User Guide

WebMarshal 6.5

June 2009

M★RSHAL™

Contents

Chapter 1

Introduction 1

Chapter 2

Planning Your WebMarshal Implementation 7

Chapter 3

Installing WebMarshal 25

Chapter 4

Understanding WebMarshal Interfaces 55

Chapter 5

Implementing Your Web Content Security Policy 69

Chapter 6

Understanding Web Access Policy, Rule Containers, and Rules 79

Chapter 9

Managing WebMarshal Configuration 207

Chapter 10

Troubleshooting 251

Chapter 11

WebMarshal and NDS 259

Chapter 12

WebMarshal and Filtering Lists 263

About This Book and the Library

The *User Guide* provides conceptual information about WebMarshal. This book defines terminology and various related concepts.

Intended Audience

This book provides information for individuals responsible for understanding WebMarshal concepts and for individuals managing WebMarshal installations.

Other Information in the Library

The library provides the following information resources:

User Guide

Provides conceptual information and detailed planning and installation information about WebMarshal. This book also provides an overview of the WebMarshal user interfaces and the Help.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as [*value*]	• Optional parameters of a command
Braces, such as {*value*}	• Required parameters of a command
Logical OR, such as *value1*|*value2*	• Exclusive parameters. Choose one parameter.

About Marshal8e6

Marshal is a global vendor of Comprehensive Secure Email and Internet Management solutions that integrate content filtering, compliance, secure messaging and archiving, to protect businesses against email and internet-based threats. Marshal's content security solutions take a proactive approach to identifying email and web vulnerabilities to protect over seven million international users in more than 18,000 companies from the risks of email and Internet threats.

Marshal helps businesses of any size to:

- secure their IT network from incoming, outgoing and internal office email as well as internet content abuse and threats such as viruses, spam, malicious code and offensive content;
- protect company networks, employees, business assets and corporate reputation;
- comply with acceptable use policies, as well as corporate governance legislation and regulations for email retention and management needs.

The Marshal Security Suite

Hosted Service:

MailMarshal Service Provider Edition – hosted email security services

Gateway:

MailMarshal SMTP – gateway email security
MailMarshal Secure – email encryption and authentication
Marshal Security Appliance – gateway email security
WebMarshal – secure web gateway
Marshal Security Reporting Center – firewall, VPN and proxy server reports

Local Network/Client:

MailMarshal Exchange – internal email management
Marshal EndPoint Security – end user access and activity monitoring and enforcement

Contacting Marshal8e6

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. If you cannot contact your partner, please contact our Technical Support team using the contact information on the website.

Telephone:	+1 714 282 6111(Americas) +1 888 786 7999 (US Toll Free) +44 (0) 1256 848 080 (EMEA) + 64 9 984 5700 (Asia-Pacific)
Sales Email:	info@marshal8e6.com
Support:	www.marshal8e6.com/support
Website:	www.marshal8e6.com

Chapter 1
Introduction

Although the Internet is an essential tool for any business, it can limit productivity and increase risk. Many organizations use written policies to govern acceptable use of the Internet but lack the capacity for policy enforcement. WebMarshal offers industry-leading web filtering technology and flexible access control, providing both monitoring and enforcement of these policies.

What Is WebMarshal?

WebMarshal is an employee Internet management solution designed to promote responsible web use while providing protection from viruses, spyware, confidentiality breaches, and the downloading of non-business material. It complements, and is compatible with, traditional Internet firewalls and proxy servers. WebMarshal can be installed as a single server, or as an array of servers (at one or more locations) with a common configuration. WebMarshal supports installation on Windows 2008, Windows Vista, Windows XP Professional or Windows Server 2003.

WebMarshal is implemented as an authenticating proxy server for HTTP, HTTPS, and FTP protocols. The product offers optional proxy caching for HTTP. WebMarshal can also provide policy-based control of HTTP connection attempts from many streaming media and instant messaging applications. Where support for other protocols is required, WebMarshal can be used in conjunction with other proxy servers running on any platform.

WebMarshal allows you to monitor and enforce organizational Web access policy based on such factors as URL, file type and size, time of day, virus and/or spyware scan, and file contents. WebMarshal can apply browsing time and volume quotas to limit web usage. Details of current Web access sessions display in the Console. You can install one or more copies of the Console on workstations that can connect to the Array Manager server.

WebMarshal provides “zero-day” protection against malicious content using the TRACEnet filtering framework. TRACEnet is updated many times a day using blended threat data generated by the TRACElabs team.

In addition to the real-time content checking mentioned above, WebMarshal can also use a number of URL filtering lists, including the Marshal Filtering List, the Marshal8e6Filter List, and the Secure Computing SmartFilter.

WebMarshal can log Web access requests and use the information to produce detailed reports. Information is logged to a SQL Server database. You can generate reports using the Crystal Reports based WebMarshal Reports suite, or the web based Marshal Reporting Console.

WebMarshal can also log activity to text logs in WELF format. You can import these logs into integrated reporting software such as Marshal Security Reporting Center.

WebMarshal helps to eliminate non-business and potentially objectionable browsing and file uploading–trimming bandwidth needs, reducing time-wasting, shielding the organization from exposure to legal liability threats, and reducing the organization’s Total Cost of Ownership for web connectivity.

WebMarshal can also be installed as a plug-in to the Microsoft Internet Security and Acceleration (ISA) server. ISA Server provides caching and support for other protocols. Some WebMarshal features are not available in the ISA plug-in.

WebMarshal can authenticate users based on Windows login or Novell NDS login. WebMarshal can also control Web access on a per-workstation basis.

How Does WebMarshal Work?

The WebMarshal Processing Server(s) function as the web gateway of an organization. When a Web request is received, WebMarshal records the user name or workstation, time of day, and requested URL. WebMarshal then retrieves basic information about the requested resource from the remote server (or the WebMarshal proxy cache, if enabled).

WebMarshal next evaluates the request using the organization's Web access policy. At any stage of the evaluation, the request can be permitted, denied, or permitted with a warning.

If TRACEnet is enabled, WebMarshal checks the TRACEnet database and blocks the request if appropriate.

If Connection Rules are in place, WebMarshal determines the connecting application (such as an Instant Messaging application) and accepts or blocks the attempt.

If the request is encrypted using HTTPS, and HTTPS Rules are enabled, WebMarshal checks the validity of the site Certificate. Depending on your policy, WebMarshal can decrypt the traffic (either upload or download) for processing by Quota, Standard, and Content Analysis rules. WebMarshal re-encrypts the traffic for transfer between the WebMarshal server and the client workstation. *All data transmitted over networks is encrypted.*

When WebMarshal evaluates a standard Web request, it first checks time and volume quotas. Next, WebMarshal checks the URL of the requested resource. After full data has been returned to WebMarshal from the Web, the results can be evaluated by file type and size, checked for viruses and spyware, stripped of cookies, and checked for specific text content before being returned to the user. WebMarshal unpacks archive files and documents, and can apply evaluation to all unpacked files.

WebMarshal can apply TextCensor rules to evaluate text content of files. TextCensor can check HTML pages, other text files, and text unpacked from archives or Word documents. Based on the result of this evaluation, WebMarshal can block the request and/or add the URL to a URL Category, potentially denying future access to the entire site.

When a file or form submission is submitted for upload, it is evaluated against all criteria before being sent. WebMarshal can enforce Safe Search on selected search engines.

Both successful and denied requests can be logged to WebMarshal's database (unless they are explicitly excluded from logging). Data logged includes user account, workstation, URL, time, permission or denial, quota usage, and one or more custom classifications according to the organization's rules. This information is available for later reporting.

WebMarshal can also notify administrators of specific actions or notify end-users of blocked pages. You can associate the appropriate rule action when you create or modify rules.

Configuring WebMarshal

You configure WebMarshal rules and server options using the Console connected to the WebMarshal Array Manager. The Array Manager coordinates the activity of all other WebMarshal Servers in the array, and optionally logs information to the database.

Database software for the optional WebMarshal database is often installed on the same computer as the WebMarshal Array Manager component. The database stores the reporting data used by WebMarshal reports. WebMarshal supports the use of Microsoft SQL Server 2005/2008 Express (suitable for smaller organizations), Microsoft SQL Server 2005 or Microsoft SQL Server 2008.

Monitoring and Reporting

WebMarshal provides user interfaces for monitoring and daily administration of Web access policy. Using the Console, administrators can monitor server performance, review user sessions and web browsing activity, and adjust user permissions and quotas.

Administrators and managers can generate reports on WebMarshal activity with a choice of reporting options:

- WebMarshal Reports uses the Crystal Reports engine to produce versatile and detailed reports and graphs on demand. WebMarshal Reports can be installed on one or more workstations. This application is included for all WebMarshal trial users and customers
- The Marshal Reporting Console is a web-based application that can be deployed to support reporting on WebMarshal and MailMarshal SMTP. Marshal Reporting Console provides report scheduling and multiple export formats. This application is included for all WebMarshal trial users and customers.
- WebMarshal can also log activity in the WELF format. You can use WELF logs with Marshal Security Reporting Center to produce reports that cover different types of proxy and firewall devices.

What's New?

This section highlights the key new features documented in this *Guide*. For a complete list of changes in a particular release, and for a history of features introduced in previous releases, please refer to the Release Notes included in the WebMarshal distribution package.

Proxy Caching: WebMarshal includes the ability to cache HTTP web resources, providing quicker access and bandwidth savings.

TRACEnet: The Marshal8e6 TRACE team provides a "zero day" service that allows WebMarshal to identify and block malicious URLs, based on analysis of web, email, and "blended" threats.

SafeSearch: WebMarshal can now enforce use of the "Safe Search" function offered by some search engines, such as Google and Yahoo!.

Automatic Configuration Backup: WebMarshal now allows automatic backups of configuration, nightly and when configuration changes.

Marshal8e6Filter: WebMarshal supports use of the Marshal8e6Filter URL filtering list.

Customer Feedback: WebMarshal re-introduces the feedback functionality found in WebMarshal 3.7. This functionality delivers anonymous information about browsing history to Marshal8e6. The feedback helps to improve product quality and functionality.

Support for Microsoft SQL Server 2008: WebMarshal now supports the use of Microsoft SQL Server 2008 and SQL 2008 Express for the logging database.

Chapter 2

Planning Your WebMarshal Implementation

When planning to install WebMarshal, you should understand how WebMarshal handles Web requests, and the available installation scenarios to suit your needs.

This chapter provides information about these concepts and includes hardware requirements, software requirements, and checklists to help you through the planning process.

Planning Checklist

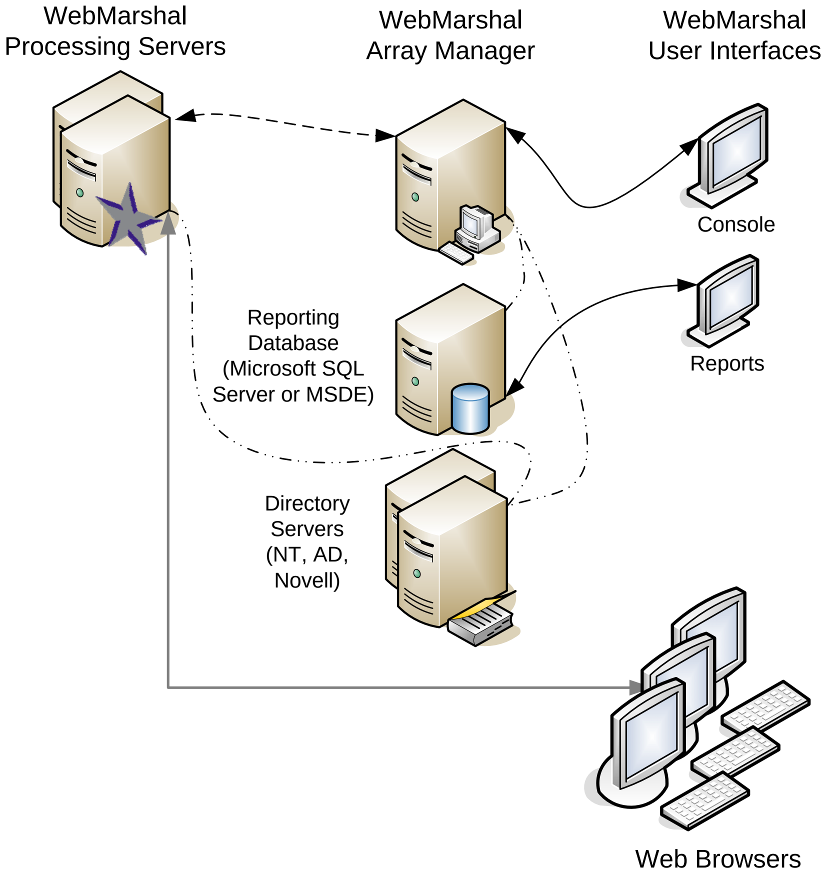
Plan your WebMarshal installation by reading the following sections and completing the following checklist:

☑	Step	See Section
□	**1.** Learn about important WebMarshal concepts.	“Understanding WebMarshal Components” on page 9.
□	**2.** Choose an *ISA Server Plug-in* or *WebMarshal Proxy Server* installation	“ISA Server Plug-in or WebMarshal Proxy Server” on page 13.

☑	Step	See Section
□	**3.** Choose a *single server* or *array* installation. ***If you selected an array installation,*** determine the number and location for the WebMarshal Processing Servers and Array Manager components, and load balancing method	“Single Server or Array” on page 13.
□	**4.** Ensure the computers meet the hardware and software requirements.	“System Requirements” on page 19.
□	**5.** Choose the malware detection software to use with WebMarshal.	“Supported Malware Protection Software” on page 21.
□	**6.** Collect installation information about your environment.	“Collecting Information for Installation” on page 22.

Understanding WebMarshal Components

WebMarshal implementations include several components. A small organization can install all components on one server. A larger organization can scale WebMarshal by installing the components on a number of different servers and workstations within the network, as shown below.



WebMarshal Components

Array Manager

Manages an array of WebMarshal Processing Servers. The Array Manager stores policy and controls communications between components.

Processing Server

Accepts Web requests, retrieves resources from the Web or local cache (Proxy service or ISA Server plug-in), and applies policy in the form of rules (Engine service). You can use one or more WebMarshal Processing Servers in your installation. Processing servers are also known as array nodes.

Note

WebMarshal caching uses a local directory to store Web content. This directory *must be excluded* from on-access or resident virus and spyware scanning**.** If it is not excluded, WebMarshal caching is disabled. The default location of the cache directory is within the WebMarshal install directory, but for most production servers it will be located elsewhere. ***If you change the location of the cache directory***, be sure that you also update virus scanner exclusions.

Console

Allows administrators to define policy (rules), configure WebMarshal, and monitor Web sessions and server health in real time.

Reports Console

Allows administrators or auditors to prepare Web management reports. Optional.

Marshal Reporting Console

Allows administrators or auditors to prepare Web management reports. Optional.

Other Software and Services

In addition to the above, most WebMarshal installations use the following software and network services.

Microsoft SQL Server or SQL Express

If you want to use WebMarshal Reports or the Marshal Reporting Console, you will need a Microsoft SQL Server to host the WebMarshal database that stores log information. If your web traffic volume and log retention requirements permit, you can use the free SQL Express. If the volume of data exceeds the 4GB limit imposed by SQL Express, use Microsoft SQL Server.

Tip

If you are installing WebMarshal as an array, you can enhance performance by installing the WebMarshal Array Manager on the same server as the SQL database.

Directory Server

If you want to import existing users and groups from your directory service for use in applying a Web Acceptable Use Policy, all WebMarshal servers must be able to connect with your directory server. WebMarshal can connect with Microsoft Active Directory or other Windows environments, as well as Novell NDS/eDirectory.

Malware Scanning Software

If you want to scan Web content for malware (viruses and spyware), you can install one or more supported malware scanners. See "Supported Malware Protection Software" on page 21. If you want to ensure protection of your servers, you can install scanning software of your choice on the servers.

Note

WebMarshal uses a temporary directory to unpack and scan Web content. This directory *must be excluded* from on-access or resident virus and spyware scanning**.** If it is not excluded, the WebMarshal Engine and/or the WebMarshal Controller service may be unable to start. By default, WebMarshal uses the `\temp` subdirectory of your install directory. You can change this location by editing XML configuration files on each processing server and restarting the WebMarshal services. ***If you change the location of the temporary directory*** for either or both services, be sure that you also update virus scanner exclusions.

Understanding Installation Scenarios

When planning a WebMarshal installation, there are two basic decisions to consider:

- Single server or Array
- ISA Server plug-in or WebMarshal Proxy Server installation

These decisions are independent. You can have a single server or an array of either type of WebMarshal installation.

Single Server or Array

You should consider an Array installation of WebMarshal if the following requirements apply:

- **High or growing Web request volume:** An Array allows you to add WebMarshal Processing Servers to provide additional capacity.
- **Multiple Web gateways:** at separate locations with the same access policies and centralized reporting. A WebMarshal Array Manager can manage policy for multiple gateways over WAN connections, with a single TCP port required for connectivity in many cases.
- **Redundancy:** Each WebMarshal Processing Server can continue to process requests independently if other servers fail.

Note

To maintain session logging correctly, each client must use a single processing server for an entire browsing session. One way to achieve this requirement is to set up Microsoft Windows Network Load Balancing using the NLB Client "Single Affinity" setting.

ISA Server Plug-in or WebMarshal Proxy Server

If you already have, or are planning to install Microsoft ISA Server 2004 or 2006 in your environment, you can install the WebMarshal sever as a WebFilter plug-in to ISA. If you do not have ISA, you can install WebMarshal as a standalone proxy server.

Note

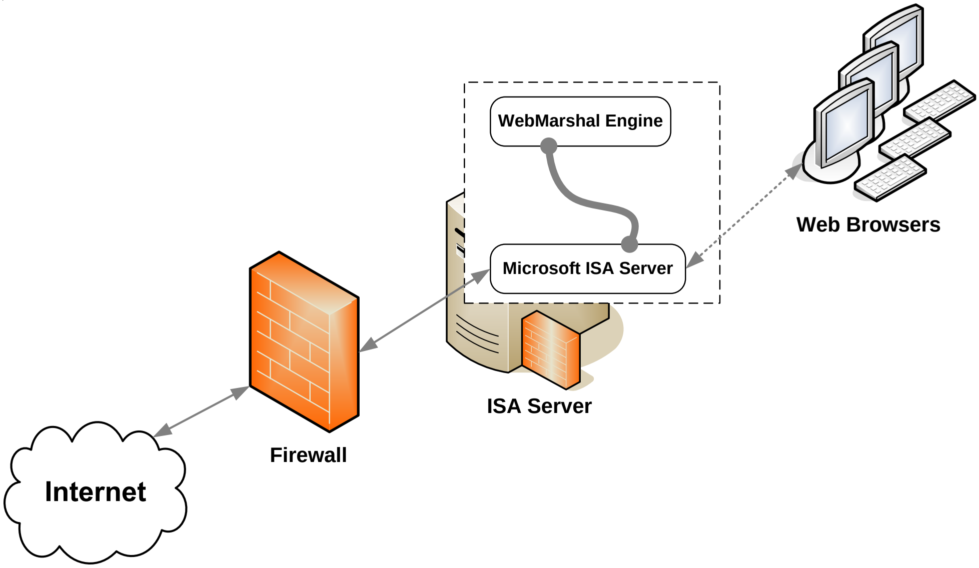
Some WebMarshal functionality is not supported in ISA Server plug-in mode. Read this section carefully to understand the limitations.

Marshal8e6 recommends you use the standalone WebMarshal proxy server unless you have a specific requirement to use ISA functionality, such as SecureNAT, that is not supported by the WebMarshal proxy server. If you want to use ISA caching, you can install WebMarshal on the same server as ISA and chain WebMarshal to ISA.

ISA Server Plug-in

WebMarshal can be installed as a “Web Filter” plug-in to Microsoft Internet Security and Acceleration (ISA) Server 2004 or 2006.

Note
You can configure WebMarshal plug-ins on multiple ISA servers using the WebMarshal array functionality.



The following points apply to Microsoft ISA Web Filter plug-in installations (additional details are available in Marshal8e6 Knowledge Base article Q10392):

- The Web Filter plug-in does not support HTTPS Content Inspection features, Connection Rules, Upload Content Analysis Rules, or Novell NDS. To use these features with ISA Server, install WebMarshal Proxy Server, and chain to ISA Server. To use proxy caching with the ISA plug-in enable caching in ISA (not WebMarshal).
- Either Windows Authentication or IP authentication (SecureNAT) can be used with the Web Filter plug-in, but not both.

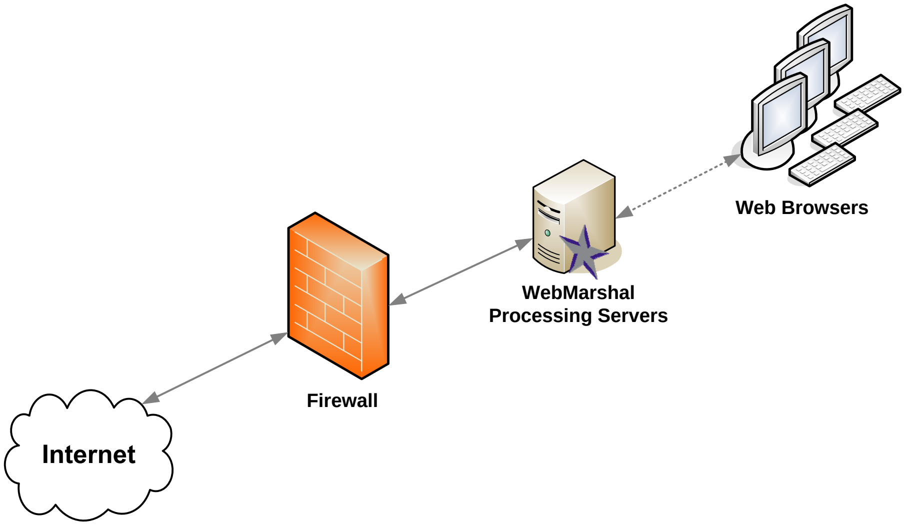
- ISA Server must be installed on all WebMarshal processing node servers before you select the ISA plug-in mode for WebMarshal. The WebMarshal configuration process installs the ISA Web Filter.
- WebMarshal must be installed to the same disk partition (drive letter) as ISA Server.
- Ensure that an Access Policy is configured, and that the user group "Everyone" *does not* have full access. Marshal8e6 recommends that you create a Windows NT group "Proxy Users" to contain all groups and users needing web access. Give this group full Web access within the ISA Server.
- All web users must be present on both the proxy and the WebMarshal user lists. The group "Proxy Users" should be added to the WebMarshal user groups so that all users are known to WebMarshal

WebMarshal Proxy Server

The WebMarshal Proxy Server can be installed in any of three scenarios.

Note
In each case you can configure a single WebMarshal server or an array of servers.

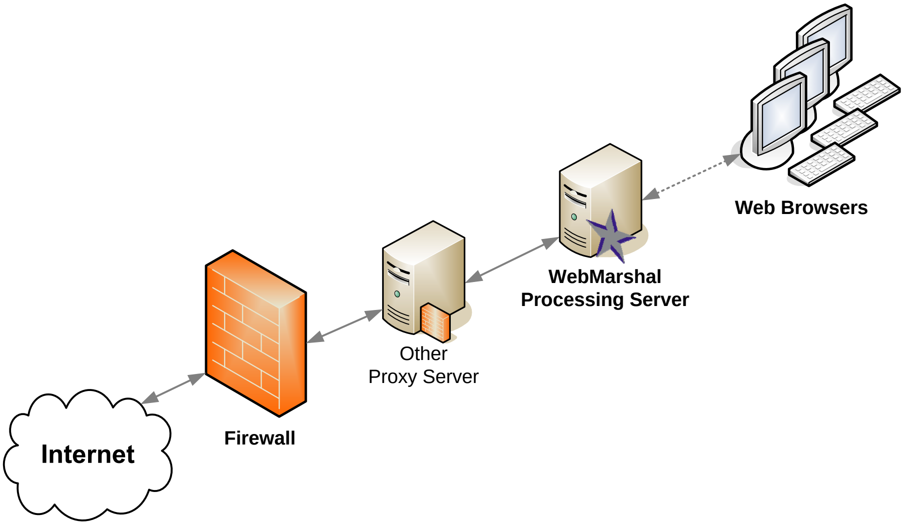
1. As a standalone proxy server. In this scenario, all Web requests are passed to the WebMarshal server, and all responses are returned from the Web (or WebMarshal proxy cache) through the WebMarshal server. Firewall rules should be configured to restrict Web traffic so that users cannot bypass WebMarshal.



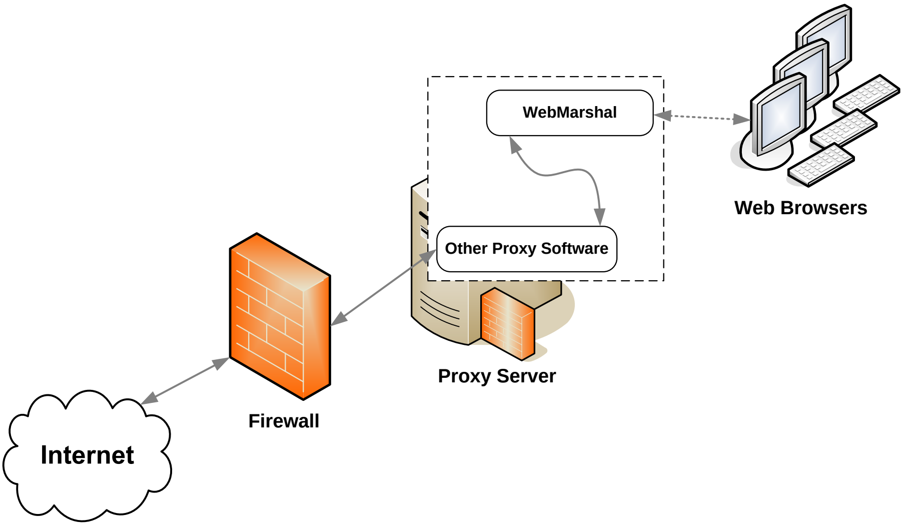
2. Chained to another proxy server running on another physical server. In this scenario, all Web requests are passed to the WebMarshal server. WebMarshal delivers the requests to the other server, and all responses are returned from the Web through the other server to WebMarshal and then to the clients. Firewall rules should be configured to restrict Web traffic so that users cannot bypass WebMarshal. Access rules on the other proxy server should be configured to allow traffic only from WebMarshal.

Note

In any chained installation, WebMarshal must be the first server in the chain (the client browsers must connect to WebMarshal directly). If WebMarshal is not the first server in the chain, the WebMarshal access policy will not be applied correctly.



3. Chained to another proxy server running on the same physical server.



If WebMarshal is installed on the same server as another proxy server, each must use a different port. Configure WebMarshal using the WebMarshal Configuration Wizard–Forward Proxy page. Be sure the other proxy software is configured appropriately.

For example, WebMarshal could be configured to accept requests at the address 10.3.1.1:8080. The other proxy software might use 127.0.0.1:8082. The other proxy should only accept requests from WebMarshal.

System Requirements

A single server installation of WebMarshal, or a Processing Server within an array, typically requires the following minimum hardware.

Category	Requirements
Processor	**Minimum**: Pentium 4, 2 GHz **Note:** Use of HTTPS Content Inspection significantly increases the increases the CPU load on processing servers (due to decryption and encryption of content). Depending on the amount of HTTPS traffic that is inspected, you may need to improve the CPU specification.
Disk Space	**Minimum**: 20 GB free. • Additional disk space will be required on each processing server if Proxy Caching is enabled (30GB additional recommended if using default settings) . See Marshal Knowledge Base article Q12720. • Additional disk space will be required on each processing server if text logging is enabled.
Memory	**Minimum**: 2 GB
Supported Operating System	• Windows Server 2008 (32 or 64 bit editions) • Windows Vista Business or Ultimate (SP1, 32 or 64 bit editions) • Windows Server Standard or Enterprise 2003 with Service Pack 1 (32 bit edition) • Windows XP Professional Service Pack 2 (32 bit edition)
Network Access	• TCP/IP protocol • External DNS name resolution to allow WebMarshal Servers to resolve Web addresses

Category	Requirements
Software	• Microsoft Visual C++ 2005 SP1 runtimes • Microsoft XML 6.0 • Microsoft .NET 2.0 **Note:** The above software will be installed as part of the WebMarshal installation if necessary. • Antivirus scanning software supported by WebMarshal. For more information, see “Supported Malware Protection Software” on page 21. For ISA Server plug-in: • ISA 2004 SP2 or above (Standard or Enterprise edition). • ISA 2006 (Standard or Enterprise edition).
Port Access	• **Port 19100:** To Array Manager, from Console (.NET remoting). • **Port 19101** To Array Manager, from Controller on processing servers • **Port 19102:** To Controller on processing servers, from Array Manager • **Port 8080** *(by default)* and/or others as configured: To processing servers, from web browsers and other client applications. • **Directory service ports:** From all WebMarshal servers to the Active Directory, Windows, or NDS directory environment. • **NetBios over TCP:** enabled for all WebMarshal servers. For more information see Marshal8e6 Knowledge Base article Q12207.

Notes

- Hardware requirements are dependent on the number and complexity of Rules enabled. The suggested configuration supports a typical rule set for about 250 to 500 concurrent sessions.
- If the optional WebMarshal reporting database will be hosted using SQL Express on the same computer, additional free disk space and RAM will be required.
- If optional URL Filtering Lists will be used, please see Chapter 12, “WebMarshal and Filtering Lists” for additional requirements

Additional Software

Some scenarios require the following additional software:

- To enable database logging for the WebMarshal Reports application, Microsoft SQL Server 2005 or Microsoft SQL Server 2008 is required. (You can use SQL 2005/2008 Express, the free runtime version of SQL Server). 32 bit SQL 2005 Express is available on the installation CD-ROM, or by download from the Marshal8e6 website. You can install SQL Express, if necessary, during the WebMarshal installation (this may require system restart). Note that the database can be located on any server accessible from the WebMarshal Array Manager component.
- To enable user authentication for Novell NDS users, the Novell client software must be installed on the WebMarshal Array Manager computer. Version 4.91 or higher is recommended. The latest version is freely available for download from Novell.

Supported Malware Protection Software

WebMarshal supports a number of third-party malware scanners to scan for and block viruses, spyware, and other threats. To ensure a good browsing experience for users, WebMarshal requires high-throughput DLL integration.

Marshal8e6 licenses several of the malware solutions directly. Licensing for these solutions is separate from the WebMarshal license. Trial versions of the malware solutions are available from the installation CD-Rom or as downloads from www.marshal8e6.com.

WebMarshal currently supports the malware scanners listed in the following table. For more information about currently supported versions, see Marshal8e6 Knowledge Base article Q10925.

Malware Scanning Application	Features
McAfee for Marshal	Antivirus
Norman Virus Control	Antivirus, Sandbox II
Sophos Anti-Virus	Antivirus
Sophos for Marshal	Antivirus
Symantec AntiVirus Scan Engine	Antivirus, remote installation
CounterSpy for Marshal	Spyware Protection
PestPatrol for Marshal	Spyware Protection

Collecting Information for Installation

Before you install WebMarshal, you may want to collect the following information about your environment. When you run the Configuration Wizard after you install the product, having the following details handy can help you quickly configure WebMarshal.

Information required	My information
Names of computers where you plan to install WebMarshal components including: Servers, Array Manager, database, Console, and optionally, Reports.	

Information required	My information
Prerequisite software for each computer where you will install software and the best time to restart each system, if necessary.	
If installing an array, load balancing configuration details for the processing servers.	
Firewall administrator contact information, and best time to make and propagate firewall settings changes.	
Proxy server or ISA Server administrator contact information (if required).	
Malware protection software to use with WebMarshal.	
Company name for WebMarshal license.	
Name or IP address and access port for your existing Microsoft SQL 2005 or 2008 server computer (if required). User name and password with Database Creator permission.	
IP address and access port for your existing proxy server.	
IP address and logon credentials for your directory servers (Active Directory/domain Controller and/or NDS).	
Email address where WebMarshal will send administrator notification emails (existing or new account).	
Server name and port of email server used to deliver administrator notification emails.	

Chapter 3

Installing WebMarshal

Before you install WebMarshal, please review the information in Chapter 2, “Planning Your WebMarshal Implementation.”

Determine the WebMarshal components that you want to install, and the computers where you plan to install each component. Collect the information required before you begin installation.

Run the product installer to transfer the program files. Then use the WebMarshal Configuration Wizard to complete the product setup. (The Wizard runs on Array Manager or standalone installations only.) Finally, use the Console to customize your Web access policy.

You can choose to install the WebMarshal Array Manager, Processing Server, Console and Reports on different computers. The Console is usually installed on the WebMarshal Array Manager computer, and can also be installed elsewhere.

If you are installing an Array with more than one Processing Server, you should install the Array Manager and complete the Configuration Wizard before installing additional Processing Servers. When you install a Processing Server you are prompted to connect to the Array Manager.

Setup Wizard

1. Run the WebMarshal installer from the CD-Rom, or from the Web download.

2. Carefully read the information given on the **Welcome to the WebMarshal Setup Wizard** page and the **License Agreement** page. When you click **I Accept** on the License Agreement page, you accept the terms of the License.

3. The installer checks for required prerequisite software that it can install. If any required prerequisites are not present, the installer offers to install them.

Notes

- You must install these prerequisites to continue with product installation. Installation of the prerequisites does not normally require system restart, and does not normally interfere with any previously installed software.

- As part of the .NET Framework 2.0 installation (if required) you must accept a Microsoft license agreement.

4. On the **Choose Destination Location** page, choose the folder where the program files will be installed.

Note

If you are installing WebMarshal as a Web Filter plug-in to ISA Server, the destination location must be on the same partition (drive letter) as the ISA Server software.

5. On the **Select Components** page, select the appropriate type of installation:

   a. ***If you are installing a single server complete installation, or an Array Manager with Processing Server:*** Select both **Install Console** and **Install Services**. On the Select Services page, select **Standalone Server** to install the Array Manager, Processing Server, and Console.

   b. ***If you are installing an Array Manager only:*** Select **Install Services**. On the Select Features page, select **Array Manager Only** to install the Array Manager.

   Note
   In most cases you should also select **Install Console** on the Array Manager computer. Installing the Console locally ensures that you will be able to manage WebMarshal. You can install the Array Manager without a Console for enhanced security (for instance, if the Array Manager is located in a DMZ). You must then install the Console in another location that can connect to the Array Manager.

   c. ***If you are installing a Processing Server only:*** Select **Install Services**. On the Select Services page, select **Content Processing Node Only**.

   d. ***If you are installing an additional Console,*** select **Install Console** and clear **Install Services**.

6. Click **Next** to continue.

7. ***If you are installing an Array Manager using the installer version that includes SQL Express,*** on the Select SQL Server page, you can select **I want to install and use Microsoft SQL Express** to start installation of SQL Express.

   a. Accept the Microsoft EULA.

   b. Click **Install** to install prerequisites. Click **Next** as required to continue with installation.

   c. You can accept all default values in the SQL Express installation wizard. For help with the fields and options on this wizard, click **Help.**

   Note
   If you already have MSDE or a SQL instance installed you will need to select other options. For details see Marshal8e6 Knowledge Base article Q11848.

d. Complete the SQL Express setup to continue with WebMarshal setup.

Note
To allow access to the database from other computers (for instance to allow Reports to connect from workstations), this setup enables the Named Pipes and TCP/IP protocols. (The screen message stating that these protocols are disabled is incorrect.) You can change these settings using the SQL Server Configuration Manager.

8. ***If you are installing a Processing Server,*** on the Array Manager Location page enter the name or IP address of the Array Manager. Enter the **Port Number** if you have changed this setting on the Array Manager (*default: 19101*). If you have restricted the accounts that can connect, select **Connect using a specific account** and enter account details.

Note
To set security at the Array Manager, see "Configuring WebMarshal Security" on page 240.

9. On the **Ready to Install the Program** page, click **Install** to start installation.

10. ***If you are installing a Processing Server,*** the server will attempt to connect to the Array Manager using the details you entered. If the connection fails you can enter corrected details.

Note
If the connection continues to fail, you can still finish the product installation. After finishing installation, correct any problems preventing connection, and then run the WebMarshal Server Tool on the processing server to create the connection.

WebMarshal Array Manager Or Complete Installation

When the Setup Wizard Complete page displays, choose whether or not to launch the Console. You must run the Console and complete the Configuration Wizard to enter your license key and finish configuration.

WebMarshal Console Installation (on a separate computer)

The first time you run the WebMarshal Console on a separate computer, you must specify the name of the WebMarshal server and a valid account to connect. You can browse the network to find the server.

WebMarshal Processing Server Installation (on a separate computer)

When the installation is complete, the WebMarshal services start. The processing server connects to the Array Manager to update configuration settings.

WebMarshal Configuration Wizard

The first time you run the WebMarshal Console on a new installation, WebMarshal launches a wizard that requests the Server Properties information needed to complete installation. For more information on Server Properties, please refer to Chapter 9, “Managing WebMarshal Configuration.”

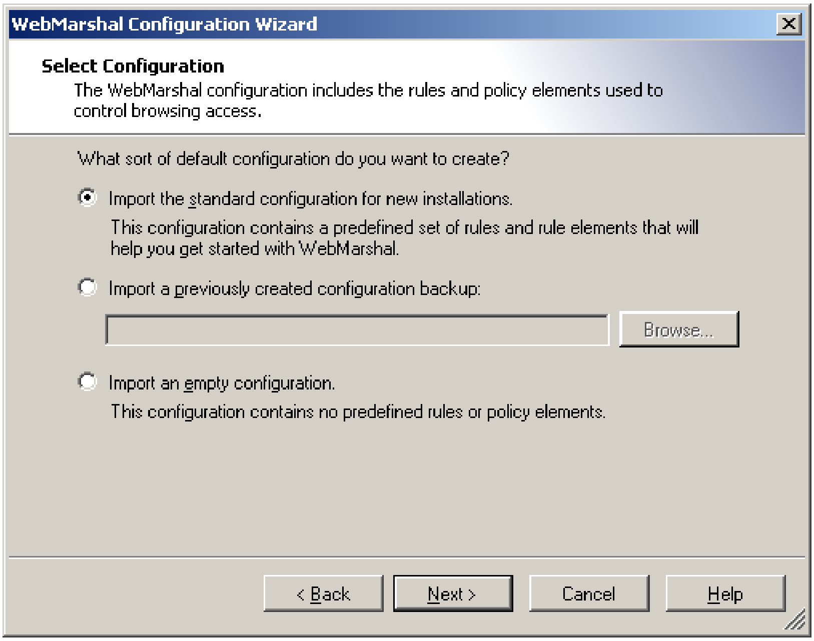
Complete the required information on each page of the wizard, and then click **Next**.

For more information about the fields on any window of the Wizard, click **Help**.

The Wizard process includes the following steps:

Select Configuration

This page of the Configuration Wizard offers three options for the initial configuration. Select an option using the radio buttons.



Select Configuration

The WebMarshal configuration includes the rules and policy elements used to control browsing access.

What sort of default configuration do you want to create?

● Import the standard configuration for new installations.

This configuration contains a predefined set of rules and rule elements that will help you get started with WebMarshal.

○ Import a previously created configuration backup:

○ Import an empty configuration.

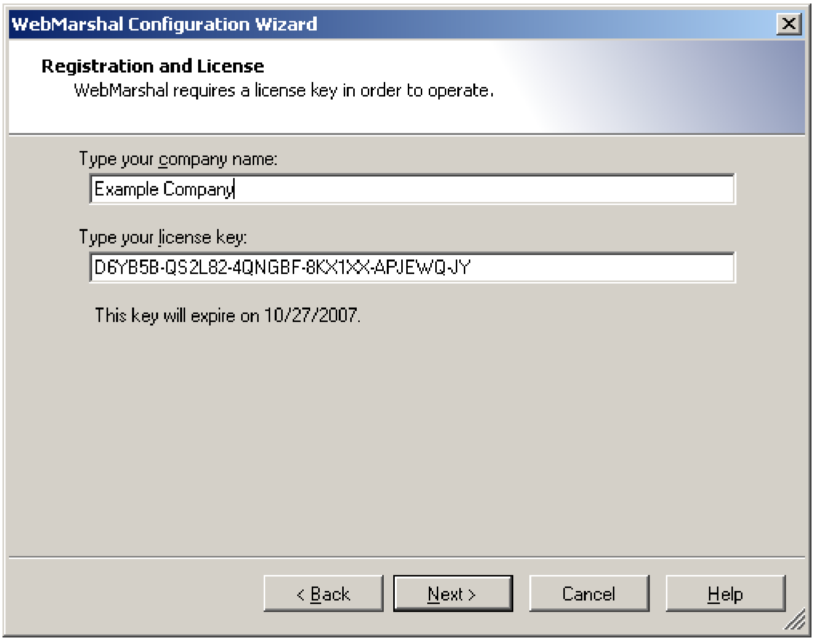
This configuration contains no predefined rules or policy elements.

- **Import the standard configuration:** Select this option to import a default configuration. This configuration includes a suggested basic Access Policy and supporting URL Categories, TextCensor Scripts, User Groups, Classifications, and other elements. After you complete the Wizard, you can customize the policy using the Console.
- **Import a configuration backup:** Select this option to import a complete configuration from a file. This option is useful for disaster recovery, or if you have obtained a custom "default configuration" from another source. Enter or browse to the name of the backup file you want to import.
- **Import an empty configuration:** Select this option to import a configuration that contains no rules or elements. After you complete the Wizard, you can create your policy using the Console.

Registration and License

On this page of the Configuration Wizard, enter basic registration information:

1. Enter your company name in the first field.
2. A trial License Key is automatically generated and entered in the second field.
3. Click **Next.**



WebMarshal Configuration Wizard

Registration and License

WebMarshal requires a license key in order to operate.

Type your company name: Example Company

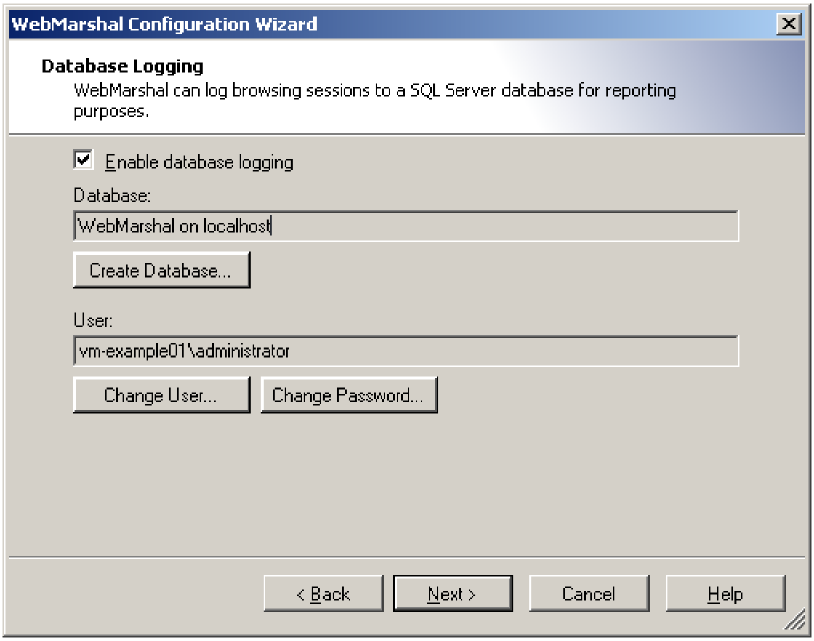
Type your license key: D6YB5B-QS2L82-4QNGBF-8KX1XX-APJEWQ-JY

This key will expire on 10/27/2007.

Database Logging

On this page of the configuration wizard, you can configure logging of WebMarshal sessions and actions to a SQL database. Database logging is required if you want to use the WebMarshal Reports application.

If you do not want to use database logging, you can leave the **Enable Database Logging** box clear and skip this page. You can enable logging later using the Console.



WebMarshal Configuration Wizard

Database Logging

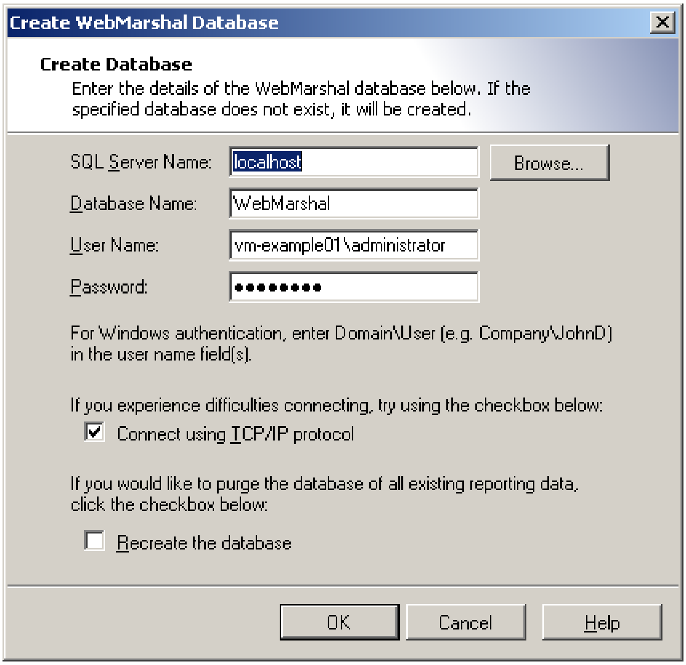
WebMarshal can log browsing sessions to a SQL Server database for reporting purposes.

☑ Enable database logging

Database: WebMarshal on localhost

User: vm-example01\administrator

To use database logging, select **Enable Database Logging**. The **Create Database** window opens.



Create WebMarshal Database

Create Database

Enter the details of the WebMarshal database below. If the specified database does not exist, it will be created.

SQL Server Name: localhost

Database Name: WebMarshal

User Name: vm-example01\administrator

Password: ●●●●●●●●●

For Windows authentication, enter Domain\User (e.g. Company\JohnD) in the user name field(s).

If you experience difficulties connecting, try using the checkbox below:

☑ Connect using TCP/IP protocol

If you would like to purge the database of all existing reporting data, click the checkbox below:

☐ Recreate the database

1. On the Create Database window, enter the name of the SQL Server computer and instance in the **SQL Server Name** field. You can browse the network if necessary.

   Note

   If you installed a default instance of SQL Express on the Array Manager, you can enter `localhost`

2. Enter the name of the new or existing database you want to use.
3. Enter a Windows or SQL user name with database creation privileges on the SQL server.
4. Enter the password for the user name.

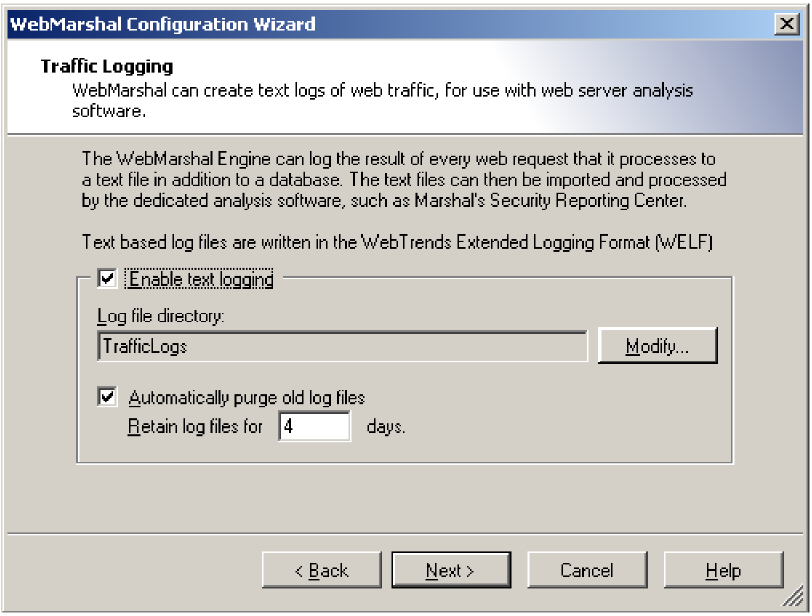
5. You can connect to the database using TCP/IP by checking the box **Connect using TCP/IP Protocol**. You might need to use this option if the SQL Server connection is through a firewall.
6. If the database you selected already exists, you can choose to recreate it. *Be sure that the existing database is not needed.*
7. Click **OK** to create the database.

After you have created the database, you can configure a user with the minimum rights required by WebMarshal. To start this process, click **Change User**. For details of this process, see Help.

You can also change the password associated with the database user on the server. To start this process, click **Change Password**. For details of this process, see Help.

Traffic Logging

On this page of the configuration wizard, you can configure logging of WebMarshal sessions and actions to text files in WELF format. You can use WELF logs to report on WebMarshal activity using Marshal Security Reporting Center.



Traffic Logging

WebMarshal can create text logs of web traffic, for use with web server analysis software.

The WebMarshal Engine can log the result of every web request that it processes to a text file in addition to a database. The text files can then be imported and processed by the dedicated analysis software, such as Marshal's Security Reporting Center.

Text based log files are written in the WebTrends Extended Logging Format (WELF)

☑ Enable text logging

Log file directory: TrafficLogs

☑ Automatically purge old log files

Retain log files for 4 days.

If you do not want to use text logging, you can leave the **Enable Text Logging** box clear and skip this page. You can enable logging later using the Console.

1. To use text logging, select **Enable Text Logging**.
2. The default location for log files is the folder `TrafficLogs` within the WebMarshal install location on the Array Manager. to change this location, click **Modify,** enter a path, and then click **OK**.

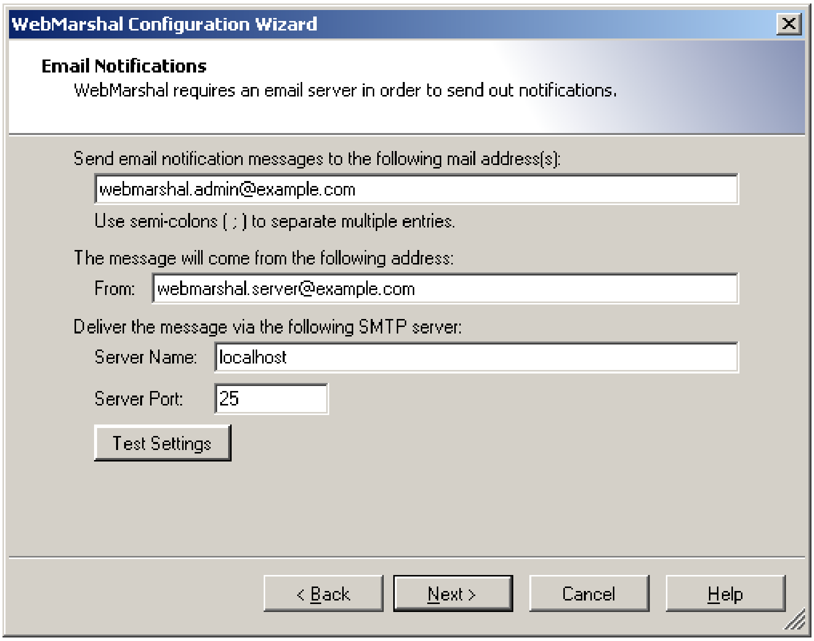
   Note
   Log files can grow quickly, so you should ensure that this location has enough free space. The log file location must be on a local device. Network locations and mapped drives are not supported.

3. To purge log files on a regular schedule, select **Automatically purge old log files**, and then enter a number of days to keep the files. In most cases log files will be automatically copied to another location for analysis.

Email Notifications

On this page of the wizard, enter details that allow WebMarshal to send notifications about critical events and rule actions.

1. Enter the administrator's SMTP email address in the first field. WebMarshal sends administrative notifications to this address. You can enter multiple addresses, separated by semi-colons. For example:
`postmaster@example.com;helpdesk@example.com`



Email Notifications

WebMarshal requires an email server in order to send out notifications.

Send email notification messages to the following mail address(s): webmarshal.admin@example.com

Use semi-colons (;) to separate multiple entries.

The message will come from the following address:

From: webmarshal.server@example.com

Deliver the message via the following SMTP server:

Server Name: localhost

Server Port: 25

2. Use the **From** field to enter the email address that will be used as the sender address for messages.

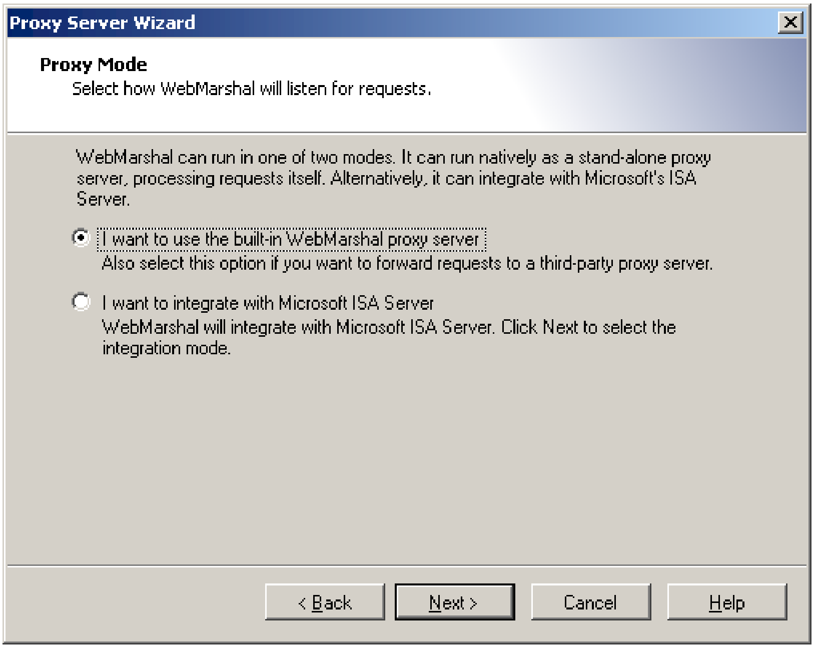
3. Use the **Server Name** field to enter the IP address or name of an email server that will accept the email message for delivery to the administrator. This server must be accessible on the network from the WebMarshal Array Manager, and it must accept email from WebMarshal for delivery to the administrator's address.

4. If the server listens for SMTP connections on a port other than port 25, enter the correct port number in the **Server Port** field.

5. Click **Test Settings** to send a test email notification.

Proxy Mode

On this page of the wizard, select a proxy server option.



Proxy Server Wizard

Proxy Mode

Select how WebMarshal will listen for requests.

WebMarshal can run in one of two modes. It can run natively as a stand-alone proxy server, processing requests itself. Alternatively, it can integrate with Microsoft's ISA Server.

● I want to use the built-in WebMarshal proxy server
Also select this option if you want to forward requests to a third-party proxy server.

○ I want to integrate with Microsoft ISA Server
WebMarshal will integrate with Microsoft ISA Server. Click Next to select the integration mode.

WebMarshal can always be configured to use its built-in proxy server. If WebMarshal processing node servers are installed on computers where Microsoft ISA Server is also installed, WebMarshal can be configured to integrate with ISA Server. You cannot mix ISA and WebMarshal proxy in the same installation.

1. To install WebMarshal with the built-in proxy, choose **I want to use the built-in WebMarshal proxy server.** Click **Next** to continue to the Local Address Table page of the Wizard.

2. To install WebMarshal as a plug-in to ISA, choose **I want to integrate with Microsoft ISA Server.** Click **Next** to continue to the ISA Integration page of the Wizard.

ISA Integration

If you are integrating WebMarshal with ISA Server, select a method of integration.

Notes

- Marshal8e6 recommends that you allow WebMarshal to handle requests unless you require specific ISA functionality.
- The wizard always allows you to select ISA Server plug-in modes. However, if the processing node servers are not on ISA Servers, WebMarshal processing services will not start.
- The ISA Server plug-in does not support Connection rules, HTTPS inspection functionality, Upload Content Analysis Rules, or Novell NDS. To use these features with ISA Server, select “I want WebMarshal to handle requests.”

Select one of the options:

- Select **I want WebMarshal to handle requests** to chain WebMarshal to ISA Server. Configure chaining later in the Wizard (see “Forward Proxy” on page 44).
- Select **I want to plug into ISA Server using Windows Authentication** to authenticate browser clients using Windows accounts (usually the account of the logged on Windows user).
- Select **I want to plug into ISA Server using Secure NAT (IP Authentication)** to authenticate browser clients using the IP address of the client workstation. Select this option if you are using ISA Server in SecureNAT mode. Please refer to the ISA Server documentation for more information on SecureNAT.

Note
When SecureNAT integration is in use, WebMarshal cannot filter FTP requests.

Click **Next.**

Updates Proxy Server

If you are installing WebMarshal as a plug-in to ISA, complete this page to define how WebMarshal will download updates for filtering lists. ISA Server may not correctly handle Web requests from the local server.

Note
For more information about configuring update access when WebMarshal is configured as a plug-in to ISA Server, see Marshal8e6 Knowledge Base article Q10286.

1. If WebMarshal can make direct web connections, select **Request the item directly from the Internet.**
2. If WebMarshal must to pass requests on to another proxy server then click the **Forward** option and enter the required information.

   Check the configuration of the other proxy server to ensure that it is using the port you have specified.

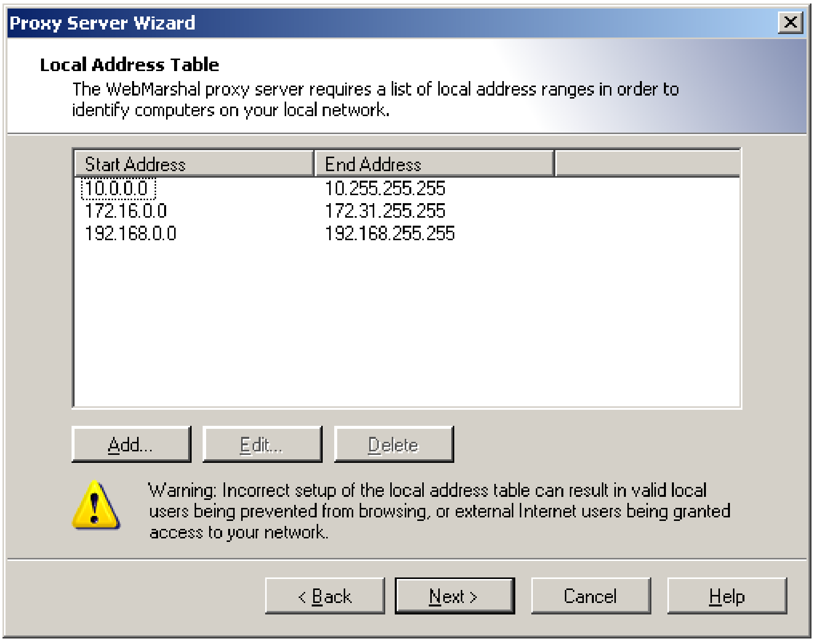
3. If the other proxy server requires authentication, you can choose to enter a user name and password. See Help for details.

Click **Next** to continue to the Streaming Content Types page. The other Wizard steps are not required in this case because ISA Server performs the functions concerned.

Local Address Table

On this page, specify the range(s) of IP addresses that are assigned to computers on your local network. By default, the LAT includes address ranges that are always reserved for local use. If your local network uses different local IP addresses you can enter them.

Note
Only computers with addresses in the LAT ranges will be allowed to use the WebMarshal proxy. If a computer whose IP address is not in the LAT attempts to connect, the connection will be refused with an error message.



Proxy Server Wizard

Local Address Table

The WebMarshal proxy server requires a list of local address ranges in order to identify computers on your local network.

Start Address	End Address
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Warning: Incorrect setup of the local address table can result in valid local users being prevented from browsing, or external Internet users being granted access to your network.

To enter a new LAT range:

1. Click **New**.
2. Enter the starting and ending addresses in the range.
3. Click **OK**.

To edit an existing address range, select it and then click **Edit**. To delete an existing address range, select it and then click **Delete**.

Click **Next** to continue.

Proxy Ports and Authentication

On this page, select the server ports that WebMarshal will monitor, and the types of user authentication WebMarshal will accept on each port.

Note

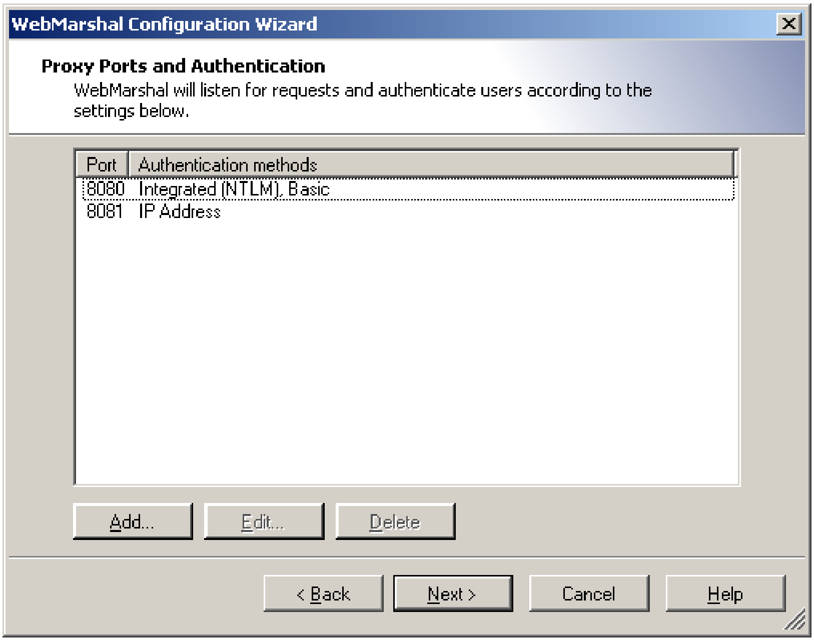
By default WebMarshal monitors each port on all available IP Addresses. If the server has multiple interfaces, you can specify IP Address:port combinations (for example, `10.1.2.3:8085`). Caution is required when binding by IP address when in a multiple node environment. See Help for more details.

WebMarshal checks the user account information for each request. WebMarshal supports authentication by integrated Windows authentication, Basic (clear text) authentication (including Novell NDS accounts), or computer IP address.

Note

By default WebMarshal accepts both NTLM (Windows) and Basic authentication on port 8080. ***If you are using NDS as well as Windows authentication,*** Marshal8e6 recommends you use a *different* port for Basic authentication of NDS users.

Be sure to adjust all clients to send their requests to the IP address and port you have selected. For instance, if you have been using Squid, which listens on port 3128 by default, you can configure WebMarshal to accept requests on this port, or reconfigure clients to use the WebMarshal default port 8080.



WebMarshal Configuration Wizard

Proxy Ports and Authentication

WebMarshal will listen for requests and authenticate users according to the settings below.

Port	Authentication methods
8080	Integrated (NTLM), Basic
8081	IP Address

1. ***If you want to edit an existing port assignment,*** select it and then click **Edit**.

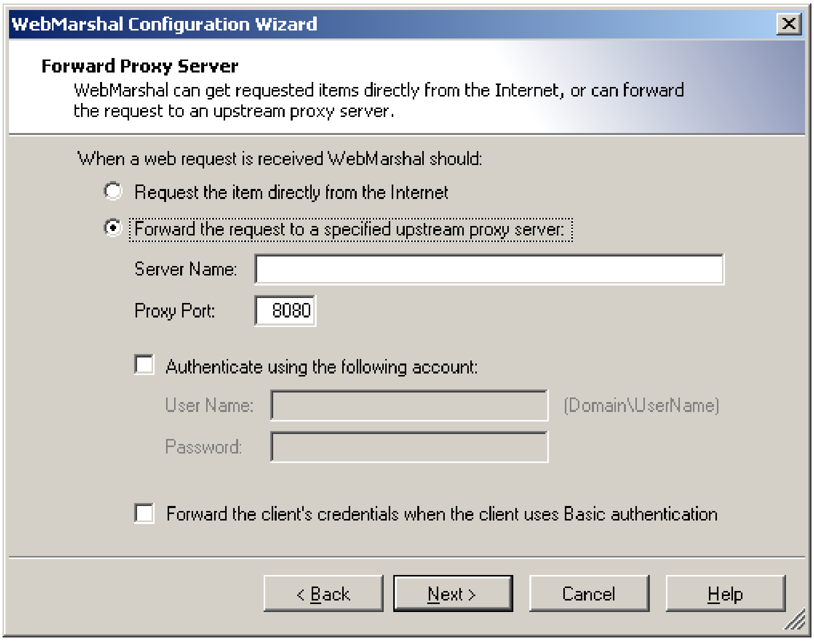
2. ***If you want to add a new assignment,*** click **Add**.

3. Enter the required information and then click **OK**. See Help for details.

To configure import of user account information, see the **Connectors** item in the main WebMarshal Console menu tree.

Forward Proxy

On this page, select the method WebMarshal will use to request material from the Web.



WebMarshal Configuration Wizard

Forward Proxy Server

WebMarshal can get requested items directly from the Internet, or can forward the request to an upstream proxy server.

When a web request is received WebMarshal should:

○ Request the item directly from the Internet

● Forward the request to a specified upstream proxy server:

Server Name:

Proxy Port: 8080

□ Authenticate using the following account:

User Name: (Domain\UserName)

Password:

□ Forward the client's credentials when the client uses Basic authentication

1. If WebMarshal can access the Web directly, choose the **Request the page directly** option. This is the default setting.

2. If WebMarshal will pass requests on to another proxy server then click the **Forward** option and enter the required information.

   For instance, if you want WebMarshal to pass requests to SquidNT running on the same computer, you can enter `localhost` as the computer name and `3128` as the proxy port (SquidNT listens on port 3128 by default).

3. Check the configuration of the other proxy server to ensure that it is using the port you have specified. If the other proxy server requires authentication, you can choose to enter a user name and password, and/or forward the client's credentials. See Help for details.

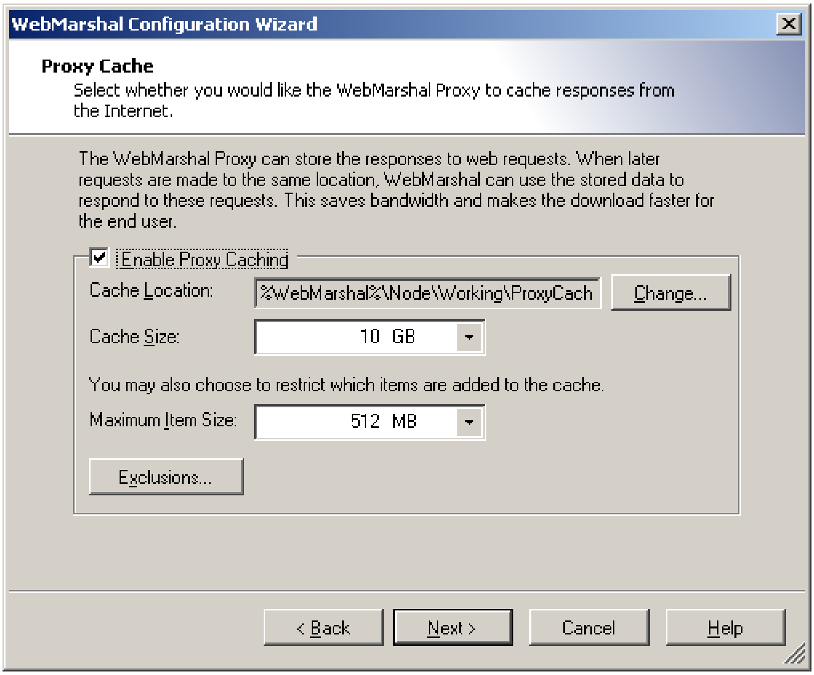
4. To force all web requests from your organization to pass through WebMarshal, be sure to set up the other proxy software to accept requests only from WebMarshal. You can configure the LAT settings on the other proxy server, or set the other proxy software to accept requests only from a specific Windows account, which is only used by WebMarshal.

Proxy Cache

On this page, choose to enable WebMarshal proxy caching if you want to use this optional feature. Caching retains local copies of items downloaded from the Web via HTTP, where appropriate. When WebMarshal later responds to a request for the same items, they are returned from the local copy, saving time and bandwidth.

Notes

- Proxy cache applies for HTTP requests only (not for HTTPS or FTP).
- WebMarshal Quotas and bandwidth reports treat cached requests as any other request.
- To see details of cache activity and bandwidth savings, use the Real-Time Dashboard in the Console.
- To log cache activity in detail, use text logging (WELF logs).



WebMarshal Configuration Wizard

Proxy Cache

Select whether you would like the WebMarshal Proxy to cache responses from the Internet.

The WebMarshal Proxy can store the responses to web requests. When later requests are made to the same location, WebMarshal can use the stored data to respond to these requests. This saves bandwidth and makes the download faster for the end user.

☑ Enable Proxy Caching

Cache Location: %WebMarshal%\Node\Working\ProxyCach

Cache Size: 10 GB

You may also choose to restrict which items are added to the cache.

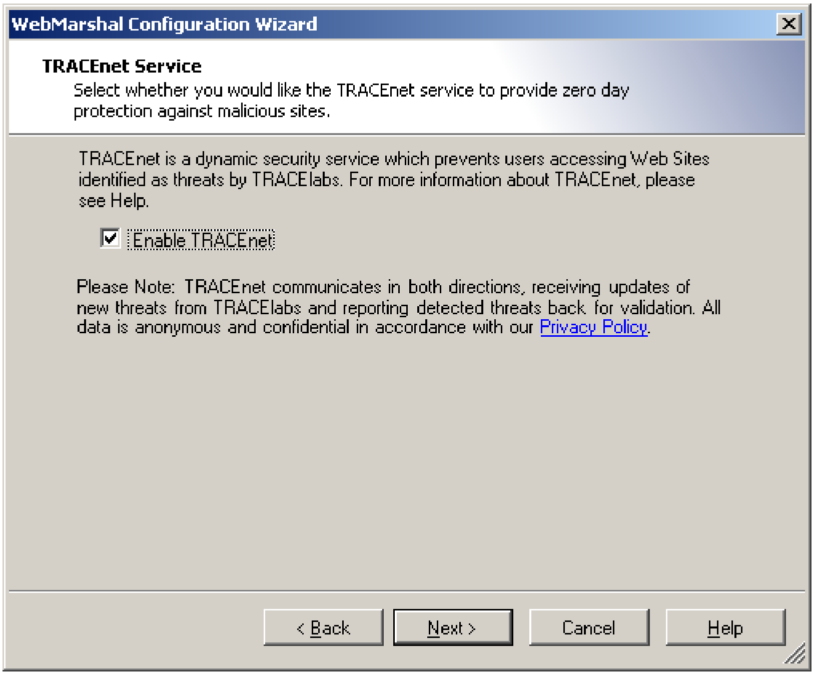
Maximum Item Size: 512 MB

To enable caching, check the box. Then configure the following options:

1. Set the cache directory location. The default location is within the WebMarshal install. *Most production installations should use a different location.* For more information, see Marshal8e6 Knowledge Base article Q12720.
2. Set the maximum size of the cache. If you set up an array with more than one processing node server, the size applies to *each* server.
3. Set the maximum size of items that will be cached. You may want to limit the size if the available space for caching is limited.
4. Optionally click **Exclusions** and enter a list of URLs that should never be cached. For more information about exclusions, see "Configuring Proxy Cache" on page 224.

TRACEnet Service

On this page, choose whether to enable the optional TRACEnet filtering service. TRACEnet is a framework that allows Marshal8e6 to provide filtering of malicious URLs with “zero day” updates. TRACEnet updates are provided to all WebMarshal trial installations and to customer installations with current product maintenance.



WebMarshal Configuration Wizard

TRACEnet Service

Select whether you would like the TRACEnet service to provide zero day protection against malicious sites.

TRACEnet is a dynamic security service which prevents users accessing Web Sites identified as threats by TRACElabs. For more information about TRACEnet, please see Help.

☑ Enable TRACEnet

Please Note: TRACEnet communicates in both directions, receiving updates of new threats from TRACElabs and reporting detected threats back for validation. All data is anonymous and confidential in accordance with our Privacy Policy.

To enable TRACEnet, check the box.

For more information about TRACEnet, and to configure additional options, after completing the wizard open the TRACEnet item under Access Policy in the WebMarshal Console. See “Understanding TRACEnet” on page 79.

Streaming Content Types

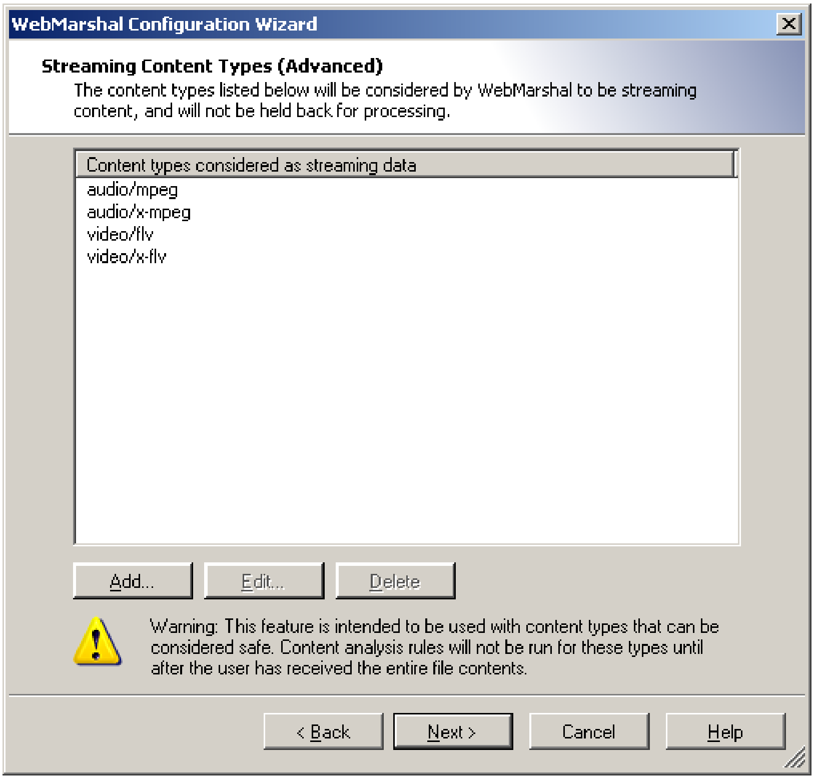
On this page, you can choose to allow specific types of streaming media content to pass through WebMarshal without being held for analysis. Setting up streaming media types in WebMarshal will help to ensure a good web browsing experience for users. WebMarshal can only control streaming content delivered over HTTP. You should ensure that other protocols such as MMS and RTSP are blocked at your firewall.

These settings may not be required if you use WebMarshal Connection Rules. You can return to this wizard if necessary (from the WebMarshal Console Tools menu) to configure additional types.

Warning

These settings should be used only to provide access to trusted streaming content types. Caution is required as *malware scanning and other content filtering will only be performed after this content is fully downloaded to the user.*

To manage the list of streaming content types, use the **Add**, **Edit**, and **Delete** buttons. See Help for details. When you have completed the list, click **Next** to continue.



Streaming Content Types (Advanced)

The content types listed below will be considered by WebMarshal to be streaming content, and will not be held back for processing.

Content types considered as streaming data
audio/mpeg
audio/x-mpeg
video/flv
video/x-flv

Warning: This feature is intended to be used with content types that can be considered safe. Content analysis rules will not be run for these types until after the user has received the entire file contents.

Finished

Please read the final page of the WebMarshal Configuration Wizard carefully. Then click **Finish** to start WebMarshal services and run the WebMarshal Console.

When installed, WebMarshal immediately begins accepting Web requests, but rule evaluation (filtering) is disabled.

Before you put WebMarshal into production, you must complete some additional steps. Use the Console to complete these steps:

1. **Create Directory Connectors:** To import user information from Active Directory, legacy Windows NT, or Novell directories, first create the appropriate Connectors. See "Users and Groups" on page 70.
2. **Import Users** from Windows NT, Active Directory, or Novell directories, or **create IP User Groups:** Since WebMarshal is an authenticating proxy server, each browser session must supply a logon credential before any browsing is permitted. You must provide account information for each permitted user or workstation so that WebMarshal can authenticate requests. See "Users and Groups" on page 70.
3. **Customize Rules:** If you have chosen to use the WebMarshal default Rules, every authenticated user will have basic browsing privileges. To adjust permissions quickly, you can add Users to additional User Groups. You can enable and edit Rules as required using the Console. See Chapter 6, "Understanding Web Access Policy, Rule Containers, and Rules."
4. **Configure Malware Protection** (optional, but strongly recommended): If you plan to use Virus or Spyware Scanners with WebMarshal, you must install the software and configure it in the Console before enabling Malware Scanning Rules. See "Using Malware Scanning" on page 178.
5. **Configure Filtering Lists** (optional): If you plan to use URL filtering lists with WebMarshal, you must enable them but ensure you have downloaded the initial databases before you enable them in any rules. See "Configuring URL Filtering Lists" on page 156.
6. **Enable Rule Processing:** When installed, WebMarshal immediately begins accepting Web requests; however, rule evaluation (filtering) is disabled by default. This means that all requests will be accepted.

   To enable Rule evaluation immediately, check the **Enable Rule Processing** box on the final page of the Ruleset Wizard.

   Warning

   If you enable rule processing before importing Users, all requests will be rejected until Users are imported.

Installing WebMarshal Reports

The Reports application is available on the WebMarshal distribution CD-Rom, or as a separate download from the Marshal8e6 Website.

1. Run the WebMarshal Reports installer from the WebMarshal CD-Rom or the Web download.
2. Carefully read and accept the license information.
3. Select a destination location and program folder.
4. Click **Install** to install the WebMarshal Reports software.

Reports are generated from information in a SQL database. You connect to the database when you run the Reports application. For more information see Chapter 4, "Understanding WebMarshal Interfaces," and Chapter 8, "Reporting on Browsing Activity."

Note
You can also use the Marshal Reporting Console, available as a separate download from the Marshal8e6 Website.

Configuring Web Browsers

All web browsers within the organization should be configured to send web requests to the WebMarshal server on the appropriate port. By default, the port for proxy requests is port 8080). If browsers are already configured to send requests to another port (for example, if ISA Server has been listening on port 80), you can configure WebMarshal to accept requests on the existing port assignment. For information on rolling the configuration out to a large number of workstations, please see Marshal8e6 Knowledge Base article Q10506.

Web browser sessions are authenticated by WebMarshal. Authentication can use Microsoft accounts through Basic Authentication or Windows Integrated authentication, Novell NDS user information through Basic Authentication, or the IP address of the user's workstation.

If you are planning to use HTTPS Rules, you should ensure that the WebMarshal Root Certificate is installed for all browsers. See "Generating and deploying a HTTPS Root Certificate" on page 233.

Upgrading WebMarshal

You can upgrade to WebMarshal 6.5 and WebMarshal Reports 6.5 from WebMarshal 6.0 or above. To upgrade, run the product installer on each computer where components are installed.

WebMarshal 6.0 introduced significant enhancements to the rules, configuration storage, and other elements, compared to previous versions. Due to the nature and scope of these changes, you **cannot** install WebMarshal 6.X as an upgrade to any previous major version. You can install WebMarshal 6.X *on the same server* as WebMarshal 3.X. Both installations will function correctly. You must configure each installation to use different ports and databases. For details, see Marshal8e6 Knowledge Base article Q11833.

Note
You cannot enable both WebMarshal 6.X ISA Server plug-in and WebMarshal 3.X ISA Server plug-in on the same server.

Uninstalling WebMarshal

1. Ensure that the WebMarshal Console is not running.
2. On the Array manager and any other Processing Servers in your WebMarshal Array, uninstall WebMarshal using **Add/Remove Programs** from the Windows control panel.

3. Uninstall any instances of the WebMarshal Console and WebMarshal Reports from other workstations.

4. If appropriate, drop the WebMarshal database from the SQL Server using the SQL administration tools.

5. If appropriate, remove other software that is no longer required from the Array Manager and any other Processing Servers in the array, using **Add/Remove Programs** from the Windows control panel. This could include McAfee for Marshal, CounterSpy for Marshal, PestPatrol for Marshal, and Sophos for Marshal. If you were using the Marshal Filtering List, Marshal8e6Filter List or the Secure Computing Filtering List, you should delete the list database (found in a subfolder of the WebMarshal installation folder).

Note

You could also uninstall prerequisite software such as the Microsoft Visual C++ redistributable. However, other applications might be using this software. Marshal8e6 recommends that you do not uninstall the prerequisites.

Chapter 4

Understanding WebMarshal Interfaces

WebMarshal provides two main interfaces to help you set up and monitor Web access policy.

WebMarshal Console

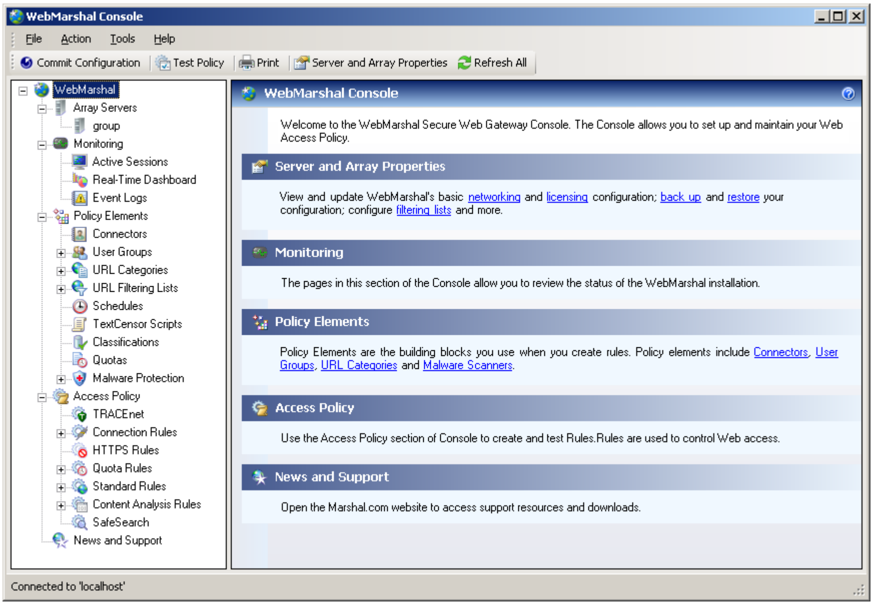
Allows you to customize your access policy, and monitor server health and Web access on a real-time basis.

WebMarshal Reports Console

Allows you to generate detailed historical reports on Web access, policy breaches, and WebMarshal actions.

Understanding the Console

The WebMarshal Console is the main interface for configuration of WebMarshal behavior. This section describes the features and elements available in the Console. Many of these elements are covered in more detail in the following chapters of this Guide.



WebMarshal Console

Welcome to the WebMarshal Secure Web Gateway Console. The Console allows you to set up and maintain your Web Access Policy.

Server and Array Properties

View and update WebMarshal's basic networking and licensing configuration; back up and restore your configuration; configure filtering lists and more.

Monitoring

The pages in this section of the Console allow you to review the status of the WebMarshal installation.

Policy Elements

Policy Elements are the building blocks you use when you create rules. Policy elements include Connectors, User Groups, URL Categories and Malware Scanners.

Access Policy

Use the Access Policy section of Console to create and test Rules.Rules are used to control Web access.

News and Support

Open the Marshal.com website to access support resources and downloads.

Connected to 'localhost'

Console Navigation

The Console features an icon tool bar, a menu bar, and two main panes. The right pane displays detailed information using "taskpad" web pages with links to common tasks and submenus. The left pane provides a menu tree that allows access to the main elements. Important notices display in the Status Bar at the bottom of the window.

- To expand a branch of the menu tree, click the associated + symbol. The items contained within this branch are displayed.
- To select an item in either pane, click it to highlight it.

- To display detailed information about an item, select it in the left pane. Detailed information displays in the right pane.
- To collapse an expanded menu element click the associated **-** symbol.
- To work with an item in either pane, right-click to view a menu of available options. The main Console and each taskpad also provide toolbar links to common tasks.
- To sort the information in a list view, click a column title.
- To customize the columns in any right pane list view:

  a. Right-click a detail item and select **Select Columns** to open an Add/Remove Columns window.

  b. To add or remove a column from the list, select it and click **Add** or **Remove**.

  c. To change the display order, select an item in the Displayed Columns list and click **Move Up** or **Move Down**.

  WebMarshal retains custom column views for each user on each computer where the Console is installed.

Note
In most cases, you can access items in the Console by multiple methods including toolbar buttons or icons, right-click context menus, and keyboard shortcuts. This *Guide* normally refers to the buttons.

Working With Properties Configuration

You can set many global properties of WebMarshal using three properties windows.

Array Properties
On this window you can control basic properties of a WebMarshal installation. To open this window, select **Server and Array Properties** from the toolbar.

Server Properties

Each WebMarshal installation includes one or more processing servers,. To see a list of these servers, select **Array Servers** in the left pane. The right pane will show a list of installed servers. To configure settings for a server, click to select that server in the right pane, then click the **Properties** icon in the taskpad toolbar.

Server Group Properties

You can group WebMarshal servers to apply customized configuration and rules for different locations in your network. To configure settings for a group, expand **Array Servers** in the left pane, right-click the group, and then select **Properties** from the context menu.

For more information about the properties and settings shown on these three windows, see "Configuring Server Properties" on page 208, "Managing Array Servers" on page 241, and "Configuring Server Group Properties" on page 244.

Array Servers

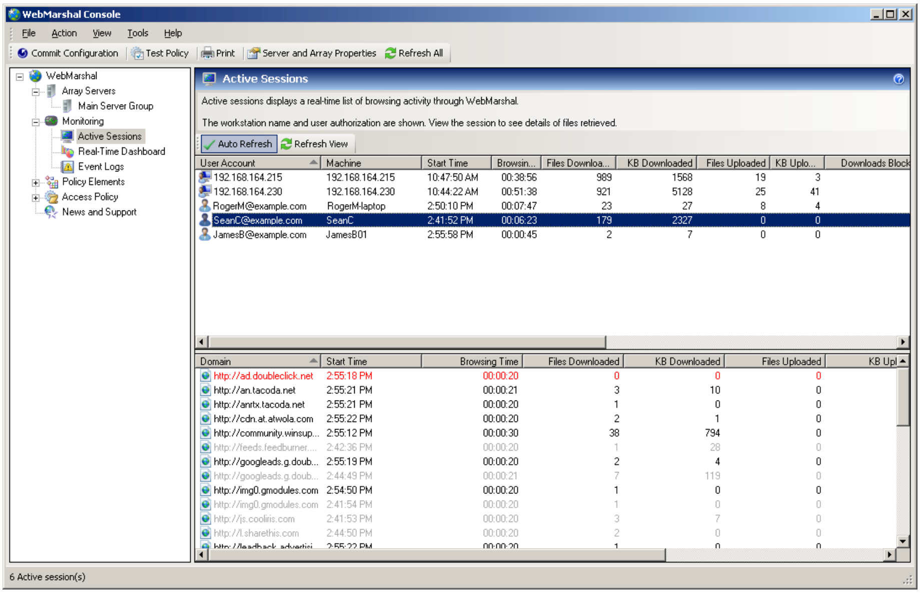
When you select this item, the right pane displays a list of all processing servers in the WebMarshal array. The list shows the status of each server. If the rule and configuration changes made in the console have not yet been reloaded into the servers, the Commit Configuration icon displays in red, and an asterisk is added to the caption WebMarshal (at the top of the left pane).

If you have configured **server groups**, the list shows the servers in their groups. To work with a group, expand the Array Servers item and select the group.

For more information on working with servers, see "Configuring Server Properties" on page 208.

Active Sessions

When you select this item (**Monitoring > Active Sessions**), the right pane shows a list of current browsing sessions through WebMarshal by user account and machine.



Active sessions displays a real-time list of browsing activity through WebMarshal.

The workstation name and user authorization are shown. View the session to see details of files retrieved.

User Account	Machine	Start Time	Browsin...	Files Downloa...	KB Downloaded	Files Uploaded	KB Uplo...	Downloads Block
192.168.164.215	192.168.164.215	10:47:50 AM	00:38:56	989	1568	19	3	
192.168.164.230	192.168.164.230	10:44:22 AM	00:51:38	921	5128	25	41	
RogerM@example.com	RogerM-laptop	2:50:10 PM	00:07:47	23	27	8	4	
SeanC@example.com	SeanC	2:41:52 PM	00:06:23	179	2327	0	0	
JamesB@example.com	JamesB01	2:55:58 PM	00:00:45	2	7	0	0	

Domain	Start Time	Browsing Time	Files Downloaded	KB Downloaded	Files Uploaded	KB Upl
http://ad.doubleclick.net	2:55:18 PM	00:00:20	0	0	0	
http://an.tacoda.net	2:55:21 PM	00:00:21	3	10	0	
http://anrtx.tacoda.net	2:55:21 PM	00:00:20	1	0	0	
http://cdn.at.atwola.com	2:55:22 PM	00:00:20	2	1	0	
http://community.winsup...	2:55:12 PM	00:00:30	38	794	0	
http://feeds.feedburner....	2:42:36 PM	00:00:20	1	28	0	
http://googleads.g.doub...	2:55:19 PM	00:00:20	2	4	0	
http://googleads.g.doub...	2:44:49 PM	00:00:21	7	119	0	
http://img0.gmodules.com	2:54:50 PM	00:00:20	1	0	0	
http://img0.gmodules.com	2:41:54 PM	00:00:20	1	0	0	
http://js.cooliris.com	2:41:53 PM	00:00:20	3	7	0	
http://l.sharethis.com	2:44:50 PM	00:00:20	2	0	0	
http://leadback.advertisi...	2:55:22 PM	00:00:20	1	0	0	

6 Active session(s)

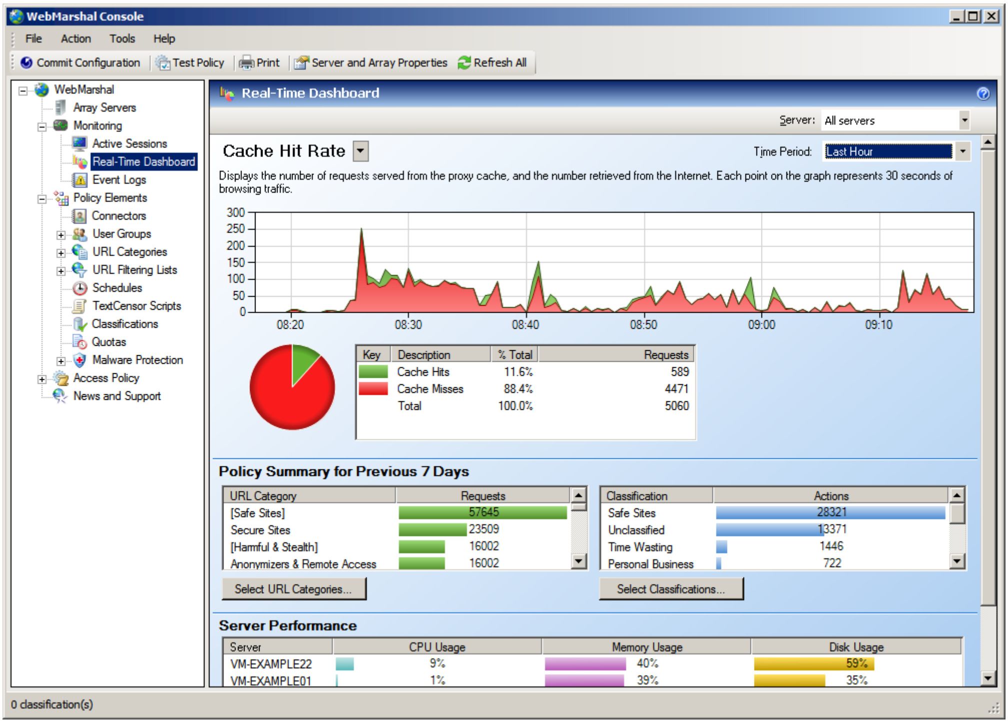
You can drill down to view a list of the domains and files for each session.

Note

A WebMarshal session ends when no new pages have been requested for a defined period (by default, 5 minutes). You can adjust this session time-out value. For more information, see “Viewing Product Information” on page 209.

Real-Time Dashboard

When you select this item (**Monitoring > Real-Time Dashboard**), the right pane shows a graphical dashboard that allows you to monitor server performance, browsing traffic, Proxy Cache statistics, TRACEnet statistics and update status, and WebMarshal action statistics. For details of the available information see Help.



Server: All servers

Time Period: Last Hour

Displays the number of requests served from the proxy cache, and the number retrieved from the Internet. Each point on the graph represents 30 seconds of browsing traffic.

Key	Description	% Total	Requests
🟩	Cache Hits	11.6%	589
🟥	Cache Misses	88.4%	4471
	Total	100.0%	5060

Policy Summary for Previous 7 Days

URL Category	Requests
[Safe Sites]	57645
Secure Sites	23509
[Harmful & Stealth]	16002
Anonymizers & Remote Access	16002

Classification	Actions
Safe Sites	28321
Unclassified	13371
Time Wasting	1446
Personal Business	722

Server Performance

Server	CPU Usage	Memory Usage	Disk Usage
VM-EXAMPLE22	9%	40%	59%
VM-EXAMPLE01	1%	39%	35%

0 classification(s)

Event Logs

When you select this item (**Monitoring > Event Logs**), the right pane shows a filtered view of the Windows event logs. Several filters are provided to allow easy monitoring of WebMarshal and related items on all servers in the Array. For more information, see “Viewing Windows Event Logs” on page 246.

Policy Elements

WebMarshal Policy Elements are the basic building blocks that you can use to construct Web access Rules. Before you enable Rules, you must create or modify these Elements to fit organizational requirements.

Connectors

This item shows the installed directory connectors, used to import user account information for authentication. Microsoft Active Directory, legacy Windows NT, and Novell connectors are currently supported. Double click a connector name to see its properties. For more information on working with Connectors, see “User Management” on page 138.

User Groups

This item shows a list of user groups configured in WebMarshal. You can import and automatically update groups through WebMarshal connectors. You can also create groups of IP addresses, and internal user groups for use only within WebMarshal. For more information on working with user groups, see “User Management” on page 138.

All Users

This item is always present in the user groups, and shows a list of all users currently available in WebMarshal. Double click any user name to see more information, including a list of the Rules that apply to the user.

URL Categories

This item shows a list of URL categories. URL categories are lists of URLs with similar content, for use in building rules. You can create categories locally, or you can retrieve and populate them from an externally maintained Filtering List. A few examples of URL categories are: search engines, objectionable sites, partner companies. For more information on working with URL categories, see “Understanding URL Categories” on page 151.

Note
Expand a category and double-click any URL to see a report of the WebMarshal Rule action, if any, that placed it in that category. (This information is not available if the URL was added manually.)

URL Filtering Lists

This item shows a list of the URL Filtering List applications configured in WebMarshal. For more information about Filtering Lists, see “Configuring URL Filtering Lists” on page 156.

Schedules

This item shows a list of available schedules. Schedules allow you to apply rules based on the time of day and day of the week. For more information on working with schedules, see “Configuring Access Using Schedules” on page 159.

TextCensor Scripts

This item shows a list of available WebMarshal TextCensor scripts. The scripts allow you to scan web pages and text files for particular key words or combinations of words. You can use TextCensor scripts to block Web requests, and also to classify visited sites into URL categories and create your own site filtering lists. Examples of TextCensor scripts are: objectionable language, sports-related terms, and active scripting keywords. For more information on working with TextCensor scripts, see “Identifying Web Content Using TextCensor Scripts” on page 169.

Classifications

This item shows a list of available logging classifications. Classifications allow you to create detailed logs of rule actions. For more information about Classifications, see "Logging Activity with Classifications" on page 182.

Quotas

This item shows a list of available quotas. Quotas allow you to limit a user's browsing activity by total time and/or volume. For more information on working with quotas, see "Configuring Access Using Quotas" on page 162.

Malware Protection

Expand this menu branch and select "Virus Scanners" or "Spyware Scanners" to see lists of third-party virus and spyware scanners that have been configured for use in scanning file downloads and uploads. For more information on configuring malware protection, see "Using Malware Scanning" on page 178. To implement malware scanning, see Chapter 6, "Understanding Web Access Policy, Rule Containers, and Rules."

Access Policy

Expand this menu branch to see its subcategories:

- TRACEnet
- Connection Rules
- HTTPS Rules
- Quota Rules
- Standard Rules
- Content Analysis Rules
- SafeSearch

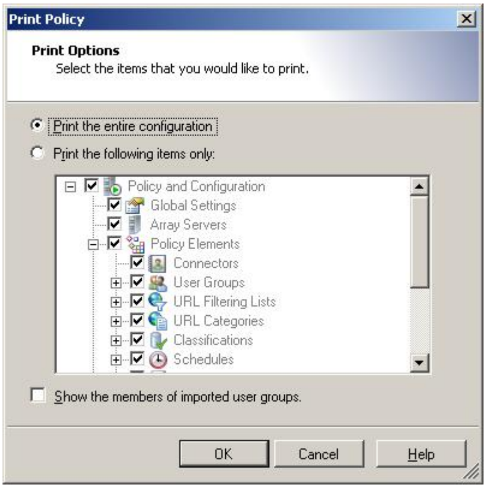
Select one of these subcategories to configure the rules or options available. For more information on working with access policy and rules, see Chapter 6, “Understanding Web Access Policy, Rule Containers, and Rules.”

Configuration and Rule Printing

You can view and print WebMarshal configuration, rules and rule elements in a convenient summary format.

To print configuration:

1. Click the **Print** icon in the tool bar to open the Print Options window. By default the entire configuration is selected.
2. Select the items to print
3. Choose whether or not to include members of imported user groups (this can result in a large listing).



Print Policy

Print Options

Select the items that you would like to print.

● Print the entire configuration

○ Print the following items only:

- ☑ Policy and Configuration
  - ☑ Global Settings
  - ☑ Array Servers
  - ☑ Policy Elements
    - ☑ Connectors
    - ☑ User Groups
    - ☑ URL Filtering Lists
    - ☑ URL Categories
    - ☑ Classifications
    - ☑ Schedules

□ Show the members of imported user groups.

4. Click **OK** to view the information in a new window.

5. Click the **Print** icon in the new window to print the information.

Tip
To print an individual item from the configuration, right-click the item in either pane of the main WebMarshal Console, and then select **Print Selected Item.**

News and Support

The News And Support item in the console tree presents the support section of the Marshal8e6 website in the right pane. This area features the latest support information, including frequently asked questions, a knowledge base, and a discussion forum. To access the full range of resources, customers should log in to the site. Obtain login details, if necessary, by contacting Marshal8e6.

Understanding the Reports Console

The WebMarshal Reports Console allows you to obtain detailed historical information about Web browsing activity and WebMarshal filtering actions.

The Console is implemented as a snap-in to the Microsoft Management Console (MMC). Users of other MMC applications (such as MailMarshal Configurator and Microsoft SQL Server Enterprise Manager) will be familiar with this interface.

For detailed information about the features and functions of the Reports Console and how to generate reports, see Chapter 8, “Reporting on Browsing Activity.”

Understanding the MMC Interface

By default, the MMC features an icon tool bar, a menu bar, and two main panes. The left pane contains a menu tree. Detailed information displays in the right pane.

- To expand an element (branch) of the menu tree, click the associated **+** symbol. This will show the elements contained within this branch.
- To select an item in either pane, click it to highlight it.
- Selecting an item in the left pane will display the associated detail information in the right pane.
- To collapse an expanded menu element click the associated **-** symbol.
- If the left pane is not visible, click the **Show/Hide Console Tree** icon in the tool bar. It should appear "pushed in."

Note
The tool bar and menu bar of MMC are context dependent. The available icons and choices depend on which item is selected in the main panes. If an icon referred to is not visible, ensure that the appropriate item is selected.

While this Guide usually refers to choices from the icon tool bar, in many cases the MMC also provides equivalent choices from the "Action" menu and from context menus, which you can see by right-clicking on the selected item.

Multiple Snap-ins in the Same MMC

If you want to use more than one MMC snap-in from the same machine, you can create a new MMC Console that contains all the required snap-ins.

To create a custom MMC Console:

1. Run `mmc.exe` from a command prompt.
2. Choose **Console > Add/Remove Snap-in** from the main menu.
3. In the *Add/Remove Snap-in* window, click **Add** to see a list of available snap-ins.
4. Double-click each desired snap-in to add it to the list.

5. When done, click **Close**.

6. Click **OK**.

7. To save the custom Console, choose **Console > Save** from the main menu. Select a location for the .msc file.

To run the custom console, open the `.msc` file by double-clicking or any other method.

Understanding Other Tools

Additional standalone tools are installed with WebMarshal. You can access these tools through the Windows menus.

The **WebMarshal Server Tool** allows you to perform additional management tasks on the local WebMarshal Processing Server:

- Start or stop WebMarshal services.
- Add the processing server to an array, or remove it from an array.
- Configure communication between the Processing Server and the WebMarshal Array Manager.

For more information, see "Managing Array Servers" on page 241. For detailed usage instructions, see Help for the tool.

The **WebMarshal Security Tool** is installed with the Array Manager. This tool allows you to set WebMarshal administrative permissions for Windows accounts. By default administrators of the Array Manager computer have full permissions. For more information, see "Configuring WebMarshal Security" on page 240.

The **WebMarshal Configuration Backup Tool** is installed with the Array Manager. This tool allows you to perform configuration backup from the command line or a scheduled task. For more information, see "Importing and Exporting Configuration" on page 237.

The **WebMarshal Support Tool** is installed with WebMarshal. This tool gathers information about the WebMarshal installation and the server WebMarshal is installed on. Its purpose is to help the Marshal8e6 support team diagnose support issues. To use the tool select **Tools > Open Support Tool**. You can also run the tool from a command prompt as `WMSupportTool.exe`, found in the WebMarshal installation directory. For more information on how to use the tool, see Marshal8e6 Knowledge Base article Q11886.

The **Proxy Cache** command line tool is installed on each WebMarshal processing node server. The tool allows you to maintain and analyze the cache folders. The tool can be used to list the URLs of files that are stored in the cache, and to delete specific items from the cache. This is useful when diagnosing cache issues and during testing. To start the tool, within a Windows command prompt navigate to the WebMarshal install location and run **WMProxyCacheTool.exe**. For more information on how to use the tool, see the tool help or Marshal8e6 Knowledge Base article Q12724.

Chapter 5
Implementing Your Web Content Security Policy

WebMarshal provides a powerful and flexible framework that allows you to enforce your organization’s Acceptable Use Policy for Web access.

A Web usage policy typically has several goals. As part of the process of implementing WebMarshal, you should develop and formalize your own policy, and make it known to users.

Common goals of a Web usage policy include:

- To maintain appropriate usage (subject matter of browsing and language of uploads).
- To protect the organization’s systems against virus infection.
- To ensure the efficient use of network resources (bandwidth and file storage).
- To allow reporting on Web usage and policy breaches.

WebMarshal includes facilities to perform these tasks. This chapter gives an overview of typical policies and policy-related tasks, and the WebMarshal elements available “out of the box” that you can use to accomplish each task.

Configuring Web Content Security

When you run the Configuration Wizard, you can install a default set of policies, rules, and rule elements. Marshal8e6 recommends the default set as a useful starting place and a source of ideas for customization. Unless you have a custom set of rules from another source, you should install the default set.

The default rules are recommended by Marshal8e6 as the minimum for a useful WebMarshal product evaluation.

Many additional options are available and are covered in detail in the other chapters of this Guide.

Users and Groups

Since WebMarshal is an authenticating proxy server, each browser session must supply a logon credential before any browsing is permitted. You must provide account information for each permitted user so that WebMarshal can authenticate requests. Typically, WebMarshal imports user account information from the local network environment. This section only covers importation of users from Active Directory, the most common environment. To learn about other supported options, including legacy Windows NT, Novell, and workstation based authentication, see "User Management" on page 138.

The default WebMarshal rules grant a basic set of permissions to every authenticated user. You can adjust permissions by adding some users to additional WebMarshal user groups.

Installing the Active Directory connector

1. Highlight the **Connectors** item in the left pane tree.
2. Click the **New Connector** icon in the tool bar to start the New Connector Wizard.

3. On the first page of the wizard, select **Active Directory**.

4. Complete the wizard. In most cases you can accept the default options. See Help for details of the available options.

Adding User Groups from Active Directory

1. Within the WebMarshal Console, ensure that User Groups is selected. Click the **New User Group** icon in the taskpad to start the New User Group wizard.

2. Choose to import groups from the Active Directory connector.

3. Enter the names of the groups that you want to import into WebMarshal. Ensure that each user who is permitted to browse is included in at least one imported group.

   To locate groups within the available Active Directory environment, click **Browse.** In the Browse Network window, select a domain or computer from which to import groups. Select the desired groups from the right pane. Use ctrl-click and shift-click to multi-select. Click **OK** to return to the Wizard screen.

   You can also enter names in standard Distinguished Name format (for instance: `CN=Domain Users,CN=Users,DC=hq,DC=example,DC=com)`. You can enter multiple names separated by semi-colons.

   Tip
   WebMarshal can import groups from trusted Active Directory domains, subdomains, and other domains that have an explicit two way trust relationship with the domain that WebMarshal is a member of. For additional details see Marshal8e6 Knowledge Base article Q11870.

4. Click **Next**, then **Finish**, to add the User Group(s).

To view a list of all users imported into WebMarshal, in the left pane of the Console expand the item **Rule Elements > User Groups > All Users.**

Basic Rule Configuration

The default policies and rules provided with WebMarshal allow you to support the basic Web access policy goals mentioned earlier in this chapter. WebMarshal rules are created and enabled using the WebMarshal Console. In many cases you can simply enable the default items. You may need to customize some rules to meet your needs. You can monitor policy compliance by using WebMarshal Reports to report on triggered rules.

This section describes the steps necessary to enable a basic access policy starting from the default installation of WebMarshal. All of the rules discussed here are found in WebMarshal's Quota, Standard, and Content Analysis rules. A number of other rules are enabled by default, including several rules, applied to all requests, which classify the files to permit logging.

Ensuring Appropriate Usage

For the purposes of this chapter, "appropriate usage" is defined in terms of the content of web pages and files.

You can help to ensure appropriate usage by enabling the WebMarshal TRACEnet facility. TRACEnet provides protection against spam-linked sites, anonymous proxies, phishing sites, and other malicious sites. For more information about TRACEnet, see "Understanding TRACEnet" on page 79. To enable TRACEnet:

1. In the left pane of the WebMarshal Console, expand **Access Policy** and select **TRACEnet.**
2. Check the box to enable the feature.

You can check for appropriate textual content of pages with Content Analysis rules such as *Block - Adult and Nudity Content, Scan - Offensive Language Content,* and *Block Upload of Offensive Text Content*. These rules invoke TextCensor scripts to check the text content of files (including HTML documents and productivity files such as Word documents) as well as web form submissions. These rules must be enabled as described below.

You can also control the subject matter of pages using Filtering Lists provided through the external Filtering List function. Within the default rules, you can implement these Lists with the Standard rules *Block - Adult & Nudity, Block Offensive Language*, *Block Gambling*, and *Block Sports*. Each of these rules is enabled by default. When you configure Filtering Lists, WebMarshal uses appropriate categories from each list in each Rule.

Blocking of files by size and by type (executable and/or audiovisual files) can also contribute to checking for appropriate usage. Most organizations will choose to limit user access to these types of content. The rules *Block Dangerous File Extensions*, *Block Dangerous File*s, *Block Multimedia*, and *Block Documents* are included in WebMarshal's default rules and enabled by default. These rules check the file extension (part of the file name) and the structure of files. You can make exceptions to these rules as described below.

You can use the WebMarshal HTTPS Content Inspection functionality to apply Content Analysis rules to secure web pages that could not otherwise be scanned. For instance, many Webmail sites now use HTTPS. For more information, see "Configuring HTTPS Content Inspection" on page 231.

When a rule is triggered, WebMarshal can take any of several actions:

- Block the file, and display an information page to the user.
- Send a notification message to the WebMarshal Administrator.
- Write a log record that includes information about the user, request, rule triggered, and classification.

Enabling rules

To enable a WebMarshal rule (such as *Block - Adult and Nudity Content*):

1. In the left pane of the WebMarshal Console, expand **Access Policy**.
2. Expand the appropriate rule type (in this case, Content Analysis rules.) A list of rules displays in the right pane. A disabled rule (such as *Block - Adult and Nudity Content*) will display with a dimmed icon and the notation **Disabled.**
3. In the right pane, right-click the rule name.

4. From the context menu choose **Enable Rule.** The rule will be enabled. This change will take effect when you commit the configuration.

5. To commit configuration, click the **Commit Configuration** button in the toolbar.

> **Note**
> When you have made changes but not committed them, the **Commit Configuration** button shows a red icon.

You can enable additional rules using the same procedure. You can also enable multiple rules by selecting them using ctrl-click and shift-click.

Exceptions to rules

You may want to allow some users to download executable files (or other blocked types). The WebMarshal default rules include an exception clause. For instance, members of the User Groups *Can Download Anything* and *Can Download Dangerous Files* are allowed to download executable files.

To implement the exceptions, add the appropriate Users or User Groups to one or more of the exception groups:

1. Select a User Group in the left pane of the Console.

2. Right click and select **Insert Users or User Groups**.

3. In the Insert Users and Groups window, select one or more users or groups you want to add. You can find a specific User or Group by typing a few characters in the bottom text field.

> **Note**
> WebMarshal supports nested User Groups. A WebMarshal Group can contain other WebMarshal or remote directory Groups.

For further information on working with users and groups, see “User Management” on page 138.

Protecting Against Malware

WebMarshal protects against virus infection, spyware, and exploits for all downloads and uploads in three ways: by TRACEnet filtering, by passing messages to third-party scanners, and by file name and file type rules.

Malware Scanning

WebMarshal can scan for viruses, spyware, and other malicious content using the Malware Scan condition in Content Analysis rules. Before you can enable rules that use this action, you must install and configure at least one scanner. For details of these processes, see “Using Malware Scanning” on page 178.

Note

WebMarshal can apply malware scanning to all types of files. However, some file types are “safe” (they are not currently known to contain malware payloads). Scanning all files provides added assurance but has a significant impact on performance.

The WebMarshal default Access Policy includes two types of Virus and Spyware scanning rules:

- The standard scanning rules **exclude** common image types and text from scanning.
- The “Extensive” rules scan all files. These rules can cause users to experience page loading times **2 to 4 times slower** than when using standard rules.

File Type and File Name rules

You can further limit download of viruses and other malicious code by the Content Analysis rules *Block Dangerous File Extensions* and *Block Dangerous Files*. Enable the pre-configured rules by the same method described in “Enabling rules” on page 73.

- The file is blocked and an appropriate information web page is presented to the user.
- A log record is written with the appropriate rule and classification information.

Conserving Network Resources

WebMarshal helps to achieve the goal of conserving network resources by proxy caching, Connection rules, Quota rules, and Content Analysis rules.

Proxy caching

You can reduce bandwidth usage by enabling WebMarshal proxy caching. For more information about caching, see “Configuring Proxy Cache” on page 224.

Connection rules

You can manage connections from many popular Instant Messaging and Streaming Media applications. Sample blocking rules are provided in the default configuration. Edit and enable the pre-configured rules by the same method described above. For more information about how to enable and use connection rules, see “Connection Rules” on page 84.

For streaming media connections that you allow, you can optimize the streaming media experience using the streaming media type selection in the Proxy Wizard. For more information, see “Streaming Content Types” on page 49.

Quota rules

You can limit each user to a quota of browsing time and/or bandwidth. Sample quotas are configured in the quota rules that are provided by default. Enable the pre-configured rules by the same method described above. If quota rules are enabled, Marshal8e6 recommends you also enable the Standard rule *Warn all users about quota limits.*

You can apply quotas to specific users, specific file types, URL Categories, applications, and/or specific times of day. For complete information, see “Quota Rules” on page 85.

Content rules

WebMarshal can stop the download of oversized files by a Content Analysis rule. The rule *Block - Large Downloads* stops large files (over 5 MB) from being accessed.

WebMarshal can stop uploading of oversized files by a Content Analysis rule. The rule *Block large uploads* stops large files (over 512 KB) from being uploaded.

These rules are enabled by default and apply to all users. When triggered, these rules take similar actions to the rules described earlier.

To allow certain users to use large files or a larger quota, you can modify the appropriate rule by adding Users or Groups to an exception group.

Blocking of multimedia files also helps save network resources.

Chapter 6

Understanding Web Access Policy, Rule Containers, and Rules

The WebMarshal Access Policy controls how WebMarshal treats requests for Web resources. The Access Policy includes several types of Rules. The Access Policy also includes the TRACEnet and SafeSearch features.

Understanding TRACEnet

The TRACEnet feature is a “zero day” protection framework supported by the Marshal8e6 TRACElabs team. TRACEnet identifies malicious URLs and allows you to block access to these sites. The TRACElabs team provides frequent updates to the listed URLs, based on data from a number of sources. This framework gives protection against “blended” threats and new risks.

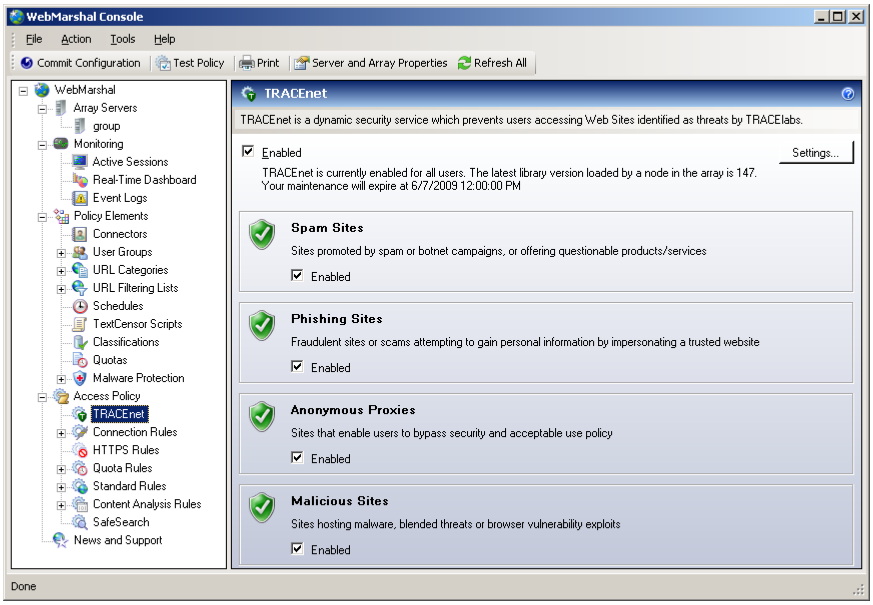
When TRACEnet is enabled, it receives updated URL information from Marshal8e6. The TRACEnet digest collator reports summary data about blocked threats to Marshal8e6 over a secure Web connection. The TRACElabs team uses the reported data as part of the threat identification process that feeds back in to TRACEnet updates.

TRACEnet initially provides four categories:

- Spam sites (URLs offering products or services, that are promoted through spam email)
- Phishing sites (URLs hosting fraudulent attempts to harvest personal information)
- Anonymous proxies (sites that allow users to bypass security by retransmitting web requests)
- Malicious sites (sites hosting malware or exploits)

Marshal8e6 may add new categories to TRACEnet. New categories can be added dynamically during the standard update process.

TRACEnet service is included for WebMarshal customers holding current maintenance contracts, as well as with product trials. The maintenance expiration for TRACEnet displays on the TRACEnet page. This information is provided by the TRACEnet update server.



TRACEnet

TRACEnet is a dynamic security service which prevents users accessing Web Sites identified as threats by TRACElabs.

☑ Enabled

TRACEnet is currently enabled for all users. The latest library version loaded by a node in the array is 147. Your maintenance will expire at 6/7/2009 12:00:00 PM

Spam Sites

Sites promoted by spam or botnet campaigns, or offering questionable products/services

☑ Enabled

Phishing Sites

Fraudulent sites or scams attempting to gain personal information by impersonating a trusted website

☑ Enabled

Anonymous Proxies

Sites that enable users to bypass security and acceptable use policy

☑ Enabled

Malicious Sites

Sites hosting malware, blended threats or browser vulnerability exploits

☑ Enabled

To configure TRACEnet, in the left pane of the WebMarshal Console expand **Access Policy** and select **TRACEnet.**

To enable or disable the feature, check or clear the box on the main TRACEnet page. To enable or disable the individual categories, check or clear the box for each.

You can configure advanced settings for TRACEnet, including User Group and URL exclusions, an end-user "request reclassification" option, and download options. To configure advanced settings, at the top right of the main TRACEnet page click **Settings**. For more information, see Help.

To review TRACEnet activity and library updates, see the TRACEnet section of the Real-Time Dashboard. You can also request an immediate check for library updates using the **Update Now** button on the Dashboard.

Enforcing SafeSearch

WebMarshal allows you to enforce use of the "Strict Safe Search" function that some search engines provide. WebMarshal SafeSearch initially supports Google and Yahoo! (the list of supported search engines can be updated dynamically). This feature adds the "safe search" parameter to each request that a user makes to the supported search engines.

Note

The search filtering provided when WebMarshal SafeSearch is enabled depends entirely on the results returned by the specific search engine, and is not based on any further evaluation by WebMarshal. The search engines do not guarantee that they can filter out 100% of the offensive or adult material returned by a search. The content excluded from the search results through WebMarshal is in line with the search engine providers' policy. See the search provider websites for more details.

To configure SafeSearch, in the left pane of the WebMarshal Console expand **Access Policy** and select **SafeSearch**.

- **To enable or disable the feature**, check or clear the box on the main SafeSearch page.
- You can choose to exclude one or more User Groups from this feature. To configure User Group exclusions, at the top right of the main SafeSearch page click **Settings**. For more information, see Help.

Understanding Rules

The main feature of WebMarshal Access Policy is the Rules. Each rule is defined with a set of conditions, and a set of actions that WebMarshal takes if a Web request meets the conditions.

The Access Policy can also use Rule Containers. A Container allows you to group a set of rules that share common conditions (for instance, user matching or request direction). Rules within a Container only apply when a request meets the conditions defined for the container.

Each WebMarshal Rule has three parts: User Matching, Conditions and Actions.

- User Matching allows you to specify the server groups where the rule applies, and the users or workstations that the rule applies to.
- If the request meets the User Matching criteria, it is evaluated using the Conditions.
- If the request meets the Conditions, WebMarshal performs the Actions.

For instance, a rule might state:

```
When a web request is received for any User (user matching),
And where addressed to any URL
If the content matches the TextCensor Script
   Sports Betting (conditions)
Classify the Domain as Sports Betting
   Add the URL Domain to the Category Betting Sites (actions).
```

Note

When WebMarshal is installed as a new installation, the Configuration Wizard offers the choice to install a basic set of rules. Each rule includes comments as to its possible use. To use these rules, add users to the appropriate user groups and modify the rules to fit your organizational policy. You can also use the default rules as models in creating new rules.

Understanding Rule Types

WebMarshal rules are divided into five types: Connection Rules, HTTPS Rules, Quota Rules, Standard (Site) Rules, and Content Analysis Rules. Within each type you can create Rules and Rule Containers.

Note

Rule Containers allow you to set a single group of conditions for several rules. For instance, you can have one Quota Rule container for rules that apply on weekends, and another Quota Rule container for rules that apply on weekdays. A Rule Container can include any of the conditions that are available for the rule type.

Connection Rules

Connection Rules are evaluated when WebMarshal receives a request from a user. Connection Rules allow you to implement policy based control of HTTP connections from many Instant Messaging and Streaming Media applications such as Windows Live Messenger or Real Media.

Notes

- For Connection Rules to be effective, you must ensure that other ports used by these applications are blocked at the firewall. For more information, see Marshal8e6 Knowledge Base article Q12021.
- Before you can use Connection Rules, you must enable this functionality in the WebMarshal Server Properties. For more information, see "Configuring Connection Rule Processing" on page 235.
- Connection rules cannot be used when WebMarshal is installed as a plug-in to ISA Server. Console items related to Connection Rules will be removed or disabled if ISA plug-in is enabled.

HTTPS Rules

HTTPS rules are evaluated when a user connects to a website that uses HTTPS (Secure HTTP). HTTPS Rules allow you to implement policy based on the encryption protocol and the security certificate used. HTTPS Rules also allow you to scan the content of selected HTTPS traffic. The HTTPS traffic is decrypted, which allows it to be scanned, and then re-encrypted for transfer to the destination.

Notes

- Before you can use HTTPS rules, you must configure the HTTPS functionality. See "Configuring HTTPS Content Inspection" on page 231.
- HTTPS rules cannot be used when WebMarshal is installed as a plug-in to ISA Server. Console items related to HTTPS will be removed or disabled if ISA plug-in is enabled.
- When HTTPS rules are enabled, content is always secured when transmitted over the network.

Quota Rules

Quota rules are evaluated when WebMarshal receives a request for a Web resource from a browser session, and if necessary after the response has been returned from the Web. These rules allow users specific amounts of web browsing time and/or volume for a period such as a day or week. Quota rules can have conditions based on time of day or day of the week, file type, URL category, and the protocol or application. For information about managing Quotas, see “Configuring Access Using Quotas” on page 162. For a full list of conditions and actions, see Help for the Quota Rules window in the WebMarshal Console.

Standard Rules

Standard (site blocking) rules are evaluated when WebMarshal receives a request from a browser session. These rules permit or deny access to URL categories by user groups. Standard rules can have conditions based on time of day or day of the week, file name, file type, presence of cookies, and the request direction (upload or download).

Depending on the outcome of rule evaluation, WebMarshal can permit or deny access to the resource, and optionally require the user to acknowledge a warning.

Note

WebMarshal only grants access by explicit standard rules. The default action is to block access. If your organizational policy is to allow most requests, you should set up a permissive Standard rule that is evaluated last. The WebMarshal default rules include rules that accomplish this.

Content Analysis Rules

Content Analysis rules are evaluated when WebMarshal receives the content of the Web request. This type of rule allows you to base policy on the actual results of a specific request, including new or dynamically generated files.

Notes

- Some Content Analysis rules require WebMarshal to fully scan the response files before returning them to the user. If you configure complex rules and scripts, the user may experience a delay during scanning. To minimize the delay, in most cases a TextCensor rule that blocks a request should also add the URL to a category. WebMarshal can then block future requests for the URL quickly, using a Standard rule
- To reduce the delay due to processing, in some cases WebMarshal "trickles" a portion of the file to the user. If the page triggers the rule, the download is aborted. For information about configuring the "trickle," see "Configuring Download Options" on page 226.
- Upload Content Analysis rules cannot be used when WebMarshal is installed as a plug-in to ISA Server.

Content Analysis rules can check for many conditions, including:

- Request direction (upload or download)
- Transfer size
- File type
- Content type (based on MIME type, such as MPEG)
- Text content (TextCensor lexical analysis)
- Malware scanning results

Content Analysis can also check items unpacked from archive files and OLE documents in many cases.

Content Analysis rules can apply a number of actions, including:

- Permit or block the request
- Display a warning page and require the user to acknowledge
- Write a log classification for the file or the request domain
- Add the user to a group
- Add the request URL to a URL category
- Notify the administrator

Working With Access Policy

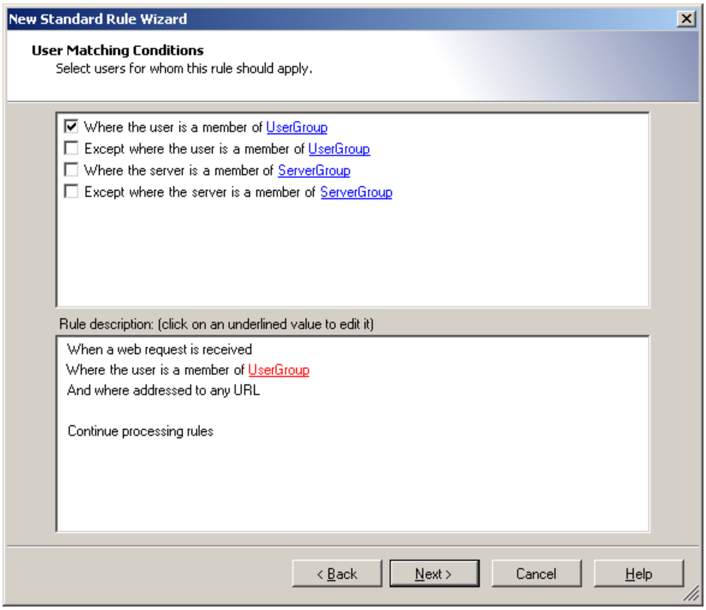
To work with rules in the WebMarshal Console, ensure that the menu item Access Policy is expanded.

Creating a Rule or Rule Container

WebMarshal Rules and Rule Containers have many elements in common. The procedure below illustrates the creation of an example rule. The available options are covered in the following sections.

1. In the left pane of the Console, expand **Access Policy**. Select a rule type.
2. ***If you want to create the rule within a container,*** double-click the container in the right pane to open it.
3. Click the **New Rule** icon in the taskpad.

4. Click **Next** to continue to the User Matching Conditions page.



User Matching Conditions

Select users for whom this rule should apply.

☑ Where the user is a member of UserGroup
□ Except where the user is a member of UserGroup
□ Where the server is a member of ServerGroup
□ Except where the server is a member of ServerGroup

Rule description: (click on an underlined value to edit it)

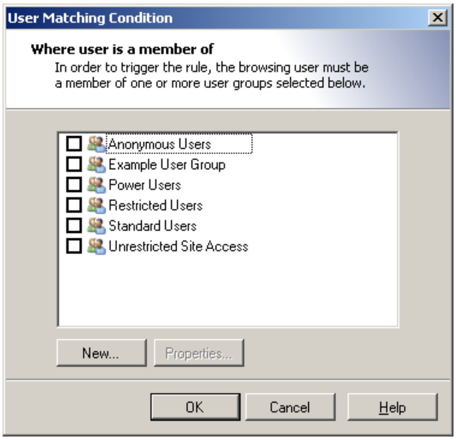
When a web request is received
Where the user is a member of UserGroup
And where addressed to any URL

Continue processing rules

5. On the User Matching Conditions page, check the boxes in the top pane to select the conditions you want to include in the rule. The items you select items display in the rule description pane, at the bottom of the page.

6. If you can specify details for a condition, each item that requires details includes a hyperlink. The hyperlink text is red if you must enter a value, or blue if a value is already specified. Click any hyperlink to enter or change the detail information. For more information about the specific expressions, see “User Matching Conditions” on page 95.

7. For instance, if you select *where the user is a member of User Group,* the text **UserGroup** in the rule description is a red link. Click this link to display the Select User Groups window.



Where user is a member of

In order to trigger the rule, the browsing user must be a member of one or more user groups selected below.

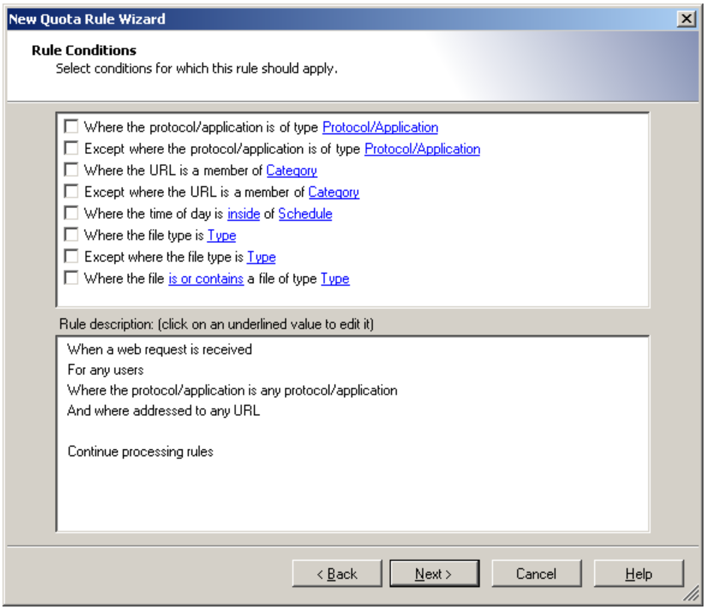
- □ Anonymous Users
- □ Example User Group
- □ Power Users
- □ Restricted Users
- □ Standard Users
- □ Unrestricted Site Access

In this window, you can select an existing user group. You can also click **New** to start the New User Group wizard, as described in "User Management" on page 138. If you create a new user group, it is selected for use when you return to the Select User Groups window.

Note

If your WebMarshal installation uses more than one type of authentication, remember to include all authentication types in Rules. For instance, if WebMarshal uses both Windows and IP authentication, User Matching should include both user names and workstation names as appropriate.

8. Click **Next** to continue to the Rule Conditions page.



Rule Conditions
Select conditions for which this rule should apply.

- □ Where the protocol/application is of type Protocol/Application
- □ Except where the protocol/application is of type Protocol/Application
- □ Where the URL is a member of Category
- □ Except where the URL is a member of Category
- □ Where the time of day is inside of Schedule
- □ Where the file type is Type
- □ Except where the file type is Type
- □ Where the file is or contains a file of type Type

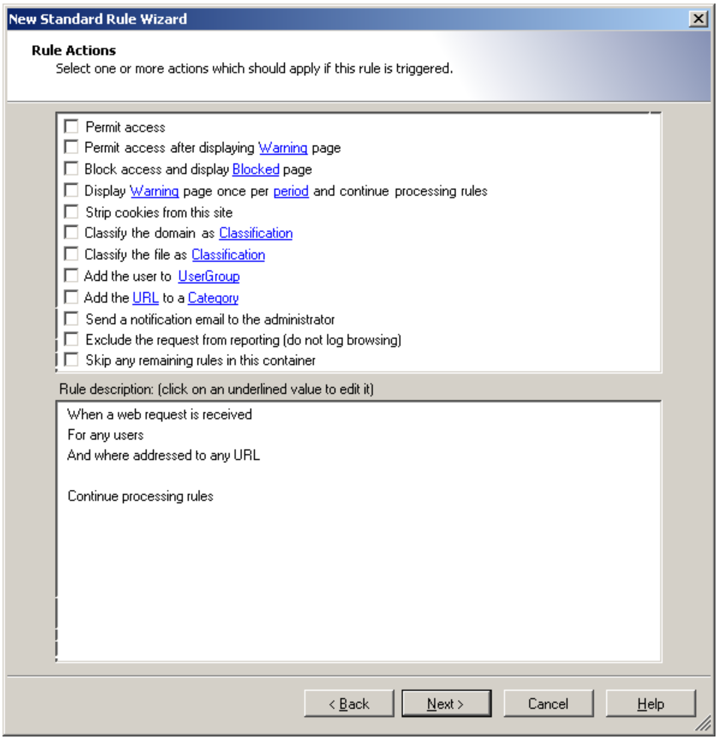
Rule description: (click on an underlined value to edit it)

When a web request is received
For any users
Where the protocol/application is any protocol/application
And where addressed to any URL

Continue processing rules

9. Select conditions and enter details on this page in the same way as for Step **5**. See "Rule Conditions" on page 98 for details on options for the specific conditions.

10. When you have entered all the details on the Rule Conditions page, click **Next** to continue to the Rule Actions page.



New Standard Rule Wizard

Rule Actions

Select one or more actions which should apply if this rule is triggered.

- □ Permit access
- □ Permit access after displaying Warning page
- □ Block access and display Blocked page
- □ Display Warning page once per period and continue processing rules
- □ Strip cookies from this site
- □ Classify the domain as Classification
- □ Classify the file as Classification
- □ Add the user to UserGroup
- □ Add the URL to a Category
- □ Send a notification email to the administrator
- □ Exclude the request from reporting (do not log browsing)
- □ Skip any remaining rules in this container

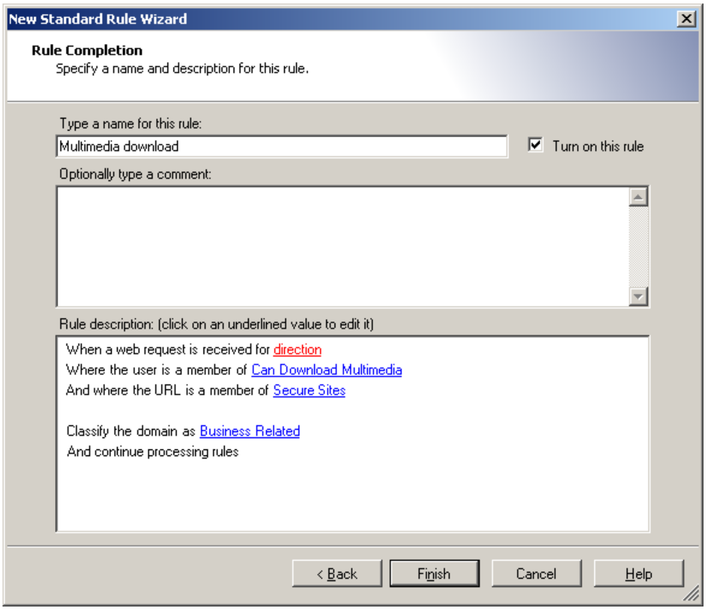
Rule description: (click on an underlined value to edit it)

When a web request is received
For any users
And where addressed to any URL

Continue processing rules

11. Select actions and enter details on this page in the same way as for Step **5**. The actions that you can select vary depending on the type of rule. See “Rule Actions” on page 122 for details on options for the specific actions.

12. When you have entered all details on the Rule Actions page, click **Next** to continue to the Rule Completion page.



New Standard Rule Wizard

Rule Completion

Specify a name and description for this rule.

Type a name for this rule:

Multimedia download

☑ Turn on this rule

Optionally type a comment:

Rule description: (click on an underlined value to edit it)

When a web request is received for direction
Where the user is a member of Can Download Multimedia
And where the URL is a member of Secure Sites

Classify the domain as Business Related
And continue processing rules

13. Enter a name for the rule.

14. Optionally enter a comment or description for the rule.

15. Choose whether to enable the rule immediately (default) or not, using the **Turn on this rule** checkbox.

16. Click **Finish** to return to the WebMarshal Console.

Notes

- The **order of evaluation** of rules is important. WebMarshal bases its action on the first rule triggered. You can adjust the order of evaluation. See "Understanding the Order of Evaluation" on page 132.
- **Changes only take effect when you commit configuration**. To commit configuration, click the Commit Configuration icon on the tool bar. When changes have been made but not reloaded, the icon is red and the item **WebMarshal** at the top of the left pane is followed by *****. A notice also displays in the status bar.

Editing Rules

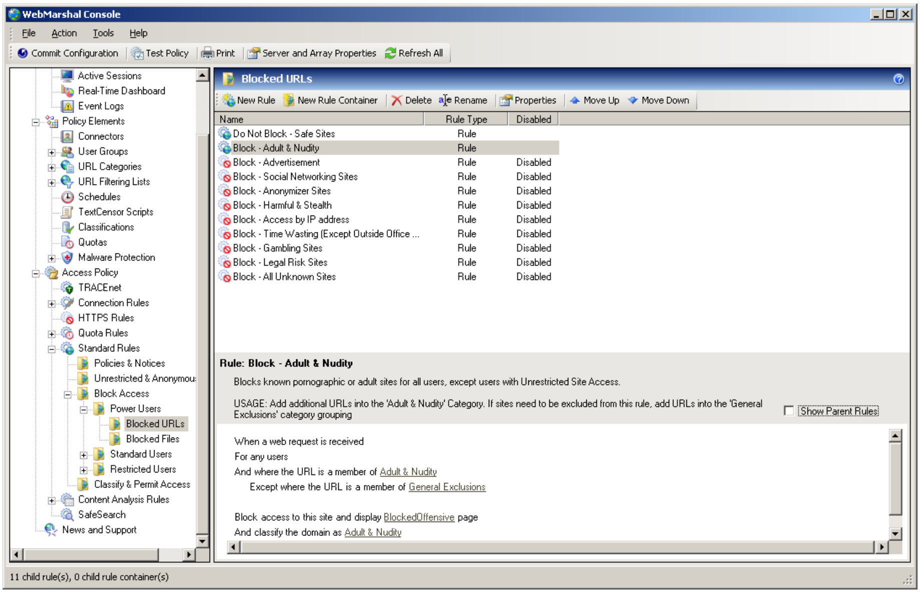
The following procedure applies to all types of WebMarshal Rules and Rule Containers.

To edit a rule or rule container:

1. In the left pane of the console, expand **Access Policy**.
2. Select the Rule type or Rule Container that includes the item you want to edit.
3. Double-click the rule or rule condition in the right pane. The rule is presented in the Rule Wizard–Rule Completion page.
4. Click any hyperlinked item to change it. If you want to make more basic changes to the actions or conditions, click **Back** to view the User Matching, Conditions, or Actions pages.
5. When satisfied, click **OK**.

Enabling and Disabling Rules

You can enable or disable individual rules or rule containers. Disabled rules (or rules in disabled containers) are not used to evaluate web requests. Disabled rules and containers display with a rule-disabled icon (dimmed, with a red ⊘, as shown below).



Name	Rule Type	Disabled
Do Not Block - Safe Sites	Rule	
Block - Adult & Nudity	Rule	
Block - Advertisement	Rule	Disabled
Block - Social Networking Sites	Rule	Disabled
Block - Anonymizer Sites	Rule	Disabled
Block - Harmful & Stealth	Rule	Disabled
Block - Access by IP address	Rule	Disabled
Block - Time Wasting (Except Outside Office ...	Rule	Disabled
Block - Gambling Sites	Rule	Disabled
Block - Legal Risk Sites	Rule	Disabled
Block - All Unknown Sites	Rule	Disabled

Rule: Block - Adult & Nudity

Blocks known pornographic or adult sites for all users, except users with Unrestricted Site Access.

USAGE: Add additional URLs into the 'Adult & Nudity' Category. If sites need to be excluded from this rule, add URLs into the 'General Exclusions' category grouping

☐ Show Parent Rules

When a web request is received
For any users
And where the URL is a member of Adult & Nudity
    Except where the URL is a member of General Exclusions

Block access to this site and display BlockedOffensive page
And classify the domain as Adult & Nudity

11 child rule(s), 0 child rule container(s)

1. Ensure that Rules is expanded.
2. Select a rule type in the left pane.
3. Double-click a particular rule or rule container in the right pane.
4. On the Rule Wizard page, check or uncheck **Turn on this rule**.
5. Click **OK**.

You can also enable, disable, or delete Rules and rule containers using a right-click context menu. You can select multiple rules for these actions by using shift-click and control-click.

Warning
When you delete a rule container, all the items it contains are also deleted.

Understanding User Matching

User Matching allows you to apply policies to specific users (login accounts) or to specific workstations.

User Matching Conditions

All WebMarshal Rules and Rule Containers can include one or more of the following User Matching conditions.

Where the user is a member of User Group

If this User Matching Condition is selected, the Rule will apply to all members of the User Group(s) listed in the Rule Description pane with this condition (except for members of any of the exception groups, as described below).

To add or edit User Groups in this condition:

1. Click a UserGroup link to open the User Matching Condition window.
2. In this window, you can select an existing user group. You can also click **New** to start the New User Group wizard and create a user group, as described in “User Management” on page 138. If you create a new user group, it is selected for use when you return to the User Matching Condition window.

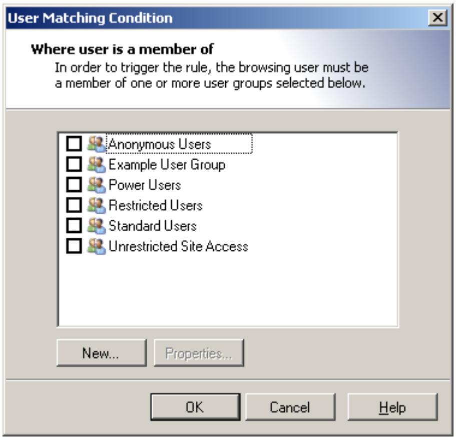
Note
If your WebMarshal installation allows more than one type of authentication, remember to include all authentication types in Rules. For instance, if both Windows and IP authentication are enabled, User Matching should include both user names and workstation names as appropriate.

Except where the user is a member of User Group

If this User Matching Condition is selected, the Rule will not apply to any member of the User Groups listed in the Rule Description pane with this condition.

To add or edit user groups in this condition:

1. Click a UserGroup link to open the User Matching Condition window.
2. Select existing or create new groups as described above.



User Matching Condition

Where user is a member of

In order to trigger the rule, the browsing user must be a member of one or more user groups selected below.

☐ Anonymous Users
☐ Example User Group
☐ Power Users
☐ Restricted Users
☐ Standard Users
☐ Unrestricted Site Access

This condition overrides the previous condition. For instance, a Rule might start:

```
Where the user is a member of Staff, except where the User is a member
of Executive)
```

Note
Exception based rules are the key to good resource management. General rules should cover most cases; use exceptions for small groups. You can also use an exception condition alone (for instance, `For any User, except where the User is a member of Executive`).

Where the server is a member of Server Group

If this Condition is selected, the Rule will apply only for requests processed on the WebMarshal Processing Servers contained in the Server Group(s) listed in the Rule Description pane with this condition (except for members of any of the exception groups, as described below).

Note
Server Group conditions allow you to enforce different policies at different locations in a large distributed installation.

To add or edit Server Groups in this condition:

1. Click a ServerGroup link to open the Server Condition window.
2. In this window, you can select an existing server group. You can also click **New** to start the New Server Group wizard and create a server group, as described in "Configuring Server Group Properties" on page 244. If you create a new server group, it is selected for use when you return to the Server Matching Condition window.

Except where the server is a member of Server Group

If this Condition is selected, the Rule will *not* apply for requests processed on the WebMarshal Processing Servers contained in the Server Group(s) listed in the Rule Description pane with this condition.

Understanding Rule Conditions

Each WebMarshal Rule or Rule Container includes one or more conditions. Not all conditions are available for all WebMarshal Rule types.

Rule Conditions

The complete list of conditions includes:

- When a web request is received for Direction
- Where the protocol/application is of type
- Except where the protocol/application is of type
- Where the URL is a member of Category
- Except where the URL is a member of Category
- Where the time of day is inside or outside of Schedule
- Where the server certificate is invalid
- Where the security protocol is
- Where the site requests a client certificate during SSL/TLS negotiation
- Where SSL/TLS could not be negotiated
- Where the content is/is not inspected HTTPS content
- Where the request contains cookies
- Where the URL domain name is an IP address
- Where the transferred data size is size
- Where the content matches all/any of TextCensor Script(s)
- Where the result of a malware scan is
- Where the file type is
- Except where the file type is
- Where the file is or contains a file of type

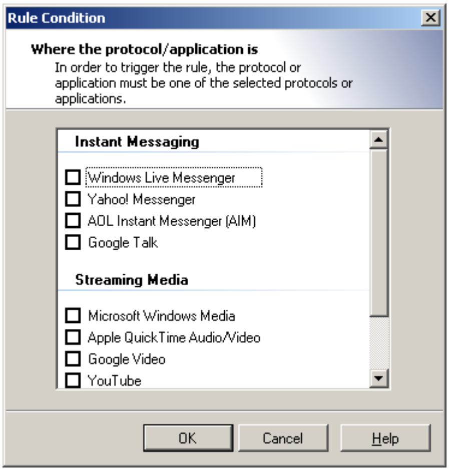
- Where the parent file type is
- Except where the parent file type is
- Where the file name matches
- Except where the file name matches
- Where the parent file name matches
- Except where the parent file name matches
- Where the download content type is
- Except where the download content type is
- Where an error occurs while unpacking

When a web request is received for direction

If this Condition is selected, the Rule will apply to all requests of the selected type (upload or download). **Downloads** include standard web page views and file access. **Uploads** include form and file posting. Click **Direction** to open the Data Direction window. Select **Downloading** or **Uploading**, and then click **OK**.

Where the protocol/application is of type

If this condition is selected, the Rule will apply for requests from specific Instant Messaging and Streaming Media applications. Click **Protocol/Application** to open the Select Application window.



Rule Condition

Where the protocol/application is

In order to trigger the rule, the protocol or application must be one of the selected protocols or applications.

Instant Messaging

□ Windows Live Messenger
□ Yahoo! Messenger
□ AOL Instant Messenger (AIM)
□ Google Talk

Streaming Media

□ Microsoft Windows Media
□ Apple QuickTime Audio/Video
□ Google Video
□ YouTube

1. Select one or more applications to match by checking the boxes. To view the detailed description of the protocol, hover over an item.

2. Click **OK** to return to the parent Wizard.

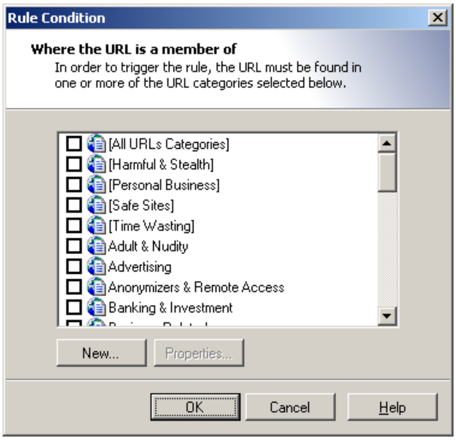
You can specifically exclude applications using the exclusion condition **Except where the URL is a member of Category**.

Except where the protocol/application is of type

If this condition is selected, the Rule will not apply for requests from specific Instant Messaging and Streaming Media applications listed in the Rule Description pane with this condition. Within a Rule, this condition overrides the condition **Where the protocol/application is of type.**

Where the URL is a member of category

If this Condition is selected, the Rule will apply for requests to all members of the URL Category (or Categories) listed in the Rule Description pane with the condition. Click **Category** to open the Select URL Categories window.



Rule Condition

Where the URL is a member of

In order to trigger the rule, the URL must be found in one or more of the URL categories selected below.

- □ [All URLs Categories]
- □ [Harmful & Stealth]
- □ [Personal Business]
- □ [Safe Sites]
- □ [Time Wasting]
- □ Adult & Nudity
- □ Advertising
- □ Anonymizers & Remote Access
- □ Banking & Investment

1. Select one or more URL Categories to match by checking the boxes. To view the detailed description of a category and the number of URLS it includes, select the category name and then click **Properties**.
2. Optionally click **New** to create a new URL Category.
3. Click **OK** to return to the parent Wizard.

You can specifically exclude URLs using the exclusion condition **Except where the URL is a member of Category**.

Except where the URL is a member of category

If this Condition is selected, the Rule will not apply for requests to any member of the URL Category (or Categories) listed in the Rule Description pane with this condition. Within a Rule, this condition overrides the condition Where the URL is a member of category.

See **Where the URL is a member of category** for details on how to select Categories to match.

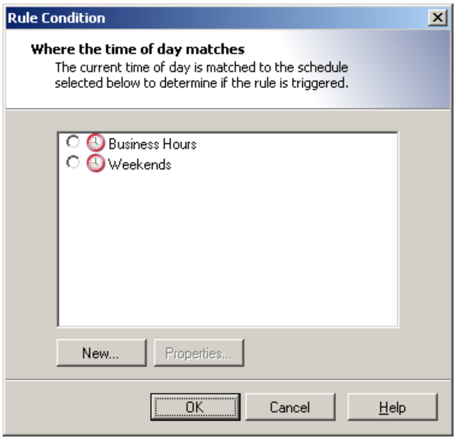
Exception based rules are the key to good resource management. General rules should be created to cover most cases; exceptions should be made for small numbers of sites. For instance, a Rule might apply

```
Where the URL is a member of News Sites, except where the URL is a
member of Tabloids.
```

You can use an exception condition alone (for instance, `Where addressed to any URL, except where the URL is a member of Tabloids`.)

Where the time of day is inside or outside of schedule

If this Condition is selected, the Rule will apply at specific times depending on the Schedule selected. Click **Schedule** to select a schedule using the Select Schedule window.



Rule Condition

Where the time of day matches

The current time of day is matched to the schedule selected below to determine if the rule is triggered.

○ Business Hours
○ Weekends

1. Select a Schedule to match using the radio buttons. To view or edit the details of a schedule, select the schedule name and then click **Properties**.

2. Optionally click **New** to create a new Schedule, as described in “Configuring Access Using Schedules” on page 159.

3. Schedule conditions normally match times within the schedule (blue area in the schedule rule element). If you want to match times outside the schedule, click **inside** and select **Inside** or **Outside**.

4. Click **OK** to return to the parent Wizard.

Where the server certificate is invalid

This condition allows you to apply a rule based on the validity conditions of a security certificate used by a HTTPS website. Click the **Invalid** link to open the Invalid Certificate window and select the certificate problems you want to check for.

1. Select one or more problems. If **any** of the problems occurs, the condition is met. WebMarshal can check for the following problems:
   - **Certificate is not valid for the web site**: The certificate presented is not valid for the website (URL) the user is trying to access.
   - **Certificate has expired**: The security certificate has expired.
   - **Certificate is not yet valid**: The start of the certificate validity period has not been reached. Security certificates can have a future start date.
   - **Certificate is self-signed**: The certificate has not been validated by a root certificate. It is validated only by the remote web server.
   - **Certificate chain is not trusted**: The certificate cannot be chained back to a trusted root certificate, or WebMarshal does not recognize enough of the certificate chain.
   - **Certificate breaks certificate validation rules**: The certificate does not conform to the industry standard for security certificates.

2. Click **OK** to return to the parent Wizard.

Where the security protocol is protocol

This condition allows you to require specific security protocols for HTTPS connections. The available protocols are distinguished by the difference in their cipher strength. The standard protocol strength now in use is TLSv1.0.

Click **Protocol** to open a window that allows you to select one or more protocols that connections can use. Select the protocols, and then click **OK** to return to the parent wizard.

Note
The protocol is selected automatically. Generally the strongest protocol advertised by the remote web server is selected. You can use this condition if you want to block connections to web servers that do not support strong ciphers.

Where the site requests a client certificate during SSL/TLS negotiation

This condition allows you to take action when the remote web server requires the client browser to supply a security certificate, which will be used in addition to the server certificate. The client certificate uniquely identifies the user and can help to ensure security of a connection.

WebMarshal cannot inspect HTTPS content when a page requires a client certificate.

Use this condition with a rule action to block access, or to permit access without inspecting content.

Note
WebMarshal can only use the configured rule action if the request for a client certificate comes during the initial HTTPS negotiation. If the client certificate is requested later in the process, WebMarshal will block the request and return a special block page titled *Client Security Certificate Required*.

Where SSL/TLS could not be negotiated

This condition allows you to take action when the user enters a HTTPS URL, but the client application and the server cannot agree a security protocol. This could happen, for instance, if the client requires SSLv3 but the server supports only SSLv2.

Where the content is inspected HTTPS content

This condition can be used in a Standard or Content Analysis rule to determine if a request has been made from inside an inspected HTTPS connection. You can use this condition to apply different rules to data that WebMarshal has extracted from a HTTPS connection.

1. Click **is** to open a window that allows you to select from the following options:

   Content is from inside an inspected HTTPS connection:
   The request was made as a HTTPS connection that WebMarshal is inspecting.

   Content is from a normal HTTP or non-inspected HTTPS connection:
   The request was a standard HTTP request, or a HTTPS request that has not been decrypted by WebMarshal.

2. Click **OK** to return to the parent window.

Where the request contains cookies

This Condition allows you to apply Rules to download responses that send HTTP "cookies" as part of the response.

To apply this condition, select the box.

Note
WebMarshal does not currently check for request cookies (sent by the client). WebMarshal cannot check for cookies created by client-side action (such as JavaScript).

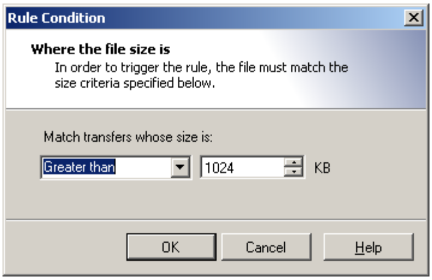
Where the URL domain name is an IP address

This Condition, available in Standard rules, allows you to check for attempts to browse by IP address.

Tip
Typically browsing by IP address is an attempt to circumvent the WebMarshal Rules. Most organizations will choose to block browsing by IP address for all users (with a few exceptions if necessary).

Where the transferred data size is size

This Condition allows you to apply Rules based on the total size of a web request (sent or received). To choose file sizes, in the Rule Wizard click **Size** to open the Data Size window.



Rule Condition

Where the file size is

In order to trigger the rule, the file must match the size criteria specified below.

Match transfers whose size is:

Greater than 1024 KB

1. Choose whether to trigger on file transfers greater than or less than a specified size, or between two sizes.
2. Enter the size(s) in KB.
3. Click **OK** to accept changes and return to the parent Wizard. Click **Cancel** to revert to the saved information.

   Note
   WebMarshal only checks the total transfer size for each request (for instance, a HTML file, image, .zip file, or .wav file). WebMarshal does not check the sizes of individual files that could be unpacked from an archive.

Where the result of a malware scan by scanner is

This condition invokes the scanners you select to check for viruses or spyware.

Note
WebMarshal can apply malware scanning to all types of files. You can limit scanning (for instance, you can choose not to scan image files), by using a file type or content type condition in the rule or rule container.

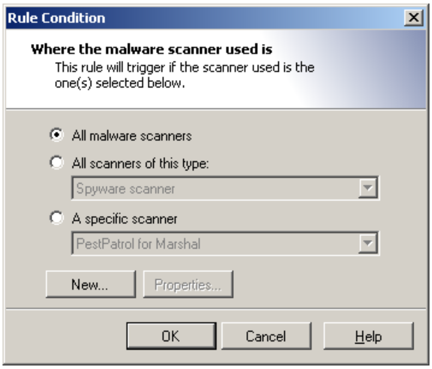
Some files are generally safe (not known to contain malware payloads). Scanning all files provides added assurance but has a significant impact on performance and user experience.

The WebMarshal default Access Policy includes two types of Virus and Spyware scanning rules:

- The standard scanning rules **exclude** common image types and text from scanning.
- The “Extensive” rules scan all files. These rules are typically **2 to 4 times slower** than the standard rules.

To select scanners:

Click the hyperlink **Scanners** to open the Malware scanner used window.



Rule Condition

Where the malware scanner used is

This rule will trigger if the scanner used is the one(s) selected below.

● All malware scanners

○ All scanners of this type:

Spyware scanner

○ A specific scanner

PestPatrol for Marshal

1. Choose which scanners to use. You can only select scanners you have configured in WebMarshal.

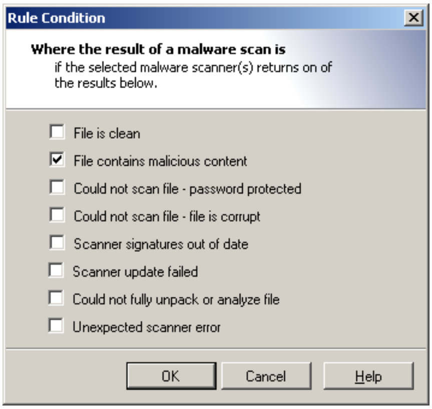
   Note
   If you have installed scanner software but you have not yet configured it, you can configure it by clicking **New**.

   - **All malware scanners:** This condition will check files using all configured virus and spyware scanners.
   - **All scanners of this type:** This condition will check files using all configured scanners of the type you select. Use the menu to select virus scanners or spyware scanners.
   - **A specific scanner:** This condition will check files using a specific scanner. Use the menu to choose from the configured scanners. To view details of a selected scanner, click **Properties**.

2. Click **OK** to return to the parent Wizard.

To select scanner results:

Click the hyperlink **Scanner result** to open the Result of malware scan window.



Where the result of a malware scan is
if the selected malware scanner(s) returns on of the results below.

- ☐ File is clean
- ☑ File contains malicious content
- ☐ Could not scan file - password protected
- ☐ Could not scan file - file is corrupt
- ☐ Scanner signatures out of date
- ☐ Scanner update failed
- ☐ Could not fully unpack or analyze file
- ☐ Unexpected scanner error

1. Check the boxes to select the desired conditions. In general, the more boxes selected, the more restrictive the conditions on downloads or uploads.

   - **File is clean:** The condition will trigger if the file is reported as clean by all scanners selected within this rule condition.
   - **File contains malicious content:** The condition will trigger if the file is reported to contain malware by any scanner selected within this rule condition. This is the basic condition.
   - **Could not scan file - Password protected:** When this box is checked, the condition will trigger if any scanner reports the file as password protected.
   - **Could not scan file - File is corrupt:** When this box is checked, the condition will trigger if any scanner reports the file as corrupt.
   - **Scanner signatures out of date:** When this box is checked, the condition will trigger if any scanner reports its signature files are out of date.
   - **Scanner update failed:** When this box is checked, the condition will trigger if the last update attempt for any scanner was unsuccessful.

- **Could not fully unpack or analyze file:** When this box is checked, the condition will trigger if any scanner reports that it could not unpack the file.
- **Unexpected scanner error:** When this box is checked, the condition will trigger if any scanner reports an unknown error or the code returned is unknown.

2. Click **OK** to return to the parent Wizard.

Note

Best practice is to block files that are reported as password protected or corrupt (since these cannot be scanned) as well as files containing malware.

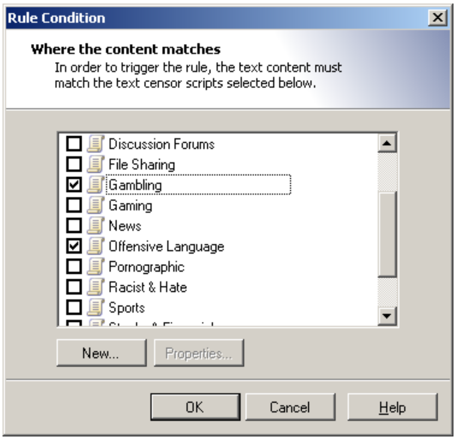
Where the content matches TextCensor script

This Condition invokes one or more TextCensor Scripts to check the text content of a web page or other text file.

Note

If a TextCensor Rule applies a “Permit” or “Block” action, all response text files which match the user group and other conditions are fully scanned before being returned to the user. If you have configured complex scripts, scanning can have an impact on perceived performance. To enhance processing speed, in most cases a TextCensor rule that blocks a request should also add the URL to a category. This allows WebMarshal to block future requests for the URL quickly, using a Standard rule

1. Select one or more Scripts to match by checking the boxes in the Select TextCensor Script window.



Rule Condition

Where the content matches

In order to trigger the rule, the text content must match the text censor scripts selected below.

- ☐ Discussion Forums
- ☐ File Sharing
- ☑ Gambling
- ☐ Gaming
- ☐ News
- ☑ Offensive Language
- ☐ Pornographic
- ☐ Racist & Hate
- ☐ Sports

2. To create a new TextCensor Script, click **New**. For more information see “Identifying Web Content Using TextCensor Scripts” on page 169.

3. To review and edit an existing TextCensor script, select the script name and then click **Properties**.

If you have selected more than one TextCensor Script from the list., you can choose whether the content must match all, or any, of the selected scripts.

To choose an option:

1. Click **All** to open the Multiple Scripts window. Choose from the following
   - Match all selected scripts: If you choose this option, the condition will only be true if all of the selected scripts trigger.
   - Match any of the selected scripts: If you choose this option, the condition will be true if any of the selected scripts trigger.
2. Select an option, and then click **OK** to return to the parent Wizard.

Where the file type is

This Condition allows you to apply Rules to specific file types. File types are recognized by their internal structure, and not by their name or extension.

Warning
Although this condition is available in both Standard and Content Analysis rules, Marshal8e6 recommends you use it only in Content Analysis rules. Standard Rules are often evaluated when only part of the data is available, and for many types this makes determining the type of the file unreliable. Content Analysis rules are always evaluated once the entire file has been downloaded and the file type has been correctly determined. For more information, see Marshal8e6 Knowledge Base article Q12839.

- In Standard rules, this Condition only checks the top level file that was directly requested.
- In Standard rules applied to uploads, this condition checks the type of files directly uploaded (attached to the upload form).

- In Content Analysis rules, this Condition checks the top level file and each file unpacked from archive files.
- For more file type matching options, see the Conditions *Where the file is or contains a file of type* and *Where the parent file type is.*

Note

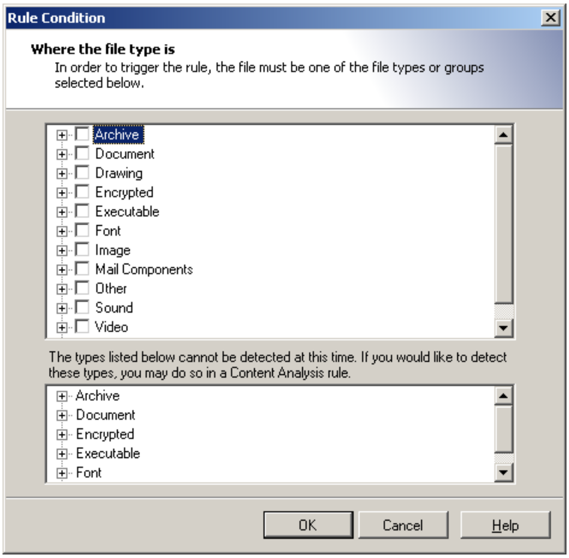
You can match files in two other ways:

- The Condition *Where the file name is* allows for file matching by name or extension.

The condition *Where the content type is* allows for file matching by the type declared in the web request headers.

To choose file types:

1. Within the Rule Wizard click Type to open the **Select File Types** window.



Rule Condition

Where the file type is

In order to trigger the rule, the file must be one of the file types or groups selected below.

- □ Archive
- □ Document
- □ Drawing
- □ Encrypted
- □ Executable
- □ Font
- □ Image
- □ Mail Components
- □ Other
- □ Sound
- □ Video

The types listed below cannot be detected at this time. If you would like to detect these types, you may do so in a Content Analysis rule.

- Archive
- Document
- Encrypted
- Executable
- Font

2. Expand any category to see the particular types available.

3. Choose the categories or specific types of files to match.

> **Note**
> Some types cannot be checked by Standard rules. The **Select File Types** window for Standard rules shows these types in the lower pane. You can check for these types in Quota or Content Analysis rules.

4. Click **OK** to accept changes and return to the parent Wizard. Click **Cancel** to revert to the saved information.

Except where the file type is

This Condition allows you to apply Rules to all files that are not of specific file types. *Before using this condition in Standard Rules*, see the note to "Where the file type is" on page 112.

- In Standard rules, this Condition only checks the top level file that was directly requested.
- In Standard rules applied to uploads, this condition checks the type of files directly uploaded (attached to the upload form).
- In Content Analysis rules, this Condition checks the top level file and each file unpacked from archive files.
- For more file type matching options, see the Conditions Condition *Where the file is or contains a file of type* and *Where the parent file type is.*

To choose file types to exclude, within the Rule Wizard click Type to open the Select File Types window. See the condition **Where the file type is** for details on how to select types.

Where the file is or contains a file of type

This Condition allows you to create Content Analysis Rules that check a condition for a file that was requested, or all files that are contained within it (if it is a document or archive that WebMarshal can unpack). For instance, you can apply a rule to document files that contain images. For other options, see the condition *Where the parent file type is.*

To choose file types to match, within the Rule Wizard click Type to open the Select File Types window. See the condition **Where the file type is** for details on how to select types.

You can choose to include or exclude the originally requested file from matching.

To choose an option:

1. Click **is or contains** to open the Trigger window. Choose from the following
   - *The transferred file or any unpacked file:* If you choose this option, the condition will consider the type of the originally requested file, and any files unpacked from it.
   - *Any unpacked file:* If you choose this option, the condition will ONLY consider the type of unpacked files, and will not consider the type of the originally requested file.

Select an option, and then click **OK** to return to the parent Wizard.

Tips

- For example, if you want to make a rule that applies to all image files, including image files within documents or archives, select *The transferred file or any unpacked file*. If you want to make a rule that applies to image files within documents or archives, but NOT directly requested images, select *Any unpacked file*.
- If you combine this condition with other conditions, such as a file name condition, the other conditions are evaluated on the main file and NOT on contained files.

Where the parent file type is

This Condition allows you to create Content Analysis Rules that apply to a file that was unpacked from an archive or other unpackable type, depending on the type of the parent file.

Note

For other file type conditions, see *Where the file is or contains a file of type, Where the file type is,* and *Except where the file type is.*

To choose file types to match, within the Rule Wizard click Type to open the Select File Types window. See the condition **Where the file type is** for details on how to select types.

You can choose to perform matching on the originally requested file, all unpacked files, or only the immediate parent container.

Tips

- You can use this condition in combination with other conditions that apply to the unpacked file. For instance, you can apply a rule where the *parent file type* is ZIP and the *file type* is DOC.
- If you combine this condition with other conditions, such as a file name condition, the other conditions are evaluated on the child file and NOT on any parent files.

To choose an option:

1. Click **the immediate** to open the Checks window. Choose from the following
   - *The immediate parent file:* If you choose this option, the condition will consider the type of the file that explicitly contains the unpacked file.
   - *The top-level parent file:* If you choose this option, the condition will consider the type of the originally requested file (that contains the unpacked file, perhaps within other archives).
   - *Any parent file:* If you choose this option, the condition will consider the type of each file in the set of archives.
2. Select an option, and then click **OK** to return to the parent Wizard.

Tip

Suppose you click a link to `archive1.zip. archive1.zip` contains `archive2.cab`, and `archive2.cab` contains `data.txt`

`archive1.zip>>archive2.cab>>data.txt`

- `archive1.zip` is the top level parent.
- `archive1.zip` is the immediate parent of `archive2.cab`.
- Both `archive1.zip` and `archive2.cab` are the any level parents of `data.txt`.

Except where the parent file type is

This Condition allows you to apply Rules to a file that was unpacked from an archive, if the parent files in the archive are **not** of specific file types.

To choose file types to match, within the Rule Wizard click Type to open the Select File Types window. See the condition **Where the file type is** for details on how to select types.

You can choose to perform matching on the originally requested file, all unpacked files, or only the immediate parent container. To choose a matching option, click **the immediate** to open the Checks window. See the condition **Where the parent file type is** for details of the options on this window.

Where the file name matches

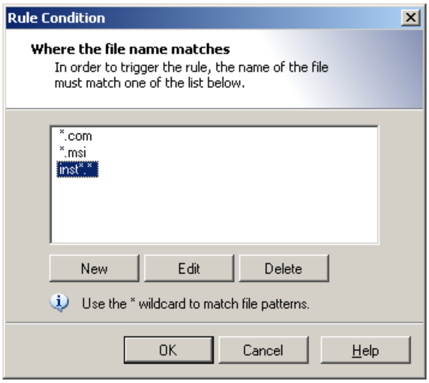
This Condition allows you to apply Rules to files with specific names or extensions. This condition is useful to allow specific files, or to block text files that WebMarshal cannot recognize by their structure or content-type header.

Note

You can match files in two other ways:

- The condition *Where the content type is* allows for file matching by the type declared in the web request headers.
- The condition *Where the file type is* allows for file matching by internal structure of files.

To choose file types, within the Rule Wizard click **Name** to open the Enter File Names window.



Rule Condition

Where the file name matches

In order to trigger the rule, the name of the file must match one of the list below.

*.com
*.msi
inst*.*

Use the * wildcard to match file patterns.

The * wildcard is supported (* matches any number of characters; for instance, *.exe matches any exe file).

1. To add a name to the list, click **Add**, and then enter the desired name or wildcard string to match partial names. Press Enter or click away from the name when done.
2. To edit an existing name, select it and then click **Edit**.
3. To delete an existing name, select it and then click **Delete**.
4. Click **OK** to accept changes and return to the parent Wizard. Click **Cancel** to revert to the saved information.

Except where the file name matches

This Condition allows you to apply Rules to all files that are not specific file names.

To choose file names to exclude within the Rule Wizard click **Name** to open the Except where the file name matches window.

The * wildcard is supported (* matches any number of characters; for instance, *.exe matches any exe file).

1. To add a name to the list, click **Add**, and then enter the desired name or wildcard string to match partial names. Press Enter or click away from the name when done.
2. To edit an existing name, select it and then click **Edit**.
3. To delete an existing name, select it and then click **Delete**.

Click **OK** to accept changes and return to the parent Wizard. Click **Cancel** to revert to the saved information.

Where the parent file name matches

This Condition allows you to apply Rules to a file that was unpacked from an archive or other unpackable type, depending on the name of the parent file.

Note
For other file type conditions, see *Where the file is or contains a file of type, Where the file type is,* and *Except where the file type is.*

To choose file names to match, within the Rule Wizard click **Name** to open the Select File Names window. See the condition **Where the file name matches** for details of this window.

You can choose to perform matching on the originally requested file, all unpacked files, or only the immediate parent container.

To choose an option:

1. Click **the immediate** to open the Checks window. Choose from the following

    - *The immediate parent file:* If you choose this option, the condition will consider the name of the file that explicitly contains the unpacked file.
    - *The top-level parent file:* If you choose this option, the condition will consider the name of the originally requested file (that contains the unpacked file, perhaps within other archives).
    - *Any parent file:* If you choose this option, the condition will consider the name of each file in the set of archives.

2. Select an option, and then click **OK** to return to the parent Wizard.

Example: Suppose you click a link to `archive1.zip. archive1.zip` contains `archive2.cab`, and `archive2.cab` contains `data.txt`

`archive1.zip>>archive2.cab>>data.txt`

- `archive1.zip` is the top level parent.
- `archive1.zip` is the immediate parent of `archive2.cab`.

Both `archive1.zip` and `archive2.cab` are the any level parents of `data.txt`.

Except where the parent file name matches

This Condition allows you to apply Rules to a file that was unpacked from an archive, if the parent files in the archive **do not** match specific names or extensions.

To choose file names to match, within the Rule Wizard click **Name** to open the File Names window. See the condition **Where the file name matches** for details of this window.

You can choose to perform matching on the originally requested file, all unpacked files, or only the immediate parent container. To choose a matching option, click **the immediate** to open the Checks window. See the condition **Where the parent file name matches** for details of the options on this window.

Where the download content type is

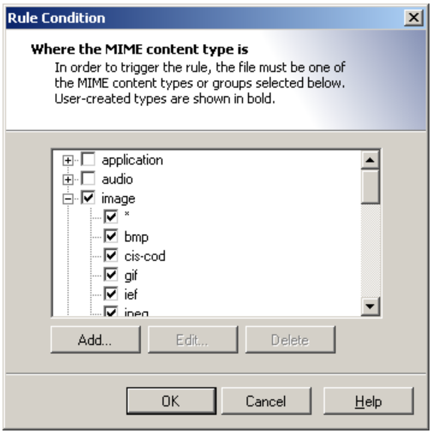
This Condition allows you to apply Rules to specific content types. Content types are recognized by the header information of the web request. Content type information is only available for downloads (not uploads or postings). The web browser uses the content type information to determine how to display the content, or what helper application to invoke. For instance, a PDF document with content type `application/pdf` usually opens in a PDF plug-in or reader.

Note

You can match files in two other ways:

- The Condition *Where the file name is* allows for file matching by name or extension.
- The condition *Where the file type is* allows for file matching by the internal structure of the file.

To choose content types, within the Rule Wizard click **Type** to open the **Select Content Types** window.



Rule Condition

Where the MIME content type is

In order to trigger the rule, the file must be one of the MIME content types or groups selected below. User-created types are shown in bold.

- □ application
- □ audio
- ☑ image
  - ☑ *
  - ☑ bmp
  - ☑ cis-cod
  - ☑ gif
  - ☑ ief
  - ☑ jpeg

1. Expand any category to see the particular types available.
2. Choose the categories or specific types of files to match.

3. To match a type not in the list, click **Add**. Enter the new type and optional subtype (for instance, `application/x-my-application`) and then click **OK**. The new type is permanently added to the list of types you can select.

Click **OK** to accept changes and return to the parent Wizard. Click Cancel to revert to the saved information.

Except where the download content type is

This Condition allows you to apply Rules to all files that are not of specific content types. Content type information is only available for downloads (not uploads or postings).

To choose content types to exclude, within the Rule Wizard click **Type** to open the Select Content Types window. See the condition *Where the content type is* for details on how to select types.

Where an error occurs while unpacking

This Condition allows you to check for archive and document files that WebMarshal cannot unpack. You may want to block files that cannot be unpacked, or notify the administrator.

To apply this condition, select the box.

Understanding Rule Actions

Each WebMarshal Rule includes one or more actions. Not all actions are available for all WebMarshal Rule types.

Rule Actions

The complete list of actions includes:

- Permit Access
- Permit Access after displaying Warning Page

- Permit access and inspect content
- Permit access and do not inspect content
- Block the connection and return a 503 service unavailable return code.
- Block Access and display blocked page
- Display Warning page once per period and continue processing rules
- Strip cookies from this site
- Classify the domain as classification
- Classify the file as classification
- Add the User to User Group
- Add the URL to a Category
- Send a notification to the administrator
- Exclude the request from reporting (do not log browsing)
- Apply Quota to the user
- Stop processing quota rules.
- Skip any remaining rules in this container

Permit access

The web page, download, or upload is delivered.

Permit access after displaying warning page

WebMarshal displays a Notification Page in the user's browser. The page asks the user to accept a note or warning. If the user accepts, the original web page, download, or upload will be delivered.

Click **Warning Page** to open the Select Web Page window.

1. Select a web page to display from the list
2. Click **OK** to return to the parent Wizard.

You can create custom notification pages. See “Notifying Users with Notification Pages” on page 185.

Permit access and inspect content

This condition is available in HTTPS rules. When this action applies, WebMarshal continues processing the web page, download, or upload. Quota, Standard, and Content Analysis rules are evaluated.

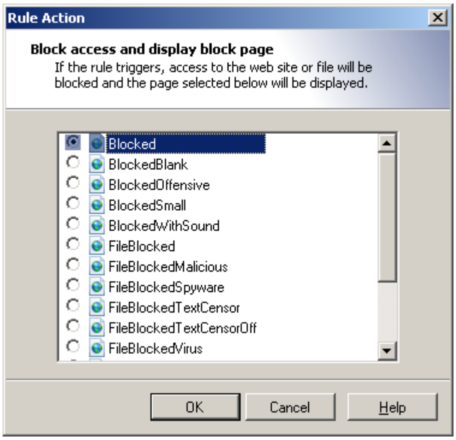
Permit access and do not inspect content

This condition is available in HTTPS rules. When this action applies, WebMarshal delivers the web page, download, or upload. Quota, Standard and Content Analysis rules are not applied.

Block Access and display blocked page

The web page, download, or upload is not delivered. A WebMarshal Notification Page is shown instead.

Click **Blocked Page** to open the Select Web Page window.



Rule Action

Block access and display block page

If the rule triggers, access to the web site or file will be blocked and the page selected below will be displayed.

● Blocked
○ BlockedBlank
○ BlockedOffensive
○ BlockedSmall
○ BlockedWithSound
○ FileBlocked
○ FileBlockedMalicious
○ FileBlockedSpyware
○ FileBlockedTextCensor
○ FileBlockedTextCensorOff
○ FileBlockedVirus

1. Select a web page to display from the list
2. Click **OK** to return to the parent Wizard.

For rules with a malware scanning action, you can choose a second notification page used for aborted downloads. This page is only shown if WebMarshal begins to "trickle" the download and then stops it due to a scanner result condition. The "aborted" page is shown the next time the user makes a web request. **To choose the page that will be shown,** in the rule description (lower pane) click **File Aborted Page** and select a web page to show for aborted downloads, using the Select Web Page window as above.

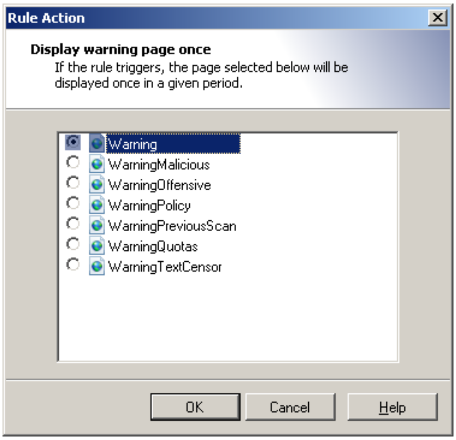
Block the connection and return a 503 service unavailable return code

When this action is selected, WebMarshal will return a 503 Service Unavailable HTTP response, and the web request will be terminated. This action is available in Connection Rules. Typically it would be used if you do not want to allow an Instant Messaging or Streaming Media application to connect through WebMarshal.

Display warning page once per period and continue processing rules

If this rule has not been triggered for this user during the time configured, a WebMarshal Notification Page is displayed in the user's browser.

Click **Warning Page** to open the Select Web Page window.



Rule Action

Display warning page once

If the rule triggers, the page selected below will be displayed once in a given period.

● Warning
○ WarningMalicious
○ WarningOffensive
○ WarningPolicy
○ WarningPreviousScan
○ WarningQuotas
○ WarningTextCensor

1. Select a web page to display from the list.
2. Select the period during which this Rule action will not display the page again. Available periods include the current browsing session, day, week, or month.
3. Click **OK** to return to the parent Wizard.

The user will be asked to accept a note or warning. If the user accepts, the original web page, download, or upload will be delivered to the user. After the user accepts, this action will not display this warning page again for the period selected.

Strip cookies from this site

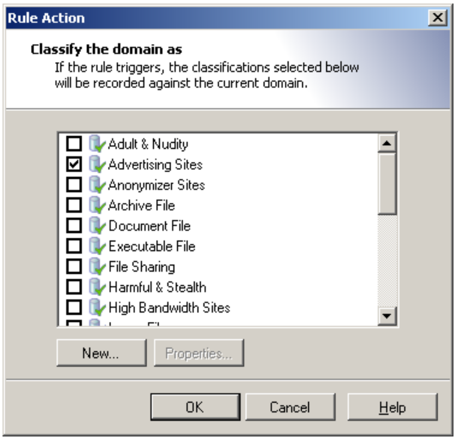
HTTP cookies returned with the response are removed.

Note
This action is only effective for responses (setting of cookies by server-side action). WebMarshal does not currently block cookies sent with a request. WebMarshal cannot block cookies set on the client by Javascript or other client side action.

Classify the domain as classification

A Domain Classification is logged in the WebMarshal database (if database logging is enabled). This record shows that the user browsed to a URL which met the Rule conditions. For instance the URL could be in a specific category, or it could be a page with content matching a TextCensor script.

Select one or more Domain classifications for this request by checking the boxes in the Select Logging Classification window.



Classify the domain as

If the rule triggers, the classifications selected below will be recorded against the current domain.

- ☐ Adult & Nudity
- ☑ Advertising Sites
- ☐ Anonymizer Sites
- ☐ Archive File
- ☐ Document File
- ☐ Executable File
- ☐ File Sharing
- ☐ Harmful & Stealth
- ☐ High Bandwidth Sites

To create a new classification, click **New**. To review and edit an existing classification, click **Properties**.

For more information about adding and editing classifications, see “Logging Activity with Classifications” on page 182.

Classify the file as classification

A File Classification is logged in the WebMarshal database (if database logging is enabled). This record shows that the user uploaded or downloaded a file which met the Rule conditions. For instance the file could be large or could contain a virus. A file classification applies to a specific upload or download request.

Select one or more File Classifications for this request by checking the boxes in the Select Logging Classification window.

To create a new classification, click **New**. To review and edit an existing classification, click **Properties**.

For more information about adding and editing classifications, see “Logging Activity with Classifications” on page 182.

Add the user to a user group

The user who triggered a Rule is added into one or more WebMarshal User Groups.

Select an existing WebMarshal User Group or new WebMarshal User Group using the Select User Groups window.

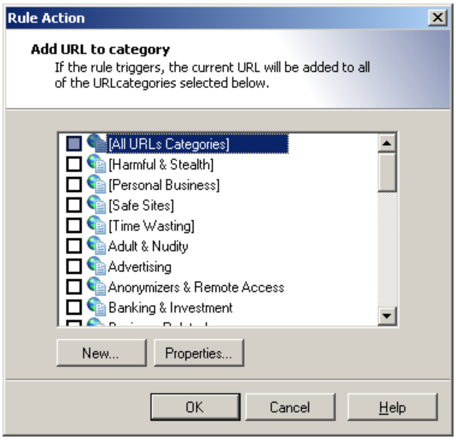
Note
You can use this action to place users who attempt to access banned sites into a “watch” group.

To create a new group, click **New**. To review and edit an existing group, click **Properties**. See “User Management” on page 138 for more information on User Groups.

Add the URL to a category

The URL domain or path of a request is added to a WebMarshal URL category. For instance, if a URL triggered an offensive language TextCensor script, you may want to add the URL to a permanent block list.

1. Click **Category** to open the Select URL Categories window.



Rule Action

Add URL to category

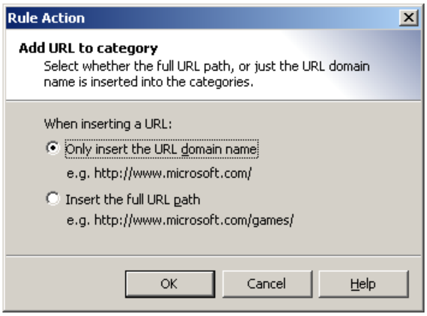
If the rule triggers, the current URL will be added to all of the URLcategories selected below.

- □ [All URLs Categories]
- □ [Harmful & Stealth]
- □ [Personal Business]
- □ [Safe Sites]
- □ [Time Wasting]
- □ Adult & Nudity
- □ Advertising
- □ Anonymizers & Remote Access
- □ Banking & Investment

2. Choose one or more categories into which this site should be placed by checking the boxes.

3. To create a new category, click **New**. To review and edit an existing category, click **Properties**. See “Understanding URL Categories” on page 151 for more information on URL categories.

4. Click **URL** to choose whether to add the entire domain, or only the subdomain (path) to the category.



Rule Action

Add URL to category

Select whether the full URL path, or just the URL domain name is inserted into the categories.

When inserting a URL:

● Only insert the URL domain name
e.g. http://www.microsoft.com/

○ Insert the full URL path
e.g. http://www.microsoft.com/games/

Send a notification to the administrator

A notification email is sent to the administrator email address as configured on the General page of Server Properties.

Note
You should be selective in applying this action. If you apply it for content block actions, the administrator will receive a large number of email messages.

Exclude the request from reporting

Any request that matches the rule conditions is completely exempted from logging (including aggregate browsing time and bandwidth records).

For instance, you can use this action:

- With a User Matching condition to allow unmonitored Web access for the corporate executive group
- With a URL Category condition to allow unmonitored access for all users to a company extranet site.

Notes

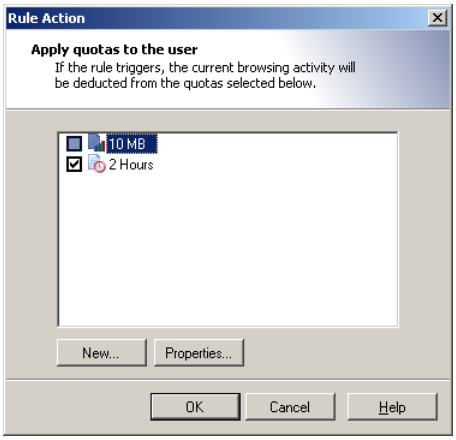
A typical site visit includes requests for many files of many different types. Therefore, if you use this action with content analysis or file type rule conditions, it is likely that traces of user activity will be logged. Also, where HTTPS content is not processed by Content Analysis rules an exclusion might not apply.

To completely exclude a site visit from logging, Marshal8e6 recommends you use this action in a Standard rule with User Matching or URL conditions.

This action functions differently from the "exclude the site from reporting" action in earlier versions of WebMarshal.

Apply quota to user

A time or volume browsing quota is applied to the user. Select one or more quotas from the Apply Quotas to User window.



Rule Action

Apply quotas to the user

If the rule triggers, the current browsing activity will be deducted from the quotas selected below.

□ 10 MB
☑ 2 Hours

To create a new quota, in the window click **New** to start the Quota Wizard. To review and edit an existing quota, click **Properties**. For more information on Quotas and the New Quota Wizard, see "Configuring Access Using Quotas" on page 162.

Stop processing quota rules

Any Quota rules that would be evaluated after this rule are not evaluated. The intended user of this action is to avoid charging a browsing action against more than one quota.

Skip any remaining rules in this container

Any additional rules in the container (or in sub-containers) are not evaluated. This action allows conditional checking of groups of rules.

Understanding the Order of Evaluation

WebMarshal evaluates Connection Rules first, then HTTPS Rules, Quota Rules, Standard Rules, and finally Content Analysis Rules. Within each type, rules are evaluated in a defined order, which you can configure.

The order of evaluation can affect the outcome, because WebMarshal bases its action on the first rule triggered. For instance, the default WebMarshal rules block the virus scanner test file `eicar.com` using the rule *Block Dangerous File Extensions*. Since this rule is applied before the malware scanning rules, `eicar.com` is not reported as containing malware.

Rules are evaluated in "top down" order as presented in the console display.

To change the order of evaluation of rules:

1. Ensure that Rules is expanded.
2. Select a rule type in the left pane.
3. Select a particular rule or rule container in the right pane.

4. Move the item up or down in the evaluation order using the up and down arrow icons in the tool bar.

5. Commit configuration to apply the changes.

Testing Access Policy

Testing rules involves entering various combinations of User, URL, and File Type or text, and viewing the results. Because the results of rule evaluation are dependent on the order of evaluation, **all applicable rules are evaluated each time a test is performed**.

To test rules:

1. In the WebMarshal Console, click the **Test Policy** icon in the tool bar to open the **Test Access Policy** window.

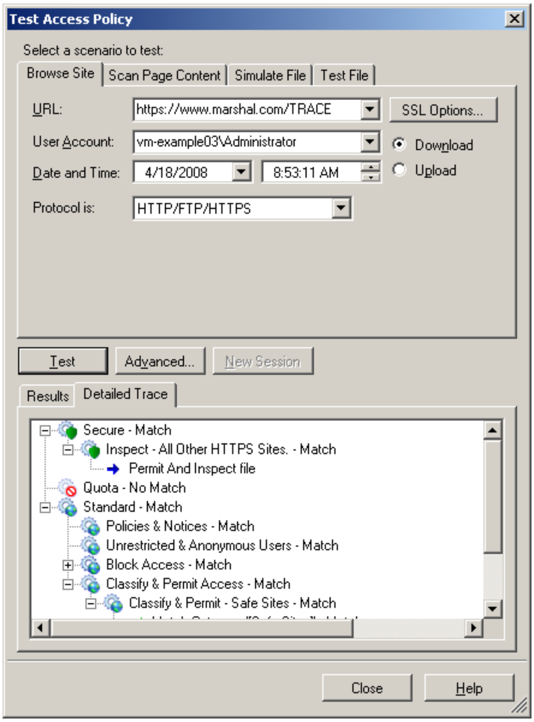
   Note
   For a more complete description of all test options and results, see Help for this window.

2. Select the test to perform using the tabs. Tests include:
   - **Browse Site** (Checks the protocol and URL)
   - **Scan Page Content** (Includes the Browse Site test as well as TextCensor)
   - **Simulate File** (Includes the Browse Site test as well as file type and content type)
   - **Test File** (Includes all rules)

3. Enter the URL and the user account you want to use for the test.

4. Enter a date and time you want to use for schedule dependent rules.

5. Choose whether to test download or upload processing.



URL: https://www.marshal.com/TRACE

User Account: vm-example03\Administrator

Date and Time: 4/18/2008 8:53:11 AM

Protocol is: HTTP/FTP/HTTPS

● Download

○ Upload

```
⊟ Secure - Match
   ⊟ Inspect - All Other HTTPS Sites. - Match
        → Permit And Inspect file
   Quota - No Match
⊟ Standard - Match
     Policies & Notices - Match
     Unrestricted & Anonymous Users - Match
   ⊞ Block Access - Match
   ⊟ Classify & Permit Access - Match
      ⊟ Classify & Permit - Safe Sites - Match
```

6. For the Scan Page Content tab, which applies TextCensor scripts to text and HTML documents, enter text in the box.

   You can enter text by typing directly, by cut-and-paste, or from a web page you are viewing in Internet Explorer (by clicking **Grab**).

7. For the Simulate File tab, you can select a number of features to simulate including the file type, MIME content type, file size, and presence of malware and cookies.

8. For the Test File tab, you can enter the path to a local file you want to use for the test.

9. Click **Advanced** for additional testing options.

10. Click **Test** to begin rule testing. The result of the evaluation is displayed in the Test Results pane.

11. Standard rules are evaluated first. If the result of Standard rule evaluation is “permit with warning page”, click **Accept Result and Reprocess Rules** (at bottom of the results) to proceed to the evaluation of Content rules. If the result of Standard rule evaluation is “deny” then Content rules are not tested.

12. Quota Rules that would be applied and Classifications that would be logged are indicated at the bottom of the results pane.

13. To view details of the rule evaluation (such as the TextCensor script results), select the Detailed Trace tab and expand the evaluation tree.

Chapter 7

Understanding Policy Elements

Policy elements are building blocks you can use when you create WebMarshal policy groups and rules. These elements help you to specify complex rule conditions and rule actions.

Some examples of each type of element are provided by default when you install WebMarshal with the default configuration. These examples are used in the default access policy.

You can edit the existing elements or create new ones to support your policy requirements.

WebMarshal provides the following types of elements:

Connectors

Allow you to import user and group information from Windows and Novell Directory. For more information, see "User Management" on page 138.

User Groups

Allow you to apply policy based on user accounts or workstation IP addresses. For more information, see "User Groups" on page 143.

URL Categories

Allow you to apply policy based on requested URLs. Categories can include manually entered URLs as well as information obtained from external filtering lists. For more information, see "Understanding URL Categories" on page 151.

URL Filtering Lists

Allow you to configure external lists sources for URL categories, including text based imports, DNS Blacklists, the Marshal Filtering List, Marshal8e6Filter List and Secure Computing SmartFilter. For more information, see "Configuring URL Filtering Lists" on page 156.

Schedules

Allow you to apply policy based on the time of day and day of the week. For more information, see "Configuring Access Using Schedules" on page 159.

TextCensor Scripts

Allow you to apply policy based on the text content of uploads and downloads. For more information, see "Identifying Web Content Using TextCensor Scripts" on page 169.

Classifications

Allow you to classify files and requests based on rule criteria. For more information, see "Logging Activity with Classifications" on page 182.

Quotas

Allow you to limit browsing activity by time and bandwidth. For more information, see "Configuring Access Using Quotas" on page 162.

Malware Protection

Allows you to check downloads and uploads for viruses, spyware, and other malicious content using third party Virus scanners and Spyware Scanners. For more information, see "Scanning Overview" on page 178.

User Management

The User Management functions allow you to import and organize user account information. This information is used to control and record browsing access.

Configuring Connectors

The Connectors item in the Console shows all installed directory connectors. Directory connectors allow WebMarshal to import user accounts, and to authenticate browser requests by pre-existing user logon.

You can install connectors for Active Directory, legacy Windows NT, and Novell (NDS). You can only have one connector of each type at a time.

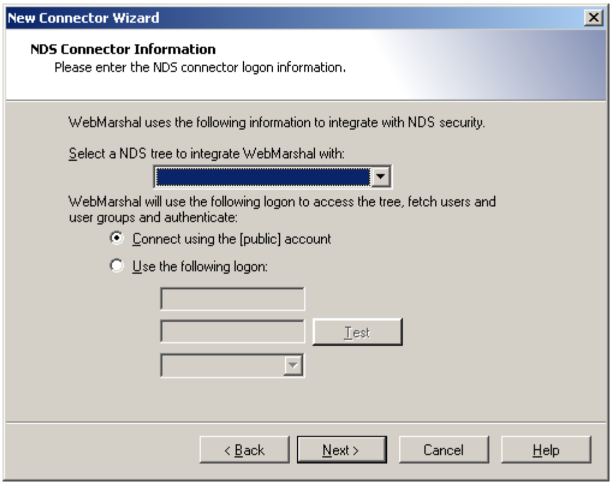
Notes

- Active Directory is the preferred connector for importing Windows user information.
- Before installing the NDS connector, you must install NDS client software on the WebMarshal server computer.
- NDS users are authenticated through Basic authentication. ***If you are using both NDS and Windows integrated authentication (NTLM),*** Marshal8e6 recommends that you configure separate ports for the two authentication types. For more information, see “Configuring Proxy Settings” on page 221 and “Proxy Ports and Authentication” on page 42.

Installing a new connector

1. In the left pane tree of the Console, highlight the **Connectors** item.
2. Click the **New Connector** icon in the tool bar to start the New Connector Wizard.
3. Select the type of connector.

4. ***If you selected a NDS connector,*** on the Novell NDS Settings page of the Wizard, enter or select a NDS Tree from which to import information. Choose whether you want to use the `[public]` account or a specific user account.



New Connector Wizard

NDS Connector Information

Please enter the NDS connector logon information.

WebMarshal uses the following information to integrate with NDS security.

Select a NDS tree to integrate WebMarshal with:

WebMarshal will use the following logon to access the tree, fetch users and user groups and authenticate:

● Connect using the [public] account

○ Use the following logon:

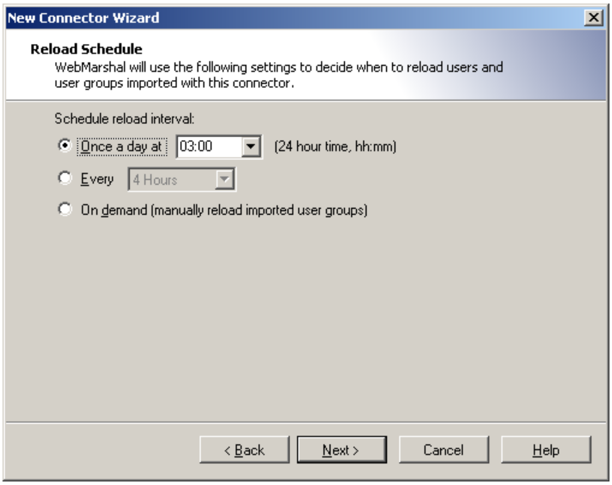
5. ***If you selected a NT connector,*** choose whether you want to connect using the default (LocalSystem) account or a user account.

6. ***If you selected an Active Directory connector,*** choose whether you want to connect anonymously or using a specific account.

7. Enter the account information if required. Click **Test** to verify the credentials.

8. Click **Next** to continue.

9. On the Reload Schedule page, select a schedule of times when WebMarshal will query this directory for updated user and group information. You can choose a periodic schedule (daily, or in hours or minutes), or manual update. If you select manual update, you can reload the Groups by right-clicking **User Groups** and selecting **Reload**, or by clicking **Reload Now** on the individual group properties window.



New Connector Wizard

Reload Schedule

WebMarshal will use the following settings to decide when to reload users and user groups imported with this connector.

Schedule reload interval:

● Once a day at 03:00 (24 hour time, hh:mm)

○ Every 4 Hours

○ On demand (manually reload imported user groups)

10. Click **Next** to continue.

11. On the **Completing** page, review the information entered. Choose whether to open the New User Group wizard on finish. In order to import any users or groups through this Connector, you must use the New User Group wizard.

Deleting a connector

To delete a connector, right click an existing Connector and then click **Delete** to delete it. Groups and users previously imported through the Connector are not deleted. This allows for import of directory information from different directories (for example, multiple NDS directories).

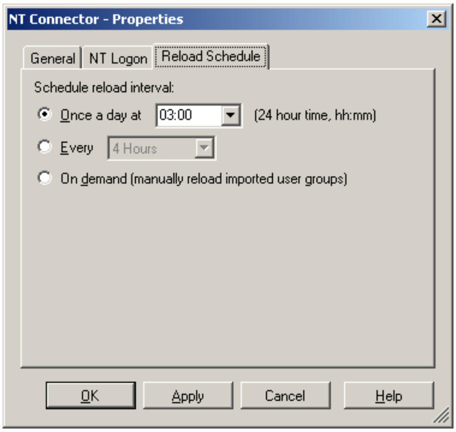
Editing a connector

To edit the properties of an existing connector, double-click it to open the Connector Properties window. This window allows you to view and change the login and reload interval for a directory connector.

1. On the Logon tab, select the account to use for access to the directory.

   - **For NT (Microsoft) directories**, the default option is the Local System account. You can select a specific domain, user name, and password if necessary.
   - **For Active Directory,** the default option is anonymous access. You can select a specific domain, user name, and password if necessary.
   - **For Novell NDS directories,** the default option is the [public] account. You can enter a specific context, user name, and password if necessary. Available contexts are shown in the menu.

2. On the Reload Schedule tab, select the schedule of times when WebMarshal will query this directory for updated user and group information. You can specify a daily update, or a schedule in hours or minutes. You can also choose to update manually.



NT Connector - Properties

Schedule reload interval:

● Once a day at 03:00 (24 hour time, hh:mm)

○ Every 4 Hours

○ On demand (manually reload imported user groups)

3. If you select manual update, you can reload all Groups by right clicking the User Groups item and selecting **Reload**. You can reload an individual Group by clicking **Reload Now** in the Group Properties window.

4. Click **OK** or **Apply** to change the settings.

User Groups

All users

Select this element to view a complete list of user names in all groups that have been imported into WebMarshal. This list is empty until at least one group has been imported (or, in the case of IP range entries, a computer in the range has browsed through WebMarshal).

Note
By default WebMarshal retains all previously imported user names on this list, even if they are not currently members of any user group visible within WebMarshal. To purge unused names, right-click **All Users** and select **Purge Unreferenced Users**.

User properties

To view additional details about a user, double-click to open the User Properties window.

- The **General** tab shows the name, description, source, and full distinguished name information for a user. You can edit the description.
- The **Rules** tab shows all rules that apply to this user. Highlight a rule and click **Jump to Rule** to view the details of that rule.
- The **Quotas** tab shows a list of quotas that apply to the user. To extend a quota for the user, click **Extend Quotas.** For more information about extending quotas, see “Editing a Quota” on page 164.

User groups

WebMarshal supports five types of User Groups. Each displays in the Console with a unique icon.

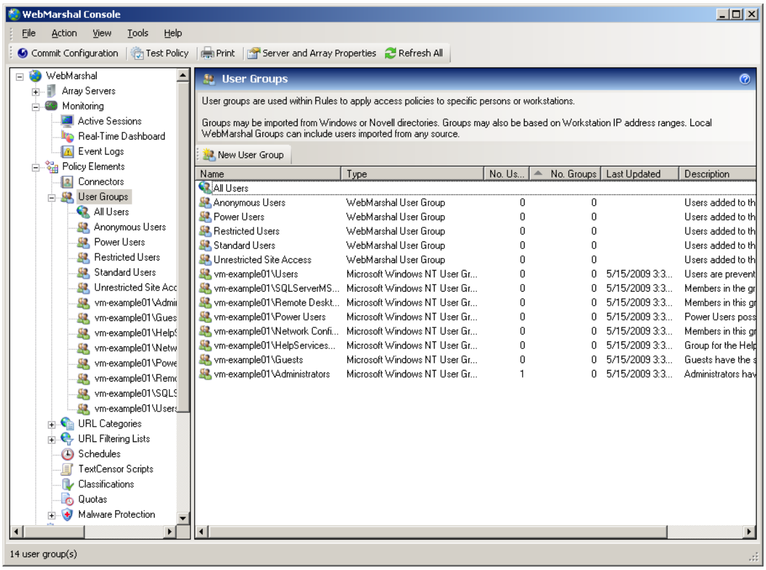
- **WebMarshal** user groups (blue and green shirts).
- **Microsoft (NT)** user groups (green shirts).

> **Note**
>
> WebMarshal supports both Global and Local NT user groups.
>
> - **Global** user groups are created on a Windows Domain Controller or Active Directory server.
> - **Local** user groups are created on domain controllers or standard workstations, and can contain users from any domain. They can also contain global user groups. Local user groups cannot contain other local groups.

- **Active Directory** user groups (blue shirts).
- **Novell NDS** user groups (red shirts).
- WebMarshal **IP address range** groups (users with workstation).

Typically, WebMarshal user groups include users that have similar Web access requirements. WebMarshal groups can include other groups, single users, and computer groups. The default configuration that you can import when you install WebMarshal includes several user groups. To use the default groups, import groups from connectors, or create computer groups, and then insert these new groups into the default groups.

To view the list of users and groups contained in a group, select that group in the left pane menu tree.



User groups are used within Rules to apply access policies to specific persons or workstations.

Groups may be imported from Windows or Novell directories. Groups may also be based on Workstation IP address ranges. Local WebMarshal Groups can include users imported from any source.

Name	Type	No. Us...	No. Groups	Last Updated	Description
All Users					
Anonymous Users	WebMarshal User Group	0	0		Users added to th
Power Users	WebMarshal User Group	0	0		Users added to th
Restricted Users	WebMarshal User Group	0	0		Users added to th
Standard Users	WebMarshal User Group	0	0		Users added to th
Unrestricted Site Access	WebMarshal User Group	0	0		Users added to th
vm-example01\Users	Microsoft Windows NT User Gr...	0	0	5/15/2009 3:3...	Users are prevent
vm-example01\SQLServerMS...	Microsoft Windows NT User Gr...	0	0	5/15/2009 3:3...	Members in the gr
vm-example01\Remote Deskt...	Microsoft Windows NT User Gr...	0	0	5/15/2009 3:3...	Members in this gr
vm-example01\Power Users	Microsoft Windows NT User Gr...	0	0	5/15/2009 3:3...	Power Users poss
vm-example01\Network Confi...	Microsoft Windows NT User Gr...	0	0	5/15/2009 3:3...	Members in this gr
vm-example01\HelpServices...	Microsoft Windows NT User Gr...	0	0	5/15/2009 3:3...	Group for the Help
vm-example01\Guests	Microsoft Windows NT User Gr...	0	0	5/15/2009 3:3...	Guests have the s
vm-example01\Administrators	Microsoft Windows NT User Gr...	1	0	5/15/2009 3:3...	Administrators hav

14 user group(s)

To edit the group description, and/or to reload the group (for Windows and NDS directory groups), right-click the group and click **Properties**.

For network security, groups imported through connectors are read-only and cannot be edited using the WebMarshal Console. These groups are synchronized with the parent directory on the schedule you specify in the Connector properties for the appropriate directory type (by default, once a day).

Adding a user group

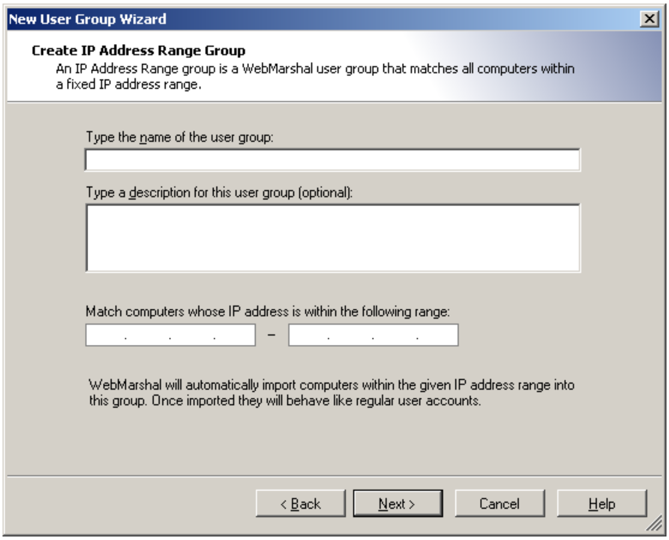
1. Ensure that **User Groups** is selected. Click the **New User Group** icon in the tool bar.

2. Select the type of group to create or import:

   - WebMarshal User Group
   - IP Address Range Group
   - Group imported from a connector

3. **WebMarshal User Group:** Enter a name and optionally a description. This type of group is internal to WebMarshal. You can use WebMarshal groups to apply rules to multiple groups and users.

4. **IP Address Range Group:** Enter a name and optionally a description.



Create IP Address Range Group

An IP Address Range group is a WebMarshal user group that matches all computers within a fixed IP address range.

Type the name of the user group:

Type a description for this user group (optional):

Match computers whose IP address is within the following range:

WebMarshal will automatically import computers within the given IP address range into this group. Once imported they will behave like regular user accounts.

Enter a starting and ending IP address for the range. Any user or process on a computer with an IP address in the specified range can browse through WebMarshal, subject to any Rules applied to the group.

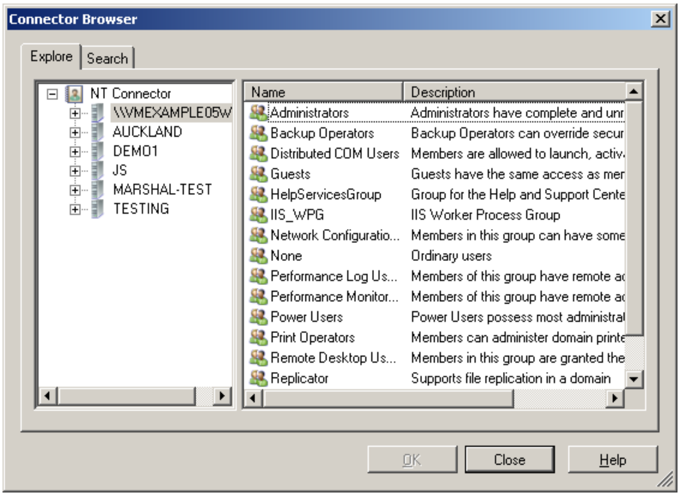
Note

WebMarshal adds the name or IP address of each computer in this range to the **All Users** list the first time that computer connects to WebMarshal. Once the computer names are included in the list, you can use them individually within Rules in the same way as any other User.

- If you want to add a specific computer to a WebMarshal User Group explicitly (when it is not included in **All Users**), see “Adding computers or IP addresses to a user group” on page 150.

IP authentication works much better if DNS is configured to support reverse DNS lookups. Reverse DNS allows WebMarshal to get a name for an IP address. If that returned name matches the NetBIOS name, WebMarshal can query the computer for its description.

5. **Import Group(s) from a Connector:** Enter the names of the groups you want to import into WebMarshal. You can use imported groups, and individual users, in WebMarshal user groups or rules.



NT Connector
- \\VMEXAMPLE05W
- AUCKLAND
- DEMO1
- JS
- MARSHAL-TEST
- TESTING

Name	Description
Administrators	Administrators have complete and unr
Backup Operators	Backup Operators can override secur
Distributed COM Users	Members are allowed to launch, activ.
Guests	Guests have the same access as mer
HelpServicesGroup	Group for the Help and Support Cente
IIS_WPG	IIS Worker Process Group
Network Configuratio...	Members in this group can have some
None	Ordinary users
Performance Log Us...	Members of this group have remote ac
Performance Monitor...	Members of this group have remote ac
Power Users	Power Users possess most administral
Print Operators	Members can administer domain printe
Remote Desktop Us...	Members in this group are granted the
Replicator	Supports file replication in a domain

To locate groups within the directory environment (NT, Active Directory, or NDS), click **Browse**. On the Explore tab of the Connector Browser window, in the left pane expand the tree and then select a domain or computer from which to import groups. Select the desired groups from the right pane and then click **OK.** Use ctrl-click and shift-click to multi-select. If a unit larger than a single Group is selected, WebMarshal imports users from all Groups in the unit.

You can also search for groups using the Search tab of the Connector Browser window.

For NT groups, names you type must be in `domain\usergroup` format. Enter multiple names separated by semi-colons. For Active Directory and NDS, names you type must be fully distinguished names.

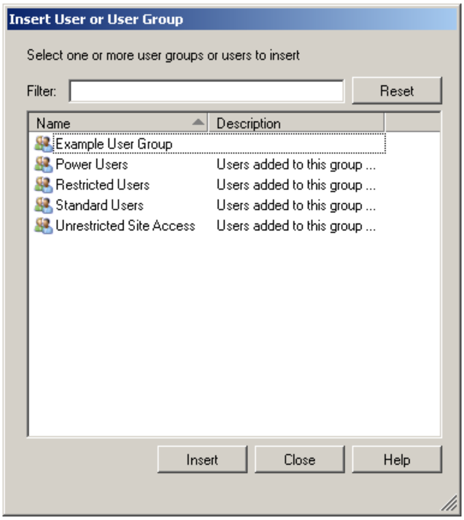
Tip
WebMarshal can import groups from trusted Active Directory domains, subdomains, and other domains that have an explicit two way trust relationship with the domain that WebMarshal is a member of. For additional details see Marshal8e6 Knowledge Base article Q11870.

6. For any type of user group, click **Next**, then **Finish**, to add the User Group.

Adding members to a WebMarshal user group

1. Ensure that **User Groups** is selected.
2. Select the name of a WebMarshal User Group in the left pane to view its members in the right pane.

3. Click the **Insert Users into this User Group** icon in the tool bar. If no users or imported groups are present, you have the option to import or create User Groups (see the procedure above).



Insert User or User Group

Select one or more user groups or users to insert

Filter:

Name	Description
Example User Group	
Power Users	Users added to this group ...
Restricted Users	Users added to this group ...
Standard Users	Users added to this group ...
Unrestricted Site Access	Users added to this group ...

4. Within the Insert Users and Groups window, select one or more users or groups with the mouse, or type the beginning of a name to select it.

5. Use the **Enter** key or click **Insert** to add the selected items into the Group.

WebMarshal also supports “drag and drop” for inclusion of members in a group. To use this feature, drag a group or user name or names (from either pane) over a group name in the left pane. Hold down the Ctrl key while dragging to copy the group or user name; otherwise it will be moved.

Adding computers or IP addresses to a user group

1. Ensure that User Groups is selected.
2. Select the name of a WebMarshal User Group in the left pane to view its members in the right pane.
3. Click the **Import Computers** icon to add a specific computer name or address to the Group. You can only add valid computer names from the local network. IP addresses are resolved to computer names if possible. You can add any well-formed IP address.

   Note
   WebMarshal attempts to resolve IP addresses to NetBIOS names. NetBIOS names are used to allow for dynamic allocation of IP addresses. You can enter fully-qualified domain names, but they might be rejected due to IP address duplication.

Changing user group properties

The User Group Properties window shows the source and reload status of a User Group. Use this window to:

- Edit the group description for WebMarshal and IP groups.
- Change the range of IP addresses included in an IP address group.

You can also click **Reload Now** to update the group membership, provided the group has an external source (Windows NT or NDS directory). Reload also updates the Status information with the result of the reload operation. To schedule automatic reloading of the group, edit the Connector properties.

Note
Reloading membership does not delete any users previously imported, even if they are no longer members of the group. To remove unused users, select **User Groups > All Users > Purge Unreferenced Users**.

Understanding URL Categories

URL categories are collections of related Web or FTP sites. You can use these lists in Rules to determine an action to take (such as permitting or blocking access, or warning the user).

Types of URL categories

WebMarshal supports two types of URL Categories.

- **WebMarshal URL Categories** are user-modifiable lists of URLs. This type of category may contain other WebMarshal Categories and may also contain imported Categories.
- **Imported categories** are populated with URL information supplied by an externally maintained Filtering List (for instance the Marshal8e6Filter List, WebMarshal's FileFilter, the MarshalFilter List, or a third party filtering solution such as Secure Computing SmartFilter). You cannot edit the contents of an imported category within WebMarshal.

You can use either type of Category in rule conditions.

WebMarshal creates several default Categories during initial configuration. You can also add or import categories at any time.

WebMarshal URL Categories

Several categories are provided by default. Some examples of WebMarshal URL Categories are:

- Offensive Content
- Business Partners
- News Sources
- Web-based Mail Servers
- Search Engines

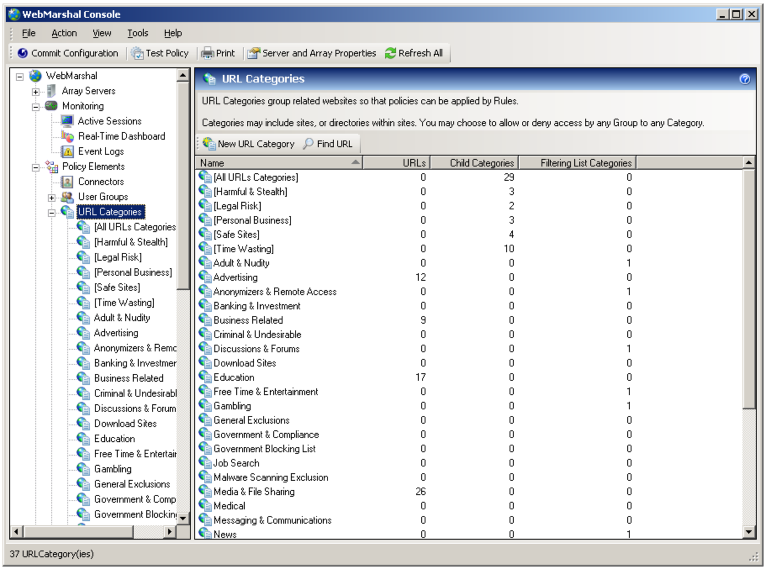
You can use text files to export or import URLs. WebMarshal TextCensor Rules can also add URLs to categories.

WebMarshal allows URLs to include an entire site or a particular sub-directory (path) at a site. The * wildcard character can be placed at the beginning or the end of a URL to match multiple similar sites.

Note

The path part of a HTTPS URL (for instance `https://example.com/folder/`) can only be evaluated if HTTPS content inspection is enabled. WebMarshal does not have access to the path information for uninspected HTTPS connections.

Expand a Category and double-click any URL to see a report of the WebMarshal Rule actions which placed it in that Category. (No information is available if the URL was added manually.)



URL Categories group related websites so that policies can be applied by Rules.

Categories may include sites, or directories within sites. You may choose to allow or deny access by any Group to any Category.

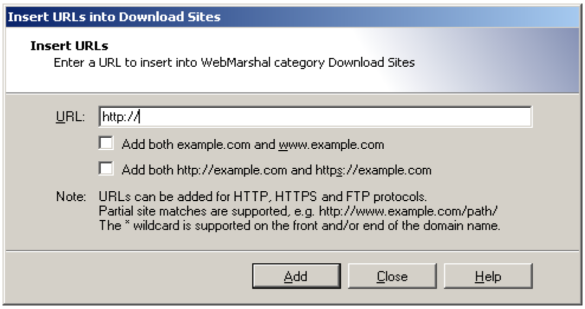
Name	URLs	Child Categories	Filtering List Categories
[All URLs Categories]	0	29	0
[Harmful & Stealth]	0	3	0
[Legal Risk]	0	2	0
[Personal Business]	0	3	0
[Safe Sites]	0	4	0
[Time Wasting]	0	10	0
Adult & Nudity	0	0	1
Advertising	12	0	0
Anonymizers & Remote Access	0	0	1
Banking & Investment	0	0	0
Business Related	9	0	0
Criminal & Undesirable	0	0	0
Discussions & Forums	0	0	1
Download Sites	0	0	0
Education	17	0	0
Free Time & Entertainment	0	0	1
Gambling	0	0	1
General Exclusions	0	0	0
Government & Compliance	0	0	0
Government Blocking List	0	0	0
Job Search	0	0	0
Malware Scanning Exclusion	0	0	0
Media & File Sharing	26	0	0
Medical	0	0	0
Messaging & Communications	0	0	0
News	0	0	1

Adding a URL Category

1. Select **URL Categories** in the left pane.
2. Click the **New Category** icon in the tool bar.
3. Enter the name for the new category. Optionally enter a description.
4. On the final page of the Wizard, click **Finish** to create the Category.

Adding URLs to a URL Category

1. Select **URL Categories** in the left pane.
2. Select the name of a URL category in the left pane to view its members in the right pane.
3. Click the **Add URLs** icon in the tool bar to open the Insert URLs window.



Insert URLs into Download Sites

Insert URLs

Enter a URL to insert into WebMarshal category Download Sites

URL: http://

□ Add both example.com and www.example.com

□ Add both http://example.com and https://example.com

Note: URLs can be added for HTTP, HTTPS and FTP protocols.
Partial site matches are supported, e.g. http://www.example.com/path/
The * wildcard is supported on the front and/or end of the domain name.

4. To add a new URL to this category, enter the URL. You can enter any of the following:
   - a full site name, such as `http://www.marshal8e6.com/`
   - a specific sub-directory, such as `http://www.marshal8e6.com/webmarshal/`
   - a string with an asterisk as a wildcard at the beginning and/or the end of the URL, such as `http://*.marsha*`

5. Optionally select the variations of the URL that you want to add (such as the www. prefix or HTTPS and HTTP protocols).

6. Click **Add** (or press **Enter**) to add the URL to this category.

7. The window remains open so you can add additional URLs.

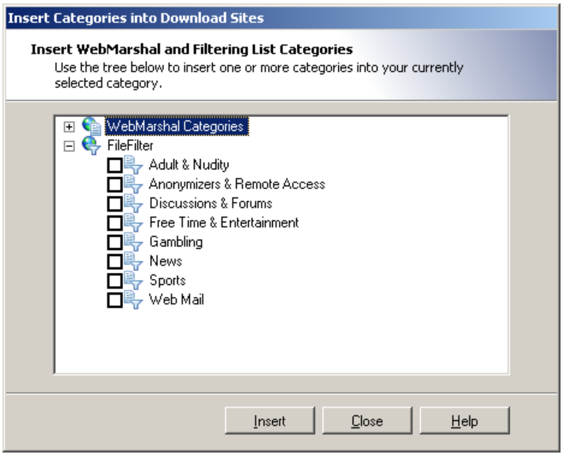
8. Click **Close** when done.

Adding Categories to a URL Category

1. Select **URL Categories** in the left pane.

2. Select the name of a URL category in the left pane to view its members in the right pane.

3. Click the **Insert Categories** icon in the tool bar to open the Insert Categories window. The Insert Categories window shows all available categories in a tree view, organized by the source (including WebMarshal categories and filtering list categories).



Insert Categories into Download Sites

Insert WebMarshal and Filtering List Categories

Use the tree below to insert one or more categories into your currently selected category.

- WebMarshal Categories
- FileFilter
  - □ Adult & Nudity
  - □ Anonymizers & Remote Access
  - □ Discussions & Forums
  - □ Free Time & Entertainment
  - □ Gambling
  - □ News
  - □ Sports
  - □ Web Mail

4. To include one or more URL categories in this category, expand the tree and select the desired categories.

5. Click **OK** to add the selected categories and return to the parent window.

You can also “drag and drop” a category name or names (from either pane) over a category name in the left pane. If you want to copy the category, hold down the Ctrl key while dragging.

Importing a URL category

You can import URLs from a file created by another application or WebMarshal installation. The imported URLs can replace or add to the existing content of the category. The file must be a simple text file with one URL per line.

Note
You can also import categories from files using the WebMarshal FileFilter filtering list. With FileFilter, you can maintain the category files outside WebMarshal, and import them daily. FileFilter is also a better choice for categories containing large numbers of URLs. See “FileFilter” on page 264.

To import URLs to a Category:

1. In the Console menu tree, expand **URL Categories** and select the category you want to use.
2. Click the **Import URLs** icon in the toolbar.

For more information about results and error handling, see Help.

Exporting a URL category

You can save the members of a URL category to a file that you can export to another application or WebMarshal installation.

To export a URL category:

1. In the Console menu tree, expand **URL Categories** and select the category you want to use.
2. Click the **Export to File** icon in the toolbar
3. Select the location where you want to save the category file. Click **Save**.

Searching a Category for a URL

To search a Category for a specific URL:

1. Select a WebMarshal category in the tree, then click the **Find URL** icon 🔎 in the toolbar.
2. Enter the name of the URL to search for.
3. If you want to search all categories, select **Search all URL categories.**
4. Click **Find**.
5. The result indicates whether the URL is in the currently selected category. If you selected Search all URL categories, the result indicates which categories if any the URL is in.

Configuring URL Filtering Lists

Lists are categorized lists of websites, maintained externally to WebMarshal. You can use the categories provided by these lists in WebMarshal URL Categories.

The Filtering Lists pane displays information about the lists currently configured in WebMarshal. You can enable or disable an existing list. You can add or delete lists. WebMarshal currently supports the following lists:

- **FileFilter:** A simple implementation that reads category lists from text files. For more details about FileFilter please see “FileFilter” on page 264.
- **URLCensor:** A real-time facility that categorizes IP addresses through DNS Blacklist lookup. For more details about URLCensor please see “URLCensor” on page 265.
- **MarshalFilter:** A URL list provided by Marshal8e6 and licensed separately. The list provides a comprehensive database of categorized Web sites with over 50 categories and 60 million entries. For more details about MarshalFilter including trial license information, please see “MarshalFilter List” on page 267.

- **Marshal8e6Filter**: A URL list provided by Marshal8e6 and licensed separately. The list consists of 116 categories. For more information on the Marshal8e6Filter List including trial license information, please see “Marshal8e6Filter List” on page 269.
- **SmartFilter**: A commercial product of Secure Computing (licensed through Marshal8e6) that categorizes millions of URLs and provides periodic updates. For more details about SmartFilter including trial license information, please see “Secure Computing SmartFilter” on page 270.

Reviewing Filtering List Status

You can check the available categories, enabled or disabled status, and update status for any configured list, and update the list or license if required.

To check the list:

1. In the left pane tree, expand **URL Filtering Lists.**
2. Select a list. The top right pane shows the status of the list on each server. The bottom right pane shows the name and description of each category available through the list.
3. To view general details of a list, to initiate an update for all servers, and to enter a license if required, right-click a list name in the left pane. Click **Update All Nodes** to force an immediate check for Filtering List updates (where internet updates are provided).

Tip
Updating can cause disruption for users browsing. This action should be performed at a time when it will have minimum effect.

4. To view details of list and license status on each server, double-click a server name in the right pane. The Node Update Status tab shows the update status and results fro the server.

Adding Filtering Lists

You can add one or more filtering lists to the WebMarshal configuration.

To add a filtering list:

1. In the left pane tree, expand **URL Filtering Lists.**
2. In the right pane, click **Add URL Filtering List** to start the Add URL Filtering List wizard.
3. Select a single list to add. WebMarshal displays the license and database information. Click **Next.**

4. If a list requires a separate license:

  a. Enter the license on the **License Key** window, and then click **Next**.

  Note
  For more information about how to obtain filtering list licenses, see Chapter 12, "WebMarshal and Filtering Lists."

  b. To allow WebMarshal to validate the license, select an Internet connection method that is valid from the WebMarshal Array Manager server, and then click **Next**.

5. Click **Finish** to add the list.
6. To add another list, repeat the above steps.
7. Commit configuration changes to propagate the new list to the WebMarshal servers.

After adding a filtering list, you can use the categories from that list by inserting them into WebMarshal URL Categories. See "Adding Categories to a URL Category" on page 154.

Note
WebMarshal will use the categories for filtering as soon as the list download is complete on the servers. In some cases the initial population of categories can take half an hour or longer, depending on Web connection speed.

Deleting a Filtering List

You can delete a filtering list from the WebMarshal configuration. Deleting a list removes any categories imported from the list from the WebMarshal URL Categories. Deleting a list does not remove database log records of categorized sites.

To delete a filtering list:

1. In the left pane tree, expand **URL Filtering Lists.**
2. Right-click the list you want to delete, and select **Delete.**
3. Commit configuration changes.

Enabling or Disabling a Filtering List

You can enable or disable use of a Filtering List. When a list is disabled, the list and imported categories will display in the Console, but the list will not be updated and it will not be used in rules.

To enable or disable a filtering list:

1. In the left pane tree, expand **URL Filtering Lists.**
2. Right-click the list you want to change, and select **Enable** or **Disable.**
3. Commit configuration changes.

Configuring Access Using Schedules

The scheduling facility allows you to apply Rules at particular times.

You can set different Quotas or Web access permissions by time of day or day of the week. For instance, an organization might block access to games sites during working hours, but allow access after hours.

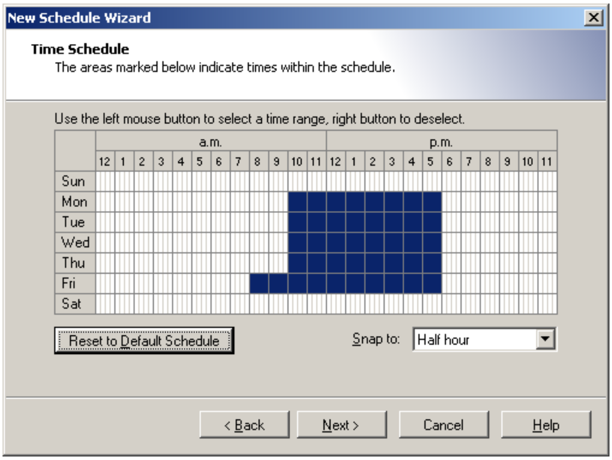
You can apply different schedules for different user groups.

Use Schedules as conditions when you create rules.

Note
Schedule times are calculated in local time on the processing server that handles a request.

Adding a Schedule

1. Select **Schedules** in the left pane.
2. Click the **New Schedule** icon in the tool bar to start the New Schedule wizard.



New Schedule Wizard

Time Schedule
The areas marked below indicate times within the schedule.

Use the left mouse button to select a time range, right button to deselect.

Snap to: Half hour

3. On the Time Schedule page of the wizard, drag with the left mouse button to add to the blue “inside” area. Drag with the right mouse button to erase from the blue “inside” area.
4. Click **Set Default Schedule** to reset the schedule to the default time block.
5. Choose to “snap” the schedule times to the nearest whole, half or quarter hour using the drop down box.
6. Click **Next.**
7. On the Schedule Name page of the wizard, give the schedule a name.

8. Optionally enter a description of the schedule.
9. Click **Next.**
10. On the Completing page of the wizard, click **Finish** to save the schedule, or **Cancel** to exit without saving.

Editing a Schedule

1. Select **Schedules** in the left pane.
2. Double-click an existing Schedule name in the right pane to edit it.
3. Drag with the left mouse button to add to the blue "inside" area. Drag with the right mouse button to erase from the blue "inside" area.
4. Click **Set Default Schedule** to reset the schedule to the default time block.
5. Choose to "snap" the schedule times to the nearest whole, half or quarter hour using the drop down box.
6. On the General tab, edit the name and optional description of the schedule.
7. Click **OK** to save the changes to the schedule, or **Cancel** to lose any changes.

Duplicating a Schedule

To duplicate a schedule:

1. Right-click the Schedule name in the right pane.
2. Select **Duplicate**.

Deleting a Schedule

To delete a Schedule:

1. Right-click the Schedule name in the right pane.
2. Select **Delete.**

Configuring Access Using Quotas

Quotas allow you to limit users' browsing activity by time or by volume (total bandwidth).

You can set different Quotas for different user groups. More than one Quota can apply to a user.

Different limits can apply at different times. For instance, the organization may wish to limit access to news sites during working hours but allow unlimited access after hours.

Quotas are applied as Rule conditions.

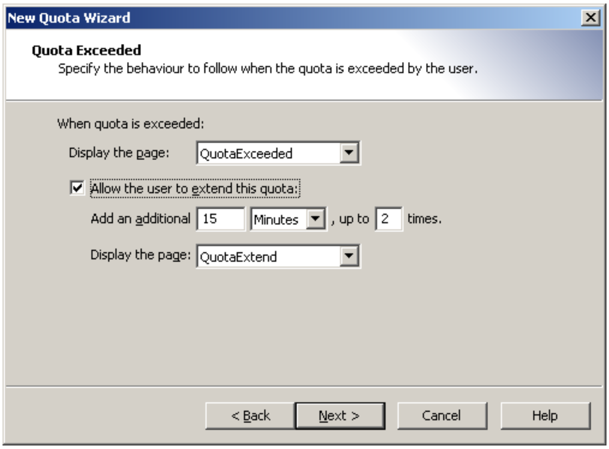
Adding a Quota

1. Select **Quotas** in the left pane.
2. Click the **New Quota** icon in the tool bar to start the New Quota wizard.
3. On the Quota Interval page of the wizard, select the allocation interval. Click **Next** to continue.

   Note
   Quotas are reset at midnight (local time at the WebMarshal processing server) at the beginning of the first day of the quota period

4. On the Quota Type page of the wizard, choose whether this will be a time or volume (bandwidth) quota.
5. For a time quota, choose the amount and period (minutes or hours).
6. For a volume quota, choose the number and unit (Kilobytes, Megabytes, or Gigabytes).

7. Click **Next** to continue.



New Quota Wizard

Quota Exceeded

Specify the behaviour to follow when the quota is exceeded by the user.

When quota is exceeded:

Display the page: QuotaExceeded

☑ Allow the user to extend this quota:

Add an additional 15 Minutes , up to 2 times.

Display the page: QuotaExtend

8. On the Quota Exceeded page of the wizard, select the actions WebMarshal will take when a user (or workstation) has exceeded the allowed quota.

   a. Select a web page to display from the list. (To learn how to add items to this list, see "Notifying Users with Notification Pages" on page 185.)

   b. To allow users to extend the quota, check the box and enter the required information:

      - Amount of time or volume to be added per extension.
      - Number of extensions allowed.
      - Web page to display.

9. Click **Next** to continue.

10. On the Quota Name page, enter identifying information.

    - Enter a name for this Quota (required).
    - Optionally enter a description indicating the intended use of the Quota.

11. Click **Next** to continue.

12. On the Completing page of the wizard, click **Finish** to save the Quota, or **Cancel** to exit without saving.

Editing a Quota

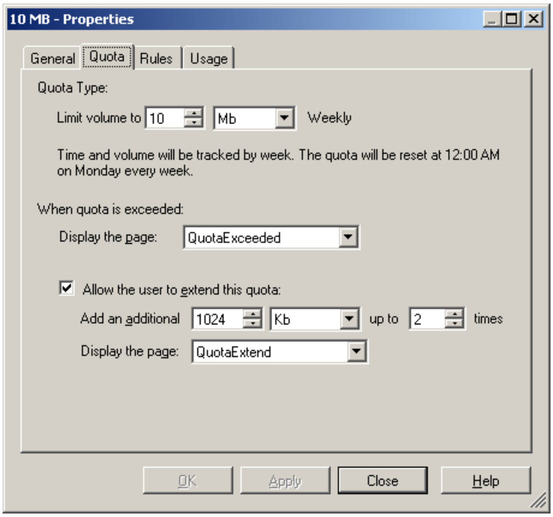
You can change the global properties of a quota. You can also extend a user’s allocation for the current quota period.

1. Select **Quotas** in the left pane.

2. Double-click an existing Quota name in the right pane to edit it.

3. On the General tab, edit the name and optional description of the Quota.

4. On the Quota tab, edit the properties of the Quota.



Quota Type:

Limit volume to 10 Mb Weekly

Time and volume will be tracked by week. The quota will be reset at 12:00 AM on Monday every week.

When quota is exceeded:

Display the page: QuotaExceeded

☑ Allow the user to extend this quota:

Add an additional 1024 Kb up to 2 times

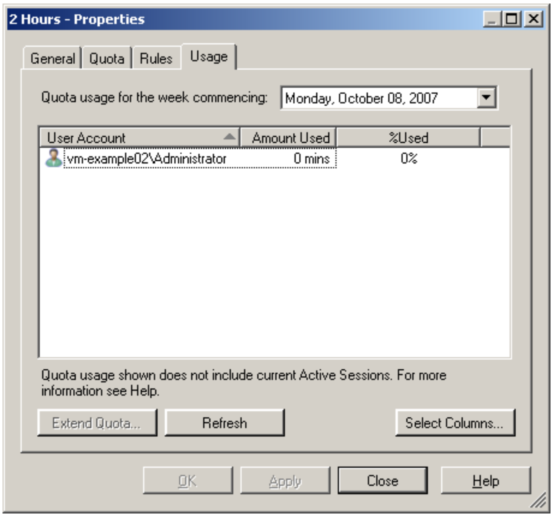
Display the page: QuotaExtend

5. On the Rules tab, you can see a list of rules that apply to this quota. Highlight a rule and click **Jump to Rule** to view the details of that rule.

6. On the Usage tab, you can see the quota usage for the current period quota usage for each user affected by the quota.

Note

This display does not reflect Quota amounts used in current Active Sessions. The usage information is updated at the end of a browsing session.

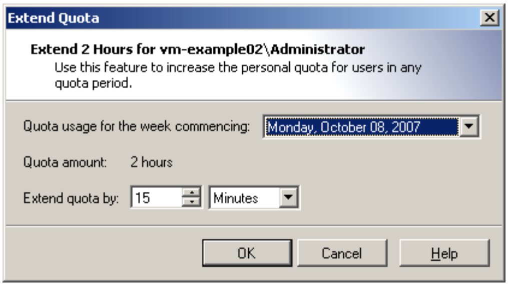


Quota usage for the week commencing: Monday, October 08, 2007

User Account	Amount Used	%Used
vm-example02\Administrator	0 mins	0%

Quota usage shown does not include current Active Sessions. For more information see Help.

7. To extend the quota for a specific user, select that user from the list then click **Extend Quota** to open the Extend Quota window.



Extend Quota

Extend 2 Hours for vm-example02\Administrator

Use this feature to increase the personal quota for users in any quota period.

Quota usage for the week commencing: Monday, October 08, 2007

Quota amount: 2 hours

Extend quota by: 15 Minutes

- The window shows the user’s current allocation. Enter the desired extension as a number of minutes, hours, KB, MB, or GB. Click **OK** to apply the change and return to the Quota Properties window.

  Note
  Changes made here only affect the current quota period (day or week). Changes made here do not affect the user's ability to extend the quota (as set in the Quota properties).

- To refresh the display, click **Refresh.**

  Note
  You can allow a user to extend their own quota when they reach the limit. See “Quota Extensions” on page 168.

8. Click **OK** to save the changes to the Quota, or **Cancel** to lose any changes.

Duplicating a Quota

To duplicate a Quota:

1. Right-click its name in the right pane.
2. Select **Duplicate.**

Deleting a Quota

To delete a Quota:

1. Right-click its name in the right pane.
2. Select **Delete.**

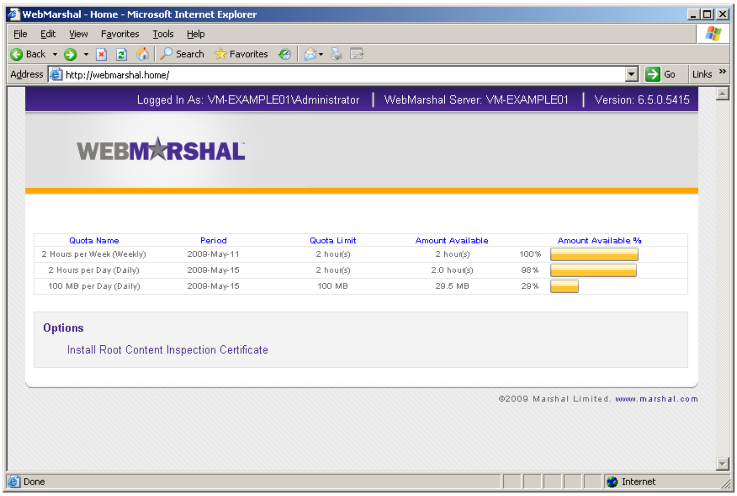
Quota Levels

If WebMarshal Quotas are in use, users can check their quota allocation and usage from the WebMarshal website.

The URL of the quota page is `http://webmarshal.home/Quotas`

This URL can only be accessed from inside the local network for which WebMarshal is the gateway. The browser must be configured to use WebMarshal as a proxy server.

This page shows the user name of the authenticated session.


WebMarshal - Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://webmarshal.home/
Go Links
WEBMARSHAL
Done
Internet

Logged In As: VM-EXAMPLE01\Administrator | WebMarshal Server: VM-EXAMPLE01 | Version: 6.5.0.5415

Quota Name	Period	Quota Limit	Amount Available	Amount Available %
2 Hours per Week (Weekly)	2009-May-11	2 hour(s)	2 hour(s)	100%
2 Hours per Day (Daily)	2009-May-15	2 hour(s)	2.0 hour(s)	98%
100 MB per Day (Daily)	2009-May-15	100 MB	29.5 MB	29%

Options

Install Root Content Inspection Certificate

©2009 Marshal Limited. www.marshal.com

Each quota for that user is displayed. The quota limit (including extensions used if any), amount remaining, and percentage remaining are shown.

Quota Extensions

If a user makes a Web request (page view, upload, or download) which would exceed their remaining quota, they will be notified by a web page.

If the quota is configured to allow user extensions, and the user has not yet used all allowed extensions, the notification web page will include a button to extend the quota.

When the user clicks the button **Request a quota extension**, the extension is recorded and the request is processed.

The WebMarshal Administrator can monitor and extend quotas for all users from the Usage tab of the Quota Properties window (see "Editing a Schedule" on page 161).

Quota and Browsing Time Calculation

WebMarshal calculates user browsing time for Quotas and to log usage for reporting, based on a session timeout value and a padding time. For information about how to set these values, see "Viewing Product Information" on page 209. For additional details see Marshal8e6 Knowledge Base article Q11755.

- Each time a page is requested, WebMarshal checks for a previous request from the same user.
- If the previous request from the user was within the session timeout value, the WebMarshal logs show a continuous period of browsing.
- If the previous request was longer ago than the session timeout value, the WebMarshal logs show that browsing activity stopped after the previous request plus padding time, and started again with the new request.
- WebMarshal Proxy Caching does not affect the quota calculations. Requests that are fulfilled from the cache consume the same bandwidth quota allocation as requests fulfilled from the Internet. Cached responses for large files could consume less browsing time (because the file is returned more quickly).

Identifying Web Content Using TextCensor Scripts

TextCensor scripts allow you to check for the presence of particular content in a HTML or plain text file.

TextCensor scripts are used in Content Analysis rules. The rule can block a request, classify a site, or add a site to a URL Category. A script can include many conditions based on text combined with Boolean and proximity operators. Triggering of the script is based on the weighted result of all conditions.

TextCensor Elements

TextCensor scripts contain one or more lines, each consisting of a word or phrase.

You can use the wildcard character * at the end of a word (`be*` matches `being` and `behave`). Parentheses should be used to clarify the order of evaluation and for grouping.

Each line can include Boolean and proximity operators. The operators must be entered in capital letters. The six supported operators are:

Operator	Function	Example
AND	Matches when all terms are present.	dog AND cat
OR	Matches when any term is present.	dog OR cat dog OR (cat AND rat)
NOT	Logical negation of terms; use after other operators; means “anything else but.”	Dog AND NOT cat Dog FOLLOWEDBY (NOT house)
NEAR	Matches when two terms are found within the specified number of words of each other. The default is 5.	Dog NEAR=2 bone
INSTANCES	Matches when a term is found the specified number of times. You must specify a value.	Dog INSTANCES=3

Operator	Function	Example
FOLLOWEDBY	Matches when one term follows another within the specified number of words. The default is 5.	Dog FOLLOWEDBY=2 house

Notes

The INSTANCES operator is provided for compatibility with earlier TextCensor scripts, but its use is discouraged. The use of appropriate weighting (see below) produces the same result with improved performance.

When you use NEAR and FOLLOWEDBY, a "word" is defined as any group of one or more contiguous alphanumeric characters, bounded at each end by non-alphanumeric characters. If any non-alphanumeric characters have been included as "special characters", each single special character is also counted as a "word".

For instance, by default "S-P-A-M" counts as four words. If the "-" character is entered as a "special character," then the same text counts as 7 words.

Weighting a TextCensor Script

Each script is given a trigger level, expressed as a number. If the total score of the content being checked reaches or exceeds this level, the script is triggered. The total score is determined by summing the scores resulting from evaluation of the individual lines of the script.

Each line in a script must be given a positive or negative weighting level and a weighting type. The type determines how the weighting level of the line is figured into the total score of the script. There are four weighting types:

Weighting Type	Description
Standard	Each match of the words or phrases adds the weighting value to the total.
Decreasing	Each match of the words or phrases adds a decreasing (logarithmic) weighting value to the total. Each additional match is less significant than the first.

Weighting Type	Description
Increasing	Each match of the words or phrases adds an increasing (exponential) weighting value to the total. Each additional match is more significant than the first.
Once Only	Only the first match of the words or phrases adds the weighting value to the total.

Negative weight and trigger levels allow you to compensate for the number of times a word could be used on an inoffensive site. For instance: if `breast` is given a positive weighting in an “offensive words” script, `cancer` could be assigned a negative weighting (since the presence of this word suggests the use of `breast` is medical/descriptive).

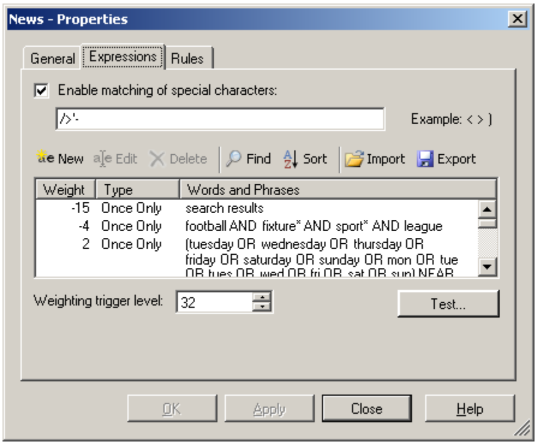
Note

Because script evaluation stops when the trigger level is reached, items with negative weighting should be evaluated first. Use the **Sort** feature on the TextCensor Script window to set the order of evaluation correctly.

Adding a TextCensor Script

1. Select **Rule Elements > TextCensor Scripts**.

2. Click the **New TextCensor Script** icon in the tool bar to open the New TextCensor Script wizard.



☑ Enable matching of special characters: />'-

Example: < >)

Weight	Type	Words and Phrases
-15	Once Only	search results
-4	Once Only	football AND fixture* AND sport* AND league
2	Once Only	(tuesday OR wednesday OR thursday OR friday OR saturday OR sunday OR mon OR tue OR tues OR wed OR fri OR sat OR sun) NEAR

Weighting trigger level: 32

3. If appropriate, check the checkbox to enable matching for special characters and enter any special characters that the script will use.

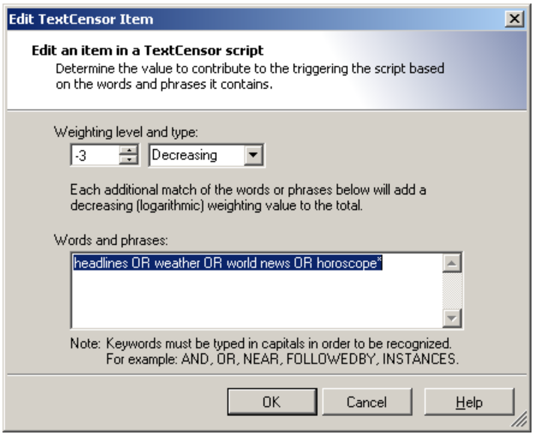
Note

By default you can only use alphanumeric characters in TextCensor items. This field provides a way to match other characters.

For instance, to match the HTML tag fragment "`<script`" you must enter the < in this field. To match parentheses ( ) you must enter them in this field.

---

4. Click **New** to open the New TextCensor Item window.



Edit TextCensor Item

Edit an item in a TextCensor script

Determine the value to contribute to the triggering the script based on the words and phrases it contains.

Weighting level and type: -3 Decreasing

Each additional match of the words or phrases below will add a decreasing (logarithmic) weighting value to the total.

Words and phrases: headlines OR weather OR world news OR horoscope*

Note: Keywords must be typed in capitals in order to be recognized. For example: AND, OR, NEAR, FOLLOWEDBY, INSTANCES.

5. Select a weighting level and type for this item (see "Weighting a TextCensor Script" on page 170 for more information).

6. Enter the item, optionally using the operators described earlier. For example:

   ```
   (Dog FOLLOWEDBY hous*) AND NOT cat
   ```

   In this example the item weighting is added to the script total if the document contains the words "`dog house`" (or "`dog houses`", and so forth) in order, and does not contain the word "`cat`".

   Note

   TextCensor items are *not* case sensitive by default. However, quoted content is case sensitive. So `textcensor` would match TextCensor, but `"textcensor"` would not.

7. Click **Add** (or press **Enter**) to add the item to this script. The window remains open so you can create additional items.

8. When all items have been entered, click **Close** to return to the New TextCensor Script window.

9. Select a Weighting Trigger Level. If the total score of the script reaches or exceeds this level, the script is triggered. The total score is determined by evaluation of the individual lines of the script.

10. Click **Sort** to set the order of evaluation. This step is important if any items have negative weighting levels. Items with negative weighting will be grouped at the top of the list. Within the negative and positive weighting groups, the items will be sorted alphabetically.
11. Click **Next**
12. On the TextCensor Script Information page, enter a name and optional description for the script.
13. .Click **Next,** then **Finish,** to add the script.

Editing a TextCensor Script

1. Select **TextCensor Scripts** in the left pane.
2. Double-click the script name in the right pane to open the Edit TextCensor Script window.
3. Double-click a line to edit it.
4. To delete a line, select it and click **Delete**.
5. Change the script name, special characters, and weighting trigger level as necessary.
6. Click **Sort** to arrange items. This step is important if negative weighting levels are used.
7. Click **OK** to accept changes or **Cancel** to revert to the stored script.

Importing a TextCensor Script

You can import TextCensor scripts from CSV (comma separated) files.

To import a Script:

1. Select **TextCensor Scripts** in the left pane.
2. Click the **New TextCensor Script** icon in the tool bar to open the New TextCensor Script wizard.

3. On the TextCensor Expressions window, click **Import.**
4. Select the file you wish to import, and click **Open**.
5. Complete the Wizard to add the script.

Note
When importing scripts that were exported from WebMarshal 2.2 and below, the Weighting Trigger Level and Special Characters settings are not set. This information must be added manually after import.

Exporting a TextCensor Script

You can export TextCensor scripts to CSV (comma separated) files.

To export a Script:

1. Select **TextCensor Scripts** in the left pane.
2. Double-click the name of the script you want to export in the right pane to open the Edit TextCensor Script window.
3. Click **Export**.
4. Enter the name of the file you want to create, and click **Save**.
5. In the Edit TextCensor Script window, click **OK**.

Using TextCensor Effectively

The effective use of TextCensor scripts depends on understanding how the Text Censor facility works and what it does.

TextCensor evaluates rules against plain text or HTML documents. The rules can be used to block a request, classify a site or add it to a URL Category. If a Content Analysis rule includes a "block" action, TextCensor scripts are evaluated before the material is returned to the user.

Blocking does not apply to content cached on the local computer.

Constructing TextCensor Scripts

The key to creating good TextCensor scripts is to enter words and phrases that are not ambiguous. They must match the content you want to block. Also, if certain words and phrases are more relevant to the match than others, those words and phrases should be given a higher weighting to reflect the greater relevance.

In creating TextCensor scripts, you should strike a balance between overly-general and overly-specific. For instance, suppose a script is required to check for sports-related sites. To enter the words `score` and `college` alone would be ineffective because those words are likely to be used on non-sports sites. Hence, the script would trigger too often, potentially stopping access to acceptable sites such as general news sites.

The same script (to find sports-related sites) would be better constructed using the phrases `extreme sports`, `college sports` and `sports scores` as these phrases are sport specific. However, using only a few very specific terms may mean that the script does not trigger often enough.

Again using the sports example used above, the initials NBA and NFL, which are very sports specific, should be given a suitably higher weighting (that is, promoting earlier triggering) than, for example, `college sports`.

Decreasing Unwanted Triggering

TextCensor scripts might trigger on pages that are not obviously related to the content types they are intended to match.

To troubleshoot this problem:

1. Use the problem script in a TextCensor Rule that classifies sites and adds them to a URL Category, such as “suspected sports sites.”

2. After using this rule for a while, check the sites that have triggered the script and determine which ones are triggering it falsely.

    - In the URL Categories display of the console, double-click a URL to view the reasons it was added (for example, TextCensor details).

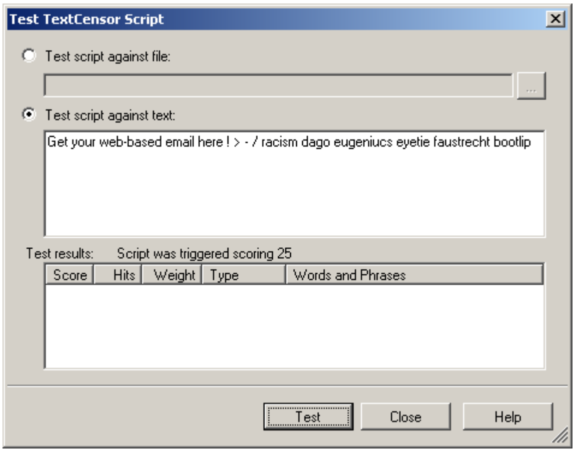
3. Revise the script by changing the weighting or key words, so as to decrease false triggering.

4. When satisfied, create a Standard Rule which denies access to sites in the URL Category generated by the script, and/or add a Block action to the original TextCensor rule.

Testing TextCensor Scripts

To test the operation of a TextCensor script:

1. Click **Test** on the New or Edit TextCensor Script window to open the Test TextCensor window.



Test TextCensor Script

○ Test script against file:

● Test script against text:

Get your web-based email here ! > - / racism dago eugeniucs eyetie faustrecht bootlip

Test results: Script was triggered scoring 25

Score	Hits	Weight	Type	Words and Phrases

2. In the Test TextCensor window, enter the sample text you want to test using one of two methods.

   - Select **Test script against file**. Enter the name of a file containing the test text (or browse using the button provided).
   - Select **Test script against text**. Type or paste the text in the field.

3. Click **Test**. The result of the test (including details of the items which triggered and their weightings) displays in the Test Results pane.

You can also test a script as part of the test of a content rule. This method allows you to test using pages drawn directly from the Web. See "Testing Access Policy" on page 133 for detailed information on Rule testing.

Using Malware Scanning

WebMarshal can invoke third-party scanners to check file uploads and downloads for malware, including viruses and spyware. Before you enable scanning Rules, you must install at least one supported scanner *on each processing server*, and configure the scanners within WebMarshal.

Scanning Overview

WebMarshal currently supports only specific malware scanners that have licensed DLL interfaces.

- **Supported virus scanners** include McAfee for Marshal, Sophos for Marshal, Norman, Symantec Anti-Virus Scan Engine, and Sophos (SAVI interface).
- **Supported spyware scanners** include PestPatrol and Counterspy.

Others may be added–consult Marshal8e6 for the latest list.

You choose which files to scan using Malware Scanning Rules. See Chapter 6, "Understanding Web Access Policy, Rule Containers, and Rules."

For enhanced protection against viruses and spyware, TextCensor and file type rules should also be used to control potentially dangerous file types such as VB Script and executable files.

Note

WebMarshal uses a temporary directory during scanning. This directory *must be excluded* from on-access or resident virus and spyware scanning**.** If it is not excluded, the WebMarshal Engine and/or the WebMarshal Controller service may be unable to start. By default, WebMarshal uses the `\temp` subdirectory of your install directory. You can change this location by editing XML configuration files on each processing server and restarting the WebMarshal services. ***If you change the location of the temporary directory*** for either or both services, be sure that you also update virus scanner exclusions.

To view and add to the list of configured scanners, select **Malware Protection** from the left pane of the WebMarshal Console.

Adding a Scanner

To add a malware scanner to the list of configured scanners:

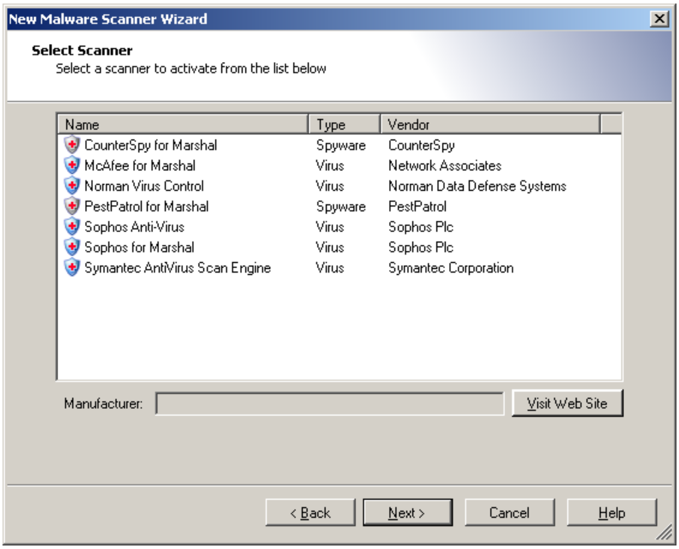
1. Select **Malware Protection** from the left pane of the WebMarshal Console.

Tip

If you select one of the sub-types of Virus scanners or Malware scanners, your choices will be limited to scanners of the selected type.

---

2. Click the **New Malware Scanner** icon in the tool bar to start the New Malware Scanner Wizard.



New Malware Scanner Wizard

Select Scanner

Select a scanner to activate from the list below

Name	Type	Vendor
CounterSpy for Marshal	Spyware	CounterSpy
McAfee for Marshal	Virus	Network Associates
Norman Virus Control	Virus	Norman Data Defense Systems
PestPatrol for Marshal	Spyware	PestPatrol
Sophos Anti-Virus	Virus	Sophos Plc
Sophos for Marshal	Virus	Sophos Plc
Symantec AntiVirus Scan Engine	Virus	Symantec Corporation

Manufacturer:

3. The Select Scanner page of this Wizard shows a list of scanners WebMarshal can use.

   To obtain more information about any scanner, select it and then click **Visit Website.**

4. Select a scanner to add.

All scanners that you add will be available for use by WebMarshal. When you create a malware scanning rule, you can choose the scanners that rule will use. You can use multiple scanners in a single rule or separate rules. Because different products have differing coverage, some sites choose to use more than one scanner of each general type (virus and spyware).

5. Click **Next** to continue to the next page.

6. If any additional parameters are required, the additional parameters pages of the wizard is shown. Enter any required parameters (such as the location of a scanner if it is installed remotely). Click **Next** to continue to the next page.

7. Click **Finish** to install the scanner and exit the Wizard.

To select an additional scanner for use, re-run the Wizard.

Note

McAfee for Marshal, Counterspy, for Marshal, Pest Patrol for Marshal, and Sophos for Marshal each require installation of a configuration Console, available in separate downloads from Marshal8e6 (and licensed separately).

You must install this software on the WebMarshal server. If you have configured an array of servers, you must install the scanning software on each processing server.

WebMarshal trial keys enable all of these products for the 30 day trial period. To obtain a permanent key, contact your Marshal8e6 supplier. If you are a customer with a permanent WebMarshal key and you want to try one of these scanner products, contact your Marshal8e6 supplier for a special time-limited key.

Deleting a Scanner

To delete a configured scanner from the list of scanners WebMarshal can use:

1. Select it in the right pane of the Console
2. Click the **Delete** icon in the taskpad tool bar.

Notes

- If any malware scanning rule is enabled, you cannot delete all scanners of the type(s) used by that rule.
- If any malware scanning rule (including disabled rules) references a specific scanner, you cannot delete that scanner.
- Deleting a scanner from the list does not uninstall the scanning software.

Testing Scanners

To test the operation of an installed malware scanner:

1. Select it in the right pane of the Console
2. Click the **Properties** icon in the taskpad toolbar.
3. Select the **Installation Status** tab. WebMarshal queries each processing server and returns the status of the scanner on each server.

Logging Activity with Classifications

WebMarshal logging classifications allow you to record more detailed information about user requests (both allowed and denied), and content downloaded or uploaded. Logging classifications are only recorded in database logging.

Types of Logging Classification

WebMarshal allows you to use Classifications in two ways.

- **Domain Classification** actions are available within Standard rules and TextCensor rules. Logging a classification for a domain shows that a user browsed to a URL which is in a specific category, or to a page which triggered a rule. A domain can receive multiple classifications within a single browsing session. A domain could also receive different classifications in different sessions, depending on the actual content requested, such as sports or entertainment sections of a news site.
- **File Classification** actions are available within all Content Analysis rules as well as download file type/size rules and malware scanning rules. A file classification applies to a specific upload or download request.

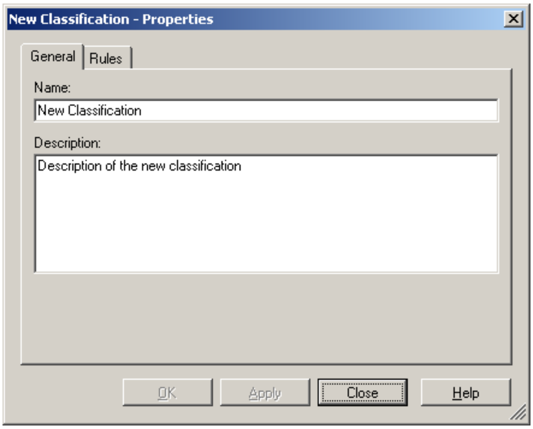
You can generate reports by user or domain based on the classifications recorded; see Chapter 8, "Reporting on Browsing Activity" for details.

In addition, when any filtering list integration is enabled, every browsing request returns a categorization as provided by the filtering list. These categorizations are recorded regardless of whether they are used within rules to filter requests. This process is separate from the logging of classifications. You can generate reports based on the categorizations.

Adding a Logging Classification

To add a classification:

1. Select **Logging Classifications** in the left pane of the console.
2. Click the **New Classification** icon in the tool bar to open the New Logging Classification window.


New Classification - Properties

Name: New Classification

Description: Description of the new classification

In the New Logging Classification window, enter a name and optionally a description for the classification.

3. Click **OK** to add the classification.

Editing a Logging Classification

To edit a Logging Classification:

1. Double-click the Classification name in the Console to open the Edit Logging Classification window.
2. Make any required changes.
3. Click **OK**.

Deleting a Logging Classification

To delete a Logging Classification:

1. Right-click the classification name in the Console.
2. Select **Delete**.

Notifying Users with Notification Pages

WebMarshal uses web pages to provide pre-configured notification messages to users. The notifications can also be customized.

Notification Web Pages

When a user requests a Web resource that triggers a rule, they may receive a notification web page. The notification could simply state that a request was denied, or it could request acknowledgement of a warning before processing the request.

The choice of notification pages is made on the Action page of each rule wizard. Choices vary according to the type of rule.

Default Notification Pages

WebMarshal is supplied with a number of default notification pages. The files are standard HTML pages, located in the `\ArrayManager\Policy\Templates` subdirectory of the WebMarshal installation directory on the Array Manager server.

Note

When you commit WebMarshal Configuration, any changes to items in this folder are copied to each processing node server, and stored in the folder `Node\Policy\Templates`. New files and subfolders are also copied.
You should only make changes to the Array Manager folder. The Node folders will be overwritten.

- **Page Blocked**
  - Standard
  - AdvertisingSmall (used in default rules for advertising sites)
  - Blank (used for images)
  - Offensive (for offensive content)
  - Small
  - With Sound (audible warning)
- **File Aborted–**for denied file type or size, where a portion of the file was trickled to the browser.
  - Standard
  - Malicious (Malware content)
  - Spyware (Spyware content)
  - Virus (virus content)
- **File Blocked–**for denied file type or size.
  - Standard
  - Malicious (Malware content)

  - Spyware (Spyware content)
  - TextCensor (lexical scan found denied content)
  - TextCensor Offensive (lexical scan found offensive content)
  - Virus (virus content)

- **Quota–**for quota rules.
  - Quotas (displays the user's quota)
  - Quota Exceeded
  - Quota Extend (allows the user to request an extension)

- **TRACEnet–**used by the TRACEnet policy.
  - TRACEnet Blocked
  - ReclassifyThanks (acknowledges the user's request to reclassify a blocked item)

- **Upload Blocked–**for upload rules.
  - Standard
  - Malicious (Malware content)
  - Spyware (Spyware content)
  - TextCensor (lexical scan found denied content)
  - Virus (virus content)

- **Warning–**before access to "permitted with warning" sites.
  - Standard
  - Malicious (Malware content)
  - Offensive (lexical scan found offensive content)
  - Policy (for policy display rules)
  - Previous Scan (site was placed in a URL category by a previous scan)

- Quotas (states that access is subject to quota)
- TextCensor (lexical scan found questionable content)

Editing Notification Pages

You can create new versions of the warning/blocking pages, or modify the existing pages.

Use HTML editing software to create or modify warning/blocking pages.

There are several types of warning/blocking pages, each identified by a filename prefix. New page names must start with one of the defined prefixes. The page types are as follows:

- **Aborted–**used when blocking websites where a portion of the file has been trickled to the browser.
- **Blocked–**used when blocking websites.
- **Warning–**used to prompt the user before permitting access to a site.
- **FileBlocked–**used when a file is blocked by a file type or malware rule.
- **UploadBlocked–**used when a file upload is blocked.
- **QuotaExceeded–**used when a WebMarshal quota has been exceeded by the user.
- **QuotaExtend–**used to allow the user to extend a quota.

For example, to create a new blocking page for pornographic content, copy the file `Blocked.htm` to a new file `BlockedPorn.htm`. From then on, `BlockedPorn.htm` is available in the list of blocking pages when editing a site rule.

Please note the following important recommendations before editing the warning/ blocking pages.

- Do not change the original page; instead, copy the file and make any changes to the copy.
- After changing pages, test them to make sure that they are still functioning correctly. Several pages include special forms that process user input; amending such a page may affect the prompting functionality.

- If you want to refer to the `\Templates` sub-directory, use the virtual domain name "webmarshal.home." For example, a link to a file placed in the `\Templates` sub-directory could be:

  ```
  <image src= "http://webmarshal.home/blocked.gif">
  ```

- If you make links to other sites, ensure that these links are full URLs, not relative paths. WebMarshal replaces the content returned from websites with the warning/ blocking pages. If you use a relative path, the link will refer back to the original blocked site

Note

- You can also customize error pages for proxy authentication and other system functions. Please see Marshal8e6 Knowledge Base article Q10318 for more details.
- When WebMarshal is plugged in to Microsoft ISA Server in SecureNAT mode, the local WebMarshal `\Templates` sub-directory must be accessed with the following URL:

  ```
  http://www.marshal.com/webmarshal.home
  ```

  Due to the possibility of confusion this URL should only be used in this specific case.

Chapter 8
Reporting on Browsing Activity

WebMarshal can log web request activity in a Microsoft SQL database (using either SQL Server or SQL Express). WebMarshal Reports allow you to examine browsing behavior, successful and denied requests over time. Available reports include bandwidth, URL, and quota information. For more information about creating the database, see “Database Logging” on page 31.

For greater precision in reporting, rules should classify requests using domain and file classifications. To learn about classifications, see “Logging Activity with Classifications” on page 182.

WebMarshal logs activity to the reporting database in UTC. When you run reports, the periods and times shown are adjusted for the time zone where the Reports Console is running.

WebMarshal Proxy Caching does not affect the data reported. A request that is fulfilled from the cache is reported as the same size (and consumes the same bandwidth quota allocation) as the same request fulfilled from the Internet. Cached responses for large files could consume less browsing time, because the file is returned more quickly.

Many reports include information about “site visits” and “sessions.” To learn more about how these terms are defined, see Marshal8e6 Knowledge Base article Q11755.

Note

For many reports, *the column summary values are NOT equal to the sum of the detail values.* To learn more about how the summary values are calculated, please see Report Help for the individual reports.

Reports Basics

For installation instructions, see “Installing WebMarshal Reports” on page 52.

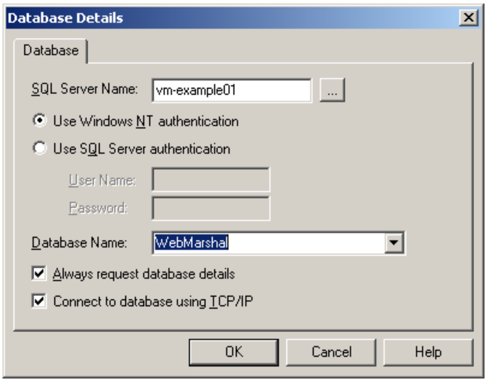
The Reports Console is implemented as a snap-in to the Microsoft Management Console (MMC). To learn more about the MMC, see “Understanding the MMC Interface” on page 66.

Note

Marshal8e6 offers two reporting solutions for WebMarshal. In addition to the WebMarshal Reports application described here, you can report on WebMarshal activity using the Marshal Reporting Console. The Marshal Reporting Console provides a web-based interface, scheduled report generation, and more export formats. for more information, visit the WebMarshal support pages at www.marshal8e6.com.

Starting the Reports Console

Run the WebMarshal Reports application from the Start menu. Enter appropriate information on the Database tab of the Database Details window, if it displays.



SQL Server Name: vm-example01

● Use Windows NT authentication

○ Use SQL Server authentication

User Name:

Password:

Database Name: WebMarshal

☑ Always request database details

☑ Connect to database using TCP/IP

1. In the SQL Server Name field enter the name of the computer where the WebMarshal database resides. Type in the name of the SQL Server computer where the WebMarshal database resides, or browse the local network using the browse [...] button.

2. Select **Windows NT authentication** or **SQL authentication** depending on whether you need to connect using the NT logon of the active user, or using a SQL user name and password.

3. Enter a **User Name.** If using SQL authentication, enter the SQL user name associated with the WebMarshal database. By default the user name is SA.

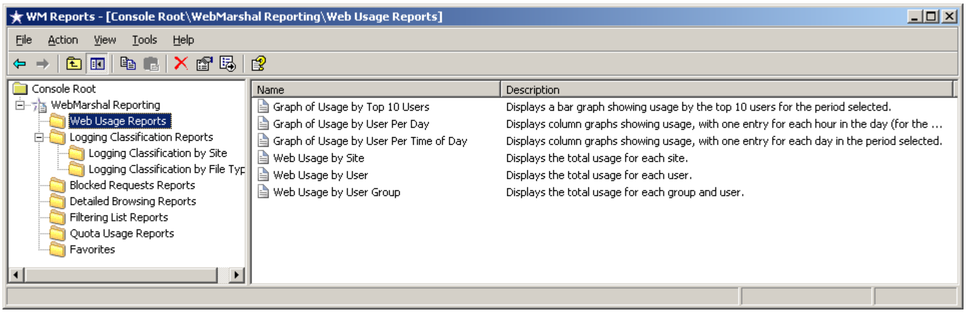
4. Enter your Password. If using SQL authentication, enter the SQL password for the database.

5. Enter the Database Name. Enter the name of the WebMarshal database. Choose a name from the drop-down list, or type in a new name.

6. Check **Always Request Database Details** if you want the database connection window to open each time WebMarshal Reports is started.

7. Check **Connect Using TCP/IP** if you want this database connection to use TCP/IP. This setting may be useful when the database server and the Reports workstation are separated by a firewall.

To view the list of available reports, expand the various branches of the left pane menu tree in the main report console, as shown below. Basic information about each folder and report is given in the Description column.


WM Reports - [Console Root\WebMarshal Reporting\Web Usage Reports]
File
Action
View
Tools
Help
Console Root
WebMarshal Reporting
Web Usage Reports
Logging Classification Reports
Logging Classification by Site
Logging Classification by File Typ
Blocked Requests Reports
Detailed Browsing Reports
Filtering List Reports
Quota Usage Reports
Favorites

Name	Description
Graph of Usage by Top 10 Users	Displays a bar graph showing usage by the top 10 users for the period selected.
Graph of Usage by User Per Day	Displays column graphs showing usage, with one entry for each hour in the day (for the ...
Graph of Usage by User Per Time of Day	Displays column graphs showing usage, with one entry for each day in the period selected.
Web Usage by Site	Displays the total usage for each site.
Web Usage by User	Displays the total usage for each user.
Web Usage by User Group	Displays the total usage for each group and user.

Viewing Report Properties

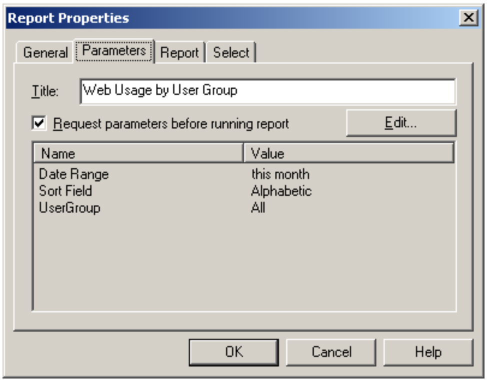
To view the properties of a particular report:

1. Select the report from the Report Console.

2. Click the **Properties** icon in the tool bar.

The Report Properties window has four tabs.

- **General:** the report name (as shown in the MMC) and a description are shown. Only the first line of the description displays in the description field. You can enter additional details but they are only visible in this window.
- **Parameters:** the report title (as seen when the report is generated) is shown. Click **Edit** to view and change the parameters using the parameters detail window.



Title: Web Usage by User Group

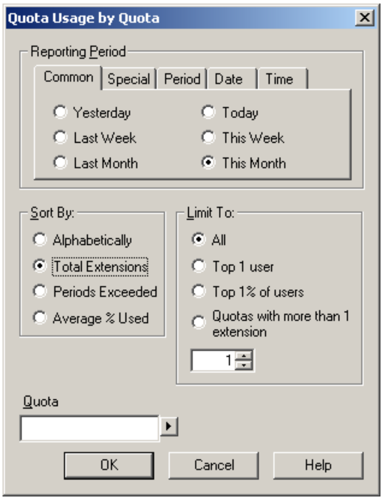
☑ Request parameters before running report

Name	Value
Date Range	this month
Sort Field	Alphabetic
UserGroup	All

- If the **Request parameters before running report** box is checked, the parameters detail window is presented (for confirmation or change) each time the report is generated. If this box is not checked, the parameters are not requested when the report is generated. In this case the last parameters entered will be used.
- **Report:** Information on the report definition file and DLL is shown.
- **Select:** You can select a new report definition file from the list. You should only select a new report definition file when creating a new custom report.

Generating Reports

To begin generating a specific report, double-click the report name in the right pane of the Reports console. Choose detailed parameters in the Parameter Detail window.



Quota Usage by Quota

Reporting Period

○ Yesterday ○ Today
○ Last Week ○ This Week
○ Last Month ● This Month

Sort By:
○ Alphabetically
● Total Extensions
○ Periods Exceeded
○ Average % Used

Limit To:
● All
○ Top 1 user
○ Top 1% of users
○ Quotas with more than 1 extension
1

Quota

Note
The Parameters Detail includes only the parameters appropriate to the specific report. Some options are not applicable to some reports.

The title of the window shows the title of the report as it will be generated. To change the title use the **Parameters** tab of the Report Properties window.

Select a Reporting Period

The period may be selected in any of five ways, each represented by a tab. When entering a date, use the drop-down arrow at the right of the date field to view a calendar.

Note
Reporting periods and action times are relative to the time zone where the Reports Console is running. The logging database records are kept in UTC.

- **Common:** Select a standard period from the list by clicking a radio button.
- **Special:** Select a reporting period by period type (month or day, for example), quantity, and starting day.
- **Period:** Select a reporting period by period type, quantity, and starting date (`dd/mm/yyyy`).
- **Date:** Select a reporting period by starting and ending dates. If you check **Inclusive**, the end date is included in the report.
- **Time:** Select a reporting period by starting and ending dates and times.

Select a Sort Method

Many sorting options are provided. Not all options are available for all report types.

Select Search Text

Optionally enter text to search for in the Quota, Site, User, User Group, or Logging Classification fields.

A menu of available wildcards is available through the button at right of each field. (See "Wildcards" on page 202 for a full explanation of the available wildcard syntax.) The following functions are available through the menu:

- **Any Character:** Match any single character (inserts "?" into the query).
- **Any String:** Match any number of characters (inserts "*" into the query).

- **Character in Range:** Match any character in the given range (inserts [ ] into the query; add a range of characters such as `a-z`).
- **Character not in range:** Match any character not in the given range (inserts [^] into the query; add a range of characters, such as `a-z` after the ^).
- **All:** show all items without limits.
- **Starting With:** show items starting with the characters entered.
- **Ending With:** show items ending with the characters entered.
- **Containing:** show items containing the characters entered.

Alternatively, where a field includes WebMarshal Rule Elements (such as User Groups, Quotas, or Classifications), click the button to the right of the field and choose **Select...** to view a list of available items. To include one or more items in a report, check the appropriate boxes.

Note
You can use either the Select option or wildcards for any one field.

Select a Report Limit

This set of options may be available if the **Sort By** selection is other than "Alphabetical". If present, this option provides a choice of how returned records are limited. Where a number or percentage is required, enter it using the spin box at the bottom of this section.

- **All:** All items are included in the report.
- **Top n:** Only the given number of items will be returned.
- **Top %:** Only the given percentage of items will be returned.
- **Over *(variable condition)*:** Only the items meeting the given condition will be returned. The condition can change based on the selections made in the **Sort By** section. For example, in the report Web Usage by User, you might choose to limit the report to users with bandwidth over 30,000KB or with more than 3 hours' browsing time.

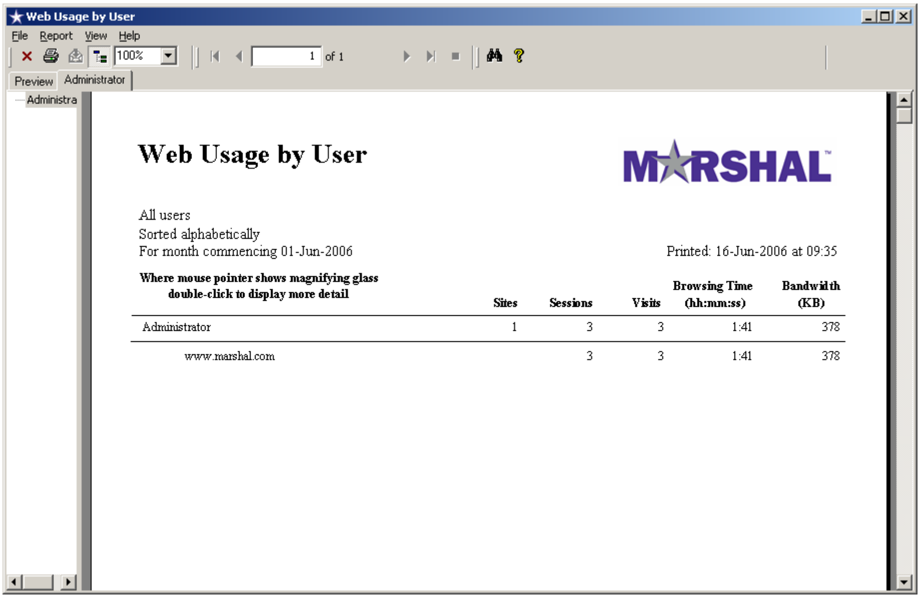
Select Rule Types

This set of options allows you to limit reports to one or more of the WebMarshal Rule types (Quota, Site, File, TextCensor, and Malware Scanning).

Select a Protocol

This drop-down menu allows you to limit reports to Web requests made using any one of the protocols supported by WebMarshal (FTP, HTTP, or HTTPS).

When all the options are chosen, click **OK** to view the report in a new window, as shown below.



Web Usage by User

All users
Sorted alphabetically
For month commencing 01-Jun-2006

Printed: 16-Jun-2006 at 09:35

Where mouse pointer shows magnifying glass double-click to display more detail	Sites	Sessions	Visits	Browsing Time (hh:mm:ss)	Bandwidth (KB)
Administrator	1	3	3	1:41	378
www.marshal.com		3	3	1:41	378

Report Window

Within the report window, several options may be available to customize the view and see additional details. The **Help** menu includes two choices: general help and help about the specific report.

Tool Bar Options

- **Close Current View**: close the drill-down tab currently showing.
- **Print:** print a copy of the report, or selected pages. (Printer setup is available from the File menu.)
- **Toggle group tree:** show a list of available detail items in a separate pane. Double-click any of these items to jump to it in the main report. If the item is a group, click the **+** icon to view the members of the group.
- **Magnification:** choose the magnification of the report on screen.
- **Page selector:** shows the number of pages in the report. Choose the page to view.
- The scroll bar in the report window is limited to the current page. Use the page selector to move between pages.
- **Stop button** (available while report is being generated): Stop generating the report. Optionally show the partial report.
- **Find:** search the report for text.

Drill-down

Some fields in a report are linked to detailed information or limited views. The mouse pointer shows a magnifying glass when moved over these fields. In addition, a tool tip indicates that drill-down is possible. Double-click to see the drill-down report.

Drill-down items which have been viewed within the current report window are saved as tabs at the top of the window. Click any tab to view the associated report. Use the **Close current view** icon to delete a drill-down view and its tab.

If the text in a field is truncated, hold the mouse over the field to see the complete information.

Customizing Reports

You can customize existing WebMarshal Reports with local parameters. You can then run these reports simply by double-clicking the report name in the Report Console. You can base customized reports on existing reports, or on the default report types.

Note
It is not currently possible for users to create new report types.

Reports Based on Existing Reports

Choose an existing report type to use as a template. Make a copy of this report by dragging it to the desired location while holding down the **Ctrl** key.

If the **Ctrl** key is not held down the existing report will be moved.

Edit the copy of the report by double-clicking it. Within the Report Properties window, make any desired customizations and changes.

To allow the report to run without confirmation, uncheck **Request parameters before running report**.

When satisfied, click **OK** in the Report Properties window. The custom report is now available.

Reports Based on Default Types

Select the group (folder icon) where you want to place the custom report. Choose **New > Report...** from the **Action** menu to start the New Report wizard.

Complete the pages of the wizard to place the newly customized report in the group. Details of the information required are given in “Viewing Report Properties” on page 194.

Wildcards

Text entries in the report parameters may be entered using several wildcard characters. The following syntax is supported:

Wildcard	Description
*****	Matches any number of characters.
?	Matches any single character.
[abc]	Matches a single character from the set a, b, and c.
[!abc] or [^abc]	Matches a single character except a, b, or c.
[a!b^c]	Matches a single character from a b c ! ^ .
[a-d]	Matches a single character in the range from a to d inclusive.
[^a-z]	Matches a single character not in the range a to z inclusive.

Examples

`*.ourcompany.com` would match:

`www.ourcompany.com` or `search.ourcompany.com`

`www[0-9].ourcompany.com` would match:

`www5.ourcompany.com` but not `www-test.ourcompany.com`
`server[!0-9].ourcompany.com` would match :

`servers.ourcompany.com` but not `server3.ourcompany.com`

Note
The !, -, and ^ are special characters only if they are inside brackets [ ]. To be a negation operator, ! or ^ must be the first character in the brackets [ ].

Exporting Reports

You can export (save) WebMarshal Reports in a variety of formats, as provided by the Crystal Reports engine. The presentation quality varies depending on the format selected. In general, the best formats to use are: Crystal Report, DHTML, text, Excel, and RTF.

Start the Export by right-clicking on the report name and choosing **Export**, or by clicking the **Export** icon from the report window tool bar.

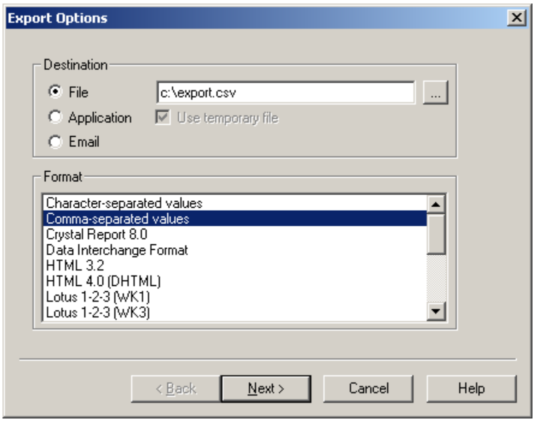
Drill-down pages are only available in the Crystal Report 8.0 export format. All other export formats show only the main report view.

Export Options

You can open the Export Options window in three ways:

- Select **Export** from the report window.
- Right-click a report name.
- Right-click a report name and choose **Export Options**.

The options selected are retained as the defaults for the report instance.



Export Options

Destination

● File c:\export.csv

○ Application ☑ Use temporary file

○ Email

Format

Character-separated values

Comma-separated values

Crystal Report 8.0

Data Interchange Format

HTML 3.2

HTML 4.0 (DHTML)

Lotus 1-2-3 (WK1)

Lotus 1-2-3 (WK3)

On the first page of the Export Options window, choose how to create the export:

- **File** saves the export as a file. A name will be entered by default. To select a specific name, use the browse button or type a file name in the field.
- **Application** opens the export directly in the required application (such as Internet Explorer or Lotus 123). Uncheck the **Use Temporary File** box to save the data in a permanent file as well.
- **Email** attaches the exported data to an email message using the default email application.

Depending on the type of export chosen, additional options may be available.

Email Options

The report can be attached to the email as a file of the type chosen on the export options page.

- **Send to**: Enter the email address to which the message should be sent.
- **Copy to:** Optionally enter an email address to which the message should be CC'd.
- **Subject:** Optionally enter a subject for the email message.
- **Message:** Optionally enter a message body describing the attachment.

HTML Options

- **Generate navigation buttons:** Add links at the bottom of each page to jump to the first, next, previous, or last page of the report.
- **Create all output on one page:** Use one HTML document for all output. Page divisions will be indicated graphically.

Pagination Option

- **Lines per page:** set the number of output lines between page break characters, using the spin box. This option is used for export of a report to paginated text.

Separator Options

These options are used when creating a values text file (character separated values, comma separated values, data interchange format, and tab separated values).

- **Format numbers as in report:** Numbers are output with text formatting (such as comma separation of thousands). If this option is unchecked, numbers are output in a basic format.
- **Format dates as in report:** Dates are output with text formatting. If this option is unchecked, dates are output in a basic format

The following additional options are available for character-separated values only:

- **Field separator:** The character (or characters) marking the boundary between two fields. In addition to printable characters, special separators include:

Separator	Description
\t	Tab
\n	New line
\r	Carriage return
\0	Null character
\	Backslash (\)
\xXX	Any character (two hexadecimal digits)

String delimiter: the character (or characters) marking the beginning and end of field text. The same choices are available as for field separators. This field may also be blank, in which case no delimiter is inserted.

Chapter 9

Managing WebMarshal Configuration

The WebMarshal Console allows control of several advanced features. These include:

- Detailed setup of processing options for the WebMarshal installation
- Detailed setup of Server Groups and customized configuration of properties for each group
- Proxy Caching options
- Automatic configuration backup and restore functions
- Console security settings
- The ability to join servers to the array
- The ability to start and stop WebMarshal Rule processing

WebMarshal also provides a filtered view of the Windows event logs, and makes performance counters available to the Windows Performance Monitor.

Configuring Server Properties

The Server and Array Properties window allows the administrator to modify properties that affect server operation. These are divided into a number of categories, each represented by an item in the menu tree of the window:

- **General:** View information about the WebMarshal version and the latest committed configuration; set session timeouts
- **Customer Feedback:** Anonymously send browsing history through WebMarshal back to Marshal8e6 to improve product quality and functionality
- **Licensing:** View current license status; enter license key
- **Email Notifications:** Set up sending of WebMarshal automated email
- **Configuration Backup:** Configure backup of the WebMarshal configuration on a nightly basis, or after every committed change
- **Advanced settings:** Configure logging level for WebMarshal services
- **Proxy settings:** Configure client and upstream connections
- **Proxy Cache:** Activate and configure the Proxy Cache feature
- **Download Options:** Configure thresholds for scanning-related delays
- **Traffic Logging:** Set up activity logging in text files
- **Database Logging:** Set up activity logging in the SQL database
- **Filtering List Schedule:** Configure update schedules for URL lists
- **HTTPS Content Inspection:** Create the Certificate required for HTTPS inspection, and enable or disable this feature
- **Connection Rules:** Enable or disable processing of this type of rule

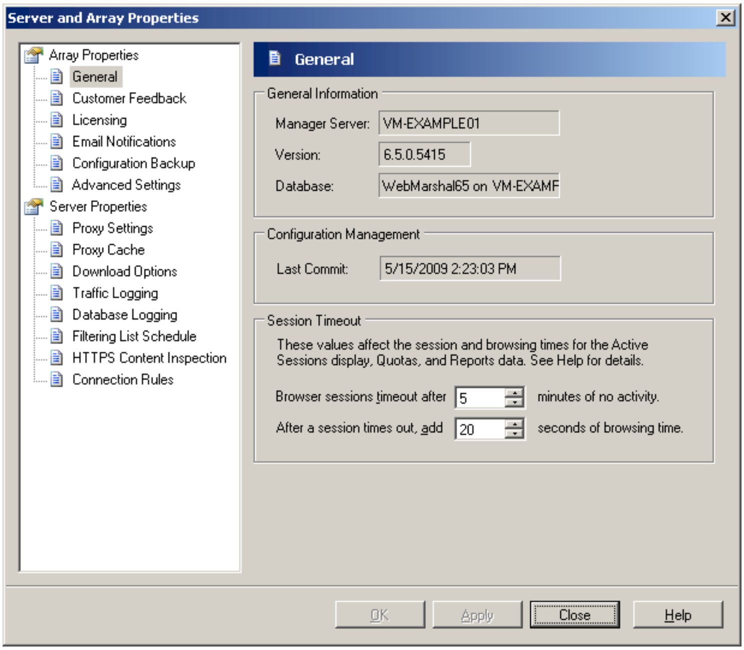
To access the Server Properties window, select **Tools > Server and Array Properties.** In most cases changes in this information require you to commit the configuration.

Note

You can also customize some settings for each Server Group in the WebMarshal installation. For more information, see "Configuring Server Group Properties" on page 244.

Viewing Product Information

The General window displays information about the Array Manager server, the product version installed, the time that configuration was last committed, and the session timeout values.



Manager Server: VM-EXAMPLE01

Version: 6.5.0.5415

Database: WebMarshal65 on VM-EXAMF

Last Commit: 5/15/2009 2:23:03 PM

These values affect the session and browsing times for the Active Sessions display, Quotas, and Reports data. See Help for details.

Browser sessions timeout after 5 minutes of no activity.

After a session times out, add 20 seconds of browsing time.

You can commit and revert configuration changes from the Console **Action** menu. You can back up and restore configuration from the Console **File** menu. See "Configuring Configuration Backup" on page 216 and "Working with Configuration" on page 236.

Session Timeout

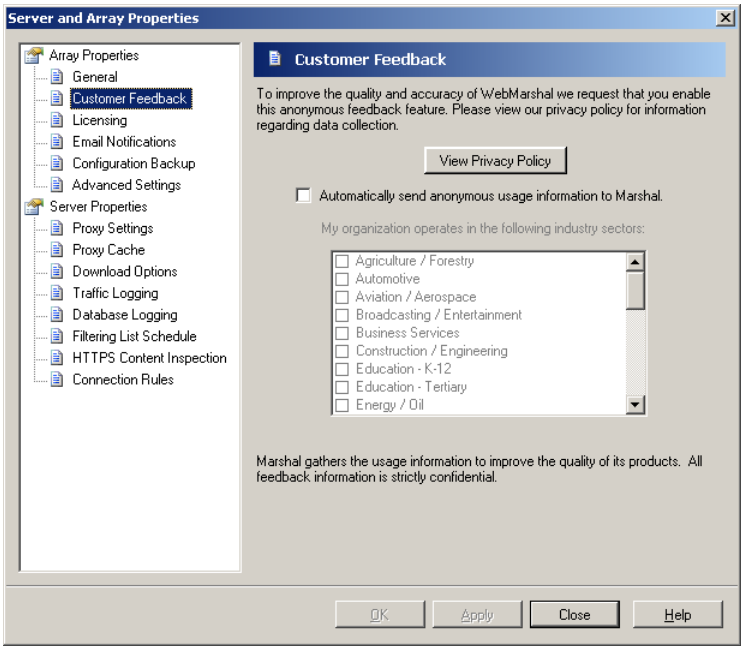
WebMarshal uses these value to calculate browsing time, time-based quota usage, session length, and visit length for Active Sessions and reporting.

- **Browser sessions time out after:** A session (and also a domain visit) is assumed to have ended if no new request is received within the time specified. The default is 5 minutes. Users who must enter a login to browse will have to re-enter it after this time.
- **After a session times out, add browsing time:** A user is assumed to be reading a page for some time after the last request. Enter the number of seconds.

For more details about these values and calculations, see Marshal8e6 Knowledge Base article Q11755.

Configuring Customer Feedback

The Feedback window allows you to configure WebMarshal to send anonymous summarized information about browsing history to Marshal8e6. Marshal8e6 uses this data to improve product quality and functionality. You can view additional information about this function by clicking the **View Privacy Policy** button.



Customer Feedback

To improve the quality and accuracy of WebMarshal we request that you enable this anonymous feedback feature. Please view our privacy policy for information regarding data collection.

□ Automatically send anonymous usage information to Marshal.

My organization operates in the following industry sectors:

□ Agriculture / Forestry
□ Automotive
□ Aviation / Aerospace
□ Broadcasting / Entertainment
□ Business Services
□ Construction / Engineering
□ Education - K-12
□ Education - Tertiary
□ Energy / Oil

Marshal gathers the usage information to improve the quality of its products. All feedback information is strictly confidential.

To configure feedback:

1. Review the privacy policy by clicking **View Privacy Policy**.
2. To enable sending of feedback, check the box **Automatically send...** To disable sending of feedback at any time, clear the box.

3. Optionally select the industry sector(s) of your organization.

4. Click **OK** or **Apply**.

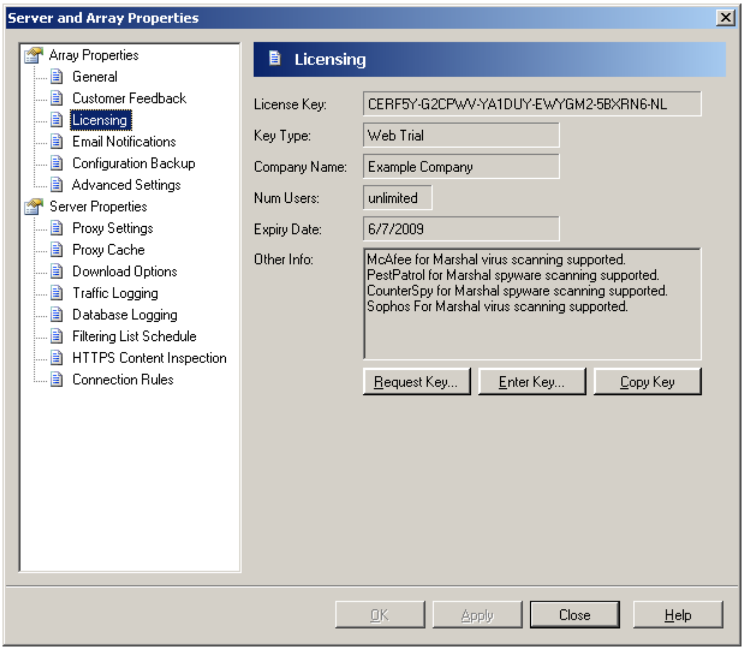
Note:
When Customer Feedback is enabled, WebMarshal summarizes browsing information and sends it to Marshal8e6 over HTTPS. Feedback is sent once a day between 12am and 1am. Feedback could be sent more often (if the number of items exceeds 100,000). WebMarshal performance is generally not affected by this process.

Configuring Licensing Information

The Licensing window displays information on the currently installed product key, including type, number of users, and expiry date.

Note

If the license key has expired, WebMarshal stops processing all rules. In this case all requests and responses are simply passed through. Users can access the Web with no limitations.



Licensing

License Key: CERF5Y-G2CPWV-YA1DUY-EWYGM2-5BXRN6-NL

Key Type: Web Trial

Company Name: Example Company

Num Users: unlimited

Expiry Date: 6/7/2009

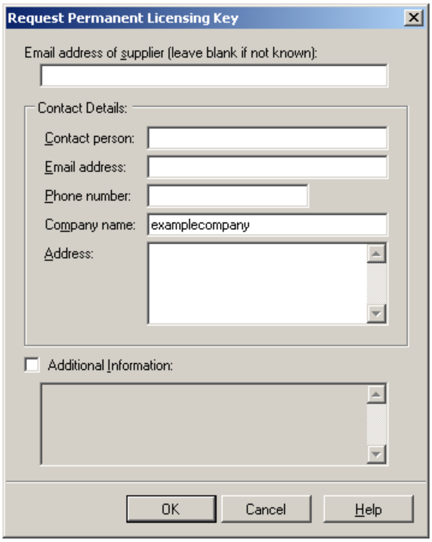
Other Info: McAfee for Marshal virus scanning supported.
PestPatrol for Marshal spyware scanning supported.
CounterSpy for Marshal spyware scanning supported.
Sophos For Marshal virus scanning supported.

To insert a different license key:

1. Click **Enter Key.**
2. Enter the license key and then click **OK**

To request a key:

1. Click **Request Key** to display the Request Permanent License Key window.



Request Permanent Licensing Key

Email address of supplier (leave blank if not known):

Contact Details:

Contact person:

Email address:

Phone number:

Company name: examplecompany

Address:

□ Additional Information:

2. Enter the appropriate contact information in the form. WebMarshal automatically appends the current key details.

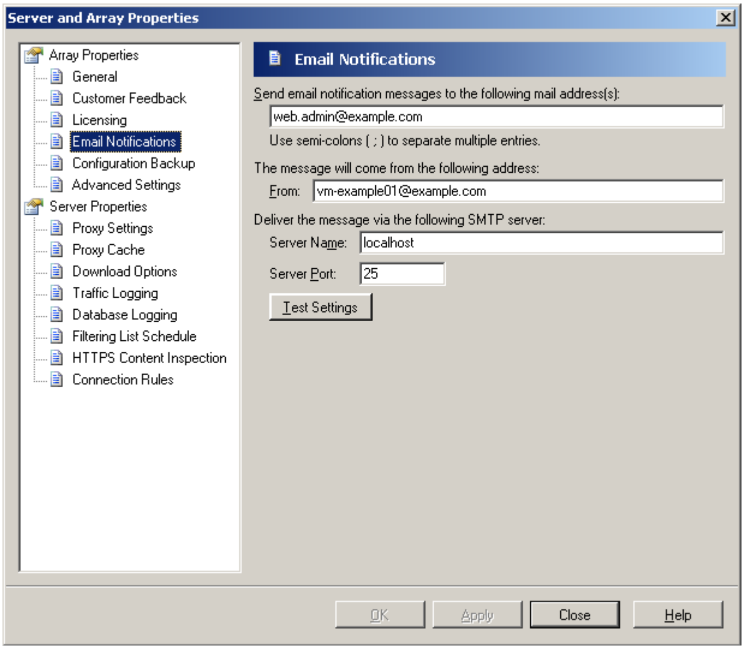
3. Enter any additional comments in the **Additional Information** field. This could include the number of new user licenses desired or a note that this is an upgrade from version 2.0 or below.

4. Click **Send Request** to send the data to Marshal8e6.

Tip
A HTTP connection to the Internet is required to send the data. This function does not depend on an e-mail server connection.

Configuring Email Settings for Notifications

The Email Notifications window allows you to configure the address and email server WebMarshal will use when sending email notifications to the administrator. These notifications include critical system problems, and alerts based on rule triggering.



Email Notifications

Send email notification messages to the following mail address(s): web.admin@example.com

Use semi-colons (;) to separate multiple entries.

The message will come from the following address:

From: vm-example01@example.com

Deliver the message via the following SMTP server:

Server Name: localhost

Server Port: 25

To configure notifications:

1. In the **mail addresses** field, enter the administrator's SMTP e-mail address. WebMarshal sends administrative e-mail notifications to this address. You can enter multiple addresses, separated by semi-colons. For example:

   ```
   postmaster@example.com; itsupport@example.com
   ```

2. In the **From** field enter the email address that will be used to send messages.

3. In the **Server Name** field to enter the IP address or name of an e-mail server that will accept the e-mail message for delivery to the administrator. This server must be accessible on the network from the WebMarshal server, and it must accept e-mail from the WebMarshal server for delivery to the administrator's address.
4. In the **Server Port** field, enter the port number used by the SMTP server to accept connections. The SMTP default is port 25.

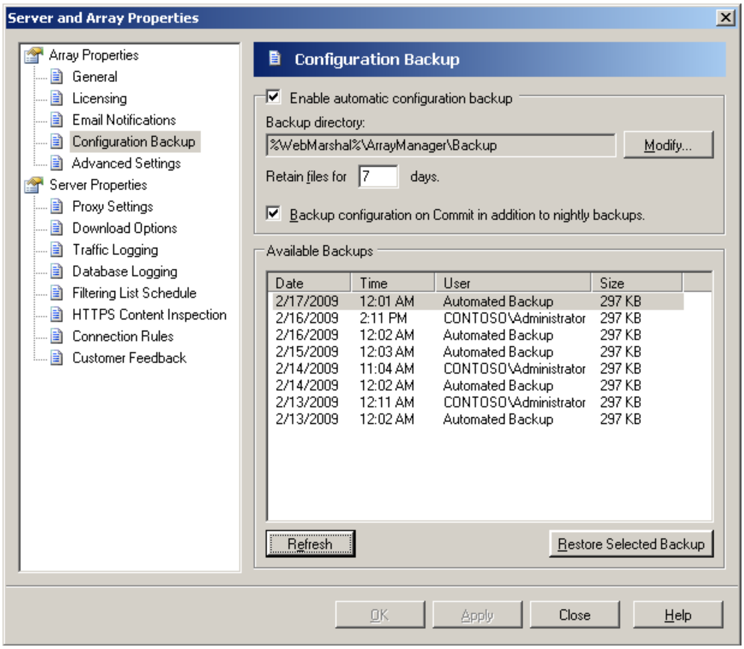
Click **Test Settings** to send a test e-mail to the administrator address. The test is successful if a message is delivered. If WebMarshal encounters a connection error, a notification displays at the Console.

Configuring Configuration Backup

The Configuration Backup window allows you to configure WebMarshal to automatically back up the configuration. The backup occurs each night after 12 o'clock if the WebMarshal Array Manager service is running. If the service is not running the Automatic Configuration backup will be created when the service becomes available again. The backup files created include the committed configuration, and not any changes made in the Console but not yet committed.

For additional information about backing up and restoring configuration, see "Importing and Exporting Configuration" on page 237.

You can also choose to back up configuration every time configuration is committed.



Configuration Backup

☑ Enable automatic configuration backup

Backup directory: %WebMarshal%\ArrayManager\Backup

Retain files for 7 days.

☑ Backup configuration on Commit in addition to nightly backups.

Available Backups

Date	Time	User	Size
2/17/2009	12:01 AM	Automated Backup	297 KB
2/16/2009	2:11 PM	CONTOSO\Administrator	297 KB
2/16/2009	12:02 AM	Automated Backup	297 KB
2/15/2009	12:03 AM	Automated Backup	297 KB
2/14/2009	11:04 AM	CONTOSO\Administrator	297 KB
2/14/2009	12:02 AM	Automated Backup	297 KB
2/13/2009	12:11 AM	CONTOSO\Administrator	297 KB
2/13/2009	12:02 AM	Automated Backup	297 KB

To configure Backup:

1. Check the **Enable automatic configuration backup** box.
2. by default the files are stored within the WebMarshal install directory. Optionally select a location for the backup files. For details, see Help.
3. Enter the number of days to keep the backup files. The default is 7 days.

The **Available Backups** section lists the available backups. To restore a configuration from a backup, select it from the list and then click **Restore Selected Backup**. To refresh the list of **Backups** click **Refresh**.

Configuring Advanced Settings

The Advanced Settings window allows you to configure the service logging level for each WebMarshal service. This window also allows you to set file size and retention options for the text logs, and control how often the processing servers check for updated policy.

Service Status Logs

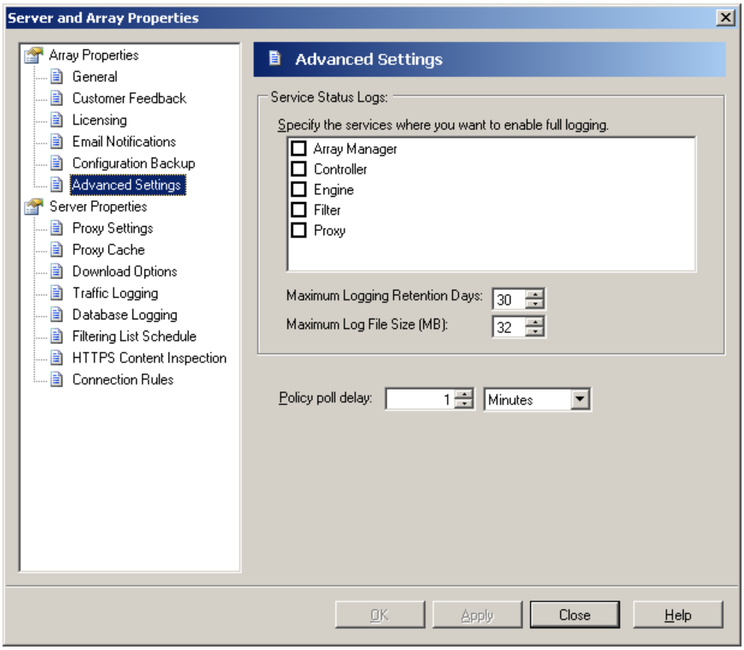
Service logs are text files on each server in the installation. By default these files include basic information about WebMarshal operation. You can choose to include full information if you need to investigate a specific problem.

Note
Including full information will cause the logs to grow more quickly. Only select this option when actively troubleshooting, and monitor disk space usage.

To configure logging level:

1. Select the services you want to configure for full (debug level) logging by checking the appropriate boxes.
2. To generate basic logs for a service, clear the box for that service.
3. Click **Apply** or **OK.** You will be reminded that you must commit configuration changes to make the logging change effective.

> **Note**
> You can also enable debug level logging for each service on each server by editing the individual ***`service`*** `.config.xml` files found in the installation folder (for instance, `WMEngine.config.xml`). Set the value of `debug fullTrace` to "true". Setting this value "true" in the file overrides the setting in the Options window.



Server and Array Properties

Advanced Settings

Service Status Logs:

Specify the services where you want to enable full logging.

- □ Array Manager
- □ Controller
- □ Engine
- □ Filter
- □ Proxy

Maximum Logging Retention Days: 30

Maximum Log File Size (MB): 32

Policy poll delay: 1 Minutes

To configure logging retention and size options, use the logging retention days and log file size fields. For more information, see Help.

Policy Poll Delay

WebMarshal processing services contact the Array Manager to check for policy updates (including group membership changes). By default the check is every 60 seconds. You can set a longer interval to reduce overhead, or a shorter interval to ensure that policy is up to date.

Note

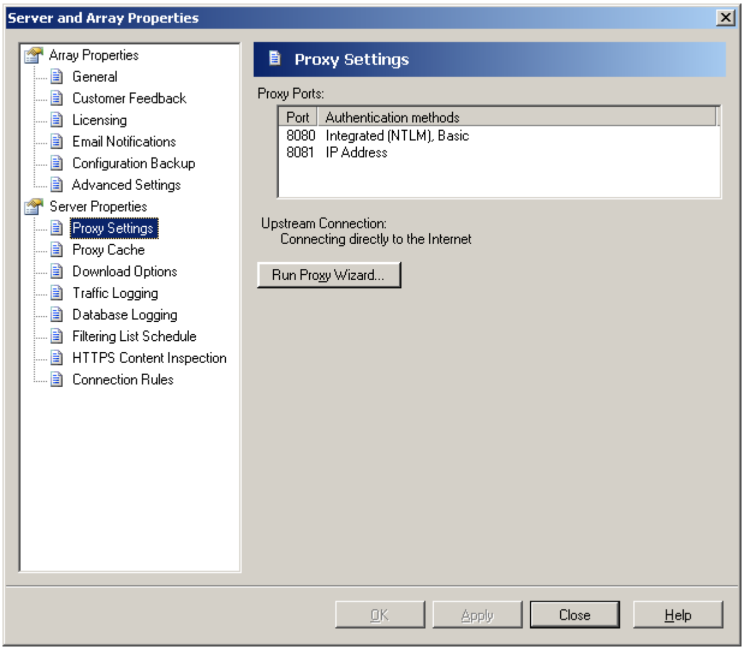
This setting affects single server installations as well as distributed arrays.

To set the policy polling interval:

1. In the **Policy poll delay** field, enter a time in seconds.
2. Click **Apply** or **OK.** You will be reminded that you must commit configuration changes to make the change effective.

Configuring Proxy Settings

The Proxy Settings tab displays information about the current proxy service settings.



Proxy Settings

Proxy Ports:

Port	Authentication methods
8080	Integrated (NTLM), Basic
8081	IP Address

Upstream Connection:
Connecting directly to the Internet

The information includes:

- Configuration as ISA Server plug-in or WebMarshal Proxy.
- Proxy ports (or IP Address:port combinations) on which WebMarshal is accepting requests for each authentication method.

Note
By default WebMarshal monitors each port on all available IP Addresses. If the server has multiple interfaces, you can specify IP Address:port combinations (for example, `10.1.2.3:8085`).

- Forward proxy information, including credentials, if applicable.

Click **Run Proxy Wizard** to start the Proxy Server Wizard, which allows you to view additional settings and change settings.

The initial pages in the Proxy Server Wizard are identical with the corresponding pages in the WebMarshal Configuration Wizard. For details of these pages, please see Chapter 3, “Installing WebMarshal.”

If WebMarshal is functioning as a standalone proxy, the wizard allows you to make changes in the LAT (Local Address Table), and it also includes two additional pages that are not present in the Configuration Wizard: HTTPS Connection Restrictions and Proxy Content Filter Bypass.

HTTPS Connection Restrictions

On this page, you can choose to allow non-standard HTTPS connections.

For details about the fields on this window, see Help.

Warning

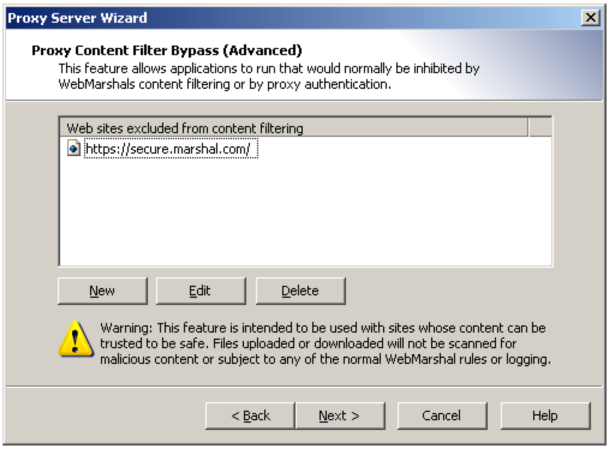
These settings should be used only to provide access to business-related secure sites with non-standard requirements. Caution is required as *no virus scanning or filtering will be performed on the sites in this list.*

Proxy Content Bypass

On this page, enter a list of web sites that you want to completely exclude from all WebMarshal Rules.

Warning

The intended purpose of this exclusion list is to provide clear access to sites required by non-browser applications that may be unable to connect through an authenticating proxy. Caution is required as *no virus scanning or filtering will be performed on the sites in this list*



Proxy Content Filter Bypass (Advanced)

This feature allows applications to run that would normally be inhibited by WebMarshals content filtering or by proxy authentication.

Web sites excluded from content filtering

https://secure.marshal.com/

Warning: This feature is intended to be used with sites whose content can be trusted to be safe. Files uploaded or downloaded will not be scanned for malicious content or subject to any of the normal WebMarshal rules or logging.

To add a new site:

1. Click **New.**
2. Enter a URL including protocol within the edit box.
   - To include a wildcard within a domain entry, use *. For example:

     `http://*.marshal8e6.com/`

     `http://www.microsoft.*/`
   - Only one wildcard character per entry is allowed.
3. Click **Enter** to accept the URL and open another editing line.

4. Press <Escape> to stop adding URLs.

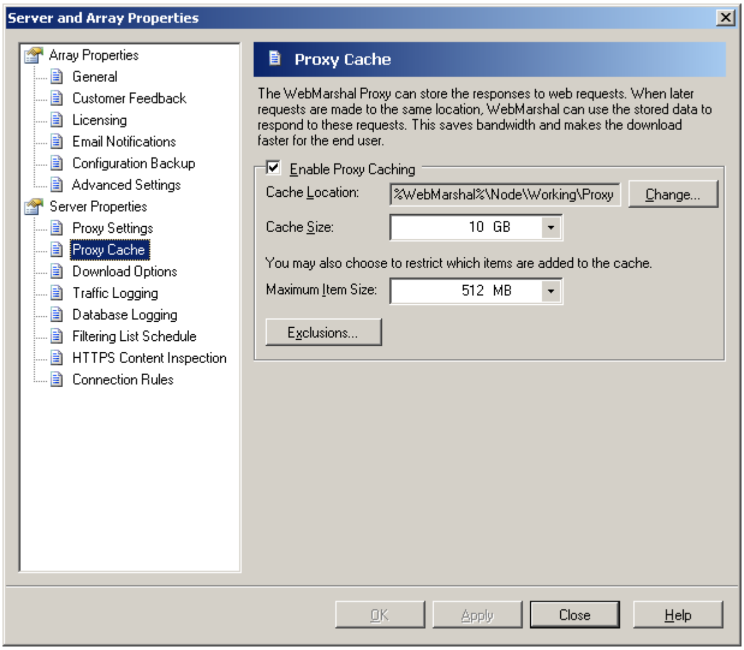
5. To edit or delete a site in the list, highlight it and then click **Edit** or **Delete.**

Configuring Proxy Cache

The Proxy Cache window allows you to configure the behavior of the WebMarshal Proxy Cache function. The Proxy Cache can save bandwidth and improve response time by storing regularly requested files locally. If a requested file is available in the cache WebMarshal serves the cached file and does not request a new copy.

Before you configure caching in a production environment, review Marshal8e6 Knowledge Base article Q12720, *Proxy Caching Recommendations*.

To review statistics for the cache, see the Cache Statistics section of the Real-Time Dashboard.



Proxy Cache

The WebMarshal Proxy can store the responses to web requests. When later requests are made to the same location, WebMarshal can use the stored data to respond to these requests. This saves bandwidth and makes the download faster for the end user.

☑ Enable Proxy Caching

Cache Location: %WebMarshal%\Node\Working\Proxy

Cache Size: 10 GB

You may also choose to restrict which items are added to the cache.

Maximum Item Size: 512 MB

To enable caching, check the box. Then configure the following options:

1. Set the cache directory location. The default location is within the WebMarshal install. *Most production installations should use a different location.*

   Note

   If you change the location, any existing cache files are not moved automatically. You can move the files manually. Stop the WebMarshal Proxy service while moving files, and be sure to copy the `cache.index` file as well as content files.

2. Set the maximum size of the cache. If you set up an array with more than one processing node server, the size applies to *each* server.

3. Set the maximum size of items that will be cached. You may want to limit the size if the available space for caching is limited.

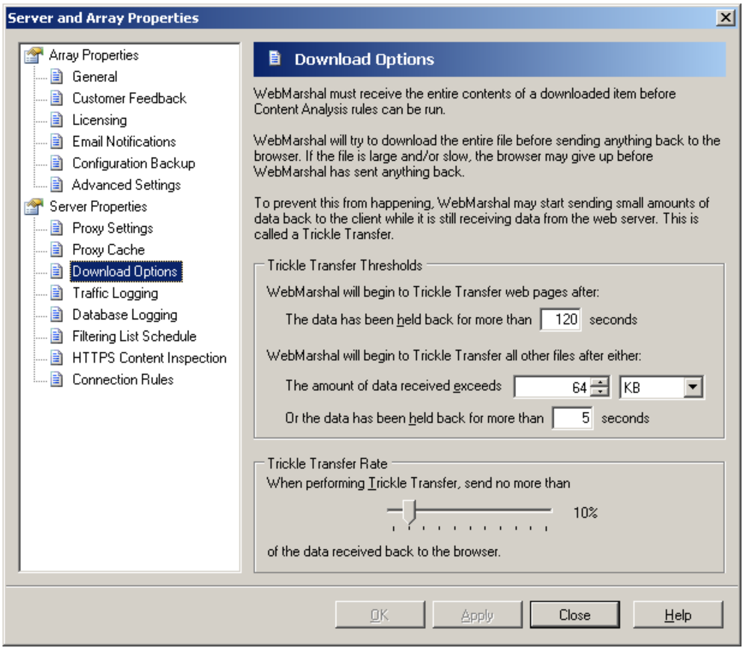
4. Optionally click **Exclusions** to open a window that allows you to enter a list of URLs that should never be cached.

   Notes

   - Caching is available for HTTP requests only (not for HTTPS or FTP).
   - Some sites do not correctly implement content expiration. Applying caching for those sites can mean that users do not receive the latest content. You should only add a site to the exclusion list if you experience problems with caching for the specific site. For details of the allowed syntax for the exclusion list, see Help.

Configuring Download Options

The Download Options window allows you to configure WebMarshal's behavior during Content Analysis scanning.



Download Options

WebMarshal must receive the entire contents of a downloaded item before Content Analysis rules can be run.

WebMarshal will try to download the entire file before sending anything back to the browser. If the file is large and/or slow, the browser may give up before WebMarshal has sent anything back.

To prevent this from happening, WebMarshal may start sending small amounts of data back to the client while it is still receiving data from the web server. This is called a Trickle Transfer.

Trickle Transfer Thresholds

WebMarshal will begin to Trickle Transfer web pages after:

The data has been held back for more than 120 seconds

WebMarshal will begin to Trickle Transfer all other files after either:

The amount of data received exceeds 64 KB

Or the data has been held back for more than 5 seconds

Trickle Transfer Rate

When performing Trickle Transfer, send no more than 10% of the data received back to the browser.

WebMarshal must receive the entire contents of a particular file before evaluating the Content Analysis rules. For large files or slow connections, this delay can affect the user's experience. In some cases the browser software could abort the attempt.

Note

Full file scanning does not substantially increase total download times. Users will see downloads start slowly, "stall," then suddenly proceed to completion.

WebMarshal can return a small portion of the file ("trickle transfer") to the user when the file is delayed. You can configure when trickle will start, and how much of the file WebMarshal will deliver.

Notes

- Because the trickled information might be usable, or text in a trickled file might be offensive, security is enhanced by minimizing trickle transfers.
- If a content analysis rule triggers to block a file after trickle transfer has started, the download to the user is aborted. WebMarshal presents a "file aborted" notice page to the user at the next opportunity. This is typically when the user next requests a web page.
- In addition to the settings on this window, you can exclude safe file types or MIME types from scanning using rule conditions.

To configure Trickle Transfer:

1. Enter the minimum time WebMarshal will wait before starting trickle of text Web files.
2. Enter the minimum time WebMarshal will wait and the minimum amount of data WebMarshal must receive before starting trickle of non-text files.

   Note

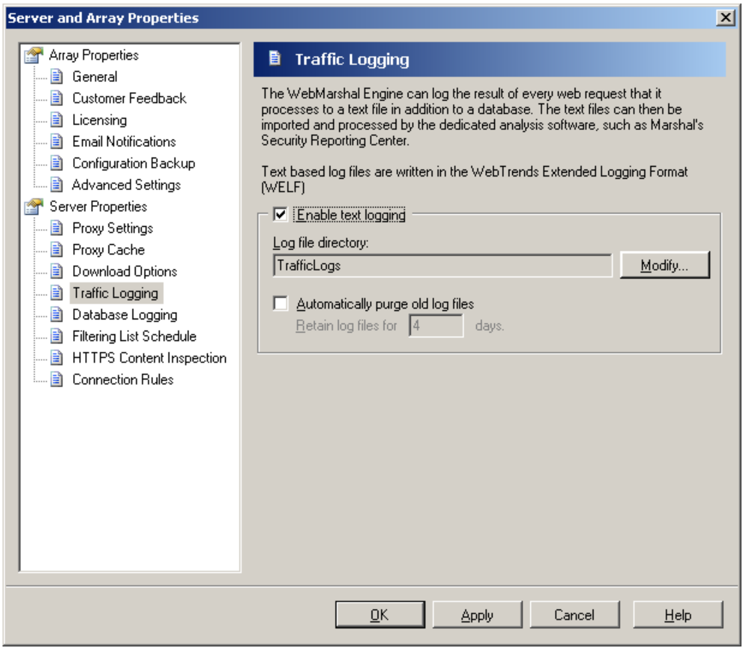
   For non-text files, the trickle will start if either of these thresholds is reached.

3. Use the Trickle Transfer Rate slider to control the maximum percentage of a downloaded file that is trickled to the user.

For more details of the settings, see Help.

Configuring Traffic Logging

The Traffic Logging window allows you to configure logging of Web requests to text files, for processing by dedicated analysis software (such as the Marshal Security Reporting Center). The currently supported format is WebTrends Extended Logging Format (WELF). Text logs primarily include information about each file request, and the rule that blocked the request if any



Server and Array Properties

Traffic Logging

The WebMarshal Engine can log the result of every web request that it processes to a text file in addition to a database. The text files can then be imported and processed by the dedicated analysis software, such as Marshal's Security Reporting Center.

Text based log files are written in the WebTrends Extended Logging Format (WELF)

☑ Enable text logging

Log file directory: TrafficLogs

□ Automatically purge old log files

Retain log files for 4 days.

To configure traffic logging:

1. Check the box Enable Text Logging.
2. By default, log files are created in the subfolder `TrafficLogs` within the WebMarshal install folder on each WebMarshal processing server. ***If you want to change the location,*** click **Modify,** enter the location in the *Modify Traffic Logging* window then click **OK.**

   Note

   The location must be on a local device. Network locations and mapped drives are not supported.

3. By default, log files are deleted after 4 days. To set a different policy for retention, clear the checkbox **Automatically purge old log files**, or change the value of the **Retain log files** field.

   Note

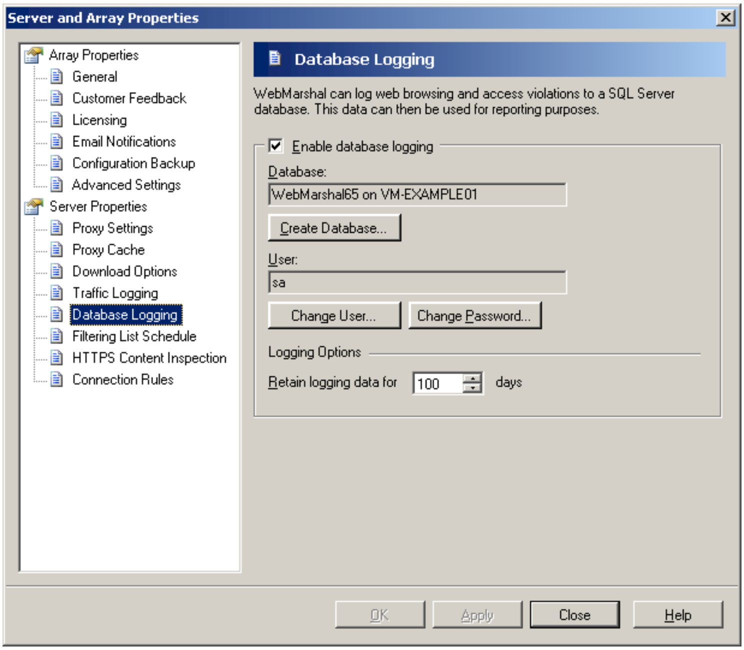
   Ensure that the disk location used for log files has sufficient free space to hold the files for the time you require. These files can grow large quickly.

4. Click **OK** or **Apply** to apply the changes. These settings are applied immediately and do not require you to reload the configuration.

For more details of these settings, see the Help.

Configuring Database Logging

The Database Logging window allows you to view and change the location of the optional WebMarshal reporting database, as well as data retention settings.



Database Logging

WebMarshal can log web browsing and access violations to a SQL Server database. This data can then be used for reporting purposes.

☑ Enable database logging

Database: WebMarshal65 on VM-EXAMPLE01

User: sa

Logging Options

Retain logging data for 100 days

To enable logging:

1. Check the box **Enable Database Logging.**
2. If you had previously enabled logging, the existing database name is displayed in the Database field. Click **Create Database** to create or select a database. For details of the Create Database window, see Help.
3. To use the database for logging and reporting, you can create a database user with limited rights. To start this process, click **Change User**. For details, see Help.
4. To change the password of the database user account, click **Change Password.**

To set data retention:

1. **Retain logging data:** Logs are only available for reporting for the number of days you specify in this field. Most organizations choose to retain logs for at least a month to give a reasonable interval for reporting. The default is 100 days.

Configuring Filtering List Updates

The Filtering List Schedule window allows you to configure automatic updates to any Filtering Lists configured in WebMarshal. The settings on this window affect the FileFilter, MarshalFilter, and Marsahl8e6Filter lists, but not URLCensor.

For more information about Filtering Lists and prerequisites for updates, see “Configuring URL Filtering Lists” on page 156.

To configure filtering list updates:

1. Check the box **Check for Updates every day** and select a time range to enable automatic checking of updates.

   Tip
   Automatic updates occur at a random time within the selected hour (to balance load on the update server).

2. Click **Update Now** to force an immediate check for Filtering List updates.

   Tip
   Updating can cause disruption for users browsing. This action should be performed at a time when it will have minimum effect.

Configuring HTTPS Content Inspection

The HTTPS Content Inspection window allows you to perform basic setup required to use HTTPS inspection in WebMarshal. You can generate a HTTPS Root Certificate and enable the HTTPS Content Inspection functionality.

HTTPS Content Inspection Concepts

HTTPS or “secure HTTP” is a protocol that allows Web applications to communicate over a secured channel (Secure Socket Layer, or SSL). HTTPS is designed to guarantee the identity of the remote web server, and to protect the data by sending it through an encrypted channel. This design makes it very difficult for intermediate devices (such as a proxy server) to view or change the data being communicated.

HTTPS guarantees the identity of a server by using a “certificate” that is issued to the server. The certificate is in turn guaranteed by an issuing authority. Web browser software typically hold a number of “root” certificates that it can use to determine whether the issuing authority for a server certificate is trusted.

HTTPS encrypts the data channel using a public-private key process. Data that is encrypted with the private key can be decrypted using the matching public key. The public key for a server is included in the server certificate. A web browser visiting a HTTPS site first requests the server certificate, and then negotiates the secure channel to the server based on this key.

WebMarshal can inspect HTTPS content as follows:

1. WebMarshal creates a unique Root Certificate for each installation. The Root Certificate guarantees the authenticity of other certificates that this WebMarshal installation creates.
2. You install the Root Certificate in each browser application on every workstation that will browse through WebMarshal.
3. When a user browses to a HTTPS site through WebMarshal, the WebMarshal server creates a certificate for that site, and returns it to the browser. The SSL connection between WebMarshal and the browser is based on this certificate.

4. WebMarshal connects to the requested site and retrieves the server certificate provided by the site. The SSL connection between WebMarshal and the server is based on this certificate.

5. **All communications are encrypted and secured**, but WebMarshal can inspect the content.

Warning

Although this method secures data in transmission, it raises a number of potential technical and legal issues for data privacy. You should carefully consider any applicable privacy laws and regulations before implementing this functionality. You should review the security of the WebMarshal processing servers. You should inform users about HTTPS content inspection as part of the terms and conditions of their web access.

WebMarshal access policy allows you to apply HTTPS content inspection selectively by user and by site. You may choose not to inspect the content of certain trusted and sensitive connections, such as online banking.

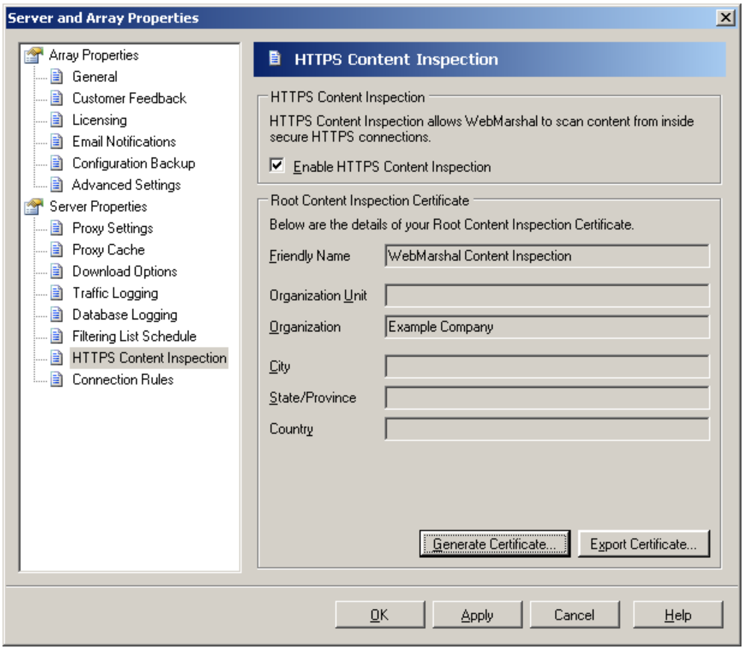
Content inspection **significantly increases the CPU load** on processing servers (due to decryption and encryption of content). Depending on the amount of HTTPS traffic that is inspected, you may need to improve the CPU specification of processing servers, or use more processing servers.

Generating and deploying a HTTPS Root Certificate

Before you enable HTTPS Content Inspection, you should ensure that the WebMarshal Root Certificate is available to all clients. Any client browser that does not have the Root Certificate installed will raise an invalid certificate warning each time the user browses to a HTTPS site.

To generate a Root Certificate:

1. On the HTTPS Content Inspection window, click **Generate Certificate**.



HTTPS Content Inspection

HTTPS Content Inspection

HTTPS Content Inspection allows WebMarshal to scan content from inside secure HTTPS connections.

☑ Enable HTTPS Content Inspection

Root Content Inspection Certificate

Below are the details of your Root Content Inspection Certificate.

Friendly Name	WebMarshal Content Inspection
Organization Unit	
Organization	Example Company
City	
State/Province	
Country	

2. On the **Generate Certificate** window, you can enter information in the fields. Most of the fields are optional and all required fields are populated by default. You can enter additional information to further identify the certificate. If you have already generated a certificate you will be asked if you want to overwrite it.

Warning

If you have deployed HTTPS Content Inspection, you should normally **not** generate a new certificate unless the old one has expired. When you generate a new certificate and commit configuration changes, the new certificate is immediately used by WebMarshal. You must ensure that the new certificate is installed on all client workstations.

To view the properties of the existing certificate, export it to a file and then double-click to view the details in Windows certificate management.

To deploy a Root Certificate:

1. To export the certificate (for instance, if you want to push the certificate to workstations using Group Policy), click **Export Certificate.** Select a location and name for the certificate file, and then click **Save.**
2. Ensure that all client browsers on all workstations have this certificate installed. You can install the certificate for Internet Explorer using Group Policy. You can install the certificate for other browsers using a link on the WebMarshal Home page. ***If Windows services also require Internet access,*** you may need to install the certificate in a special location. For more information, see Marshal8e6 Knowledge Base articles Q12014 and Q12015.

Enabling HTTPS Content Inspection

To enable HTTPS Rule processing, check the box on this window.

To disable HTTPS Rule processing, clear the box.

For more information about including HTTPS Rules in your Access Policy, see Chapter 6, "Understanding Web Access Policy, Rule Containers, and Rules."

Configuring Connection Rule Processing

The Connection Rules window allows you to enable or disable processing of Connection Rules configured in WebMarshal. Connection Rules allow you to identify and control traffic from many popular Instant Messaging and Streaming Media applications.

Notes

- In order for Connection Rules to be effective, you must ensure that other ports used by these applications are blocked at the firewall. For more information, see Marshal8e6 Knowledge Base article Q12021.
- Connection rules cannot be used when WebMarshal is installed as a plug-in to ISA Server. Console items related to Connection Rules will be removed or disabled if ISA plug-in is enabled.

To enable Connection Rule processing, check the box on this window.

To disable Connection Rule processing, clear the box.

For more information about including Connection Rules in your Access Policy, see Chapter 6, "Understanding Web Access Policy, Rule Containers, and Rules."

Working with Servers

Right-click the **WebMarshal** server icon in the left pane (or use the **Action** menu) to access the following functions:

Connect to Server

This option opens a window that allows you to connect to any WebMarshal array manager on the local network. Enter the server name, or click the browse button to find the desired server. You can also enter a user name and password with permission to connect.

Working with Configuration

You can use the WebMarshal Console to review basic configuration by re-running the WebMarshal Configuration Wizard.

You can use the Console to commit and revert configuration changes. You can also use the console to export (back up) and import (restore) configuration files.

Re-running the Configuration Wizard

If you want to review all basic configuration settings, you can re-run the WebMarshal Configuration Wizard. For details of the settings available through this wizard, see "WebMarshal Configuration Wizard" on page 29.

To re-run the Configuration Wizard, from the Tools menu of the Console select **Re-run Configuration Wizard.**

You can also set advanced proxy settings using the WebMarshal Proxy Wizard. For details of this wizard, see “Configuring Proxy Settings” on page 221.

Committing and Reverting Configuration

You can commit WebMarshal configuration changes. You can also revert *uncommitted* changes in the Console.

To commit changes, on the Action menu, select **Commit Configuration.** Changes are saved and queued for sending to the processing servers.

To revert to the previous committed configuration, on the Action menu, select **Revert Configuration.** The copy of configuration in the Console is returned to the last committed state.

Notes

- You can only revert once. Selecting **Revert Configuration** more than once has no effect.
- You cannot use **Revert Configuration** to undo committed changes.

Importing and Exporting Configuration

You can export WebMarshal configuration to a text (XML) file. Export files are useful for backup and can also be used to copy configuration between servers.

To back up configuration:

1. On the **File** menu, select **Export Configuration.**
2. When the backup file has been created, select a location and click **Save** to save the file.

Notes

- Backup can take several minutes, especially if a large number of users have been imported. WebMarshal saves information about each imported user that is used in a WebMarshal User group.
- To back up configuration regularly, you can use the automated configuration backup settings. See "Configuring Configuration Backup" on page 216.

To restore configuration:

1. On the **File** menu, select **Import Configuration.**
2. Select the file to restore, and then click **Open.**

When the restore process is complete, you are notified. Click **OK** on the notification window to continue.

Backing Up Configuration From The Command Line

WebMarshal also includes a command line backup tool that you can use to create a backup of the WebMarshal configuration. The command line backup tool can be used in conjunction with the scheduled tasks feature of Windows, so a backup of the WebMarshal configuration can be created at a predetermined interval.

The tool is named `ConfigBackup.exe` and it is found in the WebMarshal installation folder.

To run the tool from the command line, use the following format.

```
ConfigBackup.exe <file name> [/server <server>[:<port>]]
  [/user /password]
```

Parameters:

`<file name>`: The output file (required).

`/server`: The name (and optional port number) of the server running the WebMarshal Array Manager. Defaults to the current machine using the standard port.

`/user`: The user name to use when connecting to the server. Defaults to using the currently logged on user if not specified.

`/password`: The password for the user.

Note

You can run this tool from any computer. The tool requires Microsoft .NET Framework 2.0, and the following files from the WebMarshal installation folder:

- `ConfigBackup.exe`
- `Marshal.Remoting.dll`
- `WMRemoting.dll`

Working with Rules

Right-click **Access Policy** for a context menu with the following options:

Test Policy

Accesses the WebMarshal policy testing window. For more information on this window, see "Testing Access Policy" on page 133

Enable Rule Processing

Begins applying WebMarshal's list of rules to Web requests processed by the WebMarshal Server.

Disable Rule Processing

Ceases applying WebMarshal's list of rules to Web requests processed by the WebMarshal Server. This option will normally be selected only for troubleshooting purposes.

Configuring WebMarshal Security

You can control access to the WebMarshal Console and Array Manager.

To configure access to Console and Array Manager features:

1. On the Array Manager server, run the WebMarshal Security Tool found in the WebMarshal section of the Windows Start menu.
2. This application displays a list of users and groups with permission over Console and Array Manager features. By default all members of the Windows Administrators group on the WebMarshal server or Array Manager are allowed full permissions over all items that are secured through this tab.

Notes

When installing WebMarshal on a Microsoft Windows Vista or Windows Server 2008 machine it is important to note that if you are not using an administrators account you need to log off and then on again to ensure you are not denied access to the console. For more information see Marshal8e6 Knowledge Base article Q12136.

3. To add users or groups to the list, click **Add** then select groups or users using the Browse Network Users window. Each group or user you add is given full permissions by default.
4. To delete a user or group from the list, select it and click **Remove**.
5. To change permissions for a group or user, highlight the group or user name in the top pane. The lower pane shows the current permissions for this user. Set permissions for this user by selecting the appropriate boxes.
6. Repeat Step **6** for each group or user.
7. To save the changes, click **Apply** or **OK** at the bottom of the window.
8. To apply the changes, commit the configuration.

Available permissions include:

- **Full Access:** Includes all permissions.
- **Connect to Console:** Allows the user to run the WebMarshal Console.
- **View Policy:** Allows the user to view Access Policy and Policy Elements.
- **Modify Policy:** Allows the user to change Access Policy and Policy Elements.
- **Modify Array Membership:** Allows the user to add and remove Processing Servers from the WebMarshal Array.
- **Modify Security:** Allows the user to change security settings as described here.

Managing Array Servers

A WebMarshal installation consists of an Array Manager and one or more processing servers (also known as array servers or array nodes).

Managing Processing Server Services

You can view the status of the WebMarshal services on each processing server, and stop or restart the services, from the WebMarshal Console.

To see an overview of the status of services on each processing server, in the left pane of the Console click **Array Servers.**

To see details of the status of services on a particular server, and to stop or restart the services:

1. In the left pane of the Console click **Array Servers.**
2. In the right pane, select a server.
3. On the Action menu, click **Properties**.
4. On the general tab, the Services listing shows the status of each service installed on the server.

5. To stop one or more services, select them in the list then click **Stop.**

6. To start one or more services, select them in the list then click **Start.**

7. To restart all services, click **Restart all**.

Note
If you stop services from this window, they will remain stopped until you start them. Committing the configuration will not start the services.

Adding and Deleting Servers

You can add processing servers to a running WebMarshal installation when you want to add capacity or redundancy. You can also delete existing processing servers from an installation.

Adding a Processing Server

You can add a processing server at any time without affecting other servers. After adding the new server, adjust client settings so that it shares in web request proxying.

Note
Adding a server does not create automatic load balancing. You must set up load balancing outside WebMarshal.

To add a server to a WebMarshal installation:

1. Log on to the new server using an administrative account.

2. Install WebMarshal.

3. Choose to install the Processing Server only. During installation, enter the name of the existing Array Manager.

For more information, see "WebMarshal Processing Server Installation (on a separate computer)" on page 29.

Deleting a Processing Server

You should delete a server to cleanly remove it from the WebMarshal array. Before deleting a server, adjust web proxying so that the server you plan to delete does not process any requests.

To delete a server from a WebMarshal installation:

1. Stop the WebMarshal services on the server using the WebMarshal Console.
2. Uninstall WebMarshal on the server using the Add/Remove Programs application in Control Panel.
3. In the Console Array Servers view, an un-installed server will show a status of "not active." You can highlight the server and click the delete icon in the toolbar.

Joining a Server to an Array

You can join a processing server to a WebMarshal array. After joining the array, the server will retrieve policy configuration from the Array Manager.

To join an existing server to a WebMarshal installation:

1. Log on to the processing server using an account that has the WebMarshal permission, **Modify Array Membership**. (To set this permission, use the WebMarshal Security Tool on the Array Manager.)
2. Run the WebMarshal Server Tool found in the WebMarshal section of the Windows Start menu.
3. On the Server tab, from the Actions menu select **Add this server to an array.**
4. Enter the server name or IP address, and the WebMarshal port, for the Array Manager. Optionally enter credentials to connect. Click **Go** to make the connection. Click **OK.**

Configuring Server Group Properties

You can create groups of processing servers in your WebMarshal array.

You can configure different proxy connections and other settings for each group. You can also use Server Groups in rule matching to control which rules apply on each group. This feature allows you to localize configuration and rules for servers at different geographical or network locations.

You can customize the following settings for each Server Group:

- Local Address Table
- Ports and Authentication
- Forward Proxy Server
- Content Filter Bypass
- Proxy Cache
- Email Notification settings
- Advanced settings (service logging and policy polling)

For more information about the purpose of these settings, see “Configuring Server Properties” on page 208. For information about the fields and values, see Help.

To create a Server Group:

1. In the Console, select the Array Servers item.
2. Click the **New Server Group** icon in the taskpad to start the New Server Group wizard.

3. In the Wizard, give the group a name and select the servers that will be members of the group.

Note
If you select a server that is a member of another group, it will move to the new group.

4. Complete the wizard to create the new group. After creating the group, edit it to set configuration options for the group.

To edit a Server Group:

1. In the left pane of the Console, expand **Array Servers.**
2. Select the group you want to edit.
3. Click the **Server Group Properties** icon in the taskpad to open the Server Group Properties window.
4. Select the settings that you want to view and edit using the tree control at the left of the properties window. For help with the specific settings and fields, click **Help**.

Tip
The **Server Group Settings** item provides a quick overview of what types of settings are customized for the group.

5. When you have completed any changes, click **OK** to close the properties window.

To add a server to a Server Group:

1. In the left pane of the Console, expand **Array Servers.**
2. Select the group you want to edit.
3. Click the **Insert Servers** icon in the taskpad.

4. Select all servers you want to add to the group.

   Note
   If you select a server that is a member of another group, it will be removed from the other group and added to the group you are working with.

5. Click **OK.**

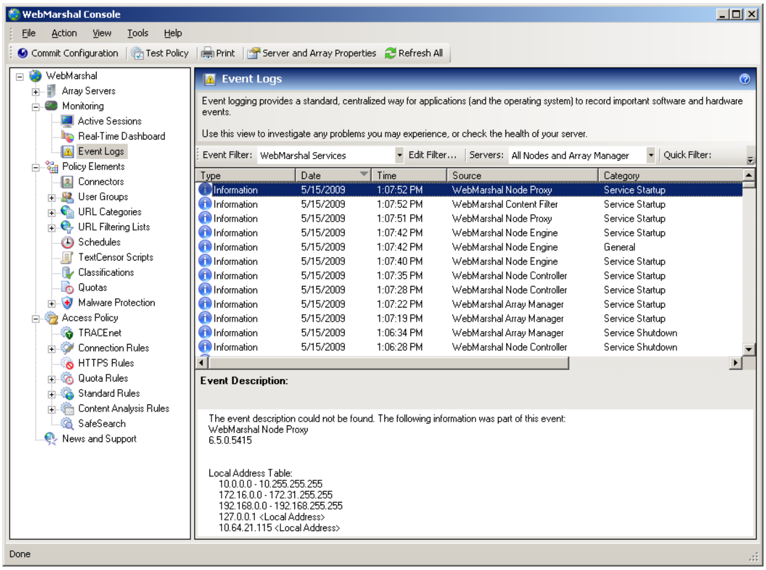
Viewing Windows Event Logs

The Event Logs item in the WebMarshal console (**Monitoring > Event Logs**) provides a convenient view of the Windows event logs for all servers in the WebMarshal array.

Event Logs have many uses, such as to monitor system health and expected events, to help with troubleshooting, and to monitor unauthorized connection requests.

You can easily filter the view so that it only shows items relevant to WebMarshal by selecting one of the preconfigured filters.

To display the full details of an entry in the lower pane, select the entry. You can also customize a filter, or limit the view to events containing specific text. For detailed instructions about the Event Logs view, see Help.



Event Logs

Event logging provides a standard, centralized way for applications (and the operating system) to record important software and hardware events.

Use this view to investigate any problems you may experience, or check the health of your server.

Event Filter: WebMarshal Services Edit Filter... Servers: All Nodes and Array Manager Quick Filter:

Type	Date	Time	Source	Category
Information	5/15/2009	1:07:52 PM	WebMarshal Node Proxy	Service Startup
Information	5/15/2009	1:07:52 PM	WebMarshal Content Filter	Service Startup
Information	5/15/2009	1:07:51 PM	WebMarshal Node Proxy	Service Startup
Information	5/15/2009	1:07:42 PM	WebMarshal Node Engine	Service Startup
Information	5/15/2009	1:07:42 PM	WebMarshal Node Engine	General
Information	5/15/2009	1:07:40 PM	WebMarshal Node Engine	Service Startup
Information	5/15/2009	1:07:35 PM	WebMarshal Node Controller	Service Startup
Information	5/15/2009	1:07:28 PM	WebMarshal Node Controller	Service Startup
Information	5/15/2009	1:07:22 PM	WebMarshal Array Manager	Service Startup
Information	5/15/2009	1:07:19 PM	WebMarshal Array Manager	Service Startup
Information	5/15/2009	1:06:34 PM	WebMarshal Array Manager	Service Shutdown
Information	5/15/2009	1:06:28 PM	WebMarshal Node Controller	Service Shutdown

Event Description:

```
The event description could not be found. The following information was part of this event:
WebMarshal Node Proxy
6.5.0.5415


Local Address Table:
   10.0.0.0 - 10.255.255.255
   172.16.0.0 - 172.31.255.255
   192.168.0.0 - 192.168.255.255
   127.0.0.1 <Local Address>
   10.64.21.115 <Local Address>
```

Event Log Filters

WebMarshal's Event Log view offers the following predefined filters:

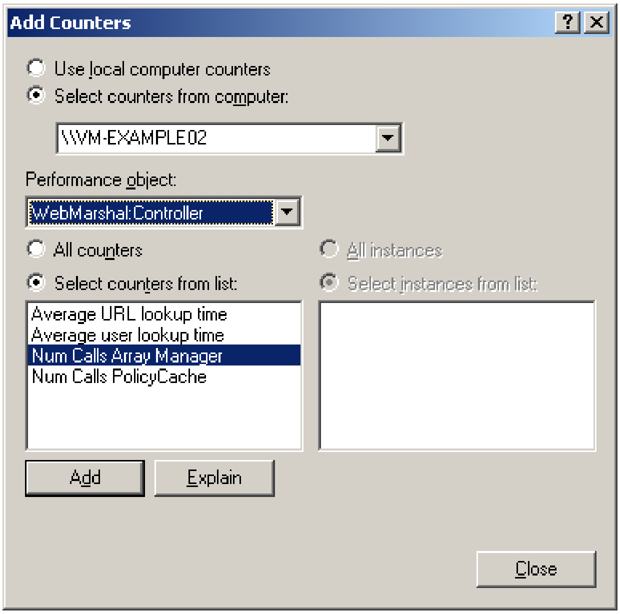
- **WebMarshal Services:** limits the view to events generated by WebMarshal.
- **Virus Scanner Services:** limits the view to events generated by virus scanners with WebMarshal DLL integration.
- **Spyware Scanner Services:** limits the view to events generated by spyware scanners with WebMarshal DLL integration.
- **Microsoft ISA Server Services:** limits the view to events generated by Microsoft ISA Server *(available if ISA plug-in is in use)*.
- **Application Event Log:** shows all events in the Windows Application Log.

- **System Event Log:** shows all events in the Windows System Log.
- **Custom Filter:** Allows you to select your own parameters to limit the view.

Viewing Windows Performance Counters

WebMarshal services provide a number of performance counters that you can use in the Windows Performance Monitor. Performance Monitor allows you to view a graphical display of performance in real time, or log data to a file. For more information on the WebMarshal performance counters please see Marshal8e6 Knowledge Base article Q11973.

You can start Performance Monitor from the Tools menu of the WebMarshal Console (or in the Windows **Administrative Tools**). Within Performance Monitor, click the + icon in the tool bar to open the Add Counters window.



Add Counters

○ Use local computer counters
● Select counters from computer:

\\WM-EXAMPLE02

Performance object:

WebMarshal:Controller

○ All counters
● Select counters from list:

Average URL lookup time
Average user lookup time
Num Calls Array Manager
Num Calls PolicyCache

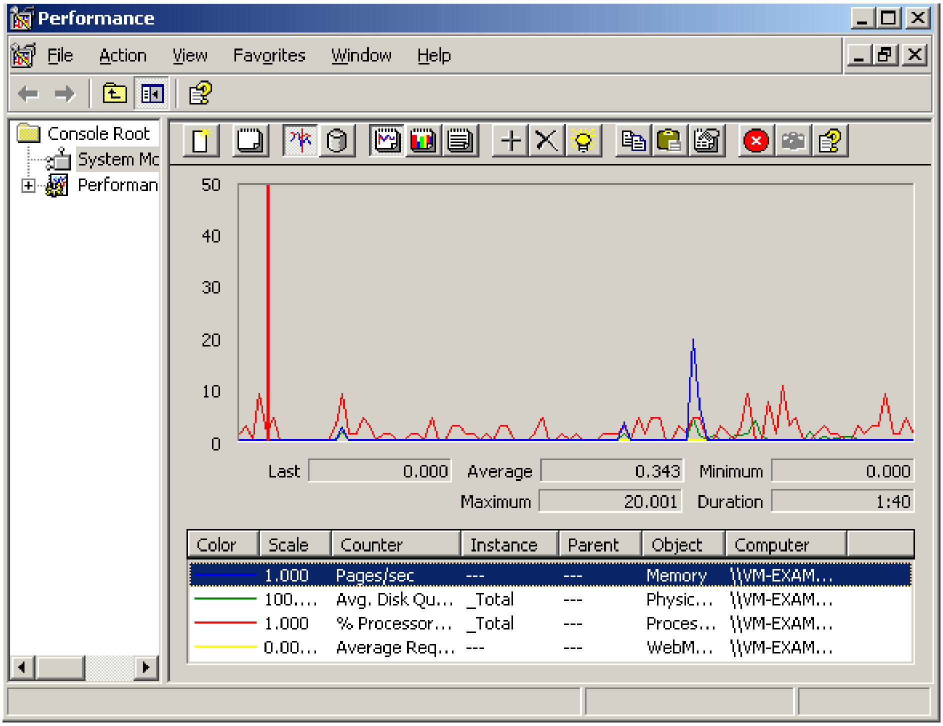
○ All instances
● Select instances from list:

You can choose to add counters from the local computer, or any other computer in the local network.

In the **Performance Object** drop-down box, you can select any of the following items to see a list of counters:

- WebMarshal Controller
- WebMarshal Engine
- WebMarshal Filter
- WebMarshal Proxy

Add the desired counters to the chart.



Last 0.000 Average 0.343 Minimum 0.000
Maximum 20.001 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
🟦	1.000	Pages/sec	---	---	Memory	\\VM-EXAM...
🟩	100....	Avg. Disk Qu...	_Total	---	Physic...	\\VM-EXAM...
🟥	1.000	% Processor...	_Total	---	Proces...	\\VM-EXAM...
🟨	0.00...	Average Req...	---	---	WebM...	\\VM-EXAM...

Please see the Performance Monitor documentation for full information on its capabilities, including monitoring of other computers.

Chapter 10
Troubleshooting

This chapter provides a list of resources you can use when analyzing problems with WebMarshal.

Windows Event Logs

If there are difficulties when starting the WebMarshal services, or there are any pop-up error messages, more information may be present in the Windows event logs. Open the Event Logs item in the WebMarshal Console, select an appropriate filter, and review the events. See "Viewing Windows Event Logs" on page 246 for details.

You can also open the Windows Event Viewer by clicking **Tools > Open Event Viewer** in the console, or from the Windows control panel.

WebMarshal Logs

WebMarshal services log configuration changes and activity in text files. By default these files are located in the Logging folder of the WebMarshal installation on each server. You can choose to enable more detailed logging. See “Configuring Advanced Settings” on page 218.

Note
To save disk space, the WebMarshal logging folders are compressed.

WebMarshal Dump Files

On rare occasions a memory dump file may be created in the WebMarshal installation folder. If your WebMarshal installation has encountered a problem, these files can help Marshal8e6 to resolve the issue. The file names have the extension `.mdmp.`

If a file of this type is present, contact Marshal8e6 Technical Support for assistance.

WebMarshal Support Tool

This tool gathers information about the WebMarshal installation and the server WebMarshal is installed on. Its purpose is to help the Marshal8e6 support team diagnose support issues. To use the tool, run `WMSupportTool.exe`, found in the WebMarshal installation directory. For more information on how to use the tool, see Marshal8e6 Knowledge Base article Q11886.

Some Common Issues

The following issues are often reported and have simple solutions.

- Rules are being ignored
- Problems using Web Browsers
- Problems with non-browser applications
- Warning Page Causes Some Websites To Fail
- Problems with Secure (HTTPS) Form Submissions
- Reports Issues

Rules are Being Ignored

- Ensure that the rule logic works as expected. Test the page which should trigger the rule using *Test Rules*. See "Testing Access Policy" on page 133 for details.
- Check that rule processing is enabled. Right-click **Access Policy** in the Console and select **Enable Rule Processing**.
- For ISA Server installations only: check that ISA Server is correctly configured to require authorization to access the web service.

Rules are being ignored when browsing from the proxy server (ISA Server only)

This problem occurs because security is managed differently for the interactive user. (The WebMarshal proxy service is able to compensate for this when run as a standalone server.) To work around the problem, test the rule processing using a browser on a different computer.

Problems Using Web Browsers

Users have to log on at the beginning of every browser session

WebMarshal requires users to be authenticated (log on) so that user matching Rules can work. Authentication can be by NTLM or Basic Authentication.

Some browser applications are not able to retrieve the credentials of the Windows user automatically. With these browsers the user must log in to start each session. In most cases users can choose to remember the password. To retrieve the Windows credential automatically, you can use Firefox or Microsoft Internet Explorer.

Users are unable to authenticate

When users try to access the web, they are repeatedly prompted to enter their user name and password.

Some browsers may support only Basic Authentication. This type of authentication involves passing a user name and password to the proxy server. The proxy server tries to perform a simulated logon to validate the credentials. If the user does not have logon rights on the WebMarshal server computer, logon fails repeatedly.

To resolve the problem, do one of the following:

- Use a browser that supports NTLM, such as Firefox or Microsoft Internet Explorer
- On the WebMarshal Server computer, grant the Windows NT permission “log on locally” to all accounts used for browsing

Problems With Non-Browser Applications

Rules which require that users accept a warning message before allowing access to a certain site are not acceptable to a non-browser based application. This is because the application requests a download but does not receive the expected file; instead it receives the WebMarshal warning message.

To resolve the problem, do one of the following:

- Create a rule to permit open access to the sites concerned
- Grant additional permissions to the users who are affected
- Set up IP/Workstation authentication for the workstations which run the non-browser applications
- Include the target site on the proxy server exclusion list (see "Configuring Proxy Settings" on page 221*)*

Warning Page Causes Some Websites To Fail

This usually happens when a site has off-site links, most often when posting a form. The problem occurs when a user enters data into a form and clicks the *Submit* button. WebMarshal presents a page that asks if temporary access is required. If the user clicks *Yes*, they find that the form data has not been correctly posted.

To resolve the problem, several actions are possible:

- Create a rule to permit open access to the sites concerned.
- Grant additional permissions to the users who are affected.

Problems with Secure (HTTPS) Form Submissions

When WebMarshal requires the user to acknowledge a warning before accessing a secure website, the user is redirected to the root page of the secure site.

Because the original request was submitted and replied to securely, WebMarshal does not have access to the details of the request and cannot return the page requested.

To resolve the problem, you can enable HTTPS content inspection.

If you do not want to inspect HTTPS content for the site, you can create a Standard Rule to allow access to the site. If you do not want to enable HTTPS content inspection, you can create a rule to allow access to all secure sites (HTTPS://*). This rule should be evaluated after any general blocking rules (for instance, a rule blocking offensive sites).

Reports Issues

These errors are most likely to occur where the default `SA` account is not used.

Unable to determine if [Name] is a valid WebMarshal database

This error indicates that the "GetVersion" stored procedure could not be run or returned an unexpected result. Generally this means that the database is not a WebMarshal database.

This error may also occur if the user does not have execution rights for GetVersion. To resolve this issue, connect to the database (from WebMarshal Reports) as a user with administrative rights. Once an administrator has used the reports database, all users are automatically granted the right to execute GetVersion.

SQL script could not be loaded

This error indicates that the user does not have sufficient rights to initialize the stored procedures in the database. If this occurs, connect to the database (from WebMarshal Reports) as a user with administrative rights. Select **Tools > Load SQL Scripts.** The result should be "SQL scripts successfully loaded."

SQL scripts failed to load. View errors?

Click **Yes** to see the Load Errors window (also available by right-clicking on the WebMarshal Reports root in the left pane of the MMC). This window provides the detailed error message. Most errors will be related to database permissions.

Further Help

For any problems not listed here, please see the Knowledge Base and Forum on the Marshal8e6 Website. If these resources do not resolve the issue please contact your Marshal8e6 supplier or Marshal8e6 Technical Support.

Web Home Page: http://www.marshal8e6.com/support

Email: support@marshal8e6.com

Chapter 11

WebMarshal and NDS

WebMarshal can import users and groups for authentication from Novell NDS.

NDS Integration Overview

The WebMarshal server retrieves NDS user information from a NDS tree. Additional details on how to use this connection can be found in “User Management” on page 138. At the client workstation, the account information can be entered manually at the start of a browsing session. WebMarshal also includes a utility to automate authentication from client workstations.

Server Considerations

Before configuring the Novell NDS connector, install the latest version of the Novell NDS client on the WebMarshal server. The latest version is always freely available from Novell’s website (http://download.novell.com/).

Public Access

Experience with the version of NDS included with NetWare has shown the following:

NetWare 5.x:

By default the [Public] account can browse all users and groups in the tree (unless the NDS administrator locks down the site).

NetWare 6:

By default the [Public] account can get a list of user groups but cannot retrieve the members of the list; therefore a user account is required to import users. Furthermore the user group ‘description’ is only available if the chosen account is an administrator.

It is possible to broaden the [Public] access to a NDS tree by adding permission for the [Public] account to access the ‘Group Membership’ property. This is performed from the ‘Tree’ item in ConsoleOne.

Logon Access

If an account logon to the NDS tree is required, remember that the Windows Novell client logs on as a Windows user as well. This user can be either a local account in your NT user database or a NT domain user. Therefore each NDS user actually has a dual identity. Most sites resolve this by creating an NT account and a NDS account with the same name and password.

NDS Limitations

The NDS client has a limitation in that it only allows *one* NDS logon per logged on NT user. This means for example that it is not possible to logon to NDS as ‘Bob’ and then run another application as ‘Bill’. By default, the WebMarshal engine service runs under the NT LocalSystem account. Because this is different to the NT account that is used by the interactive user, the engine should have the freedom to log in as any NDS account that it chooses.

It is not recommended therefore that you modify the account used by any of the WebMarshal services from the default of LocalSystem. If you did you could create the possibility of a clash between the interactive user and the WebMarshal services. (For example, when the interactive user logged out he might also log out the WebMarshal services from NDS as well).

NDS Name Conventions

By default NDS uses names as in the following example to refer to user and group objects in the tree:

```
CN=Bob.OU=Marketing.O=NewYork
```

WebMarshal also supports abbreviating this format to:

```
Bob.Marketing.NewYork
```

To convert from the shortened form back to the full form, WebMarshal uses the following rule: The left-most component (up to the period) is a CN=. The right most component is an O=. Everything in between is OU=.

Importing NDS Groups

If you import a user group, WebMarshal will fetch the members of that group. If you import an organizational unit (OU) or context (O) then WebMarshal will perform a directory search of all user accounts located in the tree under that object.

NDS Authentication in the Browser

Microsoft does not include any native support for transparent NDS authentication. Therefore, some user effort or additional configuration is required to authenticate using NDS.

Manual Authentication

By default, NDS users are prompted for a user name and password every time they open their browser (Basic Authentication). The pain of this can be eased in two ways.

- User names can be typed in shortened format. See “NDS Name Conventions” on page 261.
- Most web browser software provides a way to remember your user name and password so you only have to click **OK**.

Automatic Authentication

For Windows users, WebMarshal also includes a small utility called WMProxyLogon.exe. If this program is added to the logon script it will run as a system tray icon and periodically inform the proxy server of your NDS logon. While this program is running the user will not be prompted for authentication when beginning to browse.

By default the utility uses the current Internet Explorer settings so if Internet Explorer is not properly configured the logon procedure will not work. To override these settings see *Options* below.

Usage

Typically the WMProxyLogon.exe would be included as part of the all user logon script. The program is small enough that it can be run from its location on the WebMarshal server.

Double-click the system tray icon to see the current user information and/or exit from the program.

Options

WMProxyLogon.exe has the following command line options:

`/?` shows help information

`/Proxy:<server>:<port>` overrides the system settings and forces WMProxyLogon.exe to communicate with the stated proxy server. Note that the browser must still be configured correctly to use the proxy server.

`/NoIcon` disables display of the system tray icon.

Chapter 12

WebMarshal and Filtering Lists

WebMarshal can use the site categorizations provided by external Filtering Lists.

WebMarshal includes the Filtering Lists by default:

- **FileFilter** allows you to import URL lists from text files.
- **URLCensor** allows you to use a DNS Blacklist lookup as a source for URL categorization.

WebMarshal also supports the **Marshal8e6Filter List**, the **MarshalFilter List**, and the **SmartFilter** Filtering List provided by Secure Computing. These Lists are licensed separately. Contact Marshal8e6 for licensing information.

Technical Support

Technical support for all WebMarshal Filtering Lists, including the Marshal8e6Filter List and the Secure Computing software, is available from Marshal8e6. Contact your Marshal8e6 partner or see the Marshal8e6 website for more information.

FileFilter

FileFilter retrieves URL categorizations from files. The files must have the extension .txt and must be placed in the FileFilter directory within the WebMarshal Array Manager installation (`%WebMarshal%\ArrayManager\Policy\FilteringLists\FileFilter`).

FileFilter supports up to 256 categories. Each category must be maintained in a separate file.

Note
If there are more than 256 categories then they will not all be loaded by WebMarshal.

The file format is as follows:

```
[<Category> <Name>]
<Url>
<Url>
...
```

where:

`<Category>` is a unique integer that WebMarshal will use to record results of FileFilter categorization, such as: `101`

`<Name>` is the friendly name of the category, such as: `Porn`

`<Url>` is a protocol, domain name, and optional path.

All entries should have a trailing `/`

A domain entry matches all subdomains. For instance, `http://marshal8e6.com/` also matches `http://www.marshal8e6.com/`

Examples:

```
ftp://ftp.marshal.com/
http://google.com/
http://example.com/samples/test/
```

Several sample files are included with the WebMarshal distribution.

Note
Changes in the text files are loaded into WebMarshal once a day, on the reload schedule for filtering lists. To load changes sooner, use the **Update Now** button on the Filtering List tab of WebMarshal Properties, or commit WebMarshal Configuration.

URLCensor

URLCensor generates URL categorizations based on information retrieved in real time from DNS Blacklist facilities.

URLCensor can perform both traditional IP lookups (DNSBL) and domain name lookups (SURBL) as specified in the configuration file.

URLCensor requires the ability to perform DNS lookups for Internet sites from the computer and account used by WebMarshal.

Note
Delays in URLCensor lookups can noticeably affect user browsing experience. You can configure the timeout for these lookups. See Knowledge Base article Q12716.

You can configure the DNS lists used by URLCensor using the `config.xml` file found in the subfolder `\ArrayManager\Policy\FilteringLists\UrlCensor\`of the WebMarshal install path.

A sample entry in the file is as follows:

```
<category id="1" name="Spamhaus SBL"
       zone="sbl.spamhaus.org" enabled="1" type="ip">
  <description>Checks for domains in the Spamhaus SBL list.
       </description>
  <match>127.0.0.2</match>

</category>
```

where:

`id` is a unique integer that WebMarshal will use to record results of URLCensor categorization.

`name` is the friendly name for the source as it will display in WebMarshal interfaces and reports.

`zone` is the domain to query for the information

`enabled` indicates that this category should be used (1) or not used (0)

`type indicates what type of lookup this source supports:`

- **ip** indicates a DNSBL lookup. The domain name associated with the Web request is converted to an IP address before being passed to the blacklist query.
- **url** indicates a SURBL lookup. The domain name associated with the Web request is passed directly to the blacklist query.

`description` is a verbose description for documentation in this file only

`match` indicates the return value that is considered a match. This value can be a single dotted quad value, or a range expressed in the format x.x.x.x/nn

Note

To apply URLCensor configuration changes, restart the WebMarshal Node Controller service on each node (using the WebMarshal Server Tool or the Windows Services control panel).

MarshalFilter List

WebMarshal 6.X includes support for the MarshalFilter List server software (MarshalFilter). A separate trial license for MarshalFilter is provided with WebMarshal trial downloads. Existing customers can obtain a trial license by contacting Marshal8e6. To purchase a license, contact Marshal8e6.

Note
To start a trial of the Marshal Filter List, when you enable the list enter trial license key `WMMA`. You can enter this key once on a server. The trial is valid for 30 days from the time of installation. The trial cannot be extended.

Expiration and re-activation

If the MarshalFilter trial or customer account has expired, the local copy of the MarshalFilter database will no longer be updated. All filtering category queries will receive a response of "uncategorized" (the same response returned when the URL is not in the database). Effectively this will allow all Web requests.

An expired account can be re-activated by payment of the license fee to Marshal8e6.

Integration Information

Information on using the MarshalFilter List within WebMarshal is provided in "Understanding URL Categories" on page 151. Enabling and disabling Filtering List integration is covered in "Configuring Filtering List Updates" on page 231.

Prerequisites

The MarshalFilter software has the following prerequisites:

- 500 MB of available disk space (allowing for overhead while updating the database).
- Internet access (HTTP and HTTPS) from the Array Manager and all processing servers (to validate the license and download updates).

Note
Access can be direct or through a proxy server. For more information about configuring update access when WebMarshal is installed as a plug-in to ISA server, see "Updates Proxy Server" on page 40.

Checking and Reviewing MarshalFilter URL Listings

Marshal8e6 provides a web based service that allows you to check a specific URL against the most current categorizations in the master MarshalFilter database. You can learn whether the URL is categorized, and if so in which Filtering Categories. You can access this service in WebMarshal Console by selecting **URL Check and Review** from the **Tools** menu. You can also access the service from the WebMarshal Support area on the Marshal8e6 website.

Through this service you can also request that Marshal8e6 review the categorization of a specific URL.

If you want to allow some users access to a particular URL that would normally be blocked due to MarshalFilter categorization, set up a WebMarshal Rule allowing an exception for the required URL and allowed User Group.

Marshal8e6Filter List

WebMarshal 6.5 and above includes support for the Marshal8e6Filter List. The list contains 116 categories and is licensed from Marshal8e6 under the WebMarshal license key for the installation. A 30 day trial is provided with all trial versions of WebMarshal 6.5. Customers who are upgrading WebMarshal will also receive a 30 day trial. For information on how to purchase the filter list contact Marshal8e6.

Expiration and Re-activation

If your installation is using a WebMarshal trial key, when it expires the Marshal8e6Filter List will no longer update and will stop categorizing. If your installation is using a full Marshal8e6Filter List license and it expires the list will no longer receive updates. 30 days after the expiration date the filtering list will stop categorizing. An expired license can be re-activated by payment of the license fee to Marshal8e6.

Integration Information

Information on using the Marshal8e6Filter List within WebMarshal is provided in "Understanding URL Categories" on page 151. Enabling and disabling Filtering List integration is covered in "Configuring Filtering List Updates" on page 231.

Prerequisites

The Marshal8e6Filter List has the following prerequisites:

800 MB of available disk space on each processing node (allowing for multiple copies of the database while updating).

Ability to perform DNS lookups for Internet sites from the processing servers with the account used by WebMarshal.

Internet access (HTTP and HTTPS) from the Array Manager and all processing servers (to validate the license and download updates).

Note
Access can be direct or through a proxy server. For more information about configuring update access when WebMarshal is installed as a plug-in to ISA server, see“Updates Proxy Server” on page 40.

Checking and Reviewing Marshal8e6Filter URL Listings

To determine if a URL is listed in one or more categories, ensure that the Marshal8e6filter list is up to date in your WebMarshal installation, and then use the Test Access Policy function in the Console (**Tools > Test Policy**). Use the Browse Site option. On the Results tab, below the access result section, the section “Filtering List Categories” shows all categorizations for each active Filtering List.

To submit a URL for reconsideration, see the Submit a Site page on the Marshal8e6 website.

Secure Computing SmartFilter

WebMarshal 6.X includes support for the Secure Computing Filtering List server software (SmartFilter). The following sections provide information on licensing and setup.

Note
This software replaces the N2H2 Filtering List (Sentian CS). Upgrading to this version of WebMarshal disables N2H2. For more information, see the WebMarshal Release Notes.

Integration Information

Information on using the Secure Computing Filtering List within WebMarshal is provided in “Understanding URL Categories” on page 151. Enabling and disabling Filtering List integration is covered in “Configuring Filtering List Updates” on page 231.

Prerequisites

The Secure Computing Filtering List server software (SmartFilter) has the following prerequisites:

- 300 MB of available disk space on each processing server (allowing for multiple copies of the database while updating).
- Ability to perform DNS lookups for Internet sites from the processing servers with the account used by WebMarshal.
- Internet access (HTTP and HTTPS) from the Array Manager and all processing servers (to validate the license and download updates).

Note
Access can be direct or through a proxy server. For more information about configuring update access when WebMarshal is installed as a plug-in to ISA server, see “Updates Proxy Server” on page 40.

Obtaining a Trial License for the Secure Computing Software

1. Visit the Secure Computing Website.
2. Navigate to **Support > Downloads > Software and Evals > SmartFilter Evaluations.**
3. Select **WebMarshal.**
4. Click **Evaluate this product.**
5. Complete the form.
6. **DO NOT** download the SmartFilter software. All required software is included in the WebMarshal installation.
7. You will receive an email message containing the required Serial Number.

Enabling Filtering List integration is covered in “Configuring Filtering List Updates” on page 231.

Note
The trial is valid for 30 days from the time of installation. The trial cannot be extended.

Expiration and re-activation

If the Secure Computing trial or customer account has expired, the local copy of the Secure Computing database will no longer be updated. All filtering category queries will receive a response of “uncategorized” (the same response returned when the URL is not in the database). Effectively this will allow all Web requests.

An expired account can be re-activated by payment of the license fee to Marshal8e6.

Checking and Reviewing SmartFilter URL Listings

Secure Computing provides a web based service which allows you to check a specific URL against the most current categorizations in the master Secure Computing database. You can learn whether the URL is categorized, and if so in which Filtering Categories. You can access this service in the WebMarshal Console by selecting URL Check and Review from the Tools menu. You can also access the service from the link “URLChecker” on the Secure Computing home page (http://www.SecureComputing.com).

Through this service you can also request that Secure Computing review the categorization of a specific URL.

If you want to allow some users access to a particular URL that would normally be blocked due to Secure Computing categorization, set up a WebMarshal Rule allowing an exception for the required URL and allowed User Group.

Glossary

Access Control List (ACL). A table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file.

Acceptable Use Policy (AUP). Rules and regulations governing the use of organizational email and Internet browsing.

Active Directory. The directory service implemented in the Windows 2000 or later environment to store often accessed information. It contains information about users, groups, computers, organizational units, and domains.

Alert. An indication of a significant event. Alerts are generated by WebMarshal services.

Array. A group of WebMarshal processing servers that use the same policy.

Array Manager. A WebMarshal service that controls configuration for all processing servers in a WebMarshal array, and connects to the WebMarshal Console and database. Also, the server running the array manager service.

Attribute. Computer characteristic, typically defined by a registry key or value. In XML, an attribute is a name-value pair within an element tag.

Blended Threat. A software attack that employs more that one vector to deliver a threat. One example is an email message containing a link to a malicious URL.

Browser. A software application that allows a user to access content from the internet, notably the World Wide Web.

Browsing Session. See Session.

Cache. See Proxy Cache.

Classification. An entry written to the WebMarshal reporting database when a request triggers a rule or policy action.

Component. Individual part of a WebMarshal implementation that performs a specific function. For example, a processing server, array manager or database, are WebMarshal components.

Computer Name. A name that uniquely identifies a computer on a network. The computer name cannot be the same as any other computer or domain name on the network. The network uses the computer name to identify the computer and to allow other users to access the shared resources on that computer.

Console. Interface that allows you to edit web access policy, configure server settings, and monitor browsing activity and server health in real time. Intended to be used by web administrators, managers, and help desk personnel.

Cookie. Small data file saved to a Web browser cache area by a web site, to uniquely identify the browser on return visits to the site. Cookies allow 'remember me' functions and user behavior tracking.

Distinguished Name. An address format used to locate and access objects in an X.500 directory using the LDAP protocol. This format specifies the complete path to the object through the hierarchy of containers in a domain. Each distinguished name is unique. For example, in Windows 2000 or later, a user object with the common name J. Doe in the organizational unit container called Users on the domain marshal.com, might be represented as follows:

```
CN=JDoe,OU=Users,DC=Marshal,DC=com
```

DLL. A library of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions and a program accesses these functions.

DMZ. A part of a local network that has controlled access, both to the Internet and to the internal network of the organization. Servers that provide gateway services for an organization are typically located in a DMZ.

DNS. See Domain Name Service (DNS).

DNS blacklist. A service that provides an automated response through the DNS protocol. DNS blacklists typically attempt to list email servers that are associated with spamming, open relays, or other unacceptable behavior.

Domain Name Service (DNS). The Internet service that translates domain names into IP addresses.

Event. Any significant occurrence in the system or application that requires user notification or an entry to be added to an event log.

Event Log. A record of any event that happens on a server. Windows includes System, Security, and Application logs by default.

Extensible Markup Language (XML). A data tagging language that permits the storage and interchange of structured data.

Fault Tolerance. The ability of a product to respond to a catastrophic event (fault) that ensures no data is lost and that any work in progress is not corrupted.

Filtering List. A categorized listing of websites, maintained externally to WebMarshal.

Firewall. A security system that is placed between the Internet and the private network of an organization, or within a network, and only passes authorized network traffic.

HTTPS. Hypertext Transfer Protocol over Secure Socket Layer, or "secure HTTP". The standard method for secure encrypted Web browsing.

Hyperlink. An emphasized portion of text on a window that, when clicked, opens another document or window.

IIS. See Microsoft Internet Information Services (IIS).

ISA Server. See Microsoft Internet Security and Acceleration Server.

Lightweight Directory Access Protocol (LDAP). A network protocol designed to work on TCP/IP stacks to extract information from a hierarchical directory such as X.500. It is useful for searching through data to find a particular piece of information. An example of an LDAP directory is the Active Directory in Windows 2000 or later. Objects in an LDAP directory are identified by their distinguished names.

Load Balancing. The practice of dividing processing load between a number of identically configured servers.

Local Address Table (LAT). A list of IP addresses that belong to computers in the local network.

Local Area Network (LAN). A group of computers in the same place that are connected and typically have the same network operating system installed. Users on a LAN can share storage devices, printers, applications, data, and other resources.

MDAC. See Microsoft Data Access Components (MDAC).

Microsoft Data Access Components (MDAC). A set of network libraries and programming interfaces designed to allow client applications to connect to data providers such as SQL databases.

Microsoft Internet Information Services (IIS). A Web server application for Windows operating systems.

Microsoft Internet Security and Acceleration Server. A proxy and network edge application for Windows networks.

Microsoft Management Console (MMC). A common interface designed to host administrative tools for networks, computers, services, and other system components.

Microsoft SQL Express. A freely distributable limited version of SQL Server.

Non-browser Application. A software application without a direct user display interface, that accesses the Internet using Web protocols. Includes browser helper applications and also automation functions of other software.

Novell NDS. Netware Directory Services, the directory used to store information about elements of Novell networks. It contains information about users, groups, computers, and organizational units.

Processing Server. A computer in the WebMarshal array that accepts browsing requests and filters them, using the WebMarshal proxy and engine components.

Proxy Cache. A local copy of web documents and images that have been requested through a proxy server. When an item is requested, the proxy replies with the cached copy if possible, saving time and internet bandwidth.

Proxy Server. A computer that functions as a network gateway for particular content. Proxy servers can be used to filter requests, and also to improve access by keeping local copies of frequently used resources.

Quota. An allocation of browsing time or file size, permitted to a user or workstation over a specific interval.

Registry. A database repository for information about a computers configuration. The database is organized in a hierarchical structure of sub trees and their keys, hives, and value entries.

Regular Expressions. Search criteria for text pattern matching that provide more flexibility than simple wildcard characters.

Remote Procedure Call (RPC). A standard protocol for client server communication that allows a distributed application to call services available on various computers in a network.

Scalability. Ability to distribute loads across multiple servers, allowing for greater accessibility and balanced traffic.

Secure Socket Layer. the standard protocol to provide a secure transmission channel for Web browsing and other Interned communications, using public-private key encryption.

Server Group. A set of WebMarshal processing servers that have the same customized configuration settings and rule conditions.

Service Account. In Windows NT and Windows 200x, a user account that a service uses to authenticate with the operating system. The account must have the specific rights and permissions required by that service.

Session. A period of continual Web browsing activity by a user.

Snap-in. An administrative application component designed to be hosted by the Microsoft Management Console (MMC).

SQL Server. The Microsoft enterprise database server software.

Streaming Media. Video or audio transmitted over a network that users can begin to play immediately instead of waiting for the entire file to download.

Structured Query Language (SQL). A programming language used to retrieve information from a database.

TextCensor. The lexical analysis engine included in WebMarshal. TextCensor allows you to scan web pages, forms, and files for complex text content, using Boolean and proximity operators and numerical weighting.

TRACEnet. A proprietary service of Marshal8e6 that supplies "zero-day" updates for URL threat categories.

Visit. A set of webpage views by the same user on a single site or domain within a short period.

WELF. WebTrends Enhanced Logging Format. A well known format for proxy and firewall logs.

Wildcard Character. A character in a search pattern that represents a number of arbitrary characters within the text being searched.

X.500. A global, hierarchical directory service. For example, a domain controller hosting Active Directory on a network running Windows 2000 or later provides an X.500 directory service.

XML. See Extensible Markup Language (XML).

Index