.asus.com	32	5.3 MB (28.37%)	00:00:37 (10.22%)
[DENY]	www.oc-athlonxp.com	61	1.9 MB (9.94%)	00:00:31 (8.39%)
[DENY]	i.cnn.net	435	1.6 MB (8.65%)	00:00:47 (12.94%)
[DENY]	ftp.engardelinux.org	3	832.5 KB (4.35%)	00:00:01 (0.32%)

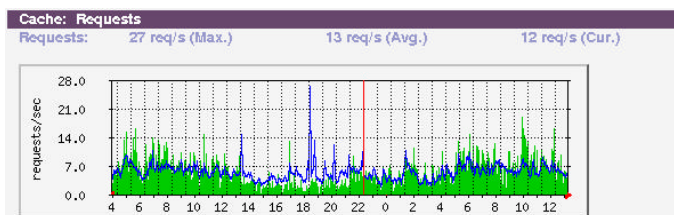
These statistics break down the sites the user visited in the given time period. From here you can see the URL of the site, the number of connections to that URL, the amount transferred from it, the amount of time spent on the site and lastly the ability to deny the user access to the site.

You can visit a site by clicking on its URL and you can deny a user access to the site by clicking on the `[DENY]` link. A denied website will appear in red if the user tried to access the site.

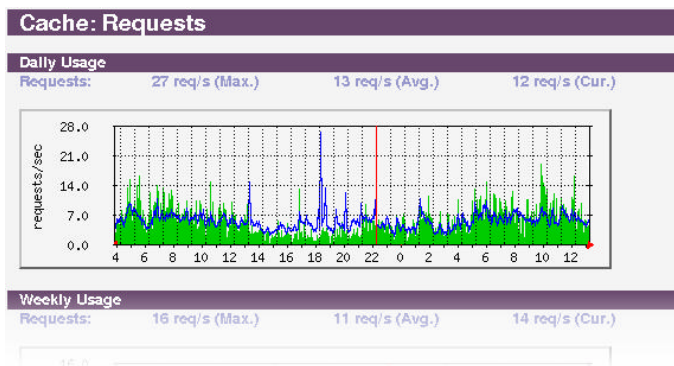
NOTE: If a user tries to access a page before being authenticated the page will show up as a denied page. For example, if the user is not logged into the proxy and tried to hit a web page they will be prompted for a password. They will enter their password and be granted access, assuming the correct password was entered. The page they originally tried to access will show up in red as denied for that first attempt to access the page.

4.2.2 Graphs

The proxy graphs represent proxy cache performance over time. Cache information including requests, errors, in/out KBs, swap size, and CPU usage are displayed.



When clicking on a graph a window will appear giving detailed time plots for daily, weekly, monthly and yearly statistics for the selected graph.



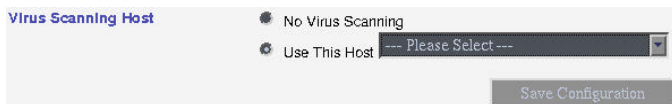
5 VIRUS DETECTION

The Guardian Digital Proxy Server has the ability to scan all incoming files for viruses and, if possible, cleanse them.

5.1 Configuring virus scanning

The main configuration screen for the *Virus Scanner Configuration* can be found under *Proxy Management* in the *System Management* section of the WebTool. However, this is inaccessible until you enable the Virus Scanner.

To enable to virus scanner you must first have created at least one virtual host. Refer to the *Virtual Host Management*, in your EnGarde Secure Professional manual for information on how to do this. Once you have a virtual host setup select *General Configuration* from the *Proxy Management* screen. At the bottom of this menu is *Virus Scanning Host*. Choose the *Use This Host* option. There will then be a list of the virtual hosts found on the EnGarde machine to choose from. Once the virtual host has been chosen click the *Save Configuration* button in the lower right corner.



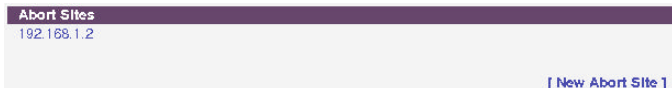
Now that virus scanning has been enabled you will see the option *Virus Scanner Configuration* is now available and ready to be used. Before Virus Scanning is enabled, this section should be reviewed and changes appropriately made or the Virus Scan may not operate properly or at all.

Virus Scanner Configuration

Set up patterns you would like to have scanned for viruses.

5.1.1 Defining Abort Sites

Abort Sites are a list of the sites the virus scanner should completely ignore. Generally these are sites you can trust information from. This is done to improve performance by removing unnecessary virus scanning.



To add a new *Abort Site* select the *New Abort Site* option and enter in the URL of the site, selecting *Define* when finished. This new site will now appear on the list. The site can be deleted or edited by clicking on the URL of the site.

The local proxy server will always be listed here by default. Virus scanning first retrieves a requested file and stores it on the proxy server for scanning. If the proxy server is not listed here the virus scanner will not be able to access downloaded files and no scanning can take place.

NOTE: It is a good idea to enter the Windows Update URL in here. Windows Update is known to have issues with virus scanners at the proxy/firewall level.

These URLs are:

- windowsupdate.microsoft.com

- windowsupdate.com

Which would be entered directly into the entry boxes.

5.1.2 Defining Abort Patterns

Like the *Abort Sites*, *Abort Patterns* are patterns that will be completely ignored by the virus scanner when requested. This refers to items such as GIF images, JPEG images, HTML files, etc.



To add a new *Abort Pattern* select the *New Abort Pattern* option. This interface works identically to the *Abort Site* interface mentioned above.

5.1.3 Defining Scan Patterns

Scan Patterns are exactly the opposite of *Abort Patterns*. *Scan Patterns* are what the virus scanner should specifically look for. Good patterns to search are .zip, .com, and .exe files.



To add a new *Scan Pattern* select the *New Scan Pattern* option. This interface works identically to the *Abort Site* interface mentioned above.

5.1.4 Scheduling Virus Updates

The IAM Server can be configured to automatically update its virus rules. This can be configured from the main *Proxy Management* menu under the option *Virus Updates*.



There are four options for how often to check, and if necessary download new virus rules.