TECHNICAL SERVICE BULLETIN (TSB)

Changes to Google

AND HOW IT MAY AFFECT YOU

ComSifter®
protect web users now!

TSB Date: May 12, 2011

IN THIS DOCUMENT

For reasons that are beyond Comsift's control, Google has recently been making changes to how their services are accessed. More and more they are trying to obscure the identity of the user making search inquiries.

These changes affect how ComSifter filters Google. This document details what the changes are, and how you can protect your users.

DIRECTORY STRUCTURE

In the past, Google used a standard web site directory structure. The main domain name was `google.com`. Sub-domains were labeled `images.google.com`, `video.google.com`, etc. These sub-domains were easily blocked by the ComSifter without affecting the main search page at `google.com`.

Google has restructured all of their services using one large JavaScript. No longer can you block `images.google.com`, as it no longer exists. ComSifter does not have the ability to look into applications (which are using JavaScript).

This leaves us with the question: Can ComSifter selectively block Google Images while still allowing the `google.com` search page? The short answer is: No. ComSifter does not have the ability to look into applications (which are using JavaScript). Comsift is exploring enhancement to the product to try and resolve this issue, but for the time being, if you do not want your users viewing Google Images then you will need to block `google.com` in its entirety and use an alternate search engine.

ENCRYPTED SEARCHING

Google has also changed how its main search page operates. In the past, all Google searches were done over port 80 (HTTP) and were un-encrypted. Google is slowly converting over to secure searches over port 443 (HTTPS). What does this mean to your users? If your user types in `encrypted.google.com` they will be taken to a secure website and all searches will be encrypted. If the browsers are set transparently (which they are by default), the ComSifter will not see the user or what they are searching. If the local network is operating in Proxy Mode then you will see the user and their searches.

WHAT CAN WE DO TO STOP THESE SECURE SEARCHES?

First, browsers must be running in Proxy Mode. If they are not, then call Comsift Support at 866-875-1254 x2 to discuss and request a white paper on Transparent vs Proxy Mode.

Next, add `encrypted.google.com` to the Banned Domain List. When the user goes to this site they will be redirected to the un-encrypted Google search page at `http://google.com`.

WHAT DOES GOOGLE SAY ABOUT ALL THIS?

The following are excerpts from Google's response posted on their website:

- How will SSL search affect our content filtering services?

  When students search using `https://encrypted.google.com`, their searches will bypass

CONTINUED

Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com

any content filters that are in place on your network. If this is problematic for your school, you can block `https://encrypted.google.com`. When students continue to search using `http://www.google.com`, your content filtering will work as it always has in the past.

If your students try searching via the `https://www.google.com` homepage, they will be redirected to `https://encrypted.google.com` and will not be able to perform encrypted searches to bypass content filters.

- If I block access to `https://www.encrypted.google.com`, will I block access to all of Google's authenticated services (like Google Apps for Education)?

  No; logins for Google Apps for Education and our other authenticated services are currently hosted at `https://www.google.com`. As long as you allow access to `https://www.google.com`, your organization should still be able to access all of our other services.

The above information is located under the section ***Information for School Administrators*** at the link:
http://www.google.com/support/websearch/bin/answer.py?hl=en&answer=173733

Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com