
WEBSweeper 4.0 Reviewer's Guide

February 2001



For more information, contact:

Anne Marshall
Public Relations Manager
Baltimore Technologies
(425) 460-6018
Anne.Marshall@baltimore.com

Contents

Introduction	3
Product Background	3
The MIMESweeper Product Family	3
Potential Security Threats Resulting From Corporate Web Access	4
Network Integrity Issues	4
Business Integrity Issues	4
The WEBSweeper Approach to Web Content Security	5
Policy-Based Content Security	5
How It Works	6
New and Enhanced Features in WEBSweeper 4	6
Bidirectional Content Checking	6
Highly Flexible, Customizable Policies	7
Additional Screening Capabilities	7
Improved Administrative and Reporting Capabilities	8
Installation and Product Walk-Through	8
Installing WEBSweeper 4.0	9
Setting Up a Sample Policy	10
Activating a Sample Policy	11
Scenarios and Classifications	12
Changing a Policy Scenario	13
Changing a Policy Classification	14
Setting Up Users and Assigning Scenarios	15
Testing the Security Policy	17
Support / Customer Help	18
Appendixes	18

WEBSweeper 4.0 Reviewer's Guide

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."

Baltimore Technologies' WEBSweeper 4.0 is a newly-rearchitected 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 WEBSweeper provide the most powerful content analysis technology available, it offers a highly flexible system for enforcing a Web usage policy companywide.

This reviewer's guide lays out some of the key features and benefits of WEBSweeper 4, and gives you a starting point for evaluating the solution yourself. If you're already familiar with the WEBSweeper product you can jump to the New and Enhanced Features section to review the substantial additions and improvements we've made in version 4. Baltimore Technologies 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

WEBSweeper was first introduced by London-based Content Technologies in April 1997, and was the first product to fully address the security issues raised by opening corporate networks to the World Wide Web. In October 2000, Content Technologies was acquired by Baltimore Technologies, a global leader in e-security.

The MIMESweeper Product Family

WEBSweeper 4.0 is a member of the Baltimore Technologies MIMESweeper family, which has been expanding to address the full range of content security challenges faced by companies today. MIMESweeper, launched in 1995, was the first product on the market to scan e-mail and attachments

for content threats. Based on the same content-analysis engine, the MIMESweeper family has since become a leading solution for content security, providing organizations with defenses against business and network integrity threats — whether transmitted over internal e-mail systems, Internet mail or the Web.

Other solutions in the MIMESweeper family include MIMESweeper for Domino, MAILsweeper for Exchange and MAILsweeper for SMTP.

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 nonwork purposes (such as downloading MP3 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, WEBSweeper 4.0 gives organizations the means to protect themselves from both kinds of potential threats and oversee the use of Web in the workplace as the valuable resource it is.

Network Integrity Issues

- **Degradation or loss of service.** Network throughput can be compromised or even suspended entirely as a result of nonwork-related Web surfing or downloading images, MP3s, videos, 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 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 and "mailto" commands, cookies and so-called "cyberwoozles."

The WEBSweeper Approach to Web Content Security

WEBSweeper 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, WEBSweeper offers organizations a content-security solution that is fully customizable, down to the individual user.

WEBSweeper is best implemented as a standalone Windows NT-based HTTP proxy server behind the Internet firewall, although it can be deployed in conjunction with an existing proxy server. A WEBSweeper server supports 500 users assuming ten per cent concurrency¹. Organizations with higher levels of concurrent Web access can deploy clustered configurations with multiple WEBSweeper servers using third-party load balancing products to distribute user sessions.

With WEBSweeper guarding the gate, 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 WEBSweeper is that it gives organizations a way to take control of the flow of Web content into and out of the enterprise — custom-fit to their own business environment, employee needs and policies about Web use in the workplace.

WEBSweeper makes Web traffic secure, as defined by the organization's security policy. Sample policies are available to help system administrators build their policy step by step, with as many exceptions and permutations as needed, even to the level of an individual employee.

For example, in addition to scanning for viruses and other potentially malicious incoming code, an organization might use WEBSweeper 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 the Web.

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 per cent concurrency means 50 of the 500 users accessing the Web will be downloading or uploading new pages/files at exactly the same time.

It's up to the IT manager and business decision makers to determine the content-security policy that best fits the organization — WEBSweeper provides the level of scrutiny and protection required.

How It Works

To implement a content-security policy, WEBSweeper manages objects and data flowing through the Internet gateway in four stages:

- 1. Policy identification.** When a user initiates a transmission, WEBSweeper first authenticates the user and applies that user's Internet access privileges according to the security policy. WEBSweeper integrates with existing LDAP, Windows NT or text-based user directories.
- 2. Content disassembly.** WEBSweeper then 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. WEBSweeper 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.
- 3. 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. WEBSweeper screens out designated file types and URLs, analyzes text to identify potential security breaches, and identifies potentially dangerous executable code, such as HTML automatic mailtos, hidden forms and data-siphoning "cyberwoozles." WEBSweeper also integrates with the leading virus scanners, and supports multiple, concurrent anti-virus solutions.
- 4. Classification.** Once the content has been fully disassembled and analyzed, WEBSweeper 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 notification to appropriate parties can be implemented via SNMP alerts, Windows NT alerts or e-mail alerts.

New and Enhanced Features in WEBSweeper 4

Version 4.0 of WEBSweeper is a substantial upgrade that extends the product's flexibility and administrative tools, ease of use, reporting and more. With its end-to-end feature set, WEBSweeper 4.0 continues to lead the category in Web content security.

Bi-directional Content Checking

Not only does WEBSweeper protect an organization from incoming threats, but it also protects from outgoing threats. With desktop Web access, users have the ability to post or upload sensitive information to the Web, either through Web-based e-mail systems or via online forums of various sorts. These channels sidestep Internet mail security systems and provide a way for sensitive information to get out if Web security is not in place. WEBSweeper analyzes all Web traffic at the gateway, whether server-to-client or client-to-server, to ensure that it complies with the organization's security policy.

Highly Flexible, Customizable Policies

Instead of applying a single, global content security policy across the enterprise, WEBSweeper 4.0 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.** WEBSweeper 4.0 allows for time-specific policies, that is, security settings that are active only during certain times of the day or week. For example, nonwork-related URLs might be blocked only during regular office hours, allowing employees full Web access during nonwork hours.
- **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.
- **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 enterprise, it can be overridden as needed on a departmental or individual basis.
- **User lists.** WEBSweeper 4.0 takes advantage of existing text-based, LDAP or NT user directories for user authentication, policy determination for a specific user, runtime statistics and reporting.

Additional Screening Capabilities

Version 4.0 also incorporates many new features for advanced content screening.

- **Enhanced text analysis.** Content can be screened for specific phrases or words using Boolean statements, now including the NEAR operator. For example, an anti-pornography policy might include a statement such as “girls” NEAR “pics” AND “must be over 18.” Screening for words such as “pics” separately could block a considerable amount of legitimate content. (Another example is “chicken” and “breast.”)
- **Cleaning contaminated or malicious content.** WEBSweeper 4.0 is able to “clean” content that has been identified as containing a virus. This ability allows content to flow through to the user, stripped of the offending elements, instead of being blocked entirely. An advantage here is that administrators don't have to be involved in allowing content to pass through to the browser — WEBSweeper takes care of the policy management.
- **Options for handling downloaded executables.** Instead of universally blocking or passing all downloaded executable files, WEBSweeper 4.0 allows

administrators to block, pass or remove ActiveX components — or JAVAscript and VBScript code — independently.

- **Additional default file types screened.** In addition to the extensive range of data types previously screened by default, version 4.0 includes the following — container formats: RAR; document formats: 1-2-3; image formats: PCX, PIC, DXF, PHG, PSP, FLI; sound formats: MIDI, AU, VOC, MP3, WAV, AIF; video formats: AVI.
- **Binary Pattern Matcher.** The Pattern Matcher identifies file types by a defined byte sequence, for the most accurate identification of content elements.
- **Authenticode compatibility.** Authenticode transactions can now be managed through the WEBSweeper user interface, ensuring that downloaded code is secure, authentic and has not been tampered with.

Improved Administrative and Reporting Capabilities

WEBSweeper 4.0 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.** WEBSweeper 4.0 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 WEBSweeper data, providing detailed information such as the most intensive system users, sites visited and threats detected.
- **Intuitive user interface and MMC integration.** The WEBSweeper UI has been enhanced for ease of use and seamless integration with Microsoft Management Console. This intuitive graphical environment makes WEBSweeper 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 MAILsweeper for SMTP will find WEBSweeper 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.** With this version, 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.

Installation and Product Walk-Through

Now that you've read about the new functionality in WEBSweeper 4, let's take a look at the product itself. This brief walk-through will familiarize you with the WEBSweeper 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 WEBSweeper, 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 WEBSweeper apart as a best-of-breed content security solution.

In addition to this reviewer's guide, we've provided an evaluation CD and Administrator's Guide. To review WEBSweeper 4.0 and take the following guided tour, you will need to install the product on a Windows NT 4-based system with Internet access. A client system is not required to test WEBSweeper 4.

The following minimum requirements apply:

- A Pentium III 800MHz processor
- 2 GB of disk space recommended and at least 512 MB of memory
- Microsoft Windows NT Workstation or Server version 4 plus Service Pack 5
- Internet Explorer 5 Service Pack 1
- Microsoft Management Console 1.2
- Microsoft Data Access Components (DAC) version 2.1 or higher
- An NTFS partition for the installation of WEBSweeper
- TCP/IP networking
- Anti-virus tools, user's choice
- Microsoft SQL 7 for auditing and reporting

Installing WEBSweeper 4.0

To install WEBSweeper 4.0, insert the evaluation CD into the CD-ROM drive. The installation program loads automatically.

Click on the products menu.

Select **WEBSweeper**.

Click **Installation** on the left menu.

Click **Install WEBSweeper Version 4.0**. The Setup window appears.

Click **Next** to install the Windows Installer Service if required.

Reboot the system when prompted.

Setup will continue when the system has rebooted. Accept all defaults until the license agreement appears.

Accept the license agreement.

Accept the default destination folder or specify another (it must be located on an NTFS partition). Click **Next**.

Select full installation. Click **Next**, and **Next** again to begin the installation.

Click **Finish** twice to complete the installation and reboot.

Before you can start using WEBSweeper, you'll need to install the user license.

From Start > Programs > WEBSweeper, select **WEBSweeper Console**. The WEBSweeper Console window appears.

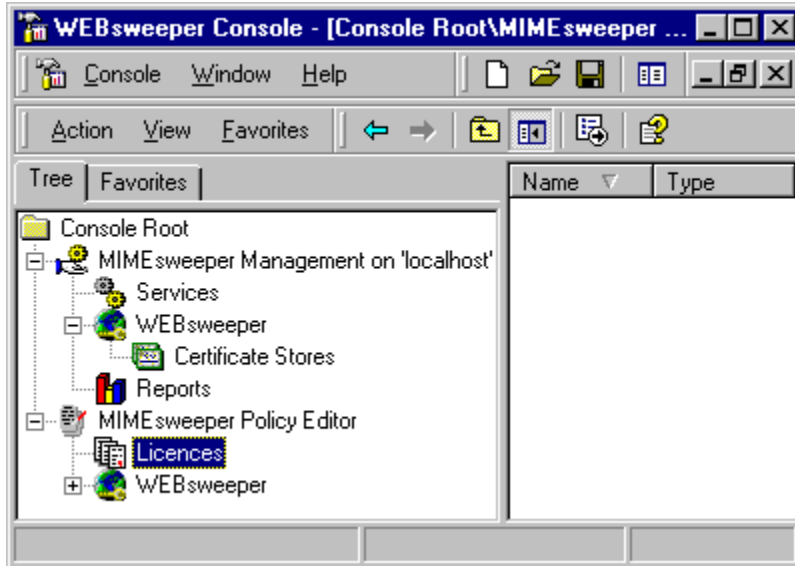


Figure 1. The WEBSweeper Console is the “home page” of the WEBSweeper user interface, which adopts the Microsoft Management Console (MMC) format.

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

Select **Licences**.

To launch the New Licence Wizard, right-click **Licences** in the navigation tree and select **New > WEBSweeper Licence** in the shortcut menu.

In the New Licence window, enter your 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**.

Now that your license information has been entered, you can activate the WEBSweeper service.

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

Right-click **WEBSweeper Security** in the right panel, and click **Start**.

WEBSweeper is now running.

Setting Up a Sample Policy

To speed your review of WEBSweeper 4.0, we've posted two sample content security policies online, which are needed for this guided tour. Go to the Baltimore Technologies site at <http://www.us.mimesweeper.com/>.

Select the nearest server (e.g., **North America**), and select **Download** from the menu at the top right corner of the page.

Click **Download** under “Extras, utilities and sample policies,” which is toward the bottom of the Download page, next to the link to more information.

The MIMESweeper Membership Center page will prompt you to register. Click the “**here**” link under “Become a Member.”

Fill in the form — all boldface fields are required.

Click **Submit**.

Select your nearest server from the following page to initiate the download.

When **Spsetup.exe** has been downloaded, move it into a temporary folder and run the program to install the sample policies utility. A wizard steps you through the simple installation. When you click **Finish**, the WEBSweeper Profile Utility window appears.

Click the **down arrow** to the right of “Set to apply” to see the drop-down menu of sample policies. In addition to the Default policy, two policies have been added—BasicPolicy and Evaluation.

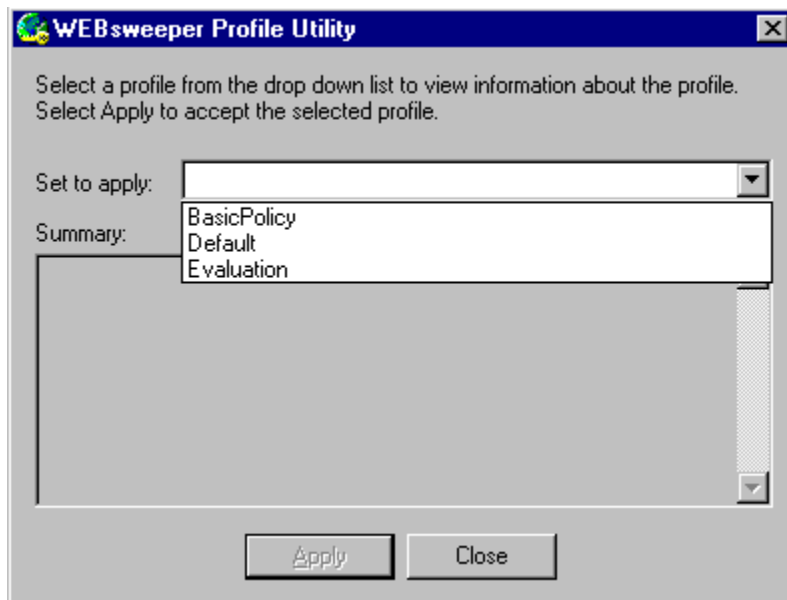


Figure 2. The installed sample policies appear in the WEBSweeper Profile Utility window.

Activating a Sample Policy

Now that the installation of WEBSweeper and the sample policies is complete, we can activate a policy and start exploring the content security features and product architecture.

Select **BasicPolicy** from the WEBSweeper Profile Utility drop-down menu. Note that a description of the configuration appears in the window.

Click **Close**.

Every time you activate or modify a policy, the WEBSweeper service must be restarted to make the new policy effective.

Click **Start > Programs > WEBSweeper > WEBSweeper Console**.

On the WEBSweeper Console, expand MIMEsweeper Management in the navigation tree and select **Services**.

Right-click **WEBSweeper Security** in the right panel, and click **Stop**.

Right-click **WEBSweeper Security** again, and click **Start**.

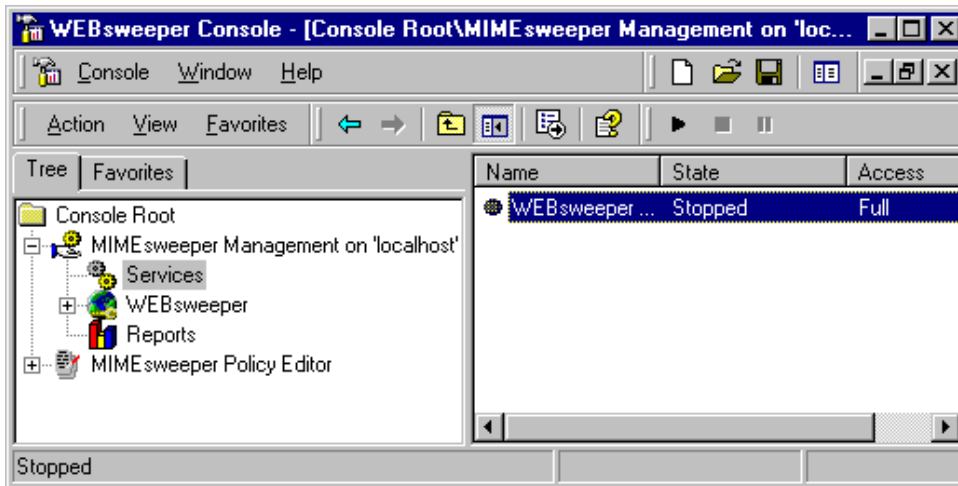


Figure 3. Whenever a new policy is activated or a modification is made to the active policy, the WEBSweeper service must be restarted to implement the change.

Scenarios and Classifications

In essence, WEBSweeper policies are built around two fundamental elements — scenarios and classifications. Scenarios define the types of things WEBSweeper screens for, and classifications define the actions WEBSweeper takes once it detects an offending transmission. Scenarios are the rules, and classifications are the consequences.

Scenarios, such as forbidding JavaScript 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.

First, we're going to load a new sample policy.

Click **Start > Program > WEBSweeper > WEBSweeper Profile Utility**.

Select **BasicPolicy** in the dropdown menu. Click **Apply**.

Click **Start > Program > WEBSweeper > WEBSweeper Console**.

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

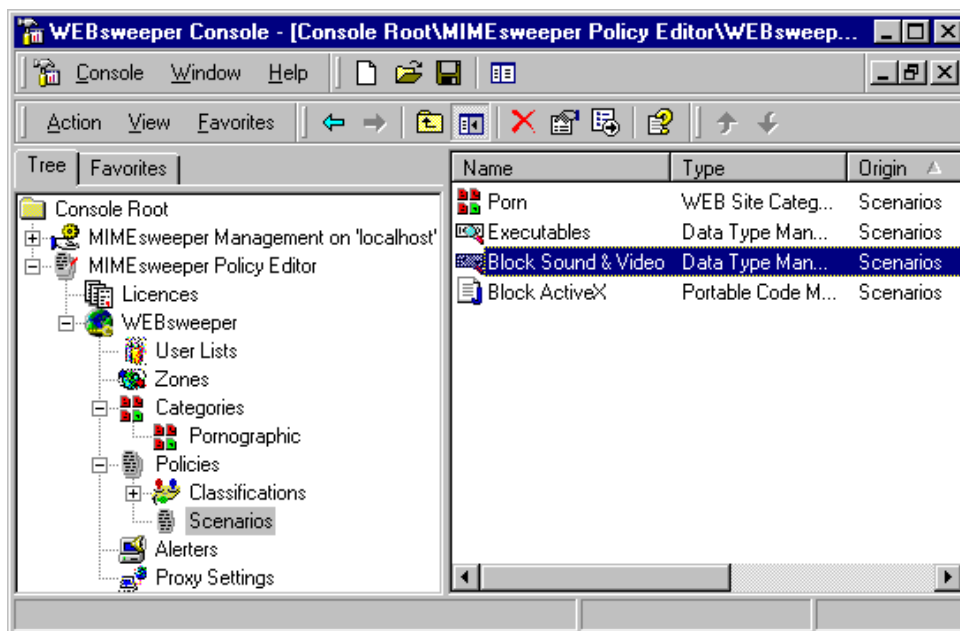


Figure 4. Block Sound & Video is an example of a policy attribute, or scenario, that establishes how certain kinds of downloads are handled.

Select **Scenarios**, and on the right panel, right-click **Block Sound & Video** and select **Properties**.

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

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.

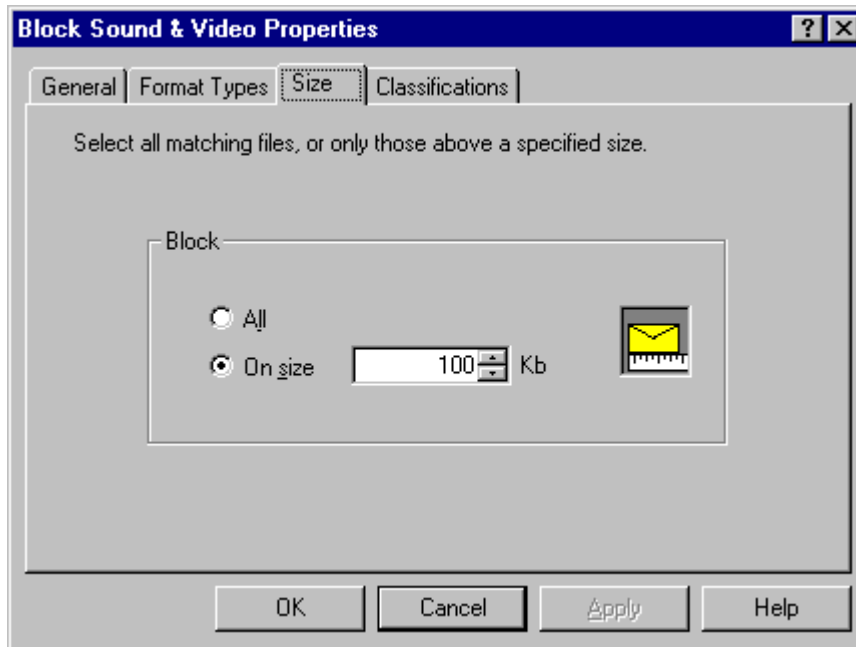


Figure 5. Scenarios can be built to take action on specific file types, file sizes, kinds of code, text parameters or any combination of attributes.

Changing a Policy Classification

Because of the change we just made to the Block Sound & Video scenario, WEBSweeper 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* WEBSweeper takes when it identifies a download over 100 Kb. The actions that result from WEBSweeper finding a policy-offending Web transmission are governed by WEBSweeper classifications.

In this case, we're going to add a log action to the Block Sound & Video classification. If WEBSweeper identifies a sound or video transmission over 100 Kb, this change will cause WEBSweeper to document the event by making an entry in the NT application log.

In the navigation tree of the WEBSweeper Console, expand **MIMESweeper Policy Editor > WEBSweeper > Policies > Classifications**, select **Block Sound & Video**, 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 NT application log every time the Block Sound & Video classification has been triggered.

Setting Up Users and Assigning Scenarios

To see WEBSweeper 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. But first we need to change back to the Evaluation policy.

Close all windows.

From the Windows desktop, click **Start > Program > WEBSweeper > WEBSweeper Profile Utility**.

Select **Evaluation** from the drop-down menu. Click **Apply**.

Click **Start > Program > WEBSweeper > WEBSweeper Console**.

On the WEBSweeper Console, expand **MIMESweeper Policy Editor**, then **WEBSweeper**.

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 **Okay**. The Administrator account appears in the User List window.

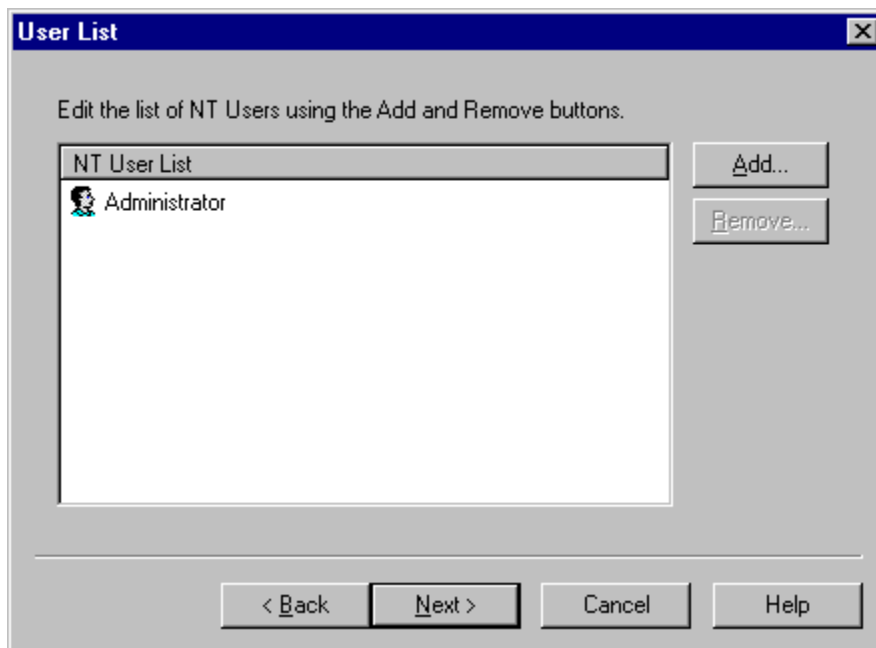


Figure 6. To activate a new content security policy, which can be customized as needed for groups or individuals, network users must first be added to the WEBSweeper User List.

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**.

Once the user named Administrator is registered with the WEBSweeper service, a scenario folder must be created specifically for that user. This folder will contain the WEBSweeper scenarios that apply to the Administrator.

In the WEBSweeper 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.

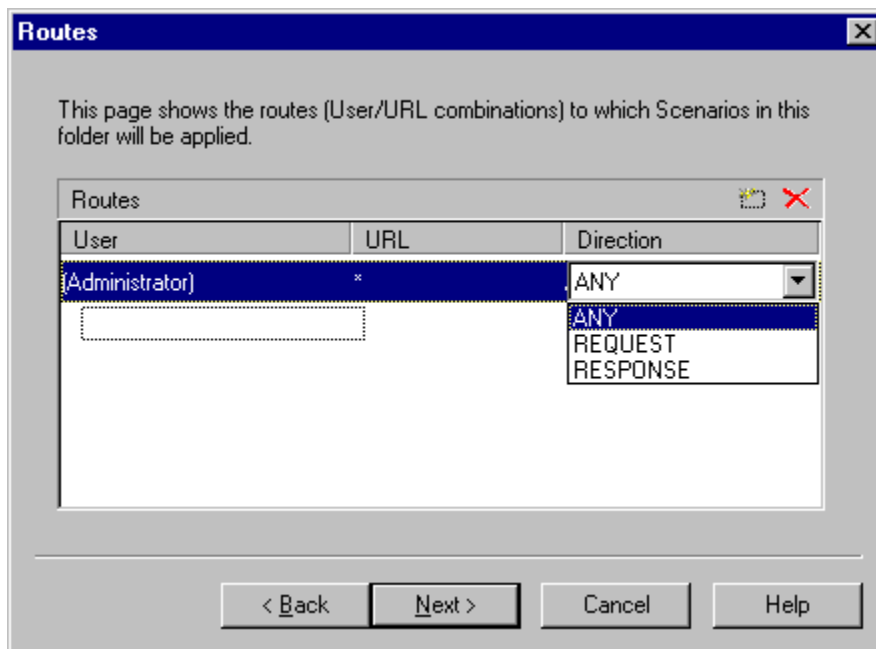


Figure 7. These settings in the Routes window indicate that all WEBSweeper scenarios applicable to the Administrator (i.e., in the Administrator folder) will govern any Web transmission — outgoing or incoming — between the Administrator and any other source.

Click **Next**.

Enter **Administrator** for the folder name, then click **Finish**. Notice that Administrator appears under Scenarios in the navigation tree of the WEBSweeper 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 now apply to this user.

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 **Executables** in the right pane, and click **Active** to deselect the scenario. Note that the State column of the right pane lists "Executables" as inactive.

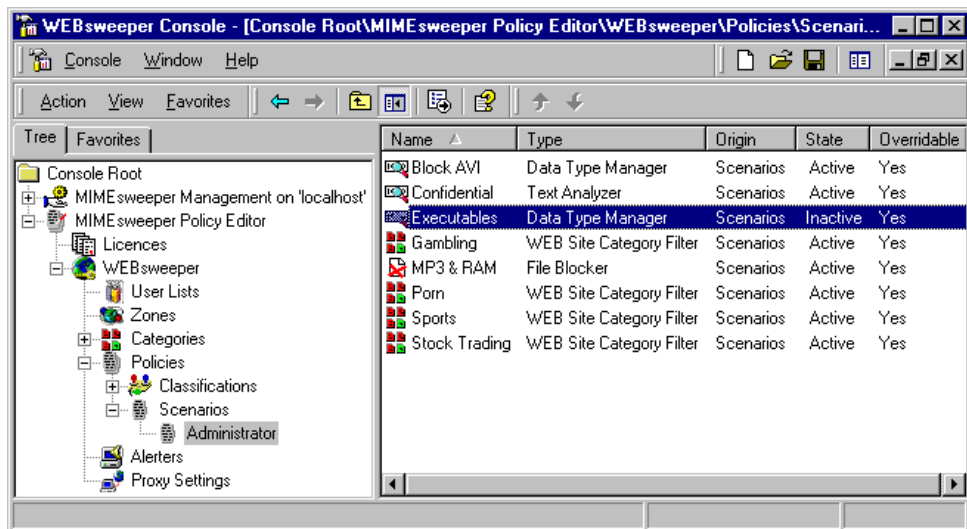


Figure 7. All policy scenarios are automatically “inherited” by new users when their scenario folder is created. In this case, the Executables scenario, which blocks the transmission of all executable files, has been disabled for the Administrator.

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 settings if you like, or even create a new scenario for the administrator. Our next step will be to test this policy with actual Web transmissions, so familiarize yourself with the rules now, in order to try to test them later.

Again, the WEBSweeper service must be restarted to activate any change or batch of changes you’ve made to a policy.

Click **Start > Program > WEBSweeper > WEBSweeper Console**.

On the console, expand **MIMESweeper Management** in the navigation tree and select **Services**.

Right-click **WEBSweeper Security** in the right panel, and click **Stop**.

Right-click WEBSweeper **Security** again, and click **Start**.

Testing the Security Policy

The final step in this walk-through is to log on as the Administrator to see WEBSweeper 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 WEBSweeper system, and leave the port default as 80.

Click **Okay** twice.

Now you are Administrator accessing the Web through the evaluation WEBSweeper service we just set up. Try visiting sites you think will conflict with some of the scenarios. Here are some easy ones:

Sports: espn.go.com

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

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

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

This walk-through has given you just a glimpse at WEBSweeper 4.0. 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 WEBSweeper 4.0 offers the deepest level of Web content security, the greatest policy flexibility and the richest administrative tools.

Support / Customer Help

At Baltimore Technologies, 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 MIMESweeper products family.

Baltimore Technologies MIMESweeper customer support in North America will respond to all requests for phone support within 4 business hours; e-mail within 2 business days after receipt of such request. Customer Support may respond via telephone or electronic mail. Telephone support hours are 5:30 a.m. to 6:00 p.m. PST at 425/460-6190; 24-hour support is also optionally available.

Appendixes

WEBSweeper Fact Sheet

WEBSweeper Data Sheet

Reporting Data Sheet

Savings Analysis Tool – available at www.mimesweeper.com/roi

MIMESweeper Family Product Guide