

# Surf Sentinel



Powered by:  
**GB-OS® 4.0**

## Feature Guide





# Contents

<b>INTRODUCTION</b>	<b>1</b>
<b>About Surf Sentinel Subscriptions</b> .....	<b>1</b>
Features .....	1
Requirements .....	1
<b>Registration &amp; Activation</b> .....	<b>2</b>
Feature Activation Codes .....	2
<b>About this Guide</b> .....	<b>3</b>
Conventions .....	3
<b>MANAGING INTERNET ACCESS</b>	<b>4</b>
<b>Surf Sentinel Proxy</b> .....	<b>4</b>
<b>Surf Sentinel Policies</b> .....	<b>4</b>
<b>Local Allow and Local Deny Lists</b> .....	<b>4</b>
<b>Remote Logging</b> .....	<b>5</b>
<b>Internet Access Policy</b> .....	<b>6</b>
Steps to Implementation .....	6
<b>USING SURF SENTINEL</b>	<b>8</b>
<b>Activation</b> .....	<b>8</b>
<b>Configuration</b> .....	<b>8</b>
Surf Sentinel Policies .....	9
Content Filtering Facilities .....	10
Content Blocking .....	10
Surf Sentinel Categories .....	10
Advanced Surf Sentinel Policy Settings .....	11
Example Policy Settings .....	11
Local Allow/Deny Lists .....	14
Surf Sentinel Proxy .....	15
Enabling the Traditional Proxy .....	16
Transparent Proxy .....	16
Using Both Proxy Types .....	16
Block Actions .....	16
<b>Licensing</b> .....	<b>17</b>
<b>REFERENCE A: CATEGORIES</b>	<b>18</b>
<b>Denied by Default</b> .....	<b>18</b>
<b>Allowed by Default</b> .....	<b>19</b>



# Introduction

## About Surf Sentinel Subscriptions

Surf Sentinel is GTA's Internet access management and content filtering subscription service for GTA firewalls using 41 content categories.

Surf Sentinel, which utilizes the SurfControl® content filtering engine, is a complete and accurate Internet content filtering solution that meets the requirements and demands of both users and technology providers. Surf Sentinel features one of the largest databases of categorized URLs, combining blocking, monitoring and policy management in a centrally managed, out-sourced solution. When used in conjunction with GTA Reporting Suite 2.0 (available separately), real-time Internet usage reports are available from current and historical firewall log data.

Surf Sentinel, utilizing SurfControl's Content Portal Authority technology, provides access to all of SurfControl's content: over 5.5 million categorized URLs available in 65 languages that are updated on a daily basis.

## Features

- 41 content categories for access control.
- Customizable using GB-OS local allow and local deny address objects.
- Over 5.5 million categorized URLs.
- Easy administration and enforcement of acceptable use policies.
- Economical deployment.
- No additional hardware required.
- Reports available through GTA Reporting Suite 2.0 (available separately).

## Requirements

- GTA firewall operating using GB-OS version 3.5 and above.
- Web browser and Internet connection.
- GTA Firewall product registration.
- Surf Sentinel subscription and feature activation code.

# Registration & Activation

If you have not yet registered your firewall products, go to the GTA Online Support Center (<https://www.gta.com/support/center/login/>). In the login screen, enter your user ID and password. Click the **Register Product** link and enter your product serial numbers and firewall activation (unlock) codes, then click **SUBMIT**.

If you do not already have a GTA Online Support Center account, click the **CREATE AN ACCOUNT Now!** link on the GTA Online Support Center login screen.

## Feature Activation Codes

Optional features on GTA firewalls require activation codes. The Surf Sentinel activation code is entered on the **Configuration>System>Activation Codes** screen.

The feature activation code can be found in **View Your Registered Products** on the GTA Online Support Center by selecting the serial number of your GTA firewall. Copy the feature activation code and enter it in the **Configuration>System>Activation Codes** screen in the next available row. Click **SAVE**. When an activation code is entered correctly, the description column will indicate “GB-X–Surf Sentinel”, where X is your firewall’s product number.



### Note

If the feature activation code does not appear in your GTA Online Support Center account, please contact [GTA support](#), putting your serial number and Support Center User ID in the message subject.

# About this Guide

This option guide is a supplement to the *GB-OS 4.0 User's Guide*. It illustrates the activation and use of the Surf Sentinel subscription service for GB-OS 4.0 and above.

## Conventions

A few conventions are used in this guide to help you recognize specific elements of the text. If you are viewing this guide in PDF format, color variations may also be used to emphasize notes, warnings and new sections.

<b><i>Bold Italics</i></b>	Emphasis
<i>Italics</i>	Publications
<a href="#">Blue Underline</a>	Clickable hyperlink (email address, web site or in-PDF link)
SMALL CAPS	On-screen field names
Monospace Font	On-screen text
<b>Condensed Bold</b>	On-screen menus, menu items
<b>BOLD SMALL CAPS</b>	On-screen buttons, links

# Managing Internet Access

GTA's Internet access management solutions provide the ability to control web access based on site content. GTA firewalls have three primary functions for access control: Surf Sentinel policies, local allow/deny lists and Surf Sentinel proxy settings. In addition, records of blocked sites can be created and sent to GTA firewall logs. See the *GB-OS User's Guide* for more information on how to use other content filtering options.

## Surf Sentinel Proxy

Content filtering requires the use of the Surf Sentinel proxy. When enabled, the Surf Sentinel proxy can either be configured to operate using a traditional or transparent proxy for HTTP (web) requests.

The transparent proxy is the more common method for implementing a HTTP proxy. It is easy to implement, especially if Surf Sentinel is being configured to manage Internet access for a large network.

The traditional proxy is used primarily for systems which were put in place prior to the introduction of transparent proxy methods and for systems that require more control by directing web request through a specific port.

## Surf Sentinel Policies

Surf Sentinel policies provide a means to select web access control facilities and specify how they will be applied to web request. With every web page request, your firewall must choose to either accept or deny transmission. Surf Sentinel policies contain the criteria that cause a web page to be accepted or denied and define any scripts or applets that should be blocked.

By default, Surf Sentinel denies all web page requests. This default will be enacted if a web page request does not meet any listed policy. To ensure that all web page requests are not rejected by default, at least one policy of type accept must be in place.

## Local Allow and Local Deny Lists

Local allow and local deny lists, configured using the Object Editor and used in conjunction with Surf Sentinel policies, allow the administrator to customize content filtering. Local allow and local deny lists take precedence over Surf Sentinel category listings, so you can allow access to specific sites in categories that have been blocked or deny access to sites in categories that are otherwise allowed. This is particularly useful for companies whose policies allow access only to a few specific sites, or for those with policies which allow web requests for a category, but deny specific sites within that category.

# Remote Logging

Both the Surf Sentinel proxy and Surf Sentinel policy entries are logged to the GTA firewall. Two examples, one of a accept (pass) and one of a deny (block) log message, are illustrated below.



## Note

To learn more about log messages, see the *GB-OS User's Guide*.

```
Oct 29 14:24:18 acmefirewall id=firewall time="2002-10-29 14:24:18"  
fw="acmefirewall-ha-1" pri=5 msg="Accept outbound NAT"  
cat_action=pass cat_site="Web Communications"  
dstname=www.leadcart.com proto=http src=192.168.71.97 srcport=2661  
nat=199.120.225.3 natport=2661 dst=205.138.3.133 dstport=80 rule=2  
duration=23 sent=536 rcvd=537 pkts_sent=6 pkts_rcvd=5  
op=GET arg=/ads1/images/digits/n7.gif
```

*Logging, Surf Sentinel Proxy*

```
Oct 29 14:24:26 acmefirewall id=firewall time="2002-10-29 14:24:26"  
fw="acmefirewall-ha-1" pri=4 msg="Block outbound NAT"  
cat_action=block cat_site="Local Deny" dstname=ad.doubleclk.net  
proto=http src=src=192.168.71.33 srcport=4991  
nat=199.20.136.33 natport=4991 dst=205.138.3.82 dstport=80 rule=2  
duration=22 sent=861 rcvd=60 pkts_sent=3 pkts_rcvd=1  
op=GET arg=/adi/caranddriver.lana.com/kw=;;ord=180587622710292244
```

*Logging, Surf Sentinel Proxy*

Table 1.1: Content Logging Fields	
Field	Description
<b>pri</b>	Priority of log message.
<b>msg</b>	Message indication Accept or Block.
<b>cat_action</b>	Action taken.
<b>cat_site</b>	Surf Sentinel category, Local Accept or Local Deny.
<b>dstname</b>	Website accepted or blocked by this action.
<b>proto</b>	Protocol (HTTP).
<b>src</b>	Source IP address of the web request.
<b>srcport</b>	Port through which the web request was made.
<b>op</b>	Operation requested.

Log messages are in WELF, the default log format.

# Internet Access Policy

The Internet changes constantly and Surf Sentinel can help you respond quickly to new and changing sites, restricting user access only to material that is consistent with your access policy.

Restricting Internet access can protect a company from drains on bandwidth, potential legal liability and lost productivity. For example, schools and libraries can set their Surf Sentinel policies to prevent access to websites that may not be appropriate for the workstation user's age.

When content filtering has been configured and Surf Sentinel is enabled, the SurfControl content filtering engine compares a requested page to its database of categorized URLs at one of several GTA server sites, then allows or denies the request based on the Surf Sentinel policies created in accordance with your company's Internet access policy.

This rating and review process includes not only the sites that a user explicitly requests by clicking on a link or typing a URL, but also protects users from material blocked as inappropriate on pages called up inadvertently (e.g., pop-up windows) when accessing sites. Blocked pop-up windows and graphics will display the firewall's content blocking message.

## Steps to Implementation

Content filtering can be implemented as part of a complete Internet Access/Acceptable Use Policy. Prior to implementing Surf Sentinel, GTA suggests completing the following steps:

- Develop an Internet Access Policy and create acceptable user guidelines.
- Create address objects and/or user groups on your GTA firewall to define the various users and groups whose access you will be controlling using Surf Sentinel.
- Create Surf Sentinel policies on your GTA firewall for the users and groups defined in the previous step, and choose which categories will be accepted and which will be denied.
- Customize your content filtering further, if desired, by adding any specific pages or sites you wish to allow or deny to the local allow or local deny lists.
- Turn on content filtering by selecting the Surf Sentinel proxy method.



# Using Surf Sentinel

This chapter describes activating and using the Surf Sentinel subscription option using the Web interface.

## Activation

Surf Sentinel is activated by entering your feature activation code, available from the GTA Online Support Center after your GTA firewall has been registered. (You must register your product and log in with your user name and password.)

To activate Surf Sentinel, log on to your GTA firewall and navigate to **Configuration>System>Activation Codes**. Click the **New** icon to enter the feature activation code in the next available line. Save the section. If the DESCRIPTION field fills automatically, the code is activated correctly and the service can be enabled.

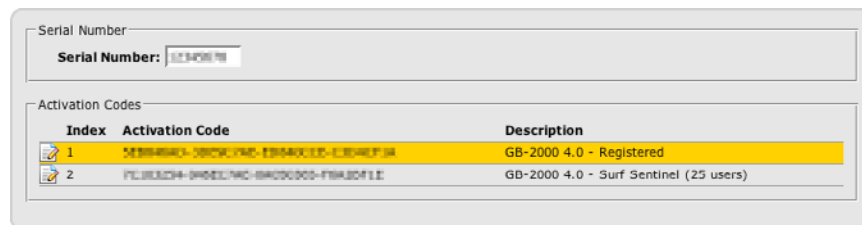


Figure 2.1: Surf Sentinel - Activated

## Configuration

The steps for configuring Surf Sentinel must be done in order to ensure continuous Internet access for users. If content filtering is already in use, some of these steps will have already been completed.

### To configure Surf Sentinel content filtering on your GTA firewall:

1. Define a DNS server (**Configuration>Services>DNS**) to access your selected list server. (See the *GB-OS User's Guide* for more about defining a DNS server.)
2. Create and enable Surf Sentinel policies.
3. Add local allow and deny lists (if desired).
4. Enable the Transparent Proxy.
5. And/or enable the Traditional Proxy.



### Note

Before Surf Sentinel can be configured, a valid feature activation code must be entered.

# Surf Sentinel Policies

Surf Sentinel policies provide a means to select web access control facilities and specify how they will be applied to web requests. Each Surf Sentinel policy consists of a description, an address object representing the source of the web request, the ability to specify content blocking preferences for the individual policy, and, with a Surf Sentinel subscription, content filtering Surf Sentinel category lists.

Like security policies, Surf Sentinel policy order is important. Each web request is compared to the list, starting at Surf Sentinel policy index #1. The packet is compared sequentially against each policy until one of two events occur:

1. A Surf Sentinel policy is matched. The web request is either allowed or blocked based on the policy's definition.
2. No Surf Sentinel policies are matched and the list is exhausted. In this case, the web request is rejected.

To configure Surf Sentinel policies, navigate to **Configuration>Threat Management>Surf Sentinel>Policies**. Click the **New** icon to define a new policy.

The screenshot shows the configuration page for a Surf Sentinel policy. At the top, there is a 'Disable' checkbox, a 'Description' text field containing 'Example Surf Sentinel Policy', and a 'Source Address' dropdown menu set to 'ANY\_IP'. An 'Advanced' button is visible on the right. Below these are three main sections: 'Content Filtering Facilities' with 'Local Allow List' (Local allow), 'Local Deny List' (Local deny), and 'Surf Sentinel' (checked); 'Content Blocking' with 'ActiveX Objects', 'Java', 'JavaScript', and 'Unknown HTTP Commands' all checked; and 'Surf Sentinel Categories' with two columns: 'Accept' (listing categories like Advertisements, Arts & Entertainment, Chat, etc.) and 'Deny' (listing categories like Adult/Sexually Explicit, Criminal Skills, etc.), with a 'Default' button between them.

Figure 2.2: Configuring a Surf Sentinel Policy

<b>Table 2.1: Configuring a Surf Sentinel Policy</b>	
<i>Field</i>	<i>Description</i>
<b>Disable</b>	Disables the policy.
<b>Description</b>	A description for the policy.
<b>Source Address</b>	If a request matches an element of the specified address object of type SURF SENTINEL, the packet will be compared to the policy.
<b>Content Filtering Facilities</b>	
<b>Local Allow List</b>	Use the firewall's local allow list by selecting its address object.
<b>Local Deny List</b>	Use the firewall's local deny list by selecting its address object.
<b>Surf Sentinel *</b>	Enable to use the Surf Sentinel Categories list.
<b>Content Blocking</b>	
<b>ActiveX Objects</b>	Enable to block ActiveX controls.
<b>Java</b>	Enable to block Java applets.
<b>Javascript</b>	Enable to block Javascript.
<b>Unknown HTTP Commands</b>	Enable to block unknown HTTP commands and unencrypted HTTP protocols.
<b>Surf Sentinel Categories</b>	
<b>Accept / Deny</b>	Specify allowed or blocked Surf Sentinel categories. Switch a category from one list to the other by selecting the item and clicking the left or right arrow button.

## Content Filtering Facilities

The **CONTENT FILTERING FACILITIES** box contains selections for the local allow and local deny lists as well as the toggle to enable the use of Surf Sentinel subscription options.

Available selections from the **LOCAL ALLOW LIST** and **LOCAL DENY LIST** are all defined address objects defined in the Object Editor that are of type **ALL** or **SURF SENTINEL**. See **Local Allow/Deny Lists** for more information.

## Content Blocking

Portable code blocking for ActiveX objects, Java, Javascript and unknown HTTP commands can protect your network from malicious programs such as viruses spread by web pages (applets or scripts appear in inbound TCP ports 443, 80, 8000 and 8080). In addition to blocking mobile programs embedded in web pages, **CONTENT BLOCKING** can also prevent tunneled, unencrypted non-HTTP connections over standard HTTP ports.

## Surf Sentinel Categories

Surf Sentinel has a default set of **ALLOWED** and **DENIED** categories. Move these categories from one list to another to reflect your Internet access policy using the arrow buttons (**-->**, **<--**). For example, if you wish to deny access to websites that would fall under the **Advertisements** category, select that category in the **ALLOWED** field (its default location) and click the **-->** button to move the **Advertisements** category to the **DENIED** field.

In order to make use of Surf Sentinel categories, the **SURF SENTINEL** checkbox in the **CONTENT FILTERING FACILITIES** box must be enabled.

Local Allow/Deny Lists take precedence over Surf Sentinel categories, and will ignore settings configured in this section of the Surf Sentinel policy.

## Default Categories

Categories can be reset to installation defaults at any time by selecting the **DEFAULT** button. See [Reference A: Categories](#) for more information on Surf Sentinel default categories.

## Advanced Surf Sentinel Policy Settings

Surf Sentinel policies contain additional, advanced settings that are new to GB-OS 4.0. Policies can now require user groups to authenticate with the firewall using GBAuth as well as control Internet access based on the destination address. Restricting access by destination address is useful if the administrator wishes to block content on a certain website, such as ActiveX objects. Regular expression can also be used when defining the policy's **DESTINATION ADDRESS**.

Advanced settings for Surf Sentinel policies are configured in **Configuration>Threat Management>Surf Sentinel>Policies** under the **ADVANCED** tab.



**Figure 2.3:** Advanced Surf Sentinel Policies

Table 2.2: Advanced Surf Sentinel Policies	
Field	Description
<b>Authentication Required</b>	Enable to require users to authenticate with the GTA firewall using GBAuth. When enabled, a pulldown will appear with configured user groups that will have the policy applied to them.
<b>Destination Address</b>	A selection of address objects that are of type ALL or SURF SENTINEL. Select <b>&lt;USER DEFINED&gt;</b> to manually enter a destination address.

## Example Policy Settings

With the new advanced settings made available in GB-OS 4.0, it is now possible to configure more restrictive Surf Sentinel policies. Example Surf Sentinel policy configurations assume that the [Surf Sentinel proxy](#) has been enabled.

### Example 1: Restricting Access to Specific Destinations

A company with a shipping department would like to restrict their shipping employees' Internet access to shipping related sites (FedEx, UPS, DHL, etc.). To do so, two address objects of type ALL or SURF SENTINEL must be defined:

1. An address object, named Shipping Employees, containing the IP addresses of all employees belonging to the shipping department.
2. An address object, named Shipping Websites, containing all websites that the shipping employees will be granted access to. (In this example, fedex.com, ups.com and dhl.com.)

Once all necessary address objects have been defined, navigate to **Configuration>Threat Management>Surf Sentinel>Policies** and click the **New** icon to define the policy that will be restricting the shipping department's Internet access.





**Figure 2.4:** Restricting Access to Specific Destinations

When defining the Surf Sentinel policy, select the <Shipping Employees> address object for the policy's SOURCE ADDRESS. Under the Advanced tab, select the <Shipping Websites> address object for the policy's DESTINATION ADDRESS.

Click **OK** and then **SAVE**. From now on, all IP addresses listed in the Shipping Employees address object will be restricted to websites listed in the Shipping Websites address object. All other Internet requests will be met with the Surf Sentinel proxy's configured BLOCK ACTION.

## Example 2: Blocking Content from Specific Websites

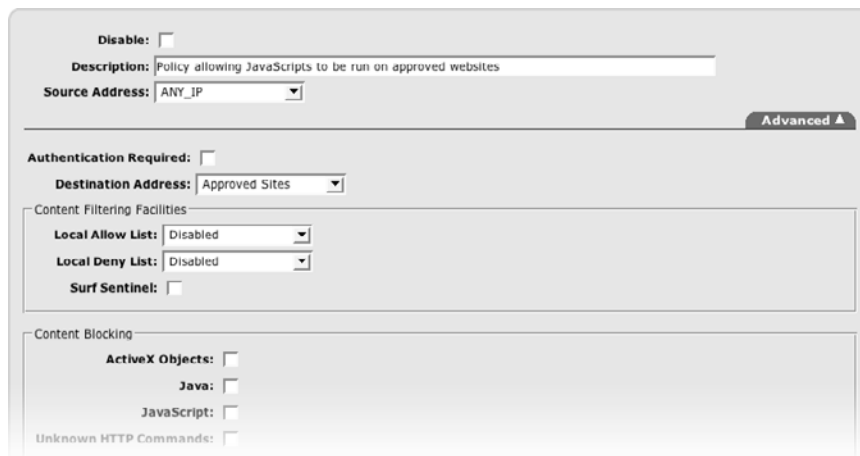
A company would like to disable JavaScripts from running on all websites except for those they explicitly allow. By using Surf Sentinel, JavaScripts and other potentially malicious content can be removed from websites, transparently to end users. To do so, two Surf Sentinel policies need to be defined:

1. A policy that allows JavaScripts to run only if they are on approved websites.
2. A policy that blocks JavaScripts from running on all other websites.

## Creating the First Surf Sentinel Policy

Before the first Surf Sentinel policy can be created, an address object of type ALL or SURF SENTINEL named Approved Sites that contains all approved websites must be defined.

Once the address object has been defined, navigate to **Configuration>Threat Management>Surf Sentinel>Policies** and click the **NEW** icon to define the policy that will allow JavaScripts to be run on the desired websites.



**Figure 2.5:** Allowing JavaScripts to be Run on Specific Websites

When defining the Surf Sentinel policy, select <ANY IP> for the policy's SOURCE ADDRESS. Under the **ADVANCED** tab, select the <Approved Sites> address object for the policy's DESTINATION ADDRESS. Next, in the **CONTENT BLOCKING** box, ensure the **JAVASCRIPT** option is unchecked.

Click **Ok** and then **SAVE**. You have now created the Surf Sentinel policy that will allow all IP addresses trying to access websites listed in the Allow JavaScript address object to view those websites with JavaScripts intact. Next, you must create a Surf Sentinel policy that will block all other websites from running Javascript.

## Creating the Second Surf Sentinel Policy

Click the **New** icon in the Surf Sentinel policy list to define the second policy. Again, select **<ANY IP>** for the policy's SOURCE ADDRESS. Under the **ADVANCED** tab, ensure that **<ANY IP >** is selected for the policy's DESTINATION ADDRESS. Finally, under the CONTENT BLOCKING box, check the **JAVASCRIPT** option.

The screenshot shows the configuration window for a Surf Sentinel policy. At the top, there is a 'Disable' checkbox (unchecked), a 'Description' field containing 'Blocking JavaScripts on unapproved websites', and a 'Source Address' dropdown menu set to '<ANY\_IP>'. Below this is an 'Advanced' tab. Under the 'Advanced' tab, there is an 'Authentication Required' checkbox (unchecked) and a 'Destination Address' dropdown menu set to '<ANY\_IP >'. Below that is a 'Content Filtering Facilities' section with 'Local Allow List' and 'Local Deny List' dropdown menus both set to 'Disabled', and a 'Surf Sentinel' checkbox (unchecked). At the bottom is a 'Content Blocking' section with checkboxes for 'ActiveX Objects' (unchecked), 'Java' (unchecked), 'JavaScript' (checked), and 'Unknown HTTP Commands' (unchecked).

**Figure 2.6:** Blocking JavaScripts on All Other Websites

Click **Ok** and then **SAVE**. You have now created the Surf Sentinel policy that will block JavaScripts from running on all other websites. Next, you must configure the Surf Sentinel policy list's order so that the first policy will match before the policy you just created.

## Sorting the Surf Sentinel Policy List

Once the policies have been configured and saved, verify that the first policy (which allows JavaScripts on approved websites) is placed above the second policy (that blocks JavaScripts on all other websites). If the order is reversed, the deny policy will match before the allow policy, resulting in JavaScripts being stripped from all websites, regardless if they are in the Approved Sites address object or not.

Index	Source Address	Description
1	<ANY_IP>	Policy allowing JavaScripts to be run on approved websites
2	<ANY_IP>	Blocking JavaScripts on unapproved websites

**Figure 2.7:** Sorting the Surf Sentinel List

## Local Allow/Deny Lists

Local allow and deny lists allow customization of content filtering using customized address objects. You can choose to execute all content filtering locally, allow access to sites that are disallowed by another content filtering facility or deny access to sites that are otherwise allowed.

To add domain names to the local allow and deny lists:

1. Navigate to **Configuration>System>Object Editor>Address Objects**.
2. Select the local list you wish to edit.
3. In the ADDRESS field, enter the desired domain name and an optional description.  
For additional domain names, enter their value in the row below.
4. Click **OK** and then **SAVE**.

Enter domain names in the following format: `example.com`. WWW and other such subdomain prefixes (`www2`, `www3`) limit the effectiveness of the local allow or deny lists. For example, the value `www.example.com` only accepts or denies access for the specific site only, not to sites such as `www2.example.com` or `subdomain.example.com`. If you wish to block an entire domain and all of its subdomains, enter `example.com`.

Additionally, you may use regular expression to create more elaborate local allow and deny lists. See the *GB-OS User's Guide* for more information.



### Caution

Using regular expression in Surf Sentinel policy definitions may result in an unexpected policy match.

Index	Object	Address	Description
1	<USER DEFINED>	gta.com	GTA Homepage
2	<USER DEFINED>	google.com	Google Search
3	<USER DEFINED>	cnn.com	CNN News
4	<USER DEFINED>		

**Figure 2.8:** Defining Local Allow/Deny Lists

# Surf Sentinel Proxy

Content filtering on a GTA firewall requires the configuration of the Surf Sentinel proxy. The Surf Sentinel proxy allows Internet requests to be managed by tunneling all requests through the proxy, where content can be filtered (as defined by Surf Sentinel policies).



### Caution

Surf Sentinel policies must be created before enabling the Surf Sentinel proxy. Enabling the proxy before creating policies will block all HTTP Internet access.

Using the transparent proxy, IP addresses that are not explicitly allowed access in Surf Sentinel policies will be able to use TCP port 80 (the port used for Internet access). If only the traditional proxy is used, only users with browsers configured to use the traditional proxy will be affected, all other users will not have their Internet access filtered.

The Surf Sentinel proxy screen allows the firewall administrator to specify the use of the transparent proxy, the traditional proxy or both. Additional settings include the selection of a block message or URL redirect when an Internet request has been denied.

Figure 2.9: Configuring the Surf Sentinel Proxy

Table 2.3: Configuring the Surf Sentinel Proxy	
Field	Description
<b>Traditional Proxy</b>	
<b>Enable</b>	Enables the traditional proxy.
<b>Port</b>	The port through which the proxy will run. Default is 2784.
<b>Advanced</b>	
<b>Automatic Policies</b>	A toggle for whether the firewall should automatically generate the required policies for the email proxy to function. If unselected, it is necessary to define remote access policies.
<b>Transparent Proxy</b>	
<b>Enable</b>	Enables the transparent proxy.
<b>Block Action</b>	
<b>Action</b>	A selection for the action to be performed when a request for blocked content is performed.
<b>Message</b>	If <Use message> is selected for the ACTION, the entered message will be displayed. Default is Local policy denies access to web page.
<b>URL</b>	If <Redirect to URL> is selected for the ACTION, the user will be directed to the entered URL.



## Enabling the Traditional Proxy

When the firewall is operating without Surf Sentinel web filtering enabled, it does not use a proxy. When the HTTP proxy is used in conjunction with a web filtering facility, it runs on TCP port 2784 by default. To run the HTTP proxy on a different port, enter the desired port number in the `PORT` field. The traditional proxy requires users located on protected networks to have browsers configured to use a proxy connection with the proxy IP address and port number. Only users specifying the traditional proxy port will use web filtering for their traffic.

If the `AUTOMATIC POLICIES` toggle, located under the **ADVANCED** tab, has been disabled, a remote access policy that allows connection to the entered `PORT` value from the protected network must be configured and enabled. Because of this, GTA recommends leaving the `AUTOMATIC POLICIES` toggle enabled to simplify configuration.

## Transparent Proxy

The transparent proxy is the most common method of implementing an HTTP proxy because it is easier to implement than a traditional proxy, especially when a network is large and widespread. This method is invisible to users located on the protected network. No modification to their browsers settings is required, and there is no `PORT` field. As the name implies, the transparent proxy allows the firewall to filter and mediate HTTP traffic transparently to end users.

## Using Both Proxy Types

If some hosts are already using the traditional proxy and have a proxy port set, or the administrator wants to direct some users' Internet requests through a specific port in order to increase control, the traditional and transparent proxy may be enabled simultaneously.

With both types of proxy enabled, users without a proxy port set in their browser will use the transparent proxy while users with the proxy port defined will make use of the traditional proxy.

## Block Actions

If a policy blocks a web address (URL) and a user attempt to load a page from that address, the user will see a custom message, or be redirected to a URL (e.g., an internal website that defines the company's Internet policies and the administrative process to gain access to a blocked website).



### Note

If your Surf Sentinel policies are configured to use local allow/deny lists, and your block action redirect is to a URL, make sure the URL is defined in your local allow list.

# Licensing

If the number of hosts using Surf Sentinel exceeds the number of licenses purchased, the next host attempting to access the Internet will be blocked. A message will be displayed in their web browser and a “license exceeded” log message will be generated by the firewall.

User licenses are reserved for ten minutes. When a user has been inactive for ten minutes, the license will be released for use by another host. Contact the GTA sales staff or an authorized GTA channel partner for information on purchasing additional Surf Sentinel user licenses.



# Reference A: Categories

Surf Sentinel contains 41 categories for the administrator to use when customizing Surf Sentinel policies. A special category for websites that do not fit neatly into a category and for requests that do not return a rating is RATING UNAVAILABLE.



## Caution

GTA recommends reviewing default category settings and modifying them to match your company's Internet access policy.

## Denied by Default

Categories denied by default are as follows:

Category	Description
<b>Adult/Sexually Explicit</b>	Sexually-oriented or erotic full or partial nudity; depictions or images of sexual acts, including animals or inanimate objects used in a sexual manner; erotic stories and textual descriptions of sexual acts; sexually exploitative or sexually violent text or graphics; bondage, fetishes, genital piercing; adult products including sex toys and CD-ROMs; adult services including video conferencing, escort services, and strip clubs; explicit cartoons and animation. <b>Note:</b> SurfControl does not block on the basis of sexual preference, nor does it block sites regarding sexual health, breast cancer, or sexually transmitted diseases (except in graphic examples)
<b>Criminal Skills</b>	Advocating, instructing, or giving advice on performing illegal acts such as phone service theft, evading law enforcement, lock-picking, fraud, plagiarism/cheating, and burglary techniques.
<b>Drugs, Alcohol &amp; Tobacco</b>	Recipes, instructions or kits for manufacturing or growing illicit substances, including alcohol, for purposes other than industrial usage; glamorizing, encouraging, or instructing on the use of or masking the use of alcohol, tobacco, illegal drugs, or other substances that are illegal to minors; alcohol and tobacco manufacturers' commercial web sites; information on "legal highs" – glue sniffing, misuse of prescription drugs or abuse of other legal substances; distributing alcohol, illegal drugs, or tobacco free or for a charge; displaying, selling, or detailing use of drug paraphernalia. <b>Note:</b> SurfControl does not block sites discussing medicinal drug use, industrial hemp use or public debate on the issue of legalizing certain drugs, nor does it block sites sponsored by a public or private agency that provides educational information on drug use.
<b>Gambling</b>	Online gambling or lottery web sites that invite the use of real money; information or advice for placing wagers, participating in lotteries, or gambling real money, or running numbers; virtual casinos and offshore gambling ventures; virtual sports leagues and sports picks and betting pools.

<b>Hacking</b>	Promotion, instruction, or advice on the questionable or illegal use of equipment and/or software for purpose of hacking passwords, creating viruses, gaining access to other computers and/or computerized communication systems; anonymous surfing sites and/or sites that provide work arounds for filtering software.
<b>Hate Speech</b>	Advocating or inciting degradation or attack of specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation; promoting a political or social agenda that is supremacist in nature and exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation; holocaust revisionist/ denial sites; coercion or recruitment for membership in a gang or cult. <b>Note:</b> SurfControl does not block news, historical, or press incidents that may include the above criteria (except in graphic examples).
<b>Violence</b>	Portraying, describing or advocating physical assault against humans, animals or institutions; depictions of torture, mutilation, gore or horrific death; advocating suicide or self-mutilation; instructions, recipes or kits for making bombs or other harmful or destructive devices; excessive use of profanity or obscene gesticulation. <b>Note:</b> SurfControl do not block news, historical or press incidents that may include the above criteria (except in graphic examples).
<b>Weapons</b>	Sites that allow online purchasing or provide ordering information, including lists of prices and dealer locations, or any page or site predominantly containing, or providing links to, content related to the sale of guns, weapons, ammunition or poisonous substances; sites displaying or detailing the use of guns, weapons, ammunition or poisonous substances.

## Allowed by Default

Categories allowed by default are as follows:

<b>Table A.2: Default Allowed Categories</b>	
<i>Category</i>	<i>Description</i>
<b>Advertisements</b>	Banner ad servers.
<b>Arts &amp; Entertainment</b>	Television, movies, music and video programming guides; comics, jokes, movie, video or sound clips; discussion forums on television, movies, music and videos; online magazines and reviews on the entertainment industry; circuses, theatre, variety magazines, and radio broadcasting firms and technologies (satellite, cable, etc.); book reviews and promotions, publishing houses, comic books, and poetry; jokes, comedians, any site designed to be funny or satirical; online museums, galleries, artist sites (including sculpture, photography, etc.); celebrity fan sites; horoscopes; city guides.
<b>Chat</b>	All web-based chat software.
<b>Computer &amp; Internet</b>	Reviews, information, buyer's guides of computers, computer parts and accessories and software; computer/software/Internet companies, industry news and magazines; sites that design and/or maintain web pages, including those of individual web designers.
<b>Education</b>	.edu sites: pre-, elementary, secondary, and high schools; universities; distance education and trade schools; online teacher resources (lesson plans, etc.); topic-specific search engines (anthropology, medicine, etc.)



<b>Finance &amp; Investment</b>	Stock quotes, stock checkers, and fund rates; online stock or equity trading; investing advice or contacts for trading securities; money management/ investment services or firms; general finances and companies that advise thereof; accountancy, actuaries, banks, mortgages, and general insurance companies.
<b>Food &amp; Drink</b>	Recipes, cooking instruction and tips, food products, and wine advisors; restaurants, cafes, eateries, pubs, and bars; food/drink magazines, reviews.
<b>Games</b>	Game playing or downloading; game hosting or contest hosting; tips and advice on games or obtaining cheat codes; journals and magazines dedicated to game playing.
<b>Glamour &amp; Intimate Apparel</b>	Lingerie, negligee or swimwear modeling; model fan pages; fitness models/ sports celebrities; fashion or glamour magazines online; clothing catalogs; beauty and cosmetics; modeling information and agencies.
<b>Government &amp; Politics</b>	Government services such as taxation, armed forces, customs bureaus, emergency services; local government sites; political debate, canvassing, election information and results; local, national, and international political sites.
<b>Health &amp; Medicine</b>	General health such as fitness and well-being; alternative and complementary therapies; medical information about ailments, conditions, and drugs; medical reference; hospital or medical insurance; dentistry, optometry, and other medical-related sites; general psychiatry and mental well-being sites; promoting self-healing of physical and mental abuses, ailments, and addictions; psychology, selfhelp books, and organizations.
<b>Hobbies &amp; Recreation</b>	Recreational pastimes such as collecting, gardening, kit airplanes; outdoor recreational activities such as hiking, camping, rock climbing; tips or trends focused on a specific art, craft, or technique; online publications on a specific pastime or recreational activity; online clubs, associations or forums dedicated to a hobby.
<b>Hosting Sites</b>	Web sites that host business and individuals' web pages (e.g., GeoCites, earthlink.net, AOL).
<b>Job Search &amp; Career Development</b>	Employment agencies, contractors, job listings, career information; career searches, career-networking groups.
<b>Kids' Sites</b>	Child-centered sites and sites published by children.
<b>Lifestyle &amp; Culture</b>	Home life and family-related topics, including parenting tips, gay/lesbian/ bisexual (non-pornographic sites), weddings, births, and funerals; foreign cultures, socio-cultural information.
<b>Motor Vehicles</b>	Car reviews, vehicle purchasing or sales tips, parts catalogs; auto trading, photos, discussion of vehicles, including motorcycles, boats, cars, trucks and RVs; journals and magazines on vehicle modification, repair, and customization; online automotive enthusiast clubs.
<b>News</b>	Newspapers online; headline news sites, newswire services, and personalized news services; weather sites.
<b>Personals and Dating</b>	Singles listings, matchmaking and dating services; advice for dating or relationships; romance tips and suggestions.
<b>Photo Searches</b>	Sites that provide resources for photo and image searches.
<b>Rating Unavailable</b>	Yet to be categorized, not categorized, or the rating is temporarily unavailable.
<b>Real Estate</b>	Home, apartment, and land listings; rental or relocation services; tips on buying or selling a home; Home loan and mortgage information; real estate agents; home improvement.
<b>Reference</b>	Personal, professional, or educational reference; online dictionaries, maps, and language translation sites; census, almanacs, and library catalogues; topic-specific search engines.

<b>Religion</b>	Churches, synagogues, and other houses of worship; any faith or religious beliefs, including “alternative” religions such as wicca and witchcraft.
<b>Remote Proxies</b>	Remote proxies or anonymous surfing.
<b>Search Engines</b>	General search engines (Google, Yahoo, etc.)
<b>Sex Education</b>	<p>Pictures or text advocating the proper use of contraceptives, including condom use, the correct way to wear a condom and how to put a condom in place; Sites relating to discussion about the use of the Pill, IUDs and other types of contraceptives; discussion sites on how to talk to your partner about diseases, pregnancy and respecting boundaries.</p> <p><b>Note:</b> Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Adult/Sexually Explicit category.</p>
<b>Shopping</b>	Internet malls and online auctions; department stores, retail stores, company catalogs online; online downloadable product warehouses; specialty items for sale; freebies or merchandise giveaways.
<b>Sports</b>	Team or conference web sites; national, international, college, professional scores and schedules; sports-related online magazines or newsletters.
<b>Streaming Media</b>	<p>Streaming media files or events (any live or archived audio or video file).</p> <p><b>Note:</b> Not included in the category are sites that have streaming media on them.</p>
<b>Travel</b>	Airlines and flight booking agencies; accommodation information; travel package listings; city guides and tourist information; weather bureaus.
<b>Usenet News</b>	Newsgroups accessed through the HTTP protocol.
<b>Web-based Email</b>	Sites that provide web-based email accounts.



## Copyright

© 1996-2006, Global Technology Associates, Incorporated (GTA). All rights reserved.

Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

## Technical Support

GTA includes 30 days “up and running” installation support from the date of purchase. See GTA’s web site for more information. GTA’s direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local GTA authorized channel partner.

**Tel:** +1.407.380.0220    **Email:** support@gta.com

## Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

## Trademarks & Copyrights

GNAT Box, GB Commander and Surf Sentinel are registered trademarks of Global Technology Associates, Incorporated. GB-OS, RoBoX, GB-Ware and Firewall Control Center are trademarks of Global Technology Associates, Incorporated. Global Technology Associates and GTA are registered service marks of Global Technology Associates, Incorporated.

The GTA Mobile VPN Client is licensed from TheGreenBow.

Microsoft, Internet Explorer, Microsoft SQL and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

BIND is a trademark of the Internet Systems Consortium, Incorporated and University of California, Berkeley.

WELF and WebTrends are trademarks of NetIQ.

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Java software may include software licensed from RSA Security, Inc.

Some products contain software licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

SurfControl is a registered trademark of SurfControl plc. Some products contain technology licensed from SurfControl plc.

Some products include software developed by the OpenSSL Project (<http://www.openssl.org/>).

Kaspersky Lab and Kaspersky Anti-Virus is licensed from Kaspersky Lab Int. Some products contain technology licensed from Kaspersky Lab Int.

Mailshell and Mailshell Anti-Spam is a trademark of Mailshell Incorporated. Some products contain technology licensed from Mailshell Incorporated.

All other products are trademarks of their respective companies.

## Global Technology Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • Fax: +1.407.380.6080 • Web: <http://www.gta.com> • Email: [info@gta.com](mailto:info@gta.com)

