Achieving CIPA Compliance
With iboss SWG Web Security

The iboss Products

Layer 7 Web Security
• Web Security
• Cloud Web Security
• Threat & Event Console

Web Security Extension Modules
• IPS & Behavioral Data Protection
• Intelligent Bandwidth Management
• Mobile Security
• Mobile Device & Application Management

About iboss Network Security


To learn more about our services:
www.iboss.com
Main: 1-877-742-6832 ext. 1
Support: 1-858-568-7051 ext. 3

iboss Network Security is recognized by Gartner, the world’s leading information technology research and advisory company. In addition to Gartner, iboss has received numerous awards related to web filtering and Internet security.

What is CIPA?

The Children’s Internet Protection Act (CIPA) was signed into law on December 21, 2000. Schools and libraries that plan on utilizing E-rate discounts on Internet access and/or internal connection services after July 1, 2002 must be in compliance with CIPA. CIPA requires schools and libraries to filter their Internet services and have implemented formal Acceptable Internet Use Policies. The FCC administers CIPA for E-Rate purposes and provides general guidelines to achieve CIPA compliance.

CIPA Requirements

General Requirements for CIPA compliance require implementation of a technology protection measure (AKA Internet Filter), such as iboss SWG Web Security. Schools must enforce a policy to monitor online activities of minors. To ensure CIPA compliance at all times, Internet access should be restricted when filtering technology is disabled.

Key Topics To Be Covered:
1. What is CIPA and what does it require?
2. Categories for CIPA compliance.
3. iboss ensures CIPA compliance.
4. Monitor online activities of minors.

Internet Filter Requirements:
• Block access to visual depictions deemed “obscene”, “child pornography”, or “harmful to minors”
• Safety and security of minors when using direct electronic communications.
• Block unauthorized access, including ‘hacking’, and other unlawful activities by minors online.
• Filtering is required for all Internet-enabled computers whether used by minors or adults.
• Filtering of adult Internet usage can be disabled for bona fide research or other lawful purposes.
Achieving CIPA Compliance
With iboss SWG Web Security

Categories For CIPA Compliance

In order to ensure CIPA compliance, managing access to the following is recommended:

**Web Categories**
- Adult Content
- Alcohol/Tobacco
- Child Pornography
- Dating/Personals
- Drugs
- File Sharing
- Gambling
- Games
- Proxies
- Pornography/Nudity
- Guns/Weapons
- Violence/Hate
- Virus/Malware

**Safe Search (Enable)**
- Safe Search

**Applications (Restricted)**
- Peer to Peer
- New Groups
- File Sharing
- RDP/Remote Desktops
- Google Encrypted Access
- Dynamic Proxy Blocking
- Hot Spot Shield
- Rogue Encrypted Connections
- SSL Domain Enforcement
- Ultrasurf/Tor Blocking

**iboss SWG EDU Google Secure (Enable)**
- Clean YouTube
- Google Clean Image Search
- Google Translation Filtering

**Keywords (Enable)**
- Adult
- High Risk

Categories are recommended to meet CIPA compliance and not specifically identified as required by CIPA.

*Safe search for Image and videos sites is recommended if access to image or video sites is desired to be opened for minors. Due to image caching by Google Images, enabling of ‘Google Image Scrubbing’ is recommended to ensure CIPA compliance. iboss Google Secure is an exclusive feature of iboss SWG Web Security.*

Comprehensive Controls

Comprehensive controls ensure CIPA compliance beyond standard URL filtering to expand security for applications, file sharing, image searching, and YouTube.com

Categories

Controls include URL, Applications, Keywords, Content Type, and Triggers

**Threat & Event Reporter**

Store Internet and user activity logs for extended periods. In addition, dynamic access to this data is required to identify and resolve obscure threats lurking in the logs.
Achieving CIPA Compliance
With iboss SWG Web Security

iboss SWG Web Security Ensures CIPA Compliance

iboss SWG Web Security provides the technology needed to ensure your network is CIPA compliant. iboss provides granular filtering tools with industry leading monitoring tools that simplify compliance and automate reporting. Additionally, the flexible group policies and directory integration gives administrators the ability to enforce CIPA compliance to certain groups yet provide more open access to others on the network (i.e. teachers vs. students).

Working With Your Support Engineer

iboss provides U.S. based support which will work with you one on one to go over configuration and ensure CIPA compliant categories are enforced. Additionally, your support engineer will review other applications that may not be a direct requirement for CIPA compliance but may add to the security of your network.

Below are general outlines of selecting categories for CIPA compliance:

1. Access the iboss SWG Web Control interface
2. Select ‘Controls’
3. Select ‘Block Web Categories’
4. Select from the tabs or the drop down list at the top of the page to identify the group you wish to configure*. Once the selected group is highlighted, choose ‘Block’ from the drop down menu next to each CIPA category based on the list from page 2 then select ‘Save’ at the bottom of the page.

*Note: Once you select the configuration for a group, the group policy can be copied to other groups. This control is found under the ‘Groups’ section.

YouTube Management

iboss SWG Web Security offers a comprehensive suite of options to manage this access. It’s designed to both prevent unwanted activity by select users and preserve network resources. These advanced YouTube management controls maintain the correct level of access based on an organization’s needs.

Clean YouTube Content

Powerful YouTube content management enables organizations to strip comments, ads, and unrelated videos dynamically and directly from YouTube search results. This blocks inappropriate comments and unwanted material.

HTTPS YouTube

Thanks to advanced algorithms and signatures, administrators can quickly and effectively block SSL access to YouTube without affecting Google Docs or other Google services. No advanced configuration is required.

iboss Clean Image

Clean Image Search and Translation Filtering, iboss Web Filter provides expanded security for Google services like Images and Translation.

--- Something safe search misses!
Once these categories are saved, the group will now be CIPA compliant. The base requirement for CIPA is to prevent exposure to minors of adult, violence, and inappropriate content. The iboss filters are now protecting HTTP and HTTPS access to these sites for the selected groups. In addition to applying these base policies, organizations can expand security by filtering applications, ports, file extension, domains, as well as apply triggers for violation attempts.

Managing Applications:
Applications can be accessed from the home page -> Controls -> Programs, Protocols and DLP.

Within the programs section, configuration to manage applications and DLP can be configured overall or on a time schedule. Common applications selected for restrictions include chat, file-sharing, online gaming, Glype proxies, SSH, RDP, FTP, and Rogue Connections. Although these are not required for CIPA compliance, they add layer 7 security to the network restricting circumvention with proxies, anonymizers and inappropriate communication.

BYOD Management
iboss SWG Web Security’s integrated BYOD Management suite provides network administrators the tools to ensure that BYOD access is filtered from malware, botnets, and DLP.

iboss SWG Web Security BYOD Benefits:
- Extend compliance and AUP to BYOD devices.
- Scan and filter known and unknown threats including Malware, Botnets, and DLP.
- BYOD bandwidth throttling and QoS to ensure mission critical traffic remains uninterrupted.
- BYOD directory integration and binding across Active Directory, eDirectory, Open Directory, and LDAP.
- High Risk User Auto Quarantine – automatically locks users attempting to conduct illegal activity such as music and file downloading.
Achieving CIPA Compliance
With iboss SWG Web Security

Integrated iboss SWG Threat & Event Reporter

The iboss SWG Threat & Event Reporter changes how we approach user-activity reporting and threat mitigation by addressing with whom and where our network is communicating. By tapping exclusive features such as threat GeoMapping and heat map technology to identify threats lurking in the background, iboss Threat & Event Reporter provides a new approach to network activity monitoring. iboss SWG Threat & Event Reporter also includes a consolidated dashboard of the iboss SWG product line in one view. Within seconds, administrators gain a 360-degree view of each network user, including Web, application, bandwidth, packet consumption, data loss, email malware, and threat activity. This consolidates compliance reporting, increases network insight, and reduces the total cost of ownership (TCO).

To access the reporter from the home page, click Reports -> Login -> and you will land on the live activity dashboard.

iboss SWG Threat & Event Reporter Benefits:
- Consolidated Version of All iboss SWG Products.
- View Across All User Activity: Web, Application, DLP, Bandwidth, Email, and Malware in One View.
- Live Threat and Bandwidth Dashboards.
- Bandwidth Heat Map Technology.
- Instant URL/Ad-Hoc Reporting Capabilities.
- A Dynamic Drill-Down Interface.
- Mobile Device Threat and Activity Reporting.
- Site Callout Capabilities.
- Automated Report Scheduling.
- Compliance-Reporting and Automated Backups.
- Consolidated Reports Across a Distributed Enterprise.

The iboss Difference – Not Just What, But Who and Where

Cyber threats, including malware and data loss — along with new potential of network peripherals “phoning home” — are constant security game-changers because they’re continually growing in sophistication. As such, these menaces have eroded and will continue to compromise the effectiveness of current log-based threat detection and reporting. iboss SWG Threat & Event Reporter alters how we approach threat identification and mitigation by looking at your connection source and then identifying to whom and where you’re connecting. With exclusive features such as threat GeoMapping and heat maps technology, iboss SWG Threat & Event Reporter provides instant visual insight to pinpoint threats across a global map. This system increases insight, shortens mitigation response, and reduces the total cost of ownership (TCO).

For more product details, see the iboss SWG Threat & Event Console Brochure.

www.iboss.com
iboss Network Security (P) 877.742.6832 Sales@iboss.com U.S. HQ 9950 Summers Ridge Rd., Bldg. 160 San Diego, CA 92121
© 2013 All rights reserved. iboss Network Security. All other trademarks are the property of their respective owners. Confidential - for intended recipients only. Distribution to third party is prohibited without prior written authorization.