
CS MIMESweeper™ for Web 5.0

About CS MIMESweeper™ for Web

What is CS MIMESweeper™ for Web?

CS MIMESweeper™ for Web is the most powerful and comprehensive Web filtering solution available today, providing much more than URL blocking. It enables organizations to implement and enforce a Web usage policy to control content downloaded from, and uploaded to, the Web. CS MIMESweeper™ for Web scans Web traffic entering and leaving an organization to protect against threats to IT infrastructure, data, intellectual property, productivity and reputation.

What are the new features of CS MIMESweeper™ for Web?

For this release of CS MIMESweeper™ for Web, Clearswift have primarily focused on improving performance, scalability and manageability. This in turn has reduced the total costs of deploying, scaling and administrating the solution.

Increased Scalability

A four-fold increase in scalability over CS WEBSweeper™ 4.1 with the ability to run an array of 4 Web proxy servers in a load balanced configuration, without the need for costly 3rd party load balancing hardware. This is achieved by using a routing protocol that shares requests between servers whilst ensuring that where a request has already been cached it is delivered from the right server's cache.

Increased Performance

CS MIMESweeper™ for Web features a 300% increase in per-server performance over previous versions. It is a full caching security Web proxy server. For this release the cache has been increased in size from 500MB to 4GB, precluding the need for a 3rd party caching product, and improving network performance by delivering more responses directly from cache.

Improved Manageability

The Web-policy can now be managed across all servers in an array as if they were a single entity, making the overall management of a consistent Web policy far easier.

Other New Functionality

- Policy configuration from anywhere on the local network
- Support for French and German operating systems
- The URL database now provides both domain and page based categorization - i.e. www.bbc.co.uk/sports is categorized as sports, whereas www.bbc.co.uk/ is categorized as arts and entertainment
- More than 5.6 million URLs, with 40 clearly defined categories that contain more than 900 million Web page references, covering 65 languages



- SMTP email alerter
- Support for Symantec AV tool
- IP addresses in User Lists for policy selection
- Web-based reporting
- Support for client to Web server NTLM authentication
- Customizable proxy error pages
- Standard format transaction log
- Intelligent script analysis
- Configurable proxy timeouts
- Configurable list of HTTPS ports
- A configurable maximum download size
- Improved streaming media detection

Why do I need CS MIMESweeper™ for Web?

Employee use of the Web is common. As a result, a company's overall content security policy needs to include a Web usage in order to address the threats that exist when employees have open access to online resources. These include:

- Business integrity threats such as the loss of confidential company information through Web postings, employees viewing undesirable material, the loss of information through the siphoning off data by malicious executables.
- Network integrity threats such as Web-borne viruses, malicious code (e.g. executables and ActiveX) and the poor utilization of available bandwidth through Web misuse.

What is e-policy based content security?

e-policy based content security is a fundamental part of business security. Essentially it's about establishing a written policy that outlines acceptable and unacceptable use of the Internet, educating employees on the policy, and then enforcing it with a range of software solutions such as those offered by Clearswift through the MIMESweeper™ family of products. CS MIMESweeper™ for Web helps organizations guard against business and network integrity threats that can arise through unrestricted access to the Web and result in confidentiality breaches, degradation in service, legal liability, lost productivity, data corruption, etc.

What defines a Web Policy?

An e-policy should include a policy for both email and Web usage. A Web policy is defined by a combination of things including the route (URL) or type of site being accessed (shopping, porn, financial, news, etc.), the content available on the site (text, images, file types, script etc.), the direction of information flow (upload/download), and the person accessing the site. The Web policy can be refined at different levels from "a one policy fits all" at the organization level, to a policy based on groups, or



individuals, where different departmental roles within an organization warrant different levels of Web access.

How does CS MIMESweeper™ for Web work?

CS MIMESweeper™ for Web protects an organization from both incoming and outgoing threats. To implement a content security policy, CS MIMESweeper™ for Web manages objects and data flowing through the Internet gateway in five stages:

- 1. Policy identification.** When a user initiates a transmission, CS MIMESweeper™ for Web begins by authenticating the user. It then applies the user's specific Internet access privileges according to the security policy in place. CS MIMESweeper™ for Web integrates with existing LDAP, Windows, text-based user directories, or can apply policy based on the client IP address.
- 2. URL Filtering.** CS MIMESweeper™ for Web compares the URL against a database of more than 5.6 million URLs to determine if the URL has been included into one of the 40 pre-defined categories. If so, then the next step is to determine if the user is allowed access to that particular category of site. If the user is not allowed access the page is blocked and no more processing takes place. If the user is allowed access, then the processing of the contents of the Web transfer continues from step 3 below.
- 3. Content disassembly.** CS MIMESweeper™ for Web identifies the primary components of the content being transmitted, breaking down Web pages, compressed files, executables, document formats, image, sound and video formats to reveal the most basic elements, such as an ActiveX object on a Web page. This is the most comprehensive recursive disassembly available, with analysis up to 50 layers deep. CS MIMESweeper™ for Web identifies content by its file architecture, rather than simply the file extension. The pattern matcher feature allows file types to be identified by their binary sequence, giving administrators the ability to block any file type.
- 4. Content analysis.** The HTTP or browser FTP content is then analyzed and evaluated according to the policy as it applies to the user who is sending or receiving the transmission. CS MIMESweeper™ for Web screens out designated file types, analyzes text to identify potential security breaches, and identifies potentially dangerous executable code. CS MIMESweeper™ for Web also integrates with the leading virus scanners in order to check the content for known viruses.
- 5. Delivery.** Once the content has been fully disassembled and analyzed, CS MIMESweeper™ for Web implements the policy by letting the content pass - cleaning and recomposing infected content beforehand - or blocking the transmission altogether. A configurable message or HTML page informs users when a page is blocked and can include the reasons why, and perhaps a restatement of the Web usage policy. A notification to appropriate parties can be implemented via an email alert.



How does CS MIMESweeper™ for Web differ from other Web solutions?

Unlike most other Web filtering solutions available today, CS MIMESweeper™ for Web provides more than URL blocking. URL blocking is an important first step in stopping access to undesirable sites. However with new Web sites being created every day, no database of undesirable URLs will ever be completely up-to-date. Besides, a Web policy is not exclusively concerned with blocking access to the Web. It's about allowing access to appropriate sites, whilst ensuring that security is maintained during access and that the Web policy continues to be enforced. Customers need to analyze the content of Web pages and decide, in real-time, whether to block or to allow access based upon the content found. For example, it may be acceptable to use Web mail accounts (from a policy point of view), but unacceptable to send spreadsheets (e.g. price book, accounting information) or receive executable files (potentially carrying malicious code) via these Web mail accounts. With CS MIMESweeper™ for Web organizations can enforce policies on content piracy, undesirable Web content and file type downloads as well as Web-based mail systems.

What are the benefits of using CS MIMESweeper™ for Web?

CS MIMESweeper™ for Web works in tandem with firewall and integrates with anti-virus solutions to provide a comprehensive security solution that guards against breaches of confidentiality and other threats, such as damage to reputation, lost productivity, pornography, theft of data, legal liability, degradation in service and data corruption.

While email-borne viruses and Trojan Horses have been widely publicized, and their effects felt everywhere, less attention has been paid to HTTP and FTP transmissions. These provide an alternate route for equally damaging code to infiltrate a network, as well as exposing an organization to more subtle threats to profitability and workplace productivity. The increasing popularity of Web based mail, such as Hotmail, underlines the increasing threats from the "back door."

When will CS MIMESweeper™ for Web be available?

CS MIMESweeper for™ Web will be available at the end of July 2003.

Where can I get an evaluation copy of CS MIMESweeper™ for Web?

When released at the end of July CS MIMESweeper™ for Web 30 day free evaluation software will be available from the download section of our Web site <http://www.mimesweeper.com/download/default.asp>.

What is the licensing cost for a 50-user license of MIMESweeper™ for Web?

CS MIMESweeper™ for Web is licensed by number of users and the list price for a 50-user license starts at £950.

Features and Functionality

Does CS MIMESweeper™ for Web check the content of uploads and downloads?

Yes. CS MIMESweeper™ for Web provides protection against content security threats entering or leaving your organization. It is commonly accepted that whilst surfing Web pages, files and executables are downloaded. However, the Web also provides a mechanism for uploading files, and these could be damaging if found to contain confidential data and/or libelous material.

Can CS MIMESweeper™ for Web check archive files such as zips?

Yes. Files can be embedded in archives or other files or encoded in a different format. To be effective, content scanning needs to extract the embedded files in their native format. CS MIMESweeper™ for Web repetitively extracts embedded files using recursive decomposition until the native format is exposed.

Does CS MIMESweeper™ for Web protect organizations from the potential threats posed by free Web-based mail accounts?

Yes. CS MIMESweeper™ for Web checks the contents of uploads to, and downloads from, the Web. This means that it can provide protection from content threats that may enter or leave an organization through use of the Web. The most common method of doing this is via Web-based mail accounts (e.g. Hotmail, Yahoo! Mail), where users are able to attach any file from their computer, therefore bypassing any SMTP email security that may be in place.

How does CS MIMESweeper™ for Web decide which pages I should look at?

CS MIMESweeper™ for Web doesn't – you do! You decide what you want it to look for. Establish the content security policy for your organization, and then use CS MIMESweeper™ for Web to enforce the policy. It's a comprehensive and flexible tool that can implement and enforce a policy at the organization, group and user level.

How can I configure CS MIMESweeper™ for Web to stop viruses being downloaded? (Accidentally or otherwise)

CS MIMESweeper™ for Web integrates with anti-virus (AV) scanning products. It identifies the data being downloaded and calls the virus scanner to check the data for viruses.

Does CS MIMESweeper™ for Web scan all IP related protocols?

CS MIMESweeper™ for Web is dedicated to the scanning of HTTP and browser FTP. Command line FTP is not validated and should be controlled via a firewall.

Can I stop real audio/real video usage with this product?

Yes, with HTTP sessions CS MIMESweeper™ for Web can identify and block these data types if required.

Can I tell (or "teach") CS MIMESweeper™ for Web which file types I wish to block, or must I select from a predefined list?

Yes, you can do both. CS MIMESweeper™ for Web contains a pre-defined list of file types that can be used to block files by type. This list looks at the file type binary pattern rather than trusting the file extension to ensure that disguised file types are recognized. The product has a pattern matcher function, which enables the administrator to define new file types that are not in the pre-defined list.

Why do I need User Authentication?

You may decide that not all employees should have the same level of access to the Web, and therefore want to apply a different Web usage policy depending on the group or individual user concerned. CS MIMESweeper™ for Web User Authentication allows you to do this easily, by integrating with your existing LDAP, NT, text files, or listing IP address ranges. In this way it can identify the user and apply the configured policy for that particular user, or group of users.

What are 'progress messages'?

When CS MIMESweeper™ for Web downloads large files it keeps the user informed of what is happening via a 'progress message' in an HTML page. These can be customized by the system administrator and typically inform the user of the percentage of time elapsed for the download.

Does CS MIMESweeper™ for Web have reporting features? If so, can it report any event to an administrator?

Yes. CS MIMESweeper™ for Web is supplied with standard graphical reports that provide detailed information on Web usage (e.g. Top 10 Internet users, Top 10 Internet sites accessed, Top 10 threats detected). It also has a real-time reporting feature that provides data on current Web users. Any event can be used as a trigger to send an e-mail alert.

I cannot get the URL Filter Category working, why?

To use the URL Filter Category, you must have the URL Filter Category option included in your CS MIMESweeper™ for Web product license. Contact your local Clearswift Customer Service Center for details.

What are the 40 categories provided by the URL Filter Category?

The 40 categories are - Adult/Sexually Explicit, Advertisements, Arts & Entertainment, Chat, Computing & Internet, Criminal Skills, Drugs-Alcohol-Tobacco, Education, Finance & Investment, Food & Drink, Gambling, Games, Glamour & Intimate Apparel, Government & Politics, Hacking, Hate Speech, Health & Medicine, Hobbies & Recreation, Hosting Sites, Job Search & Career Development, Kid's Sites, Lifestyle & Culture, Motor Vehicles, News, Personals & Dating, Photo Searches, Real Estate, Reference, Religion, Remote Proxies, Sex Education, Search Engines, Shopping, Sports, Streaming Media, Travel, Usenet News, Violence, Weapons, Web based Mail



Deployment and Operation

What type of machine do I need to run CS MIMESweeper™ for Web?

The recommended requirement is a dedicated Pentium™ III 1GHz machine, dual processor with 1GB memory, and 10GB free disk space.

Can I manage multiple CS MIMESweeper™ for Web servers from one management GUI?

Yes, the interface allows you to manage and configure all the servers in an array consisting of 4 CS MIMESweeper™ for Web servers as if they were a single entity.

Can CS MIMESweeper™ for Web coexist with my current Web proxy server?

It is not recommended to have CS MIMESweeper™ for Web coexist with another proxy on the same machine. Clearswift recommend that CS MIMESweeper™ for Web is deployed on its own dedicated machine, however it may be chained to another Web proxy if required.

Can CS MIMESweeper™ for Web and CS MAILsweeper™ for SMTP coexist on the same machine?

CS MIMESweeper™ for Web cannot coexist on the same machine as CS MAILsweeper™ for SMTP. However, the MIMESweeper™ for Web management interface has many similarities with the MAILsweeper for SMTP interface, and provides much overlap in the policy configuration and management aspects. This maximizes the potential for skills transfer with minimal training where both solutions have been deployed alongside each other.

Does CS MIMESweeper™ for Web affect my browsing performance and response times?

On a correctly specified installation the latency due to the comprehensive content security operations is negligible for the majority of pages. There is a security/performance trade-off, which will be more noticeable with complex downloads such as zipped files. The use of DLL based anti-virus tools and dedicated servers are recommended.

Is CS MIMESweeper™ for Web a proxy server? If so, can I use it to replace my current proxy server? By de-selecting the "connect via proxy" in my browser, can I bypass it?

Yes. CS MIMESweeper™ for Web is a fully authenticating, caching proxy server and could therefore replace any other proxy. To prevent users bypassing CS MIMESweeper™ for Web, we recommended its deployment in conjunction with a firewall.

Is CS MIMESweeper™ for Web multi-threaded?

Yes. CS MIMESweeper™ for Web uses multi-threading to efficiently check the contents of any Web downloads/uploads.



Can I replace my firewall with CS MIMESweeper™ for Web?

No. CS MIMESweeper™ for Web is not a firewall and should be used in conjunction with a firewall to implement a comprehensive access and content security solution.

Can I use Explorer and Navigator?

Yes. CS MIMESweeper™ for Web supports Internet Explorer versions 5 and 6 as well as Netscape Navigator version 4 to 7 inclusive.

What databases does CS MIMESweeper™ for Web support for auditing?

CS MIMESweeper™ for Web supports SQL Server 2000 for auditing and is supplied with MSDE 2000 as standard.

What platforms does CS MIMESweeper™ for Web support?

Windows 2000 Server and Windows 2000 Advanced Server.

How many users can one CS MIMESweeper™ for Web server support?

Each Server in the array can protect approximately 2000 users when enforcing a comprehensive Web policy consisting of AV, lexical analysis, file blocking, and URL filtering. This represents a 300% increase in performance per server over CS WEBSweeper™ 4.1. As might be expected, performance per server is dependant on the Web policy, thus with a less comprehensive Web Policy of just URL blocking the performance would increase dramatically, albeit with reduced security.

I have more than 2000 users in my organization but still want to enforce a comprehensive Web policy, can I deploy more than one server?

Yes most definitely. CS MIMESweeper™ for Web has been designed to scale using 4 servers deployed in an array configuration. These servers use a caching array routing protocol to distribute HTTP requests between servers without the need for 3rd party load balancing hardware or software. As a general guideline each server can protect 2000 users and enforce a comprehensive Web policy, therefore an array of 4 servers can serve approximately 8,000 users.