smoothwall

The Web You Want

Connect for Chromebooks

Product Release: Glamis

Educating with Chromebooks

Google Chromebooks™ are fast becoming the global educational device of choice due to their simple setup, long battery life and low cost.

The up-front cost of a Google device has been a key factor in establishing their foothold in schools, with some machines retailing in the sub-£200 domain. Chromebooks are cheaper to repair or replace should they come to damage in the hands of over-eager children; the price point is so low that it can be easier just to replace a broken unit, saving service time.

As well as the lower initial outlay, the reductions in the cost of setup are huge when compared to traditional Windows-based machines or iPads. Setting up a Windows-based system involves deploying applications and imaging every laptop, which is time consuming for Systems Administrators. With iPads, apps also have to be loaded onto the device and need to match the needs of the user, and are often specific to their school grade. Once loaded, the need to keep these systems up to date can provide a constant workload across networks of thousands of devices.

Chromebooks are ideal for sharing as user data for apps are all stored in the cloud. This allows a user to pick up any Chromebook, sign in to their account, and access their own work and settings. The fact that a Chromebook isn't tied to the user means that schools can operate a pool of devices rather than issue one to every student. If a student breaks or loses their device they are able to just pick up another immediately, without losing time or work.

Recent Google development has placed specific emphasis on educational tools, for example, Google's recently released Classroom app is highly focussed for education, allowing teachers to communicate with students, organise and grade assignments and give real-time feedback via specialised folder creation.

The need to protect children online

With the convenience of Google portable devices comes a new set of challenges for keeping students safe online. Unlike a desktop device, students using laptops are able to browse and use the internet without direct supervision both at school and in the home. Browsing safety is a key concern for parents; according to a January study from the PEW research centre, 61% of parents had looked at their teenagers

web browsing history at least once, to check which websites they had visited. In spite of the desire to keep their teens protected on the internet, only 39% of parents used parental controls for blocking, filtering or monitoring.

The difficulty with traditional blocking or filtering methods, or even checking a child's history online, is it only tells part of a story of what they have viewed. Traditional filtering works by examining the URL of a web request, and comparing it against 'lists' of sites which have been categorised, and subsequently deemed "good" or "bad". What this means is URL-based filtering can only ever be as good as yesterday's information, which is far from ideal when on average over 571 new websites are created per minute.

571
new websites are created per minute
meaning traditional blocklists can't keep up

The problem with URL history

The problem with looking at search engine history alone to protect children is it may not reveal the full story. A large amount of web browsing is no longer done via browsers, but via third party applications such as Facebook. Tools such as anonymous proxies allow circumvention of traditional URL-based filtering, while also providing a way to browse without leaving any history. Anonymous proxies provide a VPN which masks the URL of the site being viewed. As well as potentially letting through dangerous content, the limited nature of blocking based on a URL alone can lead to overblocking, which can limit learning if a legitimate site is blocked.

What is needed to help children work safely on a growing internet is the ability to filter based on analysis of the actual content on the page. Content-aware analysis is able to analyse search terms, domains and text of a website to decide in real-time if it will display content. By looking at the actual content, filtering doesn't go 'out of date' like URL lists do, and can even pick up bad content on an otherwise allowed site, such as explicit comments on a YouTube™ video. This allows users of school devices to be protected in the school and also in the home when on a school owned device.

Bringing content aware filtering to Chromebooks with simplicity

Managing devices across a school or trust using Google credentials presents a different style of system architecture. Traditional methods of authentication against Microsoft's Active Directory® become unnecessarily complex for System Administrators who are happy to filter against trusted Google credentials. If a school is "Google only", Active Directory isn't even present. What is needed is a simple way to filter using the Google architecture and existing groups.

Google as a Directory Service allows Chromebook users to be filtered against their Google user accounts, without the need to set up an Active Directory domain to replicate Google Apps Directory Sync (or GADS). Removing the need for an Active Directory allows “Google only” schools to take advantage of Smoothwall’s advanced content-aware filtering via single sign-on with Google. It is possible to map Smoothwall groups to Google groups, allowing rules such as content filtering policies from the Smoothwall to be applied based on groups.

Chromebooks should be enrolled with Google on their management console in order to prevent users being able to browse in Chrome with their personal credentials. User settings and policies for apps can also be configured there, and unwanted apps and extensions should be blocked from being installed on the Chromebook.

Smoothwall’s Connect for Chromebooks app allows system administrators to lock the device down to enforce your chosen filtering rules.

The Connect for Chromebooks feature can be set up in 3 simple steps:
1. Distribute the Smoothwall HTTPS certificate to all Chromebooks
2. Distribute the Connect for Chromebook extension to your users
3. Set up filtering and access policies on the Smoothwall

The Connect for Chromebooks feature retrieves the username from the Chromebook directly and passes it to the Smoothwall. It is even possible to set up the Smoothwall to filter Chromebooks when they are outside of the school network, setting parent’s minds at ease when students are studying at home on a school device.

Non-enrolled Chromebooks (such as students bringing in their own devices) appear on the Smoothwall as “unauthenticated IP’s”. This group is still subject to filtering, and so the user is unable to bypass policies.

Schools that run their infrastructure on Google have not previously been able to take advantage of Smoothwall's content-aware filtering due to the lack of an Active Directory in their system. Google as a Directory Service allows advanced filtering methods to be used via Google single sign-on. Content-aware filtering via Smoothwall's Google as a Directory Service keeps children safe online, both in school and at home on school devices, allowing parents to have confidence that their children are in safe hands wherever they use the web.

For further information

Please contact our Product team via email or by submitting feedback to our customer forum.

Email: product@smoothwall.com
Visit: smoothwall.uservoice.com

For help or support, please call
08701 999 500

smoothwall
The Web You Want