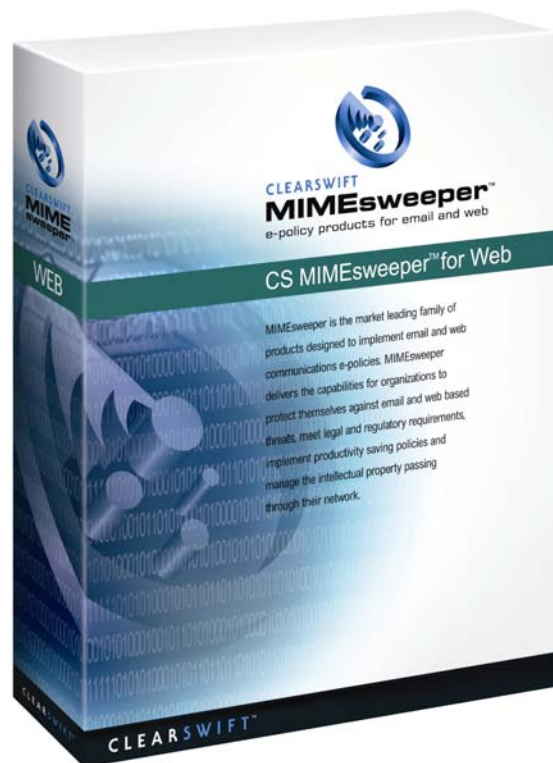




CS MIMESweeper™ for Web Reviewer's Guide



For more information, visit

www.re-soft.com

Contents

Introduction	3
Product Background	3
The CS MIMESweeper™ Product Family	3
Potential Security Threats Resulting From Corporate Web Access	5
Network Integrity Issues	5
Business Integrity Issues	6
The CS MIMESweeper™ Approach to Web Content Security	6
Policy-Based Content Security	7
How CS MIMESweeper™ for Web Works	7
Highly Flexible, Customizable Policies	8
Administrative and Reporting Capabilities	9
New and Enhanced Features in CS MIMESweeper™ for Web	9
Reporting	10
Installation and Product Walk-Through	10
Installing CS MIMESweeper™ for Web	11
Pre-installed Evaluation Policy	13
Scenarios and Classifications	13
Changing a Policy Scenario	14
Changing a Policy Classification	15
Setting Up Users and Assigning Scenarios	16
Creating a New Policy Using the URL Category Filter	18
Testing the Security Policy	21
Support / Customer Help	22

Introduction

The value of Web access to businesses is undeniable. From gathering news and information to communicating with partners and customers to streamlining business transactions, organizations aren't looking back when it comes to leveraging the medium. As a result, desktop access to the Web has become standard functionality across enterprises large and small.

But for IT managers and other decision makers, the business benefits are tempered by an array of threats to an organization's IT infrastructure, data, intellectual property, productivity and reputation.

While e-mail-borne viruses and Trojan Horses have been widely publicized, and their effects felt everywhere, less attention has been paid to HTTP and FTP transmissions, which 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 e-mail, such as Hotmail, underscores the increasing threats from the "back door."

CS MIMESweeper™ for Web is a content security solution that protects organizations from virtually every kind of Web-related threat, giving IT managers the ability to implement a comprehensive policy for Web transmissions and employee access — including an extensive set of security options not offered by URL blockers and anti-virus tools. Not only does CS MIMESweeper™ for Web provide the most powerful content analysis technology available, it offers a highly flexible system for enforcing a Web usage policy company-wide.

This reviewer's guide lays out some of the key features and benefits of CS MIMESweeper™ for Web version 5.0, and gives you a starting point for evaluating the solution yourself. If you're already familiar with CS MIMESweeper™ for Web then you can jump to the New and Enhanced Features section to review the substantial additions and improvements we've made in version 5.0. Clearswift is committed to maintaining its leadership in the content-security category, and you'll see how with this product we're giving organizations the most comprehensive content-security product on the market today.

Product Background

Clearswift is the world's leading provider of software for managing and securing electronic communications. Clearswift delivers the capabilities for organizations to protect themselves against email and Web-based threats, meet legal and regulatory requirements, implement productivity-saving policies and manage intellectual property passing through their network.

The CS MIMESweeper™ Product Family

Organizations can face many network and business integrity threats through unprotected employee email and the Web usage. CS MIMESweeper™ solutions provide market

leading content security, protecting over 15,000 customers and 20 million users worldwide with policy-based content security defenses.

CS MIMESweeper™ for Web, unlike anti-virus and URL blocking tools, provides a full content security solution enforcing comprehensive security policies on otherwise unsecured internal/external email and Web-based information exchanges within and around your organization.

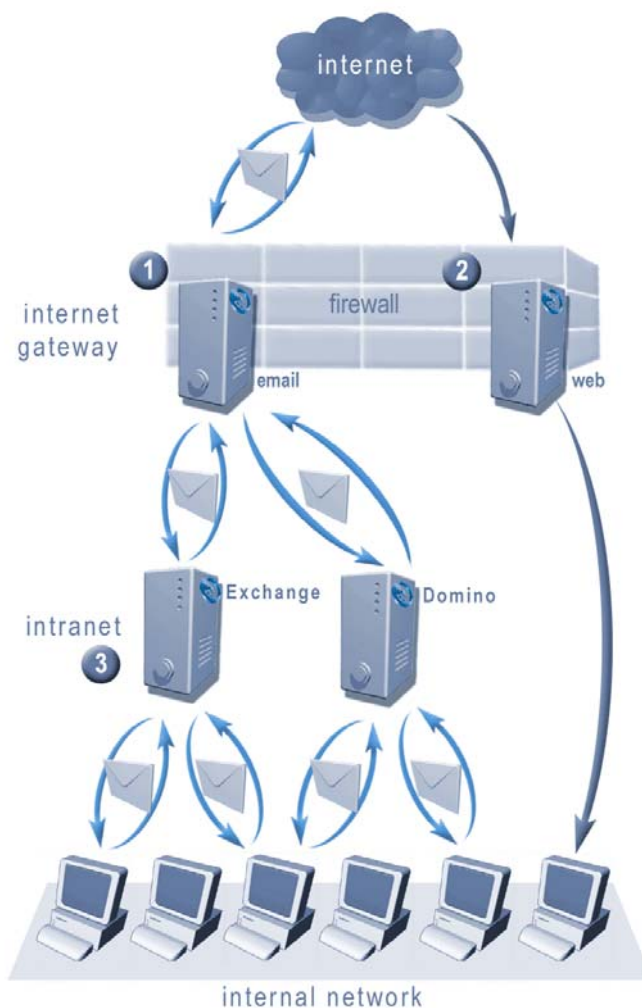


Figure 1. The CS MIMESweeper™ range provides protection from external threats.

(1) CS MAILsweeper™ for SMTP prevents damaging e-mail from entering or leaving the network at the firewall. **(2)** CS MIMESweeper™ for Web provides content security for Web downloads and uploads. **(3)** CS MAILsweeper™ for Domino and CS MAILsweeper™ for Exchange protect against threats that are introduced and propagate within an organization's internal e-mail system.

Other solutions in the CS MIMESweeper™ family, such as CS PORNsweeper™ and CS SECRETsweeper™, provide additional tools for implementing robust content security policies.

Potential Security Threats Resulting From Corporate Web Access

The dangers of a Web gateway fall into two main areas: network integrity threats and business integrity threats. Network integrity threats are what most people think of when they consider security issues — protecting the IT infrastructure from anything that might compromise system operations or performance. These could include viruses or damaging code downloaded from the Web, or simply inappropriate network use that slows or even overloads the Web server.

Business integrity threats are primarily a side effect of opening up another channel through which employees obtain and distribute content. Network bandwidth can be compromised when employees use desktop Web access for non-work purposes (such as downloading music, video files or games). In addition, transmitting inappropriate content (uploading confidential intellectual property or damaging messages, downloading pirated software or inappropriate Web pages, etc.) can expose the organization to lawsuits or damage its reputation.

As a content security solution, CS MIMESweeper™ for Web gives organizations the means to protect themselves from both kinds of potential threats and manage Web access in the workplace as the valuable resource it is.

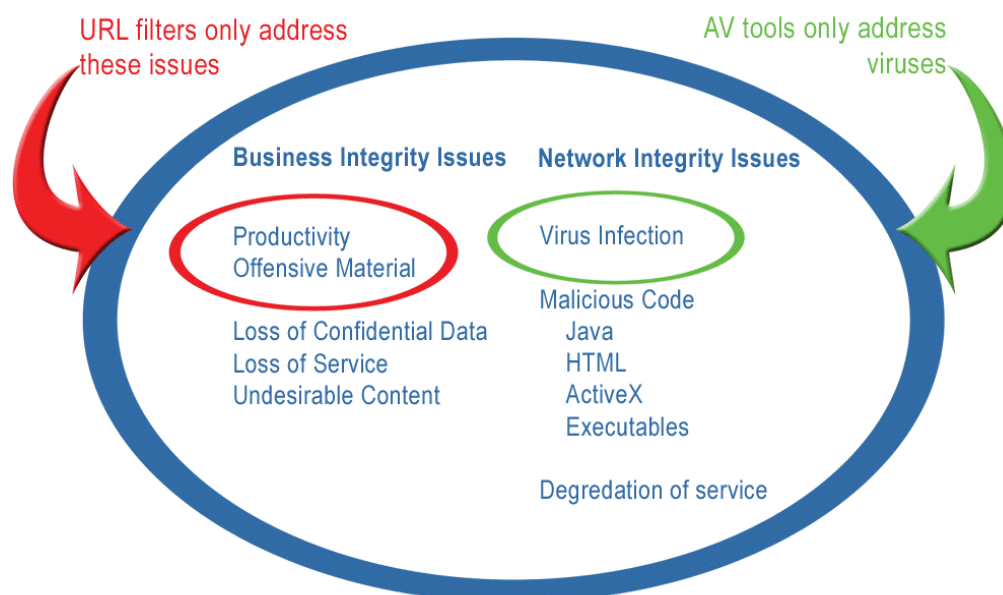


Figure 2. CS MIMESweeper™ Web protection extends well beyond that of URL blocking and anti-virus applications.

Network Integrity Issues

- **Degradation or loss of service.** Network throughput can be compromised or even suspended entirely as a result of non work-related Web surfing or downloading images, MP3 files, video clips, illegal software, etc.
- **Data corruption.** Web-borne viruses can be downloaded in files, in addition to the danger of downloading malicious code and executable files, which impact network and business performance.

Business Integrity Issues

- **Breaches in confidentiality.** The Web provides a way around SMTP e-mail security systems, allowing employees to transmit confidential materials or information through online postings or Web-based e-mail accounts such as Hotmail.
- **Damage to an organization's reputation.** Because the Web is open to literally every kind of content and perspective, it opens the door to any number of possibilities that could damage the reputation of the organization. Whether an inappropriate link is unintentionally distributed to a broad group, or an employee lawsuit highlights offensive workplace conduct related to Web use, the long-term consequences can be damaging to the reputation of the organization, reducing customer confidence and employee morale, and even causing stock prices to drop.
- **Legal liability.** By downloading copyrighted material or pirated software, employees can expose the organization to copyright infringement lawsuits. In addition, sexual harassment suits can emerge from the display of inappropriate images.
- **Lost productivity.** Based on data gathered from 600 client companies with annual revenues of \$100 million or more, employees spend from one to 10 hours per week shopping, checking stocks and looking at pornography on the Internet. (*Newsbytes*. "Personal Web Use at Work Cost \$5.3 Billion in 1999" — February 2000)
- **Theft of important information.** Without the user being aware, downloaded code can siphon off network data via hidden forms, "mailto" commands and cookies.

The CS MIMESweeper™ Approach to Web Content Security

CS MIMESweeper™ for Web helps organizations protect themselves from all these threats, based on organizational policies for maximum network protection and appropriate Web use by employees. Instead of attempting to be a one-size-fits-all solution, CS MIMESweeper™ for Web offers organizations a content-security solution that is fully customizable, down to the individual user.

CS MIMESweeper™ for Web is implemented as a Windows 2000-based HTTP proxy server behind the Internet firewall, although it can be deployed in conjunction with an existing proxy server. A CS MIMESweeper™ for Web server will support approximately 2,000 users per server, assuming 10 percent concurrency.¹ Factors that impact system performance include the number of concurrent users, the intensity of their Web activities (e.g., browsing vs. downloading), the complexity of the configured Web policy, available bandwidth, server specifications, etc. However, as a general rule, CS MIMESweeper™ for Web will serve at least 2000 users with 10 percent concurrency on a Pentium 4 dual processor machine. Organizations with higher levels of concurrent Web access can

¹ It is typical that many users will be accessing the Web at the same time, but the number of users in the process of downloading/uploading new pages/files will be some fraction of this number. Ten percent concurrency means 200 of the 2000 users accessing the Web will be downloading or uploading new pages/files at exactly the same time.

deploy an array of up to four CS MIMESweeper™ for Web servers where the inbuilt Cache Array Routing Protocol is used to share requests between servers.

With CS MIMESweeper™ for Web guarding the gateway, all Web-based transmissions, whether entering or leaving the network, are disassembled, evaluated against the governing security policy and scrutinized at the binary level before being allowed to pass through.

Policy-Based Content Security

The power of CS MIMESweeper™ for Web is that it gives organizations a way to take control of the flow of Web content into and out of the organization — custom-fit to their own business environment, employee needs and policies about Web use in the workplace.

CS MIMESweeper™ for Web makes Web traffic secure, as defined by the organization's security policy. Sample policies are available as part of the install process to help system administrators build their policy step by step, with as many exceptions and permutations as needed.

For example, in addition to scanning for viruses and other potentially malicious incoming code, an organization might use CS MIMESweeper™ for Web to block MP3 and AVI downloads as well as various news, shopping and personal finance Web pages during work hours for most employees, but allow the finance and marketing departments special access because of work-related needs. Or the company might employ text-based analysis to ensure that confidential content is not sent out of the company via Web-based mail.

It's up to the IT manager and business decision makers to determine the content-security policy that best fits the organization; CS MIMESweeper™ for Web provides the level of scrutiny and protection required.

How CS MIMESweeper™ for Web Works

Not only does CS MIMESweeper™ for Web protect an organization from incoming threats, it also protects from 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 first authenticates the user and applies that user's Internet access privileges according to the security policy. CS MIMESweeper™ for Web integrates with existing LDAP, Windows authentication methods or can apply policy based on the client IP address.
- 2. URL Filtering.** CS MIMESweeper™ for Web compares the URL against the extensive URL database of more than 5.6 million URLs to determine if the URL has been categorized into one of the 40 categories. If so, then the next step is to determine if the user requesting this page is allowed access that particular category of sites. If the user is not allowed access then the page is blocked and no more processing takes place. If the user is allowed access then the processing of the actual 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, and 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, and 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™ screens out designated file types, analyses 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 before letting it pass, 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.

Highly Flexible, Customizable Policies

Instead of applying a single, global content security policy across the organization, CS MIMESweeper™ for Web gives customers the ability to apply different screening policies to different groups of users — or even individuals. This added flexibility enables administrators to implement targeted security policies that are appropriate and relevant to people with different roles and responsibilities.

- **Scenario folders.** System administrators can create scenario folders to define the security settings for groups of users. For example, a Sales scenario folder might contain the security parameters appropriate for an employee in that role, and could also be easily applied to an individual.
- **Access times.** CS MIMESweeper™ for Web allows for time-specific policies, that is, security settings that are active only during certain times of the day or week. For example, non work-related URLs might be blocked only during regular office hours, allowing employees to access them during non-work hours. Of course, all other policies would still be active during non-work times.
- **URL zones.** Groupings of URLs can be specified for exclusion from content analysis, to speed delivery of trusted Web content.
- **Web categories.** Categories are types of Web pages, such as sports or news sites, which can be identified using a combination of screening techniques, for example, text analysis, PICS filtering and URL lists. The new URL Filter Category (see New Features below) is a powerful plug-in that draws on a perpetually updated database of millions of categorized URLs, eliminating the administrative overhead of managing URL lists and categories manually.

- **Inherited policies.** Policies are arranged in a hierarchical structure, so that employees at lower levels in the organization can “inherit” the policies specified at higher levels. Alternatively, while a policy might cover the whole organization, it can be overridden as needed on a departmental or individual basis.
- **User lists.** CS MIMESweeper™ for Web takes advantage of existing text-based, LDAP or Windows NT/2000 user directories for user authentication, policy determination for a specific user, runtime statistics and reporting.

Administrative and Reporting Capabilities

CS MIMESweeper™ for Web includes broad enhancements to help system administrators oversee their Web gateway and content security system, including more powerful features for gathering, analyzing and presenting data about system use and security threats.

- **Auditing and graphical reporting capabilities.** CS MIMESweeper™ for Web includes comprehensive auditing and reporting functions that integrate with a SQL Server back end. The system can generate standard or custom-built graphical reports based on accumulated CS MIMESweeper™ data, providing detailed information such as the most intensive system users, sites visited and threats detected.
- **Intuitive user interface and MMC integration.** The CS MIMESweeper™ for Web UI plugs right into Microsoft Management Console. This intuitive graphical environment makes CS MIMESweeper™ easier to implement and administer — and easier still for IT organizations that already take advantage of MMC to manage other IT systems. Users already familiar with CS MAILsweeper™ for SMTP will find CS MIMESweeper™ for Web easy to deploy and administer because of the common interface.
- **Real-time monitoring.** A runtime statistics function provides a snapshot of the number of users, concurrent connections and more. This data can be linked to the Performance Monitor to generate, for example, a graphical representation of cache usage.
- **Security alerts.** Security events can be configured to trigger administrator alerts via e-mail, using Windows NT alerts, or in SNMP format routed to a management package such as HP Openview.

New and Enhanced Features in CS MIMESweeper™ for Web

CS MIMESweeper™ for Web 5.0 introduces major new benefits that reduce costs and stop all web-based threats.

Increased Scalability

CS MIMESweeper™ for Web makes it very easy for organizations to increase the total number of users, without having to rely on costly third party load-balancing software, and means up to 4 servers can now be run in an array in a load-balanced configuration.

Increased Performance

A 300% increase in performance per server means each server in the array can support

approximately 2000 users enforcing a comprehensive Web policy consisting of AV, lexical analysis, file blocking, and URL filtering.

Increased Cache Size

CS MIMESweeper™ for Web is a full caching security Web proxy server. 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 the cache.

Easier to manage

The Web-policy can now be managed across all servers in an array as if they were a single entity, providing easier management of a consistent Web policy. The management interface is similar to the CS MAILsweeper™ for SMTP interface, and this overlap in policy configuration maximizes skills transference, with minimal training where both solutions have been deployed alongside each other.

Detection

- **Page based categorization**
The URL database now provides both domain and page based categorization – for example www.bbc.co.uk/sports is categorized as sports, whereas www.bbc.co.uk/ is categorized as arts and entertainment.
- **Improved URL database**
Now more than 5.6 million URLs, with 40 categories clearly defined that contain more than 900 million Web page references, covering 65 languages.
- **Malicious script analysis**
Improved security by detecting and blocking suspicious and potentially malicious script, whilst allowing the many pages that include safe script to pass.
- **Symantec Anti Virus tool**
Added flexibility by providing additional AV support for Symantec AV via the Content Scanner scenario.
- **Policy selection based on IP address**
Allows policy to be defined in terms of the client IP addresses rather than individual user credentials, an often requested enhancement in organizations where the IP address better determines the level of Web access required.

Reporting

- **New email Action**
Generates important notification emails immediately a particular type of threat or content type is detected, regardless of whether the page was delivered to the user or not.
- **SMTP email alerter**
By replacing the Windows Messaging alerter with an equivalent email alerter
CS MIMESweeper™ for Web allows greater flexibility by enabling the use of the mail server's distribution lists when sending alerts.
- **Web-based reporting**
Web-based reports mean greater accessibility by being viewable via a standard Web browser, included is "The Top 100 Users", "Top 50 web sites requested", "Top Internet Users by Volume", "Top threats detected" etc.
- **Standard format transaction log**
Support for 3rd party reporting tools has been improved because the transaction log files now conform to the W3C Extended Log File Format providing more choice and better operation with your existing reporting tools.

Installation and Product Walk-Through

Now that you've read about the new functionality in CS MIMESweeper™ for Web, let's take a look at the product itself. This brief walk-through will familiarize you with the CS MIMESweeper™ interface and give you an understanding of how a content security policy is implemented, as well as how it looks to the end user. While this guide only gives you a glimpse of the features in CS MIMESweeper™ for Web, it provides step-by-step installation instructions and a straightforward introduction to the product. We hope you will

continue on to review and test the many features that set CS MIMESweeper™ for Web apart as a best-of-breed content security solution.

In addition to this reviewer's guide, there is also an evaluation CD and Administrator's Guide. To review CS MIMESweeper™ for Web and take the following guided tour, you will need to install the product on a Windows™ 2000 server system with Internet access. A client system is not required to test CS MIMESweeper™ for Web.

You need the following minimum hardware and software to install CS MIMESweeper™ for Web Policy Engine.

Hardware

- Pentium III 1 GHz or above (dual processor recommended)
- 1Gb RAM
- 500Mb disc space (plus up to 4G for the cache)

Software

- Windows 2000 (Server or Advanced Server) with Service Pack 3
- TCP/IP network protocol
- Internet Explorer 5.5 or later
- Microsoft .NET Framework 1.1.4322 *
- Microsoft Messaging Queuing Services **

* The Microsoft .NET Framework 1.1 can be found on the CS MIMESweeper™ for Web CD-ROM. Alternatively, you can download it from the Microsoft web site:
<http://www.microsoft.com/downloads/details.aspx?FamilyId=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en>.

** When installing Message Queues, it is recommended that you select Workgroup (or Private) mode. Microsoft Messaging Queuing can be found under Control Panel > Add/Remove programs > Windows components

Installing CS MIMESweeper™ for Web

To install CS MIMESweeper™ for Web, insert the evaluation CD into the CD-ROM drive. The installation program loads automatically.

- Select **Install CS MIMESweeper™ for Web**.

Or from a location on the network run the set up program (**setup.exe**)

- Continue to click **Next** until the **Setup type** menu is reached
- Select **MIMESweeper for Web Policy Engine** from the three options
- Continue to click **Next** until the **Service configuration** screen is reached

- Enter the account details for the MIMESweeper for Web service
- Continue to click **Next** until the **Policy Selection** screen is reached
- Select **Evaluation Policy** from the three policies available
- Continue to follow prompts until MIMESweeper for Web is installed
- Click **Finish** twice to complete the installation and reboot.

Before you can start using CS MIMESweeper™ for Web you'll need to install the user license.

From Start > Programs > MIMESweeper for Web, select **MIMESweeper for Web Console**. The MIMESweeper for Web Console window appears.

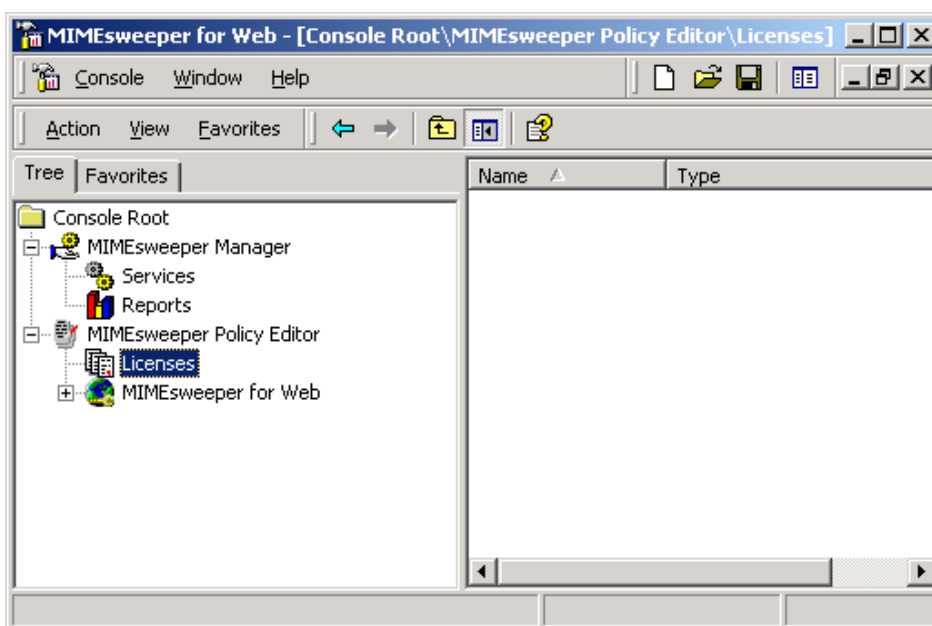


Figure 3. The CS MIMESweeper™ for Web Console is the “home page” of the MIMESweeper™ user interface, which adopts the Microsoft Management Console (MMC) format.

Expand the MIMESweeper Policy Editor (click the “+” to the left of the icon) in the navigation tree.

Select **Licenses**.

To launch the New License Wizard, right-click **Licenses** in the navigation tree and select **New > MIMESweeper for Web License** in the shortcut menu.

In the New License window, enter the company name, as well as the key and serial number that were provided with your evaluation materials. This must be exact.

Click **Next**.

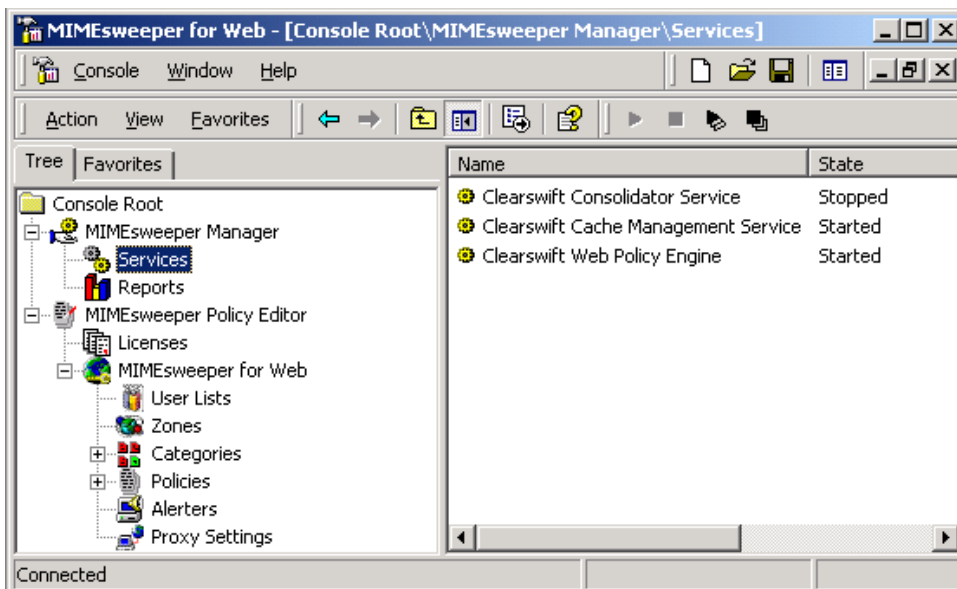
Enter any license name, such as “Lab License.”


Click **Next**, and **Finish**.

To test the URL Filter Category option (page 19), you may need to enter an additional license that includes the URL Filter Option. If this is the case then simply repeat the license installation procedure given above, entering the company name, key and serial number, as provided with your evaluation materials.

Now that your license information has been entered you must exit and enter the CS MIMESweeper™ for Web program because the license details are read on start up. You can now activate the CS MIMESweeper™ for Web services.

On the MIMESweeper for Web Console, expand MIMESweeper Management in the navigation tree and select Services.



Click the  icon above the right panel to start all services.

Note: The **Consolidator service** is related to the Web based reporting and will fail to start at this time and an alert will be displayed, and can safely be ignored. However, the **Cache Management** and **Web Policy Engine** service states should now be shown as being started.

Pre-installed Evaluation Policy

During the CS MIMESweeper™ for Web software installation you will recall that the option to install an Evaluation policy was selected. By selecting this option CS MIMESweeper™ for Web has been pre-configure with a Web policy consisting of some default Scenarios and Classifications.

Scenarios and Classifications

In essence, CS MIMESweeper™ for Web policies are built around two fundamental elements; scenarios and classifications. Scenarios define the types of things or content that CS MIMESweeper™ for Web searches for within the content sent to or received from the Web under specified conditions, and classifications define the actions CS MIMESweeper™ for Web takes once it detects an offending transmission. Scenarios are the rules, and classifications are the consequences.

Scenarios, such as forbidding suspicious JAVA script code to be downloaded from the Web, are applied to users or groups of users. And while an organization's policy will have a default set of scenarios, any user can be exempted from any scenario, or have custom scenarios created to fit specific circumstances.

Changing a Policy Scenario

Let's say that we want to modify an existing policy attribute, or scenario, that blocks the download of any sound or video file. In this case, we're going to relax the policy, allowing employees to download sound and video files less than 100 Kb, instead of blocking them altogether.

On the MIMESweeper for Web Console, expand **MIMESweeper Policy Editor** in the navigation tree, then expand **MIMESweeper for Web** and expand **Policies**.

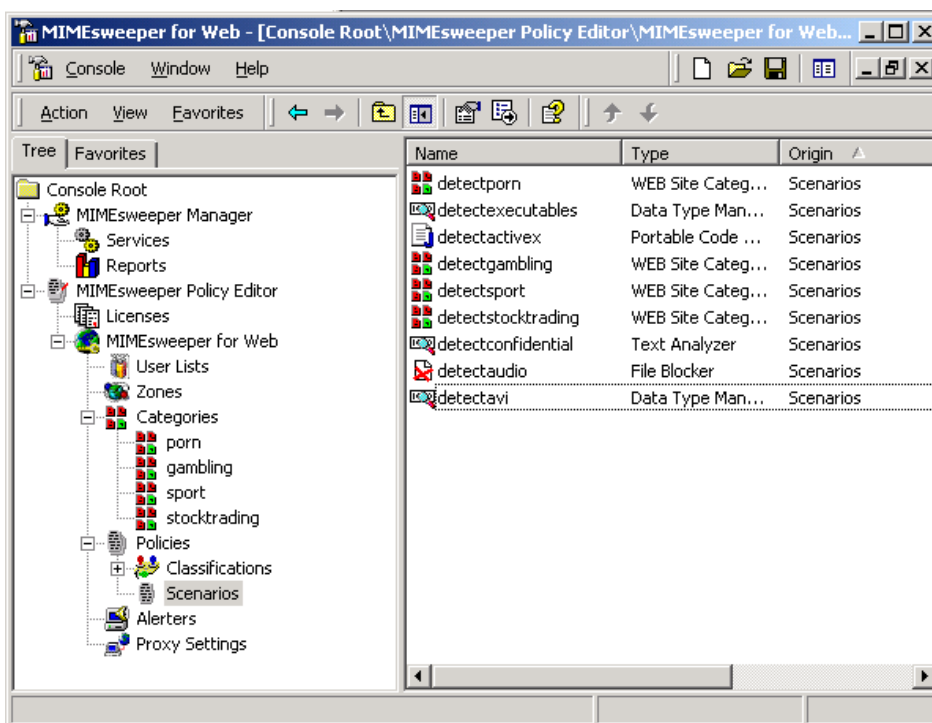


Figure 6. *detectavi* is an example of a policy attribute, or scenario, that establishes how certain kinds of downloads are handled.

Select **Scenarios**, and on the right panel, right-click **detectavi** and select **Properties**.

Click the **Size** tab and tick the **On size** button. Enter 100 Kb, and click **Ok**.

Look at the properties of some of the other scenarios to get a sense of how scenarios are built and what parameters they can include.

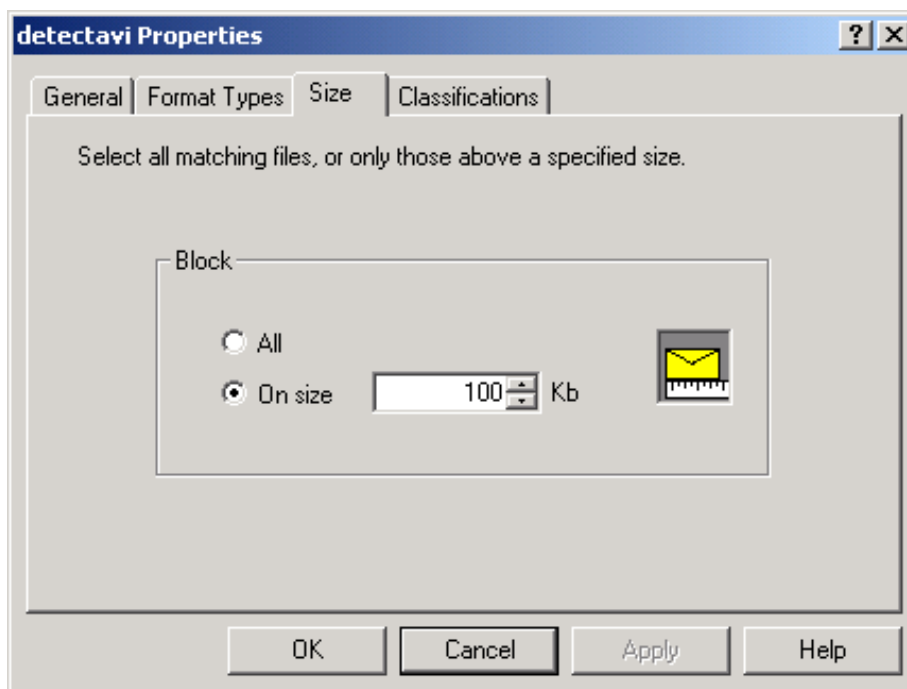


Figure 7. Scenarios can be built to take action on specific file types, file sizes, kinds of code, text parameters or any combination of attributes.

Changing a Policy Classification

Because of the change we just made to the **detectavi** scenario, CS MIMESweeper™ for Web will now look only for sound and video downloads over 100 Kb, and let smaller downloads pass through to the end user. But now we want to change the *actions* CS MIMESweeper™ for Web takes when it identifies a download over 100 Kb. The actions that result from CS MIMESweeper™ finding a policy-offending Web transmission are governed by classifications.

In this case, we're going to add a log action to the **AVidetected** classification. If CS MIMESweeper™ identifies a sound or video transmission over 100 Kb, this change will cause CS MIMESweeper™ to document the event by making an entry in the Windows NT/2000 application log.

In the navigation tree of the MIMESweeper for Web Console, expand **MIMESweeper Policy Editor > MIMESweeper for Web > Policies > Classifications**, select **AVIDetected**, and then right-click the same item to view the shortcut menu.

Click **New > Log**. This opens the New Notification window. Click **Next**.

The Log Text window, which appears next, allows you to create a customized log entry for any transmission that triggers a classification action. "Tokens" are placeholders that stand for variables in log entries; such as the user name, URL visited, time detected and so on.

Click the Token drop-down button, select **UserName**, which then appears in the log text box, and complete the log entry as follows (or compose your own with any combination of text and tokens):

```
%USERNAME% attempted to download an image or video
over 100 Kb.
```

Click **Next**, and enter "Log Entry" into the text box.

Click **Next**, then **Finish**. This entry, including the actual user name, will appear in the Windows application log every time the Block Sound & Video classification has been triggered.

Setting Up Users and Assigning Scenarios

To see CS MIMESweeper™ for Web at work, we need to create a user list and assign scenarios. In this case, we'll define a user named Administrator (for simplicity). In addition to setting up this user, we'll create an exception to the global policy for this specific individual.

On the MIMESweeper for Web Console, expand **MIMESweeper Policy Editor**, then **MIMESweeper for Web**.

Select **User Lists**.

Right-click **User Lists** and select **New > NT User List**.

Click **Next** when the New User List window appears, and click **Add**.

Click **Show Users**, and select the **Administrator** account.

Click **Add**, and **Ok**. The Administrator account appears in the User List window.

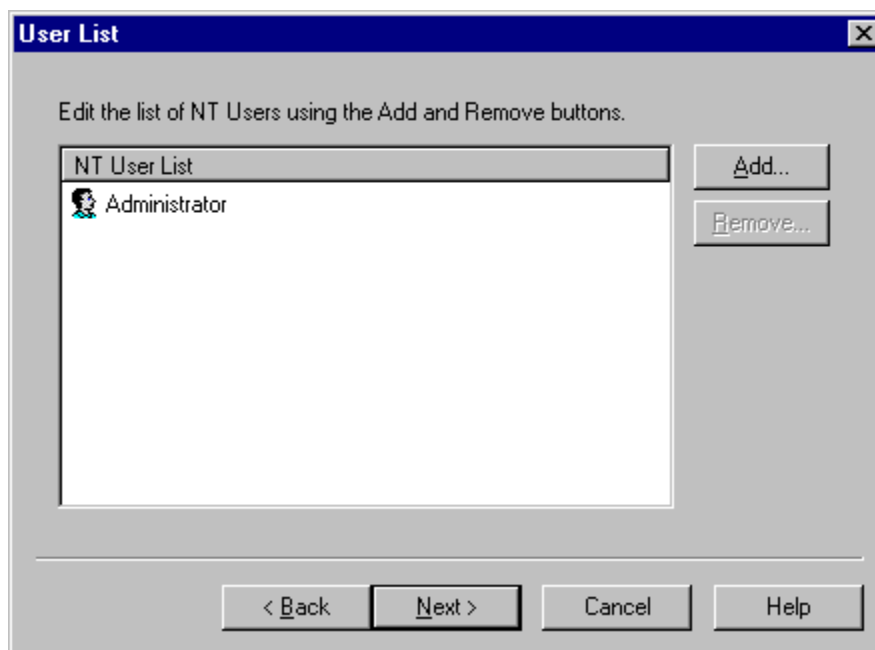


Figure 8. To activate a new content security policy, which can be customized as needed for groups or individuals, network users must first be added to the CS MIMESweeper™ for Web User List.

Click **Next**.

Leave the refresh time at the default 24 hours, and click **Next**.

At the New User List window, enter **Administrator**, and click **Next**, then **Finish**.

Note: For the moment ignore the Text file user list called *Administrators*

Once the user named Administrator is registered with the CS MIMESweeper™ for Web service, a scenario folder must be created specifically for that user. This folder will contain the MIMESweeper scenarios that apply to the Administrator use list.

In the MIMESweeper for Web Console navigation tree, expand **Policies** and select **Scenarios**.

Right-click **Scenarios** and select **New > Folder** from the shortcut menu.

Click **Next** in the New Folder window. The Routes window appears.

Click the down arrow under “User”, and select **Administrator**.

Click twice under “URL” and type “*” (asterisk).

Click twice under “Direction”, and select **Any** from the drop-down menu.

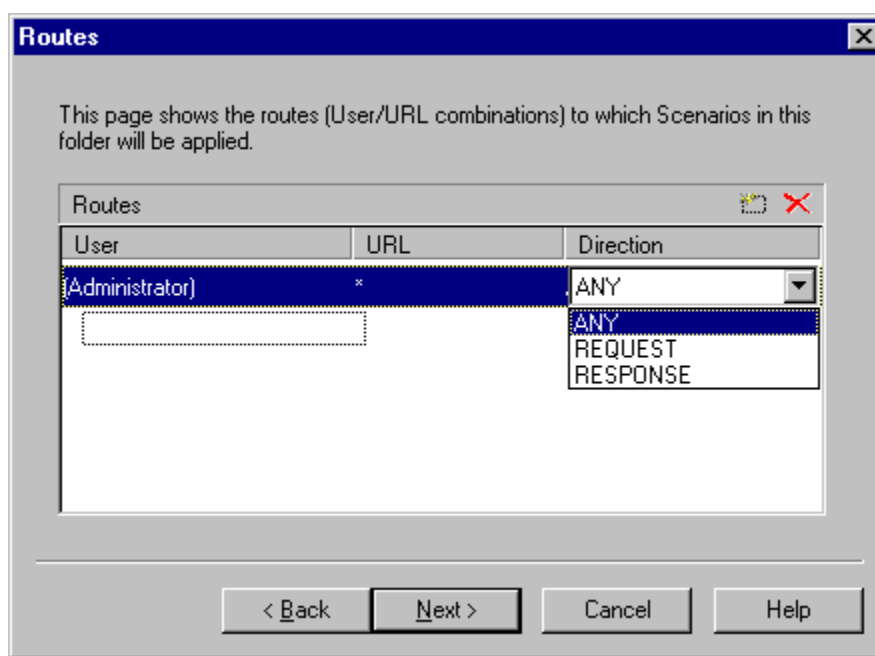


Figure 9. These settings in the Routes window indicate that all MIMESweeper™ scenarios applicable to the Administrator (i.e., in the Administrator folder) will govern any Web transmission — outgoing or incoming — between the Administrator and any other source.

Click **Next**.

Enter **Administrator** for the folder name then click **Finish**. Notice that Administrator appears under Scenarios in the navigation tree of the MIMESweeper for Web Console.

We’ve just created a scenario folder for Administrator that defines how transmissions that involve this user are to be handled. All of the global policies defined by the Evaluation sample policy are inherited and now apply to this user too.

Next we’re going to disable one of those policies, to create an exception for the administrator.

Select the new **Administrator** folder in the left pane of the Console. The global policies inherited automatically by the Administrator appear in the right-hand pane.

Right-click **detectexecutables** in the right pane, and click **Active** to deselect the scenario. Note that the State column of the right pane lists “Executables” as inactive.

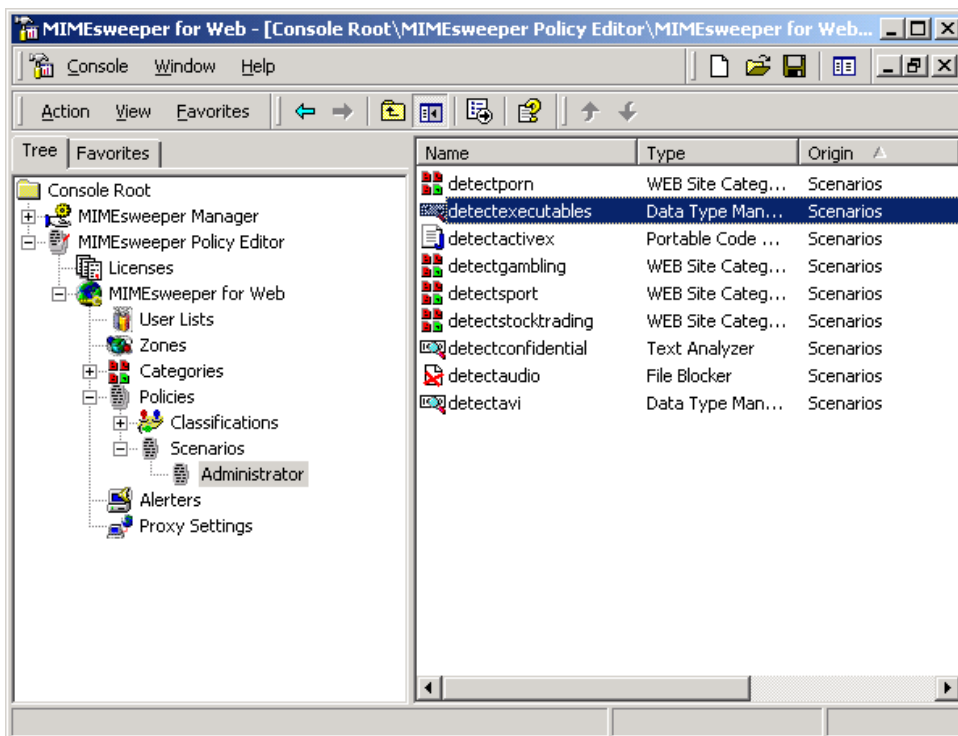


Figure 10. All policy scenarios are automatically “inherited” by new users when their scenario folder is created. In this case, the Executables scenario, which blocks the transmission of all executable files, has been disabled for the Administrator.

This would be a good time to review some of the scenarios that apply to the Administrator, as well as the corresponding classification properties. Modify some of the administrator’s settings if you like.

Creating a New Policy Using the URL Category Filter

Now that you have a sense of how to modify an existing policy, we’re going to create a new policy that prevents employees from browsing news-related sites at work. To do this, we will first define the category of URLs we want to block, then create the classification to define the actions CS MIMESweeper™ for Web will take, then create the scenario, which defines the circumstances under which the classification will be triggered.

To set up a new category, go to Categories in the MIMESweeper for Web Console under MIMESweeper Policy Editor.

Right-click **Categories**, and select **New > WEBSweeper Categorizer**. The New Category wizard appears. Click **Next**. Name the category “News URLs”. Click **Next** and **Finish**.

Back in the navigation tree, right-click **News URLs** under Categories, and select **New > URL Filter**. The wizard appears. Click **Next** and select **News** as well as **Government & Politics** from the list of URL filter categories. Click **Next**.

Name the category "News Filter" and click **Next** and **Finish**.

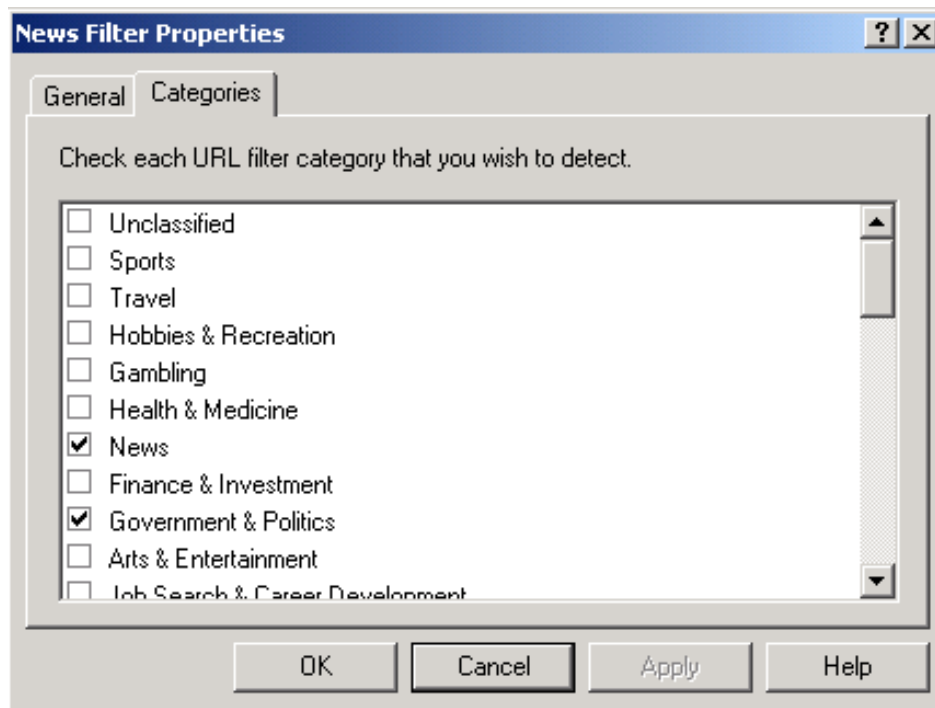


Figure 11. The URL Filter Category feature is based on a continually updated database of hundreds of millions of categorized Web pages.

To create the classification, right-click **Classifications** from the navigation tree, select **New > Classification**, and click **Next**. Name the classification "News URLs" as you move through the wizard screens. Click **Next** and **Finish**.

Right-click **News URLs** from the Classification list, and select **New > Block** from the shortcut menu. (Note: If no action is selected, the downloaded Web page will pass through to the user by default.) When the wizard appears, click **Next**.

Select the second option i.e. **File to replace blocked page** and then use the **browse button** to browse to the **templates** directory under the CS MIMESweeper™ for Web installed location.

Select the default block page template with the file name **default_blockpage.htm** to use one of the already defined templates. Then Click **Next** and name the action "News URL Message." Click **Next** and **Finish**.

Note: These templates are a useful starting point when creating your own look and feel for the block pages, progress message pages, and error pages.

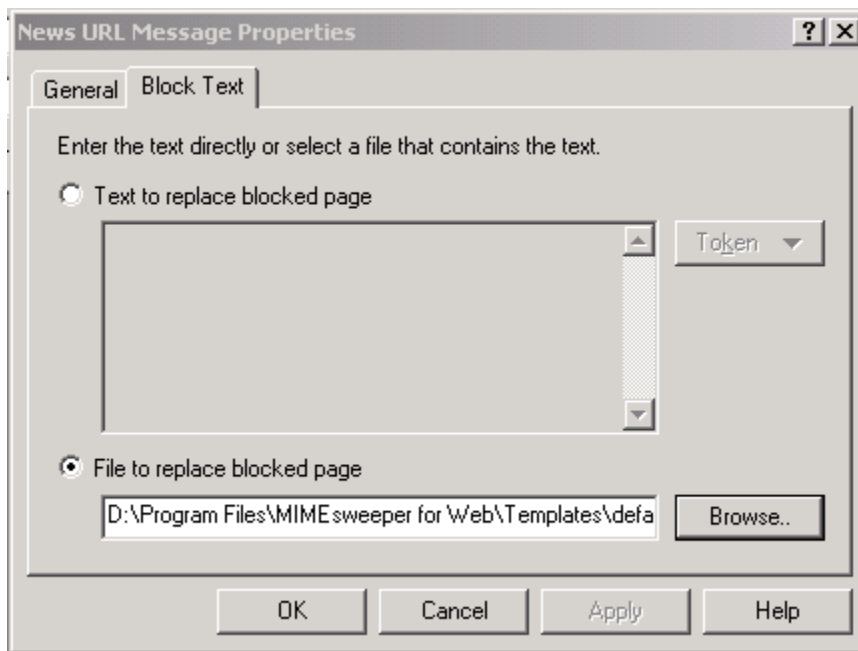


Figure 12. Creating an HTML message indicating that the URL has been blocked.

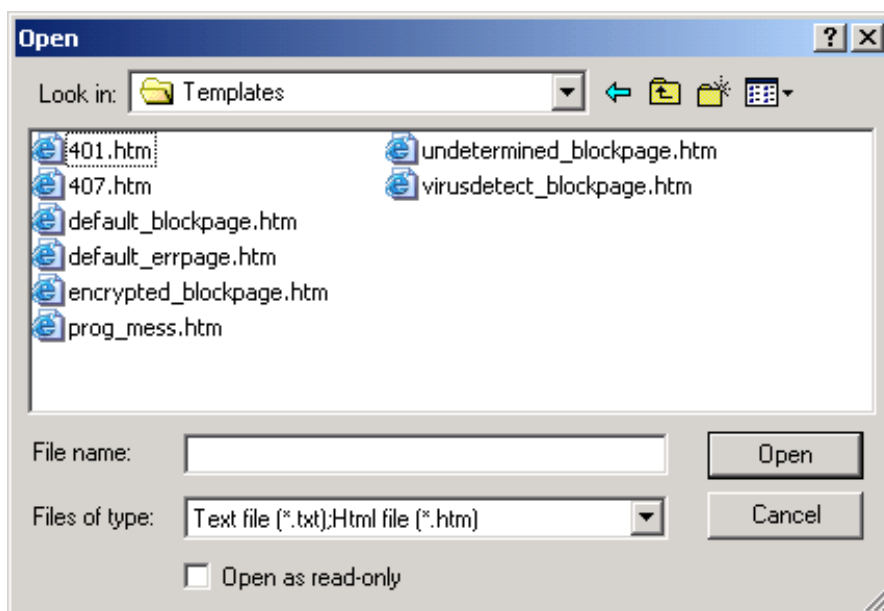


Figure 13. Default templates are pre-installed but many more can be created

Now, to finish defining the policy, we'll create the scenario.

Right-click **Scenarios** in the navigation tree. Select **New > Scenario > Web Site Category Filter**.

Click **Next** and leave both boxes checked on the Options screen. Click **Next**.

In the Filter window, select **News URLs** from the drop-down menu, and tick the **Always Detect** option. Click **Next**.

In the Detected Classification window, select **News URLs** as the action for News-related Web pages. Click **Next**.

Name the scenario "Block News URLs". Click **Next** and **Finish**.

Our next step is to test this policy with actual Web transmissions, but first the **Clearswift Web Policy Engine** service must be restarted to activate the changes we've just made.

Expand **MIMESweeper Management** in the navigation tree and select **Services**.

Right-click **Clearswift Web Policy Engine** in the right panel, and click **Stop**.

Right-click **Clearswift Web Policy Engine** again, and click **Start**.

Testing the Security Policy

The final step in this walk-through is to log on as the Administrator to see MIMESweeper function from the standpoint of the end user.

For evaluation purposes, these instructions apply to Internet Explorer.

Log onto your system as Administrator.

Launch Internet Explorer.

Select **Internet Options** from the **Tools** menu.

Click the **Connections** tab and click **LAN Settings**.

Tick the "Use a proxy server" check box.

Enter the IP address of the MIMESweeper for Web system, and leave the port default as 80.

Click **Ok** twice.

Now log on as the Administrator defined earlier and try accessing the following Web sites through the CS MIMESweeper™ for Web proxy with the policy we've just set up. Try visiting sites you think will conflict with some of the scenarios. Here are some easy ones:

News: <http://www.cnn.com/>

Sports: <http://espn.go.com/>

Gambling: <http://www.gambling.com/>

Pornography: <http://www.whitehouse.com/>

Stock trading: <http://www.charlesschwab.com/>

You should see the following access denied block page displayed in your browser and for each URL the classification given is automatically updated.

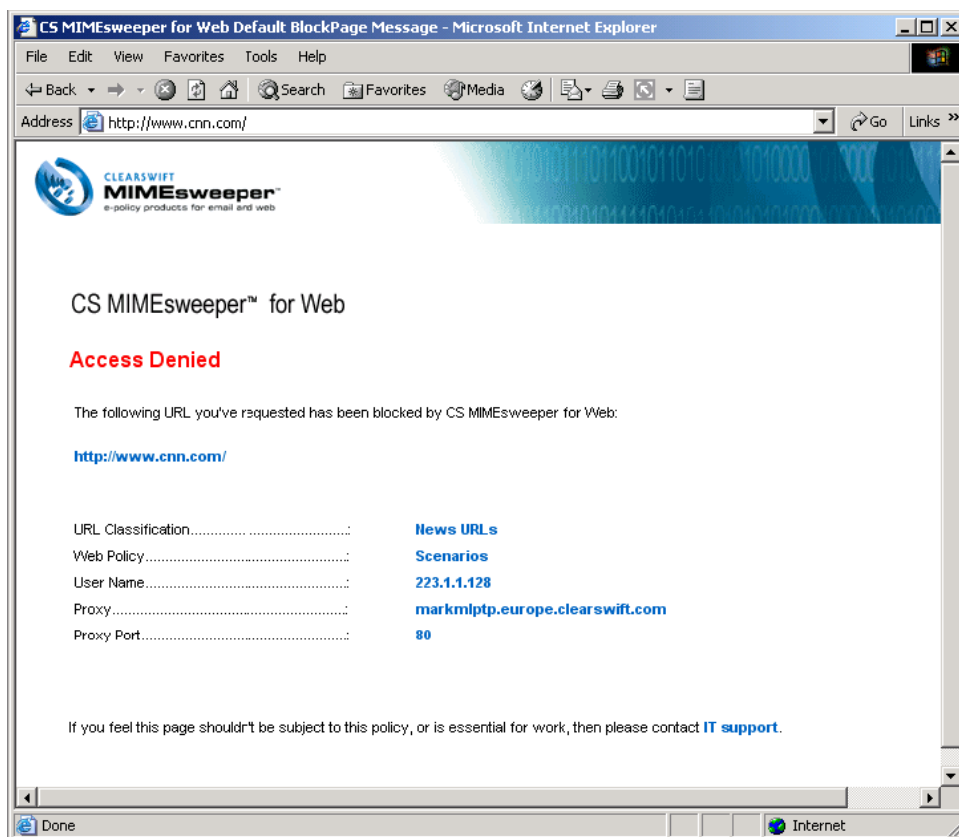


Figure 13. An access denied block page from the end-user's perspective.

This walk-through has given you just a glimpse at CS MIMesweeper™ for Web version 5.0 and Now that you have a feel for the interface, we encourage you to spend more time reviewing the features and comparing the capabilities of this product. We're confident you'll find that CS MIMesweeper™ for Web offers the deepest level of Web content security, the greatest policy flexibility and the richest administrative tools available today.

Finally, for details on Anti Virus tools supported by CS MIMesweeper™ for Web:

http://www.clearswift.com/products/msw/msw_web/scenarios.asp

Support / Customer Help

At Clearswift, our engineers work diligently to research, resolve and respond to customer inquiries through a combination of methods including telephone, e-mail, and voice-mail. Our team performs first-level problem resolution for delivery systems issues; acts as the front-line interface to customers, accepting trouble reports, and either resolve problems or dispatch/ escalate them where appropriate. Our Technical Support team members insure that all major technical support issues are properly addressed through proper training and a strong knowledge of the CS MIMesweeper™ products family. For Support queries please visit our website at www.clearswift.com/support



CLEARSWIFT™

Managing and securing
electronic communications

EUROPE

United Kingdom
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire, RG7 4SA
UNITED KINGDOM
Tel: +44 (0) 11 8903 8903
Fax: +44 (0) 11 8903 9000

Germany
Aminckstrasse 67
20097 Hamburg
GERMANY
Tel: +49 40 23 999 0
Fax: +49 40 23 999 100

France
54-56 Avenue Hoche
75008, Paris
FRANCE
Tel: +33 1 56 60 58 00
Fax: +33 1 56 60 56 00

Sweden
Skeppsbron 16
111 30
Stockholm
SWEDEN
Tel : +46 708 89 0001
Fax : +46 8 21 78 10

AMERICA

US West Coast
15500 SE 30th Place
Suite 200
Bellevue
Washington, 98007
UNITED STATES
Tel: +1 425 460 6000
Fax: +1 425 460 6185

US East Coast
1050 Winter Street
Suite 1000
Waltham
Massachusetts, 02451
UNITED STATES
Tel: +1 781 839 7321
Fax: +1 781 522 7488

ASIA PACIFIC/JAPAN

Australia Ground Floor 165 Walker Street North Sydney New South Wales, 2060	Japan Eisho Takanawadai Bldg 6F 2-11-8, Minato-ku Shirogane-dai Tokyo-to, 108-0071
AUSTRALIA Tel : +61 2 9424 1200 Fax : +61 2 9424 1201	JAPAN Tel : +81 (3) 5423 8171 Fax : +81 (3) 5423 1274

www.clearswift.com