

[Web Filtering Update – February 2007](#)

Web Filtering in Ontario School Boards

New in this Update –

In our **November School Board Update**, we told you about many of the more applicable ContentKeeper features that will deliver greater protection against unauthorized Internet access and Web browsing in the school environment (see below for “**Previously described CKWeb Features**”)

The following recently delivered CKWeb features are designed to provide even greater network security when Internet sessions are **initiated through irregular and unauthorized avoidance techniques**.

Being who they are, it is clear that there are many ways for IT-savvy, senior students to **bypass network security** in accessing the Internet. ContentKeeper will continue to address these challenges and we're pleased to let you know about our most recent advances:

- Various techniques are used to try to bypass filtering systems, including **Proxy sites, TLS/SSL Tunneling**, and **Scripting** methods.
- New protocols such as **Skype and music/video sites** can be the source of massive bandwidth usage.
- Various **non-standard Search Engines** are also used to discover inappropriate content not yet on blocking lists.

Protection from all of these threats is now available to users of ContentKeeper Web Filtering (CKWeb) and its superior Ethernet-bridge appliance design.

The most recent CKWeb release includes these extensions to our standard filtering features. These features are easily selected in the CKWeb Blocking Policy process that is accessed via our standard, browser-based Administrator interface....***Select and click and the enhanced protection is in place.***

With previously delivered **Keyword Blocking** for Search Engine sites, **Custom URLs** with wildcards, **Protocol blocking**, and the **"Force Google Strict SafeSearch"** options (see Related Notes), CKWeb provides the ability to manage student browsing activity to a greater extent than ever, to keep inappropriate web content out of Ontario schools.

Related Notes:

- All Internet searches can be directed by CKWeb to Google's **"Strict SafeSearch"** option.
- CKWeb Keyword Blocking allows you to define banned keywords in search engine submit strings.
- Proxy Sites are classified into the CKWeb URL Category for these, or may be identified by clients via Custom URL or Custom Categories selections. ContentKeeper's patented **Collaborative Filtering** process identifies new proxy sites and blocks them immediately. ContentKeeper's worldwide collection process delivers all new sites found elsewhere to your database **on an hourly basis**.
- ContentKeeper's Protocol blocking section now protects you from more than 80+ protocols - new protocols are added on an ongoing basis as they are discovered. ContentKeeper's superior **Transparent Ethernet Bridge** design is well-equipped to monitor and manage these threats.

The following **ContentKeeper Modules** can provide additional **management oversight** of the security avoidance techniques described above:

- **CK-Monitor** provides **real-time monitoring** of student activity by automatically scanning log files for your pre-set thresholds and alarm conditions.
- **CK-ARM** (Advanced Reporting Module) provides fully-featured, template-driven, **automated reporting** for any volume of student activity - with automated delivery to designated management desktops.

Please contact us at the locations shown on page 3 below for more information on these latest, and other ContentKeeper capabilities. The following screen shots are examples of the CKWeb Administrator interface and some of the key features described above.

Web Filtering Update – February 2007

CKWeb Administration Screens

The screen segments below demonstrate some of the advanced features delivered by ContentKeeper for the development of effective filtering Policies for students, including (clockwise from top-left): search-engine keyword blocking; Google thumb image replacement and "Force Google Strict SafeSearch"; User-defined Protocol blocking; blocking of HTTP Post/Get and SSL tunneling; P2P Protocol blocking.

Click Here to enable Keyword Matching against URL Arguments for this Policy.

Keywords	URLS
4teen	ask.jp
4teens	au.altavista.com
adult	ca.altavista.com
adultos	emulti.pl
adultpics	gooru.pl
al4a	images.google
amateur	netsprint.pl
amateur-facials	search.aol.ca
amateur-facialspodryv	search.aol.co.uk
amateurpages	search.aol.com
	search.aol.com.au

When a Keyword is found:

Replace Google Thumb Images	<input type="text" value="Yes"/>
Force Google Strict Filtering (SafeSearch)	<input type="text" value="Yes"/>
Replace Image Components	<input type="text" value="No"/>
HTTP Header Error Code for Block Pages	<input type="text" value="403 Forbidden"/>
Block JavaScript URLs with HTML or JavaScript	<input type="text" value="JavaScript"/>
Coach Block Page Frequency for all Sites	<input type="text" value="60 Seconds"/>
Coach Block Page for SSL Sites	<input type="text" value="Simple"/>
Apply Special Category Classification	<input type="text" value="Yes"/>

Note In ContentKeeper, an Image is a URL ending with one of the following file type suffixes: (.jpg, .jpeg, .gif, .bmp, .png)

Google Thumb Images

For Google Thumb Images, if the Image is NOT in the Allow or the Non-Managed state but classified as Adult Content it will be replaced with the first image, while those classified in all other Categories will be replaced with the second image.



Force Google into Strict Filtering

Google's SafeSearch blocks web pages containing explicit sexual content from appearing in search results.

See [Google's Safe Search](#) facility for more information.

ContentKeeper can force Google to operate in Strict Filtering (mode 1)

Peer to Peer / File Transfer					
#	Code	Protocol Description	Report	Block	Help
1	FTP	File Transfer Protocol	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>

Proxy					
#	Code	Protocol Description	Report	Block	Help
1	GHOSTSURF	Anonymous proxy network	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>
2	SOCKS	SOCKS Proxy Protocol	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>

Web					
#	Code	Protocol Description	Report	Block	Help
1	GOPHER	Gopher Protocol	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>
2	HTTPS	HTTP over SSL	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>

Mail and Cooperation					
#	Code	Protocol Description	Report	Block	Help
1	IMAP	Mail transfer to end user	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>
2	NETMEETING	Virtual meetings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>
3	NNTP	Network News Transfer Protocol	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>
4	NNTPS	Secure Network News Transfer Protocol	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 8px;" type="button" value="?"/>

ContentKeeper Rules for Policy : **newpolicy1**

Other Policy Rules	
Report Blocked URLs in Blocking/Click-Thru Reports	<input type="text" value="Yes"/>
Generate a Blocking Page if URL Blocked	<input type="text" value="Yes"/>
Anonymize Source IP Address in all reports	<input type="text" value="No"/>
Anonymize Username in all reports	<input type="text" value="No"/>

HTTP Request Methods	
Block all HTTP GET Requests	<input type="text" value="No"/>
Block all HTTP POST Requests	<input type="text" value="No"/>
Block all HTTP CONNECT Requests (SSL)	<input type="text" value="Block"/>

CONTENTKEEPER CONTENTKEEPER TECHNOLOGIES

User Defined Protocols

Select Protocol Code Name	<input type="text"/>
Enter Protocol Code Name (Maximum 14 Characters)	<input type="text"/>
Protocol Description (Maximum 60 Characters)	<input type="text"/>
TCP Port Numbers (Port numbers semi-colon separated)	<input type="text"/>
UDP Port Numbers (Port numbers semi-colon separated)	<input type="text"/>
Detail Description (1024 Characters)	<input type="text"/>

ContentKeeper continues to be the leading provider of blocking technology for emerging methods which attempt to defeat Internet filtering systems.

.....please refer to the next page for previously described CKWeb features.

[Web Filtering Update – February 2007](#)

CKWeb features described in recent updates:

The following ContentKeeper features, either individually or together, may be useful to School Boards where Web browsing is allowed within guidelines, but where some controls may be required to identify exceptions to guidelines and to allow Board oversight and intervention in some extreme cases. ContentKeeper provides these tools to be selected and implemented by each Board to meet each Board's individual requirements.

Filtering Profiles to fit Grades and Departments

ContentKeeper Web Filtering features provide each Board with the ability to define filtering profiles by Grade or Department to reflect each Board's guidelines and individual needs for protection. ContentKeeper also provides a number of features that allow trusted student groups a degree of self-monitoring of their Web activity.

Teacher Override Options

Various options are provided for authorized teachers to unblock specific Web sites for legitimate classroom work. This can apply to downloading excessive file sizes, material normally unrelated to schoolwork or material that is otherwise inappropriate. Overrides can be applied to an individual student or an entire class, for specific class durations or for specific workstations (e.g., in a lab), and can be configured in advance or as required in the classroom.

Administration Delegation with Audit Trail

This feature enables authorized department or school personnel to allow exceptions to standard filtering profiles but at the same time provide the Board administrator with an audit trail of the delegated actions.

Monitoring Facility with Automated Alert Delivery

"ContentKeeper Monitor" provides immediate observation and notification of user activity that is contrary to established Board guidelines, including the ability to send automated notification to designated staff, and provides full flexibility for limit setting such as bandwidth quantity & time thresholds.

Student Log-on Authentication

Authentication of individual users may aid in the investigation of inappropriate Web use in extreme situations where guidelines have been exceeded for downloads, excessive browsing or access to sites considered harmful, such as sites containing criminal, hate or similar material. This ContentKeeper feature may be useful where this functionality is not already available in existing network configurations.

Google Images

ContentKeeper blocks all identified Google thumbnail images, especially applicable for Web access by junior grades.

Performance

ContentKeeper Web Filtering is proven in organizations with Gigabit networks, as are used in many Ontario Boards.

Price

Recognizing the financial needs of the School Board community in Ontario, ContentKeeper has established a very competitive price that is available to all Boards that implement the ContentKeeper Web Filtering solution. For information on this Ontario School Board price and ContentKeeper's no-charge trial, please contact ContentKeeper Education Sales.

For information on other proven ContentKeeper Web Filtering features available to School Boards, such as information security, Collaborative Filtering, Gigabit networks, alerts and large information storage & reporting capability, please see the Contact information below.

Contacts

For sales, trial installation or additional information contact:

APL Borealis Inc. - Canada-wide distributor for ContentKeeper Technologies Inc.

(416) 457-7828 or info@aplborealis.com

1-866-888-6377 www.contentkeeper.ca

