

Surf Sentinel[®]

Feature Guide



SSFG200912-01



Table of Contents

Introduction	1
About Surf Sentinel Subscriptions	1
Features	1
Requirements	1
Registration & Activation	2
Feature Activation Codes	2
About this Guide	2
Conventions	2
Managing Internet Access	3
Surf Sentinel Proxy	3
Surf Sentinel Policies	3
Local Allow and Local Deny Lists	3
Remote Logging	4
Internet Access Policy	5
Steps to Implementation	5
Using Surf Sentinel	6
Activation	6
Automatic Activation	6
Manual Activation	6
Configuration	7
Surf Sentinel Policies	7
Content Filtering Facilities	8
Content Blocking	8
Surf Sentinel Categories	9
Advanced Surf Sentinel Policy Settings	9
Example Policy Settings	10
Example 1: Restricting Access to Specific Destinations	10
Example 2: Blocking Content from Specific Web sites	11
Creating the First Surf Sentinel Policy	11
Creating the Second Surf Sentinel Policy	12
Sorting the Surf Sentinel Policy List	12
Local Allow/Deny Lists	13
Surf Sentinel Proxy	14
Enabling the Traditional Proxy	15
Transparent Proxy	15
Using Both Proxy Types	15
Block Actions	15
Licensing	16
Expired Licenses	16
Reference A: Categories	17
Denied by Default	17
Allowed by Default	18
Reference B: Category Mapping	22
New Categories for Surf Sentinel with GB-OS 5.0.6 and Above:	22



Introduction

About Surf Sentinel Subscriptions

Surf Sentinel is GTA's Internet access management and content filtering subscription service for GTA Firewall UTM Appliances using over 70 content categories.

Surf Sentinel 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, that combines blocking, monitoring and policy management in a centrally managed, out-sourced solution. When used in conjunction with GB Commander or GTA Reporting Suite (available separately), real-time Internet usage reports are available from current and historical firewall log data.

Surf Sentinel provides URL filtering via access to a database of over 100 million categorized URLs into over 70 categories. Categories are updated on a daily basis.

Features

- Over 70 content categories for access control.
- Customizable local allow and local deny address objects.
- Over 100 million categorized URLs.
- Easy administration and enforcement of acceptable use policies.
- Economical deployment.
- No additional hardware required.
- Reports available through GB Commander or GTA Reporting Suite (available separately).

Requirements

- GB-OS version 5.0.6 and above.
- Web browser and Internet connection.
- GTA Firewall UTM Appliance or GB-Ware 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 for GB-OS require activation codes. Surf Sentinel activation can be automated or entered manually through the GB-OS Web interface.

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 UTM Appliance. The activation code is also accessible through the GB-OS Web interface by navigating to **Configure>Configuration>Runtime>Update**. If no updates display, click on **Check Now**. All available feature codes and runtime updates will display.



Note

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

About this Guide

This feature guide is a supplement to the *GB-OS User's Guide*. It illustrates the activation and use of the Surf Sentinel subscription service for GB-OS 5.0.6 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.

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



Managing Internet Access

GTA's Internet access management solutions provide the ability to control Web access based on site content. GB-OS has three primary functions for access control: Surf Sentinel proxy settings, Surf Sentinel policies and local allow/deny lists. In addition, records of blocked sites can be created and sent to GTA firewall logs.

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 or 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 page requests. With every Web page request, GB-OS 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 address objects 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 by GB-OS. 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*.

```
May 15 18:37:16 pri=5 msg="Accept persistent outbound, NAT" cat _
action=pass cat _site="Sports" dstname=www.cmdarts.com proto=80/
tcp src=192.068.71.199 srcport=3817 nat=24.227.126.130 natport=3817
dst=64.34.176.47 dstport=80 rule=11 duration=6 sent=1205 rcvd=12709
pkts _sent=11 pkts _rcvd=12 op=GET arg=/images/newlogo.gif
```

Figure 1.1: Surf Sentinel Persistent Connection Message

```
May 15 18:39:03 pri=5 msg="Accept outbound, NAT" cat _action=pass
cat _site="News and Media" dstname=technology.timesonline.co.uk
proto=80/tcp src=192.068.71.199 srcport=2452 nat=24.227.126.130
natport=2452 dst=72.247.134.216 dstport=80 rule=11 duration=327 sent=260
rcvd=636 pkts _sent=5 pkts _rcvd=3 op=GET arg=/tol/img/global/chevron-
back-to-top.gif
```

Figure 1.2: Surf Sentinel Proxy Accept Message

```
May 15 18:39:27 pri=4 msg="Block outbound, NAT" cat _action=block
cat _site="Adult and Pornography" dstname=www.playboy.com proto=80/
tcp src=192.068.71.199 srcport=3827 nat=24.227.126.130 natport=3827
dst=216.163.137.3 dstport=80 rule=11 duration=22 sent=486 rcvd=48 pkts _
sent=3 pkts _rcvd=1 op=GET arg=/favicon.ico
```

Figure 1.3: Surf Sentinel Proxy Deny Message

Table 1.1: Content Logging Fields	
Field	Description
pri	Priority of log message.
msg	Message indication Accept or Block.
cat_action	Action taken.
cat_site	Surf Sentinel category, Local Accept or Local Deny.
dstname	Web site accepted or blocked by this action.
proto	Protocol (HTTP).
src	Source IP address of the Web request.
srcport	Port through which the Web request was made.
op	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 bandwidth abuse, potential legal liability and lost productivity. For example, schools and libraries can set their Surf Sentinel policies to prevent access to Web sites that may not be appropriate for the workstation user's age.

When content filtering has been configured and Surf Sentinel is enabled, the 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:

1. Develop an Internet Access Policy and create acceptable user guidelines.
2. Create address objects and/or user groups in GB-OS to define the various users and groups whose access you will be controlling using Surf Sentinel.
3. 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.
4. 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.
5. 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. Instructions in this chapter assume a prior working knowledge of common GB-OS configuration tasks and settings. For detailed instructions on the operation and configuration of GB-OS, see the *GB-OS User's Guide*.

Activation

Surf Sentinel can only be activated after your GTA Firewall UTM Appliance or copy of GB-Ware has been registered through the [GTA Online Support Center](#).



Note

Activating Surf Sentinel will require the firewall to reboot.

Automatic Activation

Surf Sentinel can be automatically activated through the GB-OS Web interface. Navigate to **Configure>Configuration>Runtime>Update**. If no updates display, click on **Check Now**. All available feature codes and runtime updates will display. Click on **Update** and Surf Sentinel will be automatically activated.

Manual Activation

To manually activate Surf Sentinel, retrieve the feature activation code by logging into the [GTA Online Support Center](#) and navigate to **View Your Registered Products**. Select the serial number of your GTA Firewall UTM Appliance to display the activation code.

Next, login to GB-OS and navigate to **Configure>System>Activation Codes**. Click the **New** icon to enter the feature activation code in the next available line. **Save** the section. When an activation code is entered correctly, the **DESCRIPTION** field will indicate “GB-X–Surf Sentinel”, where X is your firewall’s product number.

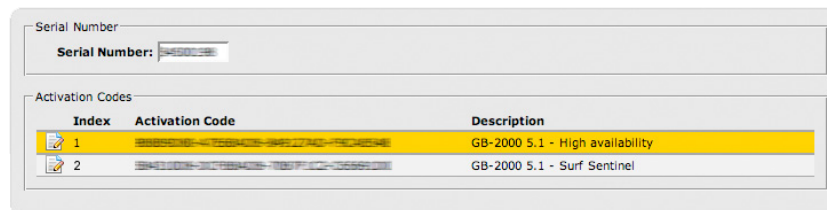


Figure 2.0: Surf Sentinel - Activated



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:

1. Define a DNS server (**Configure>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 **Configure>Threat Management>Surf Sentinel>Policies**. Click the **New** icon to define a new policy.

Figure 2.2: Configuring a Surf Sentinel Policy

**Table 2.0: Configuring a Surf Sentinel Policy**

Field	Description
Disable	Disables the policy.
Description	A description for the policy.
Source Address	If a request matches an element of the specified address object of type SURF SENTINEL, the packet will be compared to the policy.
Time Group	Select a user-defined time group in which the policy will be enabled. Time groups are defined at Configure>System>Objects>Time Groups .
Advanced	
Authentication Required	Enable to require users to authenticate with the GTA firewall using GBAuth. When enabled, a pull down will appear with configured user groups that will have the policy applied to them.
Destination Address	A selection of address objects that are of type ALL or SURF SENTINEL. Select <USER DEFINED> to manually enter a destination address.
Content Filtering Facilities	
Local Allow List	Enable to use the firewall's local allow list by selecting its address object.
Local Deny List	Enable to use the firewall's local deny list by selecting its address object.
Surf Sentinel	Enable to use the Surf Sentinel Categories list.
Content Blocking	
ActiveX Objects	Enable to block ActiveX controls.
Java	Enable to block Java applets.
Javascript	Enable to block Javascript.
Unknown HTTP Commands	Enable to block unknown HTTP commands and unencrypted HTTP protocols.
Surf Sentinel Categories	
Accept / Deny	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 Objects 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 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 ACCEPT and DENY 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 Web sites that would fall under the `Sports` category, select that category in the ACCEPT field (its default location) and click the --> button to move the `Sports` category to the DENY field. Categories can be reset to installation defaults at any time by selecting the **DEFAULT** button.

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



Note

See [Reference A: Categories](#) for more information on Surf Sentinel default categories.

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

Advanced Surf Sentinel Policy Settings

In addition to allowing or blocking by category, Surf Sentinel policies can 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 Web site, 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 **Configure>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
Authentication Required	Enable to require users to authenticate with the GTA firewall using GBAuth. When enabled, a pull down will appear with configured user groups that will have the policy applied to them.
Destination Address	A selection of address objects that are of type ALL or SURF SENTINEL. Select <USER DEFINED> to manually enter a destination address.

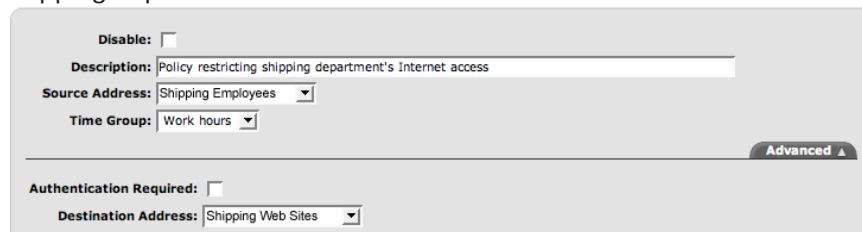
Example Policy Settings

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.) during work hours. To do so, two address objects of type ALL or SURF SENTINEL and a time group must be defined:

1. An address object, named Shipping Employees, containing the IP addresses of all employees belonging to the shipping department.
2. The time group, Work hours, is selected for the time periods in which this policy is applied.
3. An address object, named Shipping Web sites, containing all Web sites that the shipping employees will be granted access to. (In this example, fedex.com, ups.com and dhl.com.)
4. Once all necessary address objects have been defined, navigate to **Configure>Threat Management>Surf Sentinel>Policies** and click the **New** icon to define the policy that will be restricting the shipping department's Internet access.



Disable:

Description: Policy restricting shipping department's Internet access

Source Address: Shipping Employees

Time Group: Work hours

Advanced

Authentication Required:

Destination Address: Shipping Web Sites

Figure 2.4: Restricting Access to Specific Destinations

5. When defining the Surf Sentinel policy, select the **<Shipping Employees>** address object for the policy's SOURCE ADDRESS.
6. Select **<Work hours>** for the policy's TIME GROUP.
7. Under the Advanced tab, select the **<Shipping Web sites>** address object for the policy's DESTINATION ADDRESS.
8. Click **OK** and then **SAVE**. From now on, all IP addresses listed in the SHIPPING EMPLOYEES address object will be restricted to Web sites listed in the Shipping Web sites address object. All other Internet requests will be met with the Surf Sentinel proxy's configured BLOCK ACTION.



Example 2: Blocking Content from Specific Web sites

A company would like to disable JavaScripts from running on all Web sites except for those they explicitly allow. By using Surf Sentinel, JavaScripts and other potentially malicious content can be removed from Web sites, 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 Web sites.
2. A policy that blocks JavaScripts from running on all other Web sites.

Creating the First Surf Sentinel Policy

1. 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 Web sites must be defined.
2. Once the address object has been defined, navigate to **Configure>Threat Management>Surf Sentinel>Policies** and click the **New** icon to define the policy that will allow JavaScripts to be run on the desired Web sites.

The screenshot shows the configuration window for a Surf Sentinel policy. The 'Basic' tab is selected, displaying the following fields:

- Disable:**
- Description:** Allow Javascript on approved Web sites
- Source Address:** ANY_IP
- Time Group:** ALWAYS

The 'Advanced' tab is also visible, showing the following options:

- Authentication Required:**
- Destination Address:** Approved Sites
- Content Filtering Facilities:**
 - Local Allow List:**
 - Local Deny List:**
 - Surf Sentinel:**
- Content Blocking:**
 - ActiveX Objects:**
 - Java:**
 - JavaScript:**
 - Unknown HTTP Commands:**

Figure 2.5: Allowing JavaScripts to be Run on Specific Web sites

3. When defining the Surf Sentinel policy, select **<ANY IP>** for the policy's SOURCE ADDRESS.
4. Under the **ADVANCED** tab, select the **<Approved Sites>** address object for the policy's DESTINATION ADDRESS.
5. In the **CONTENT BLOCKING** box, ensure the **JAVASCRIPT** option is unchecked.
6. Click **OK** and then **SAVE**. You have now created the Surf Sentinel policy that will allow all IP addresses trying to access Web sites listed in the Allow JavaScript address object to view those Web sites with JavaScripts intact.

Next, you must create a Surf Sentinel policy that will block all other Web sites from running Javascript.

Creating the Second Surf Sentinel Policy

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

Figure 2.6: Blocking JavaScripts on All Other Web sites

5. Click **OK** and then **SAVE**. You have now created the Surf Sentinel policy that will block JavaScripts from running on all other Web sites.

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 Web sites) is placed above the second policy (that blocks JavaScripts on all other Web sites). If the order is reversed, the deny policy will match before the allow policy, resulting in JavaScripts being stripped from all Web sites, regardless if they are in the Approved Sites address object or not.

Index	Source Address	Description
1	<ANY_IP>	Allow JavaScript on approved websites
2	<ANY_IP>	Block JavaScript 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 **Configure>System>Objects>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.

Disable:

Name: Local allow

Description: Surf Sentinel local allow list

Type: All Surf Sentinel Mail Sentinel Network Security Policies VPN

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

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
Traditional Proxy	
Enable	Enables the traditional proxy.
Port	The port through which the proxy will run. Default is 2784.
Advanced	
Automatic Policies	A toggle for whether the firewall should automatically generate the required policies for the Surf Sentinel proxy to function. If unselected, it is necessary to define remote access policies. View at Monitor>Activity>Security Policies .
Transparent Proxy	
Enable	Enables the transparent proxy.
Block Action	
Action	A selection for the action to be performed when a request for blocked content is performed.
Message	If <Use message> is selected for the ACTION, the entered message will be displayed. Default is Local policy denies access to Web page.
URL	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 attempts to load a page from that address, the user will see a custom message, or be redirected to a URL (e.g., an internal Web site that defines the company's Internet policies and the administrative process to gain access to a blocked Web site).



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. Block actions on SSL will not display a block message.

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 upgrading Surf Sentinel licenses for additional users.

Expired Licenses

If the Surf Sentinel license has expired, a message will be displayed in the Web browser and a “License expired” log message will be generated by the firewall. A verification warning that the license has expired will also display in the GB-OS Web interface.

```
May 24 07:58:16 pri=4 msg="Block outbound, NAT" cat_action=block cat_site="License expired" dstname=l.yimg.com proto=80/tcp src=192.068.172.4 srcport=63652 nat=69.244.247.28 natport=63652 dst=209.73.188.78 dstport=80 rule=2 duration=22 sent=530 rcvd=44 pkts_sent=3 pkts_rcvd=1 op=GET arg=/a/i/ww/thm/1/grd-lpx_1.4.gif
```

Figure 3.1: Surf Sentinel License Expired Log Message



Reference A: Categories

Surf Sentinel contains over 70 categories for the administrator to use when customizing Surf Sentinel policies. A special category for Web sites that do not fit neatly into a category and for requests that do not return a rating is `UNCATEGORIZED`.



CAUTION

GTA recommends reviewing default category settings and modifying them to match your corporate Internet Access Policy.

Denied by Default

Categories denied by default are as follows:

Table A.1: Default Denied Categories	
Category	Description
Abused Drugs	Sites that provide discussion or remedies for illegal, illicit, or abused drugs such as heroin, cocaine, or other street drugs. Information on “legal highs”: glue sniffing, misuse of prescription drugs or abuse of other legal substances.
Adult and Pornography	Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. Adult products including sex toys, CD-ROMs, and videos. Online groups, including news groups and forums, that are sexually explicit in nature. Erotic stories and textual descriptions of sexual acts. Adult services including video conferences, escort services, and strip clubs. Sexually explicit art.
Confirmed Spam Sources	Sites- usually IP addresses- that have been reported to be origination sources of Spam by trusted sources.
Cult and Occult	Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, satanic or supernatural beings. Includes sites containing alternative religions such as Wicca or witchcraft.
Hacking	Sites providing information on hacking, or illegal, or questionable access to or the use of communications equipment/software.
Malware Sites	Sites that carry malicious content including executables, scripts, or viruses.
Marijuana	Sites covering Marijuana.
Nudity	Sites containing nude or semi nude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals
Online Gambling	Online gambling or lottery Web sites that invite the use of real or virtual money. Information or advice for placing wagers, participating in lotteries, gambling, or running numbers. Virtual casinos and offshore gambling ventures. Sports picks and betting pools. Virtual sports and fantasy leagues that offer large rewards or request significant wagers. Casino/Hotel/Resort sites that do not enable gambling on the site are categorized in Travel.
Open HTTP Proxies	Sites- typically IP addresses- that can be used as http proxies.
Phishing and Other Frauds	Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user.
Proxy Avoidance and Anonymizers	Sites providing information on how to bypass proxy server features or gain access to URLs in any way that bypasses the URL filter or proxy server. Web-based translation sites that circumvent filtering.

Table A.1: Default Denied Categories	
Category	Description
Questionable	Sites that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. Also includes sites that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics. Includes questionable humor, or sites that promote the purchase of academic content such as term papers or book reports for the purpose of plagiarism. Also includes “get rich quick” sites that promise easy financial gains for some investment or participation by the user.
Spam URLs	URLs contained in Spam.
Spyware and Adware	Sites Associated with Spyware or Adware. Sites that provide or promote information gathering, tracking, or enabling of ad delivery that is unknown to, or without the explicit consent of, the end user or the organization.
Swimsuits and Intimate Apparel	Sites that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing.
Weapons	Sites that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications.
Web Advertisements	Sites that provide online advertisements or banners.

Allowed by Default

Categories allowed by default are as follows:

Table A.2: Default Allowed Categories	
Category	Description
Abortion	Sites whose main purpose is to inform users about abortion, including pro-choice and pro-life sites, or sites which articulate a particular philosophy toward or opposition to abortion. Sites that provide information or arguments in favor of a woman’s choice, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion. Sites that provide information or arguments in against a woman’s choice, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.
Alcohol and Tobacco	Sites that provide information about, promote, or support the sale of alcoholic beverages or tobacco products, or associated paraphernalia.
Auctions	Sites that support the offering and purchasing of goods between individuals as their main purpose. Does not include classified advertisements.
Botnets	Sites that are part of a botnet.
Business and Economy	Sites devoted to business firms, business information, economics, marketing, business management and entrepreneurship. Includes corporate Web sites.
Computer and Internet Information	General computer and Internet sites, technical information.
Computer and Internet Security	Computer\Internet security sites, security discussion groups.
Content Delivery Networks	Sites whose main purpose is to deliver third party content, such as images, links, or text.
Dating	Dating Web sites focused on establishing personal relationships.
Dead Sites	These are dead sites that do not respond to http queries.
Dynamically Generated Content	Sites that read information from an end user’s browser- typically cookies- and which generate content based on that information.



Table A.2: Default Allowed Categories

Category	Description
Educational Institutions	Sites with pre-, elementary, secondary, and high school educational content and information, and well as university Web sites.
Entertainment and Arts	Sites that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment. Performing arts (theatre, vaudeville, opera, symphonies, etc.). Museums, galleries, artist sites (sculpture, photography, etc.). Includes sites about celebrities and famous people.
Fashion and Beauty	Fashion or glamour magazines online Beauty and cosmetics
Financial Services	Sites that provide or advertise banking services (online or offline) or other types of financial information, such as loans. Includes accountancy, actuaries, banks, mortgages, and general insurance companies. Does not include sites that offer market information, brokerage or trading services.
Games	Sites that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. Also includes sites dedicated to selling board games as well as journals and magazines dedicated to game playing. Includes sites that support or host online lotteries, sweepstakes, and giveaways.
Government	Sites sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. Also includes sites that discuss or explain laws of various governmental entities. Includes local, county, state, and national government sites, as well as international governmental institutions.
Health and Medicine	General health such as fitness and well-being, including western and eastern methods and topics. Medical information and reference about ailments, conditions. Dentistry, optometry, and other medical-related sites. General psychiatry and mental well-being. Hospital, medical insurance. Medical procedures, including elective and cosmetic surgery. It includes alternative and complementary therapies, including: yoga, chiropractic and cranio-sacral analysis.
Home and Garden	Sites covering issues revolving around the home, including maintenance, home safety, décor, cooking, home electronics, design, etc
Hunting and Fishing	Sport hunting, gun clubs, and fishing sites.
Image and Video Search	Sites that provide resources for photo and image searches, Online photo albums/digital photo exchange, Image hosting;
Individual Stock Advice and Tools	Sites that provide or advertise trading of securities and management of investment assets (online or offline). Also includes sites that offer financial investment strategies, quotes, and news.
Internet Communications	Sites that include Instant Messaging or Internet Telephony clients, or VoiP clients or services. News sites covering the computer industry and the Internet. Sites where Internet Telephony clients can be downloaded
Internet Portals	Web sites that aggregate a broader set of internet content, and which typically serve as the starting point for an end user interested in that class of Web site, such as MSN or Yahoo. Does not include Adult Web sites.
Job Search	Sites that provide assistance in finding employment, and tools for locating prospective employers, or employers looking for employees.
Keyloggers and Monitoring	Sites that provide or discuss the usage of software agents that track a user's keystrokes or monitor their Web surfing habits.
Kids	Sites designed specifically for children.
Legal	Legal Web sites, including sites of law firms, and sites that discuss or analyze legal issues
Military	Sites that promote or provide information on military branches or armed services, including sites that discuss military topics, such as military strategy or military history sites

**Table A.2: Default Allowed Categories**

Category	Description
Motor Vehicles	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.
News and Media	Sites that primarily report information or comments on current events or contemporary issues of the day. Also includes radio stations and magazines. Newspapers online, Headline news sites, news wire services, and personalized news services, Weather sites.
Online Greeting Cards	Online greeting card sites.
Online Music Sales	Sites that distribute music for download, including sites that sell music.
Online Personal Storage	Sites that offer personal online storage, including documents, photos or other individual information.
Parked Domains	Domains that are not active, but contain content. These include domains that monetize traffic to the domain using paid listings from an ad network, or are domains “squatters” own hoping to sell the domain name for a profit.
Pay to Surf	Sites that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or Web pages.
Peer to Peer	Sites where peer to peer clients can be downloaded or peer to peer content is hosted.
Personal Sites and Blogs	Personal Web sites posted by individuals or groups, as well as blogs. Some content may be for mature audiences.
Philosophy and Political Advocacy	Sites that discuss or advocate philosophy and political advocacy.
Private IP Addresses	IP addresses defined in RFC 1918, ‘Address Allocation for Private Intranets.
Real Estate	Sites that provide information on renting, buying, or selling real estate or properties. Tips on buying or selling a home. Real estate agents, Rental or relocation services, and Home improvement.
Recreation and Hobbies	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 Traditional (board, card, etc.) games and their enthusiasts Animal/pet related sites, including breed-specific sites, training, shows and humane societies;
Reference and Research	Sites containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related sites and scientific information.
Religion	Sites that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. Does not include sites containing alternative religions such as Wicca or witchcraft (Cult/Occult) or atheist philosophies (Political/Activist Groups).
Search Engines	Web sites that enable the user to conduct searches, including by key words, images, or phrases.
Sex Education	Sites that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. Also includes sites that offer tips for better sex as well as products used for sexual enhancement. Sites with text or pictures advocating the proper use of contraceptives or which discuss sexually transmitted diseases.
Shareware and Freeware	Sites that offer the downloading of software that is free or free to test, or ask for a contribution to aid with development, including open source software.
Shopping	Department stores, retail stores, company catalogs and other sites that allow online consumer or business shopping. Sites that provide or advertise the means to obtain goods or services as their main purpose.



Table A.2: Default Allowed Categories	
Category	Description
Social Networking	Sites used for social networking such as Facebook and Myspace.
Society	Web sites that cover a variety of topics relevant to the general populace, such as broad issues that impact a variety of people, safety, societal issues, adoption, etc. These sites usually represent an area of one or more “special interests” to some segment of Society, are considered benign from a policy standpoint, and are not covered by other categories.
Sports	Team or conference Web sites, international, national, international, college, professional scores and schedules, Sports-related online magazines or newsletters or fantasy sports.
Streaming Media	Sites that sell, deliver, or stream music or video content in any format, including sites that provide downloads for such viewers. Personal (non-explicit) Webcams or sites with real time views of points of interest or traffic.
Tourist Information	City guides and tourist information, including restaurants and local points of interest.
Training and Tools	Distance education and trade schools, including online courses. Online vocational training. Online software training, skills training, teacher resources (lesson plans, etc.).
Translation Sites	Sites providing language translation.
Travel	Airlines and flight booking agencies. Sites that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos. Car Rentals.
Uncategorized	Sites which do not fit into any specific category.
Unconfirmed Spam Sources	Sites (usually IP addresses) that may be origination sources of Spam.
Web Based Email	Sites offering Web based email and email clients.
Web Hosting	Sites that provide Web hosting services to clients.

Reference B: Category Mapping

GB-OS 5.0.6 and above include enhancements to Surf Sentinel category listings. The Surf Sentinel categories will be modified when a GTA firewall running GB-OS 5.0.5 or below is updated to GB-OS 5.0.6 or above. Existing Surf Sentinel categories will be automatically mapped to the enhanced categories. This automatic mapping is detailed in the chart below. For example, a policy set to deny *Weapons* will now deny both *Weapons* AND *Military* categories.

There are new Surf Sentinel categories which are included with GB-OS 5.0.6 that have no comparable category in Surf Sentinel versions with GB-OS 5.0.5 and below. These categories are allowed by default. If this does not match your corporate Internet Access Policy, you should revise your Surf Sentinel settings for these categories.



Note

GTA strongly recommends reviewing the settings for all (new and automatically mapped) categories and making any necessary revisions to your Surf Sentinel settings and policies to ensure they meet your corporate Internet Access Policy.

New Categories for Surf Sentinel with GB-OS 5.0.6 and Above:

- Abortion
- Business and Economy
- Dead Sites
- Dynamically Generated Content
- Legal
- Online Greeting Cards
- Online Personal Storage
- Parked Domains
- Pay to Surf
- Private IP Addresses

Table B.1: Category Mapping

Category Name (5.0.5 and Below)	Category Name(s) (5.0.6 and Above)
Adult/Sexually Explicit	Adult and Pornography Nudity
Advertisements	Web Advertisements
Arts & Entertainment	Entertainment & Arts
Chat	Internet Communications Peer to Peer
Computing & Internet	Computer and Internet Information Computer and Internet Security Shareware and Freeware
Criminal Skills	Questionable
Drugs, Alcohol & Tobacco	Abused Drugs Alcohol and Tobacco Marijuana
Education	Educational Institutions
Finance & Investment	Individual Stock Advice and Tools Financial Services
Food & Drink	Tourist Information
Gambling	Online Gambling
Games	Games



Table B.1: Category Mapping

Category Name (5.0.5 and Below)	Category Name(s) (5.0.6 and Above)
Glamour & Intimate Apparel	Swimsuits and Intimate Apparel Fashion and Beauty
Government and Politics	Government Philosophy and Political Advocacy
Hacking	Botnets Confirmed Spam Sources Hacking Keyloggers and Monitoring Malware Sites Phishing and Other Frauds Spam URLs Spyware and Adware Unconfirmed Spam Sources
Hate Speech	Questionable
Health & Medicine	Health & Medicine
Hobbies & Recreation	Home and Garden Hunting and Fishing Personal Sites and Blogs Recreation and Hobbies
Hosting Sites	Web Hosting
Job Search & Career Development	Job Search
Kid's Sites	Kids
Lifestyle & Culture	Society
Motor Vehicles	Motor Vehicles
News	News and Media
Personals & Dating	Dating
Photo Searches	Image and Video Search
Real Estate	Real Estate
Reference	Reference and Research Training and Tools
Religion	Cult and Occult Religion
Remote Proxies	Content Delivery Networks Proxy Avoidance and Anonymizers Open HTTP Proxies
Search Engines	Internet Portals Search Engines
Sex Education	Sex Education
Shopping	Auctions Online Music Sales Shopping
Sports	Sports
Streaming Media	Streaming Media
Travel	Travel
Rating Unavailable	Uncategorized
Usenet News	Uncategorized
Violence	Questionable
Weapons	Weapons Military
Web Based Email	Web Based Email



Copyright

© 1996-2009, 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 Authorized GTA 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

GB-OS, Surf Sentinel, Mail Sentinel and GB-Ware are registered trademarks of Global Technology Associates, Incorporated. GB Commander is a trademark of Global Technology Associates, Incorporated. Global Technology Associates and GTA are service marks of Global Technology Associates, Incorporated.

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/or 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/>.

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

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