Trustwave®

WebMarshal

October 2023

Legal Notice

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Format and Symbols	Meaning
<u>Crimson Underline</u>	A blue underline indicates a Web site or email address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
`Code`	Text in this format indicates computer code or information at a command line.
Italics	Italics are used to denote the name of a published work, the current document, or another document; for text emphasis; or to introduce a new term. In code examples italics indicate a placeholder for values and expressions.
[Square brackets]	In code examples, square brackets indicate optional sections or entries.
	Note: This symbol indicates information that applies to the task at hand.
	Tip: This symbol denotes a suggestion for a better or more productive way to use the product.
	Caution: This symbol highlights a warning against using the software in an unintended manner.

Table of Contents

List of Tables

List of Figures

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.

1.1 What Is WebMarshal?

WebMarshal is an employee Internet management solution, designed to promote responsible web use while providing protection from viruses, malware, confidentiality breaches, and downloading of non-business material. It provides an additional layer of security beyond what is offered by traditional Internet firewalls and proxy servers.

1.1.1 What Does WebMarshal Do?

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 is implemented as an authenticating proxy server for HTTP, HTTPS, and FTP protocols. WebMarshal can provide policy-based control of HTTP connection attempts from web browsers, as well as 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 malware checks, and file contents. WebMarshal can apply browsing time and volume quotas to limit web usage.

WebMarshal also 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 Trustwave SpiderLabs team.

In addition to the real-time content checking mentioned above, WebMarshal can also use the Trustwave Web Filter Database and URLCensor (a DNS based real time URL checking service).

To assist with bandwidth management, WebMarshal offers optional proxy caching for HTTP.

You can monitor details of current Web access sessions using the WebMarshal Console. You can install one or more copies of the Console on workstations in your network.

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 web based Marshal Reporting Console.

WebMarshal can also log activity to text logs in W3C or WELF format. You can analyze these logs with external tools.

You can install WebMarshal as a single server, or as an array of servers (at one or more locations) with a common configuration. WebMarshal supports installation on current versions of Windows.

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

1.1.2 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 Content Inspection is enabled, WebMarshal checks the protocol version and 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 malware, 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 the WebMarshal 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.

1.2 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 Marshal Reporting Console. WebMarshal supports the use of recent versions of Microsoft SQL Server. Smaller organizations can use the free Express editions of Microsoft SQL Server. For details, see "Additional Software" on page 24.

1.3 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:

- The Marshal Reporting Console is a web-based application that can be deployed to support reporting on WebMarshal and MailMarshal. 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 W3C or WELF format. You can use these text log files with external tools to produce reports that cover different types of proxy and firewall devices.

- WebMarshal can log activity using the Syslog protocol.

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.

2.1 Planning Checklist

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

Table 1: Planning checklist

☑	Step	See Section
☐	1. Learn about important WebMarshal concepts.	"Understanding WebMarshal Components" on page 18.
☐	2. 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 21.
☐	3. Ensure the computers meet the hardware and software requirements.	"System Requirements" on page 23.
☐	4. Choose the malware detection software to use with WebMarshal.	"Supported Malware Protection Software" on page 25.
☐	5. Collect installation information about your environment.	"Collecting Information for Installation" on page 26.

2.2 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.

Figure 1: WebMarshal components

WebMarshal
Processing Servers

WebMarshal
Array Manager

WebMarshal
User Interfaces

Console

Reporting Database
(Microsoft
SQL Server
or SQL Express)

Marshal Reporting
Console

Directory
Servers
(NT, AD,
Novell)

Web Browsers
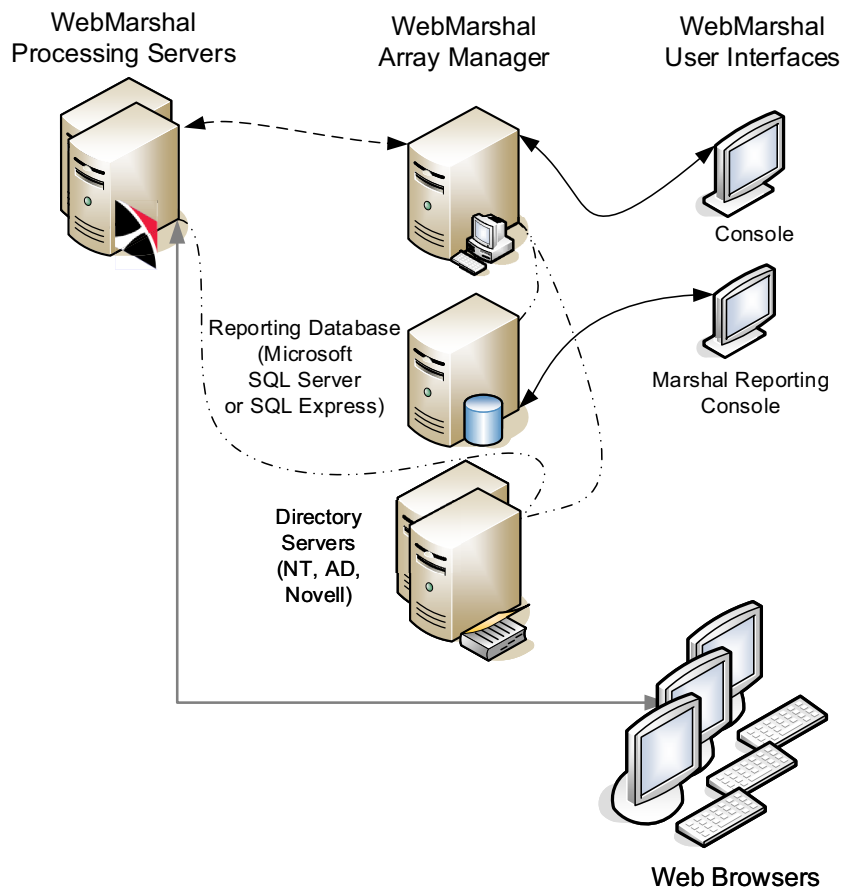
2.2.1 WebMarshal Components

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), 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 malware 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.

Marshal Reporting Console

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

2.2.2 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 the Marshal Reporting Console (MRC), 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 (this could be the SQL Express Advanced instance required by MRC). If the volume of data exceeds the 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, you can install one or more supported malware scanners. See "Supported Malware Protection Software" on page 25. 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 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.

2.3 Understanding Installation Scenarios

When planning a WebMarshal installation, you can use a single server for all functions, or an array of servers. You can install the WebMarshal Proxy Server in several scenarios.

2.3.1 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.

2.3.2 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.

Figure 2: WebMarshal proxy installation
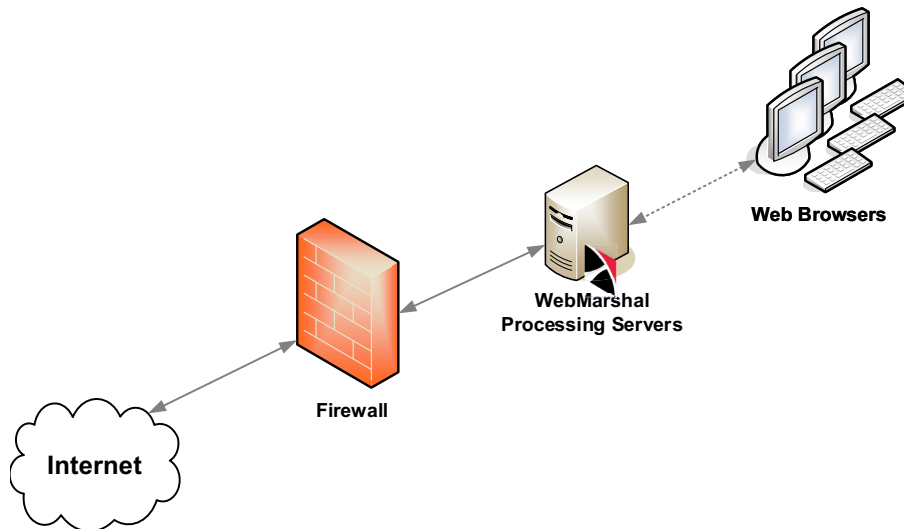
2. Chained to another proxy server running on another physical server. In this scenario, all Web requests are passed to the WebMarshal server. WebMarshal delivers the requests to the other server, and all responses are returned from the Web through the other server to WebMarshal and then to the clients.

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 usually 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 because the client cannot be determined.

- A proxy server or load balancer can be inserted before WebMarshal if it can forward the client credentials, or if it inserts an X-Forwarded-For header and you use IP based authentication (see Trustwave Knowledge Base article Q21183).

Figure 3: Separate server chained installation
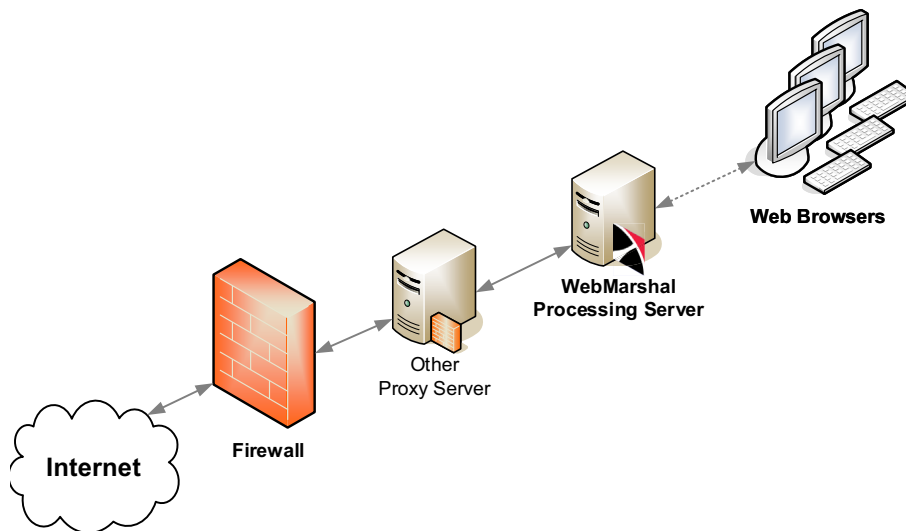
3. Chained to another proxy server running on the same physical server.

Figure 4: Same server chained installation
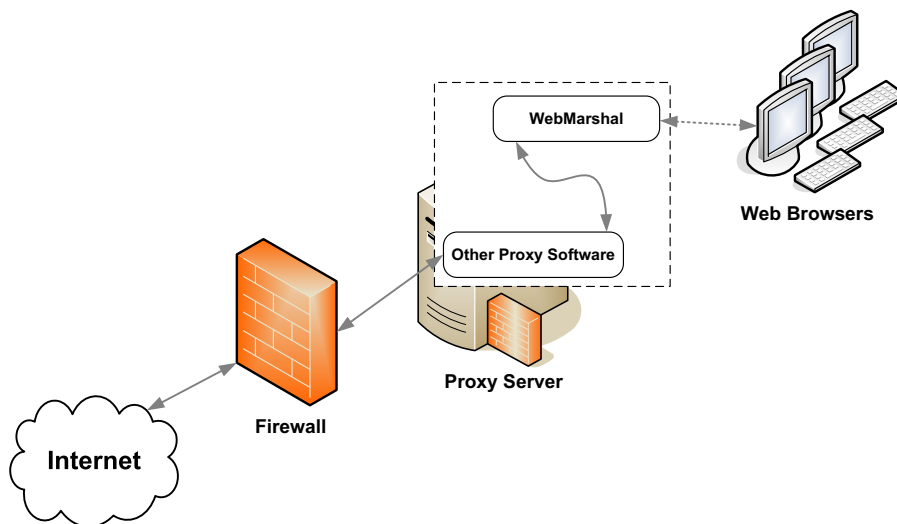
If WebMarshal is installed on the same server as another proxy server, each must use a different port. Configure WebMarshal using the WebMarshal Configuration Wizard or the Proxy Settings pages in WebMarshal Global Settings. Be sure the other proxy software is configured appropriately.

22

For example, WebMarshal could be configured to accept requests at the address 10.3.1.1:8080. The other proxy software might use 127.0.0.1:3128. The other proxy should only accept requests from WebMarshal.

2.4 System Requirements

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

Table 2: System requirements

Category	Requirements
Processor	**Minimum**: Dual core, 2 GHz
	Note: Use of HTTPS 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
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 Trustwave Knowledge Base article Q12720
	• Additional disk space will be required on each processing server if text logging is enabled
Memory	**Minimum**: 4 GB available to the application *(more if CRL checking is enabled)*
Supported Operating System	• Windows Server 2022
	• Windows Server 2019
	• Windows Server 2016
	• Windows 10 *(permitted but not recommended)*
	Note: WebMarshal does not prevent installation or upgrade on earlier Windows versions. However, Trustwave cannot provide technical support if you encounter issues with these earlier versions
Network Access	• TCP/IP protocol
	• External DNS name resolution to allow WebMarshal Servers to resolve Web addresses
Software	• Microsoft Visual C++ 2015 runtimes
	• Microsoft .NET 4.6.2
	Note: The above software will be installed as part of the WebMarshal installation if necessary. Installation of .NET might require system restart
	• Antivirus scanning software supported by WebMarshal. For more information, see "Supported Malware Protection Software" on page 25

Planning Your WebMarshal Implementation

Table 2: System requirements

Category	Requirements
Port Access *(IPv4 and/or IPv6)*	• **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 and 8181** (by default) and/or others as configured: To processing servers, from web browsers and other client applications. By default WebMarshal accepts authenticated connections on port 8080 and controls access by IP address on port 8081. • **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 Trustwave Knowledge Base article Q12207

Note: 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

2.4.1 Additional Software

Some scenarios require the following additional software:

• To enable database logging for the Marshal Reporting Console (MRC) application, use Microsoft SQL Server or SQL Server Express. You can use SQL 2014 (SP1 or above), 2016, 2019, or 2022. Apply the latest service pack.

Note: Be aware of the database size limitations set by Microsoft for SQL Express. Supported versions of Express allow databases up to 10 GB in size.

• The database can be located on any server accessible from the WebMarshal Array Manager component.

• With SQL Express, you can use the instance installed by the MRC installer. You can also install SQL Express during the WebMarshal installation from the "with SQL Express" version of the installation package, or download a standalone installer from the Trustwave website.

• To enable user authentication for Novell NDS users, the Novell client software must be installed on the WebMarshal Array Manager computer. The current version is Novell Client 2. The latest versions of this client support all Windows versions supported by WebMarshal and are freely available for download from Novell.

2.4.2 Supported Operating Systems for WebMarshal Console

The WebMarshal Console can be installed on the following Windows versions:

- Windows Server 2016

- Windows Server 2019

- Windows Server 2022
- Windows 10

2.5 Supported Malware Protection Software

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

Trustwave licenses several of the malware solutions directly. Licensing for these solutions is separate from the WebMarshal license. Trial versions of several malware solutions are included in the main product installer, or as downloads from www.trustwave.com

Note:

Note: The "spyware" scanners supported in previous WebMarshal versions are no longer available. The available scanners provide good protection against "spyware" type threats.

Symantec AntiVirus Scan Engine and Sophos Anti-Virus (SAVI interface) are not available with this release because the interfaces are not available in 64 bit format.

Customers using Sophos Anti-Virus (SAVI interface) can move to Sophos for Marshal and should contact Trustwave for details.

Kaspersky for Marshal is no longer sold. Signature updates end December 31, 2023.

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

Table 3: Supported malware scanners

Malware Scanning Application	Features
Bitdefender for Marshal	Antivirus
McAfee for Marshal	Antivirus
Sophos for Marshal	Antivirus

2.6 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.

Table 4: Environment information

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

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, and Console 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.

3.1 Setup Wizard

1. Run the WebMarshal installer 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.

    Note: You must install these prerequisites to continue with product installation.

    • Installation of .NET Framework may require system restart. As part of the .NET Framework installation you must accept a Microsoft license agreement.

    • Installation of the prerequisites does not normally interfere with any previously installed software.

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

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.

> **Note:** If the installer identifies a usable installation of SQL Server or SQL Express on the server, this page does not display.

   a. Accept the Microsoft EULA.

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

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

   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 the Marshal Reporting Console to connect from another server), this setup enables the Named Pipes and TCP/IP protocols. 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 159.

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.

11. If you are installing a Processing Server or Complete installation, on the Anti-Malware Scanners page, you can choose to install or update one or more anti-malware scanners included in the installation package.

Figure 5: Installation Wizard, Anti-Malware Scanners window
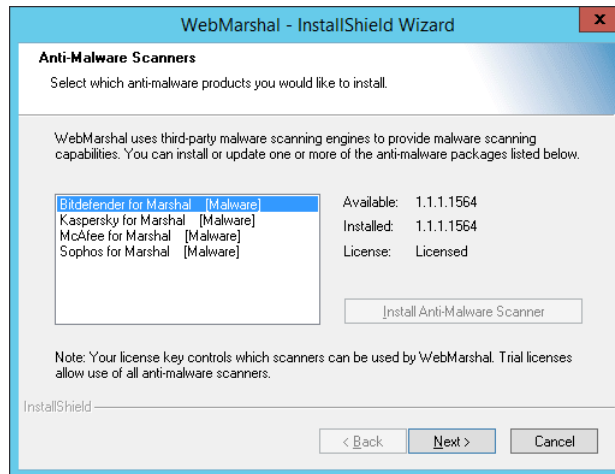
- The list shows available scanners. Select a scanner to view details of the available version, installed version if any, and licensing status.

- To install or update the selected scanner, click **Install Anti-Malware Scanner.**

- At the end of installation of the selected scanner, you can choose to configure scanner updates. You can also configure updates later by running the scanner configuration tool, found in the Web-Marshal program group on the Windows Start menu.

- Once installation of the selected scanner is complete, control returns to the WebMarshal installer. You can choose to install another scanner, or click **Next** to finish WebMarshal installation.

Note: To complete integration of the scanner with WebMarshal, add it from the Configuration Wizard, or the Malware Scanners item in the WebMarshal Console.

- WebMarshal checks the readiness of each scanner including initial download of updates. Configure and verify updates for each scanner **before** you add it in the Console.

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.2 WebMarshal Configuration Wizard

The first time you run the WebMarshal Console on a new installation, WebMarshal launches a wizard to gather configuration information needed to enable product functionality. For more information about the settings, refer to Chapter 9, "Managing WebMarshal Configuration."

Complete the required information on each page of the wizard, and then click **Next**. Where possible, the wizard attempts to discover details automatically

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

The Wizard process includes the following steps:

3.2.1 Select Configuration

This page of the Configuration Wizard offers three options for the initial configuration.

Select an option using the radio buttons:

Figure 6: Configuration Wizard, Select Configuration window
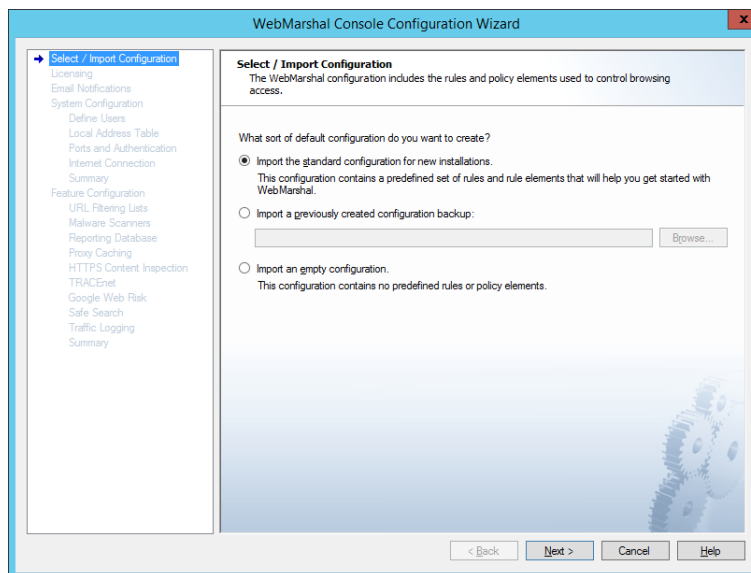
- **Import the standard configuration:** Select this option to import a default configuration. This configuration includes a suggested basic Access Policy and supporting URL Categories, TextCensor Scripts, WebMarshal Groups, Classifications, and other elements. After you complete the Wizard, you can 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.

Note: When you select this option and click **Next**, the remainder of the Wizard is not presented. To make any changes to imported configuration, use the main Console interface.

- **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.

3.2.2 Registration and License

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

1. Enter your company name.

2. WebMarshal generates a trial License Key automatically. If you have a full key, you can enter it.

3. Click **Next.**

Figure 7: Configuration Wizard, Registration and License window
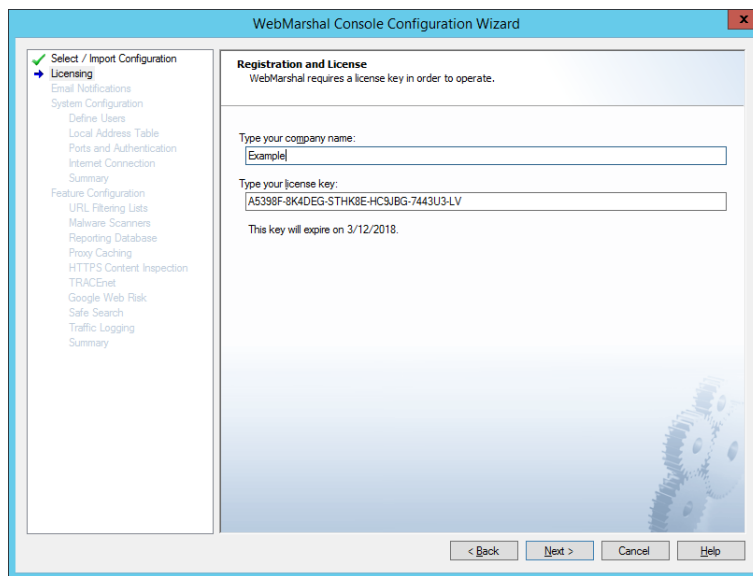
3.2.3 Email Notifications

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`

Figure 8: Configuration Wizard, Email Notifications window
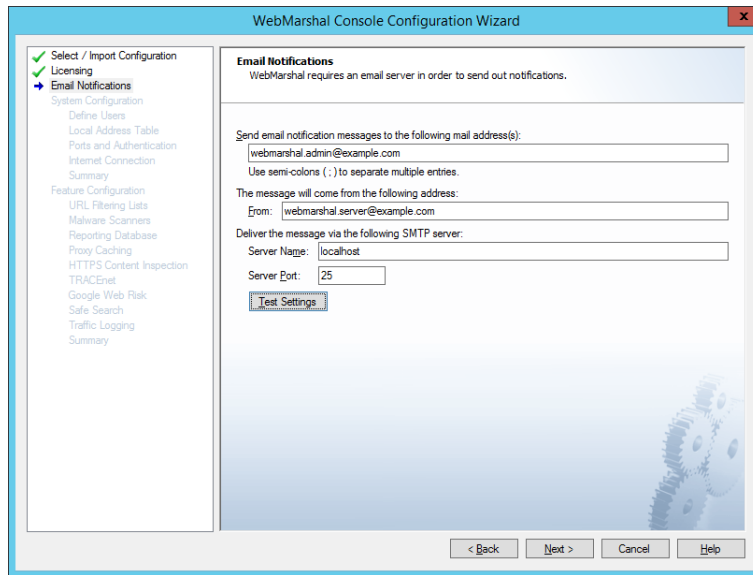
2. Use the **From** field to enter the email address that will be used as the sender address for messages.

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.

3.2.4 System Configuration

On this page of the configuration wizard, WebMarshal attempts to detect and configure environmental items that affect connectivity and authentication.

If configuration cannot be completed automatically, WebMarshal presents a window that allows you to configure the values.

The system configuration items are:

*   Users

*   Local Address Table

*   Ports and Authentication

*   Internet Connection

For details of these items, see the following sections.

3.2.5 Define Users

On this window, you can set up directory connectors, import user groups, and create IP range groups. WebMarshal uses this information to control user browsing permissions.

Automatic configuration attempts to create a directory connector and import a sample user group. The sample group is assigned standard browsing privileges based on the default WebMarshal rules.

Figure 9: Configuration Wizard, Define Users window
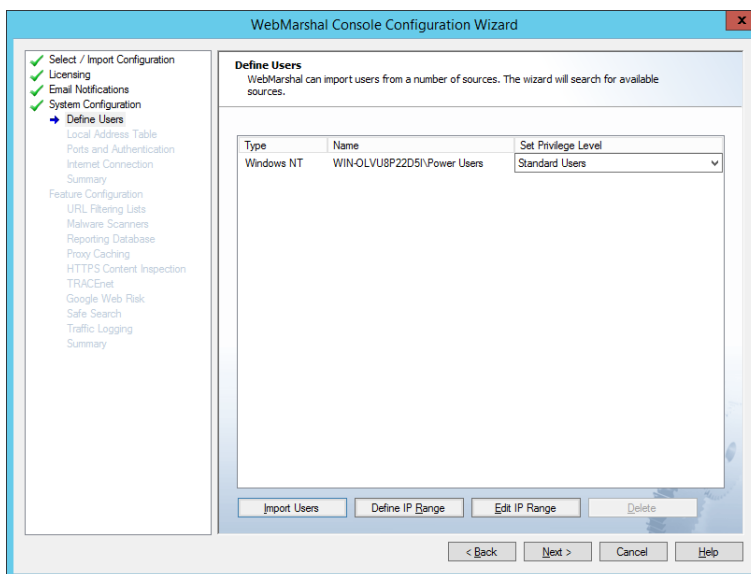
If no connector can be created, or if the connector needs login credentials, you can enter the required information. You can also add other connectors, or import additional groups. You can complete these tasks within the wizard, or in the User Groups section of the main Console.

For a production installation, you should review the connectors and imported groups to ensure that all internal users will be able to browse through WebMarshal.

For details of the fields on this window, see Help. For more information about Users and Groups, see "User Management" on page 96.

3.2.6 Local Address Table

On this page, specify the range(s) of IPv4 and/or IPv6 addresses that are assigned to computers on your local network. By default, the LAT includes IPv4 address ranges that are always reserved for local use. Automatic detection adds entries based on the networking configuration of the server. If your local network uses different local IP addresses you can enter them.

Note: Only computers with addresses in the LAT ranges are 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.

Figure 10: Configuration Wizard, Local Address Table window
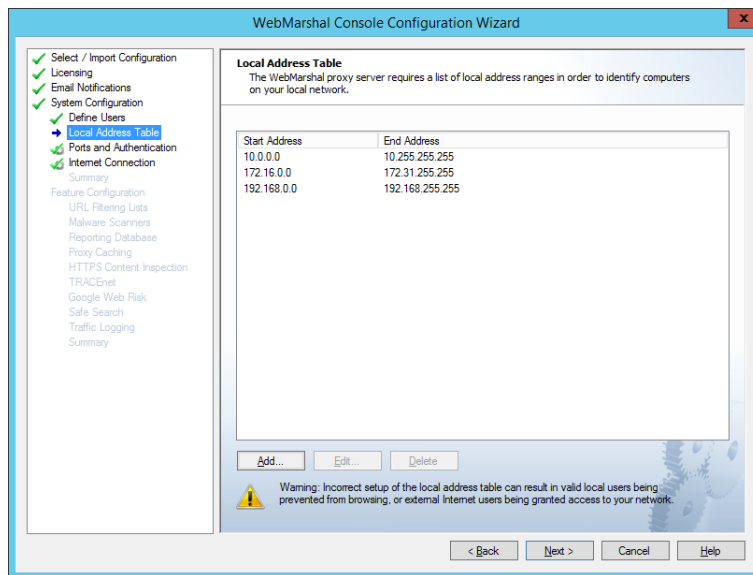
To enter a new LAT range:

1. Click **New**.

2. Enter a single IP address, a CIDR specification (such as the default IPv6 unique local address space `fc00::/7`) or starting and ending addresses of a range (such as `192.0.2.5–192.0.2.25`).

3. Click **OK**.

To edit an existing entry, select it and then click **Edit**. To delete an existing entry

, select it and then click **Delete**.

Click **Next** to continue.

3.2.7 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 IPv4 and/or IPv6 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.

Notes:

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

- IP authentication normally checks the IP address of the connecting computer. IP authentication can also extract the client IP from an X-Forwarded-For header (see Trustwave Knowledge Base article Q21183).

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.

Figure 11: Configuration Wizard, Proxy Ports and Authentication window
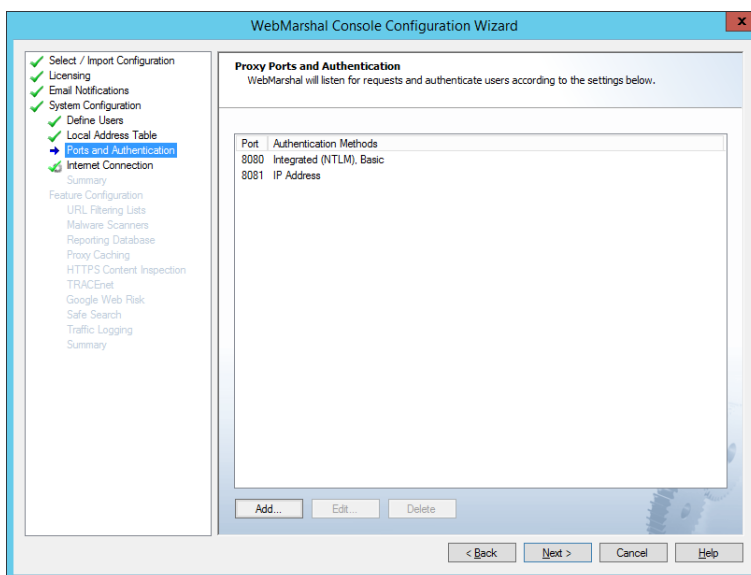
1. If you want to edit an existing port assignment, select it and then click **Edit**.

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.

3.2.8 Internet Connection

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

Figure 12: Configuration Wizard, Internet Connection window
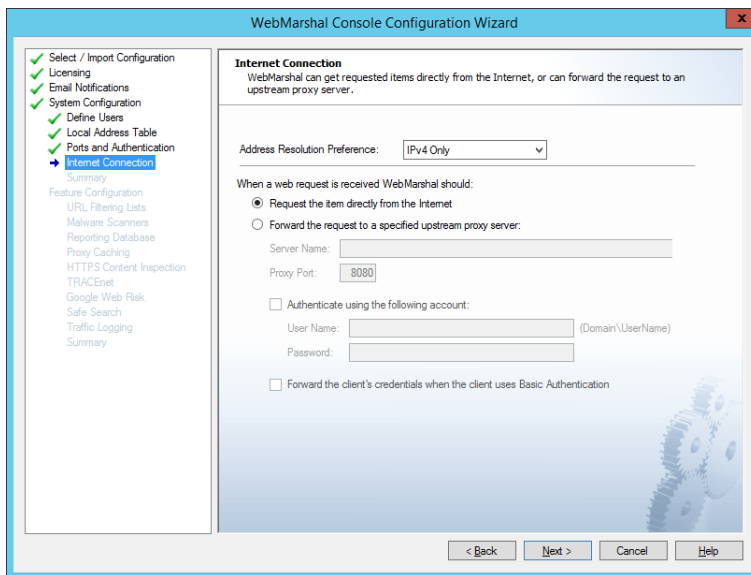
These settings define how all client browsing requests will be forwarded to external servers.

1. Choose the address resolution preference (IP protocol version to use when resolving outbound connections). This setting applies when WebMarshal resolves external websites or forward proxy names. *IPv4 only* is the default setting. For details of all options, see Help.

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

3. 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).

4. Check the configuration of the other proxy server to ensure that it is using the port protocol version 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.

5. You can choose to resolve names to IPv4 and/or IPv6 addresses. IPv4 is the default. See Help for details.

If your environment includes another proxy server, be sure to set up the other proxy software to accept requests only from WebMarshal. If you do not, then users may be able to bypass WebMarshal rules. 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.

3.2.9 System Configuration Summary

On this window you can review the system configuration settings that have been automatically detected or manually configured. Each section of the window summarizes the information entered on one of the previous windows of the Wizard. To see more details or edit the information, click **Edit** for the section.

To continue with feature configuration, click **Next.**

Tip: The tree at the left of the window shows:

- ✅ Automatically detected settings

- ✔ Manually entered or reviewed settings

3.2.10 Feature Configuration

On this page of the configuration wizard, WebMarshal attempts to detect and configure items that enhance the filtering abilities of the product.

If configuration cannot be completed automatically, WebMarshal presents a window that allows you to configure the values.

The system configuration items are:

- URL Filtering Lists

- Malware Scanners

- Reporting Database

- Proxy Caching

- HTTPS Content Inspection

- TRACEnet

- Safe Search

- Google Web Risk

- Traffic Logging

For details of these items, see the following sections.

3.2.11 URL Filtering Lists

On this window, you can configure WebMarshal to use one or more externally maintained categorized lists of URLs. When a filtering list is configured here, you can use the categories that it provides in WebMarshal Rules and reporting.

For details of the available lists, see Chapter 12, "WebMarshal and Filtering Lists."

The FileFilter list is enabled by default. If the installed Product Key supports the Trustwave Web Filter Database, auto-detection enables this item.

3.2.12 Malware Scanners

On this window, you can configure WebMarshal to use one or more third-party products to scan traffic for viruses or other malware activity. When a scanner is configured here, you can enable WebMarshal Rules to perform scanning.

Auto-detection searches for and adds supported scanners that are installed on the server.

> **Note:** Because auto-detection only adds scanners that are ready to use immediately, scanners that have just been installed might not be auto-detected if they have not yet downloaded a full set of scanning signatures. You can add additional scanners manually here, or in the Malware Protection section of the main Console.

For more information about supported scanners and other requirements, see "Scanning Overview" on page 124.

3.2.13 Reporting Database

On this window 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 report on WebMarshal activity using the Marshal Reporting Console application.

Database logging is not enabled by default. You can enable logging on this window, or later using the Database Logging window in the Console Global Settings.

Figure 13: Configuration Wizard, Reporting Database window
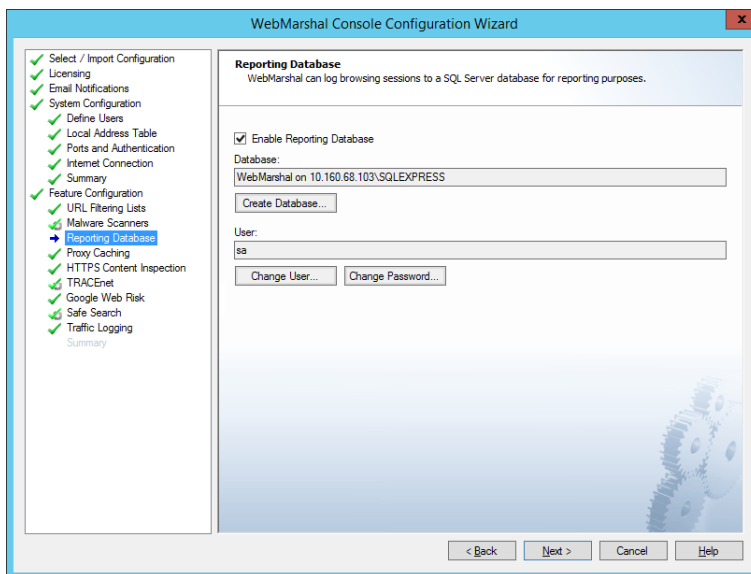
To use database logging:

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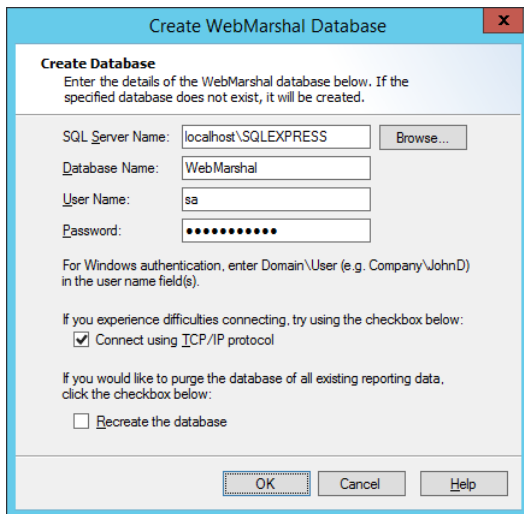
2. On the Create Database window, enter the name of the SQL Server computer and instance in the **SQL Server Name** field. You can browse the network if necessary.

    > **Note:** If you installed SQL Express on the Array Manager from the WebMarshal installer with the default options, you can enter `localhost\SQLEXPRESS`. If you installed SQL Express on the Array Manager using the Marshal Reporting Console installer, you can enter `localhost\MRC_SQLEXPRESS`.

3. Enter the name of the new or existing database you want to use.

4. Enter a Windows or SQL user name with database creation privileges on the SQL server.

5. Enter the password for the user name.

6. 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.

7. If the database you selected already exists, you can choose to recreate it. *Be sure that the existing database is not needed*.

8. Click **OK** to create the database.

After you have created the database, you can configure a user with the minimum rights required by WebMarshal (known as the "operational user." To start this process, click **Change User**. For details of this process, see Help for the Change Operational User window.

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.

3.2.14 Proxy Caching

On this window, you can choose to enable or disable WebMarshal proxy caching. This feature is enabled by default. Caching retains local copies of items downloaded from the Web via HTTP or HTTPS, where

appropriate. When WebMarshal later responds to a request for the same items, they are returned from the local copy, saving time and bandwidth.

> **Note:** Proxy caching applies for HTTP and HTTPS requests by default (never for FTP). You can disable caching of content delivered over HTTPS, For more information see Trustwave Knowledge Base article Q21204.

- WebMarshal 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 WebMarshal Traffic Logging.

- You can choose to include or exclude cached content from volume Quotas. See "Configuring Access Using Quotas" on page 109.

Figure 14: Configuration Wizard, Proxy Cache window
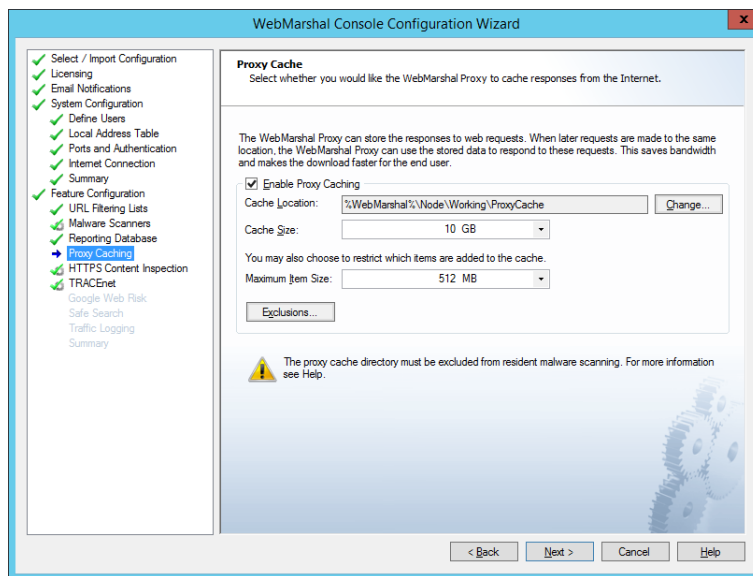
To enable caching, check the box. Then review the additional options. The default settings are reasonable for a trial installation. When setting up a production installation you should carefully consider the values.

For more information about the options, see "Configuring Proxy Caching" on page 141.

For information about the fields on this window, see Help.

3.2.15 HTTPS Content Inspection

This window allows you to perform basic setup required to use HTTPS Content Inspection in WebMarshal. You can generate a HTTPS Root Certificate and enable the HTTPS Content Inspection functionality.

HTTPS Content Inspection allows WebMarshal to perform the full range of content filtering on HTTPS (secure) web requests.

This feature is disabled by default. Before enabling HTTPS inspection in a production environment, you should review the legal implications of the feature, and notify users. For more information about the issues, see "Configuring HTTPS Content Inspection" on page 151.

For information about the fields on this window, see Help.

3.2.16 TRACEnet

On this window, you can choose to enable or disable WebMarshal TRACEnet filtering. TRACEnet is a "zero day" protection framework supported by the Trustwave Security Labs team. TRACEnet identifies malicious URLs and allows you to block access to these sites. The Security Labs 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 Trustwave. The TRACEnet digest collator reports summary data about blocked threats to Trustwave over a secure Web connection. The Security Labs team uses the reported data as part of the threat identification process that feeds back in to TRACEnet updates.

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

Note: TRACEnet updates require a working Internet connection from each WebMarshal processing node.

3.2.17 Google Web Risk

On this window, you can choose to enable or disable WebMarshal Google Web Risk integration. Google Web Risk is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.

To enable Google Web Risk, you must enter a Google API key. For more information see Trustwave Knowledge Base article Q21059.

When Google Web Risk is enabled, WebMarshal retrieves URL listings from Google. WebMarshal validates individual URLs based on the locally cached information, or if necessary by an individual query to the Google servers.

3.2.18 Safe Search

On this window, you can choose to enable or disable the Safe Search enforcement feature of WebMarshal. This feature is enabled by default.

This feature allows you to enforce use of the "Strict Safe Search" function that some search engines provide. At this release, WebMarshal Safe Search supports Google, Yahoo!, and Bing safe search, as well as YouTube Safety Mode. When this feature is enabled, WebMarshal adds the "safe search" parameter to each request that a user makes to the supported search engines.

Note: The search filtering provided when WebMarshal Safe Search 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.

3.2.19 Traffic Logging

On this window, you can configure logging of WebMarshal sessions and actions to text files in W3C or WELF format. You can use these logs to further analyze WebMarshal activity using external tools.

Figure 15: Configuration Wizard, Traffic Logging window
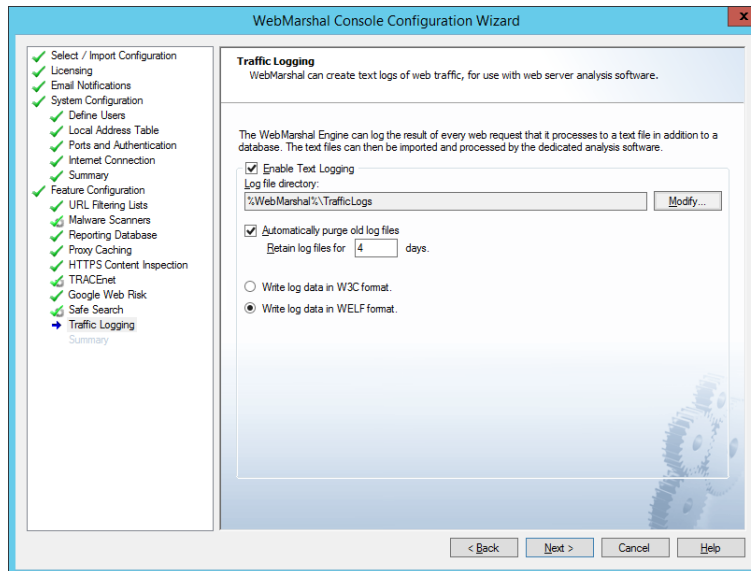
Traffic logging is not enabled by default. You can enable logging later using the Global Settings section of the Console.

To use text logging, select **Enable Text Logging**.

For a production installation, you should review the file location and choose a retention policy.

For details of the fields on this window, see Help.

3.2.20 Feature Configuration Summary

On this window you can review the system configuration settings that have been automatically detected or manually configured. Each section of the window summarizes the information entered on one of the previous windows of the Wizard. To see more details or edit the information, click **Edit** for the section. Click **Finish** to start WebMarshal services and run the WebMarshal Console.

3.2.21 Additional Configuration Steps

When installed, WebMarshal immediately begins accepting and filtering Web requests.

The default and auto-detected settings are designed to ensure that users in a test environment will have basic browsing privileges.

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

1. **Verify user information:** Since WebMarshal is an authenticating proxy server, each browser session must supply a logon credential before any browsing is permitted. Check the status of connectors,

imported groups, and IP range groups. Adjust settings as required. See "Users and Groups" on page 53.

2. **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 WebMarshal Groups. You can enable and edit Rules as required using the Console. See Chapter 6, "Understanding Web Access Policy, Rule Containers, and Rules."

3. **Configure Malware Protection** (optional, but strongly recommended): If you plan to use Virus Scanners with WebMarshal, verify that the software is installed and initial signatures are downloaded, then enable Malware Scanning Rules. See "Using Malware Scanning" on page 124.

4. **Configure Filtering Lists** (optional): If you plan to use URL filtering lists with WebMarshal, you must enable them and ensure that the initial database downloads are complete before you enable them in any rules. See "Configuring URL Filtering Lists" on page 106.

5. **Configure browser proxy settings to use WebMarshal:** To use WebMarshal, in most cases web browsers must be configured with proxy settings. See "Configuring Web Browsers" on page 43.

3.3 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 SquidNT has been listening on port 3128), 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 Trustwave 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 153.

3.4 Upgrading WebMarshal

You can upgrade to this version of WebMarshal from WebMarshal 7.4.0 or above.

To upgrade, run the product installer on each computer where components are installed.

Note: To upgrade from versions below 7.4.0, you must first upgrade to 7.4.0 and then upgrade again. Before upgrading, be sure to review the upgrade notes and detailed instructions for each version you are upgrading to. See the Release Notes and *User Guide* for earlier versions if necessary.

3.5 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.

Installing WebMarshal

3. Uninstall any instances of the WebMarshal Console 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 integrated malware scanner software such as McAfee for Marshal. If you were using the Trustwave Web Filter Database (or other filtering lists previously available), 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. Trustwave recommends that you do not uninstall the prerequisites.

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.

Marshal Reporting Console

Allows you to generate detailed historical reports on Web access, policy breaches, and WebMarshal actions. For detailed information about how to install and use this application, see the separate documentation for MRC.

WebMarshal also provides a number of freestanding tools to assist with specific tasks.

4.1 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.

Figure 16: WebMarshal Console
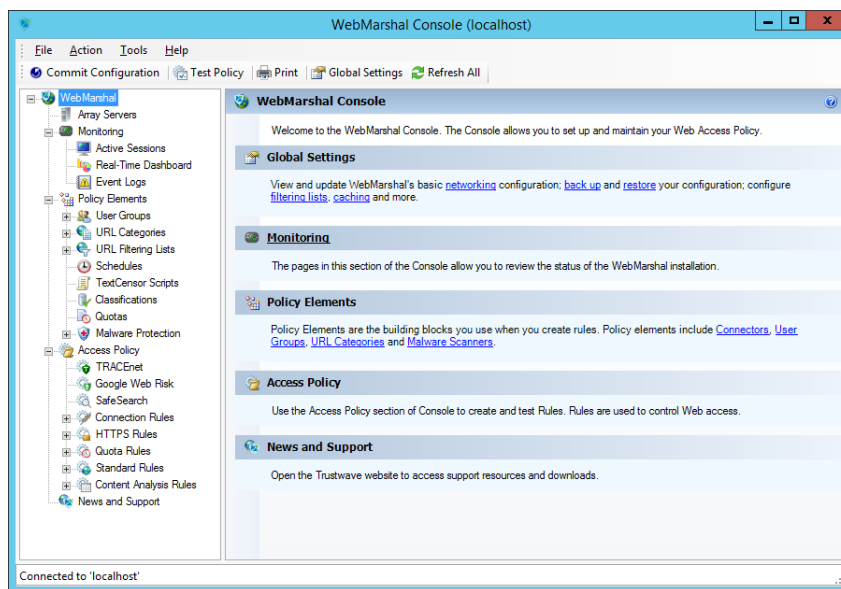
4.1.1 Console Navigation

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.

4.1.2 Working With Properties Configuration

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

Global Settings

On this window you can control basic properties of a WebMarshal installation. To open this window, select **Tools > Global Settings** 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 Global Settings" on page 133, "Managing Array Servers" on page 160, and "Configuring Server Group Properties" on page 162.

4.1.3 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 Global Settings" on page 133.

4.1.4 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. You can drill down to view details. You can right-click items for more options. For detailed information see Help.

> **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 135.

Figure 17: WebMarshal Console, Active Sessions window
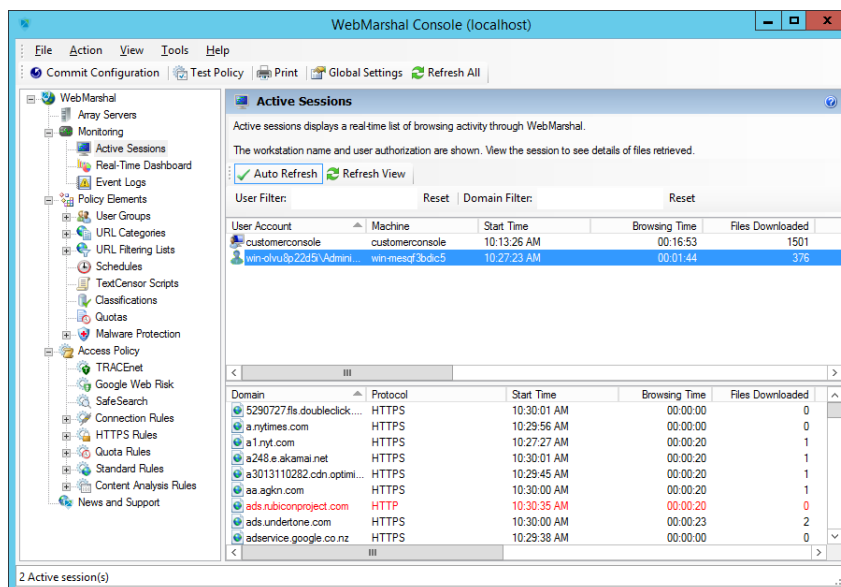
4.1.5 Real-Time Dashboard

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.

Figure 18: WebMarshal Console Dashboard
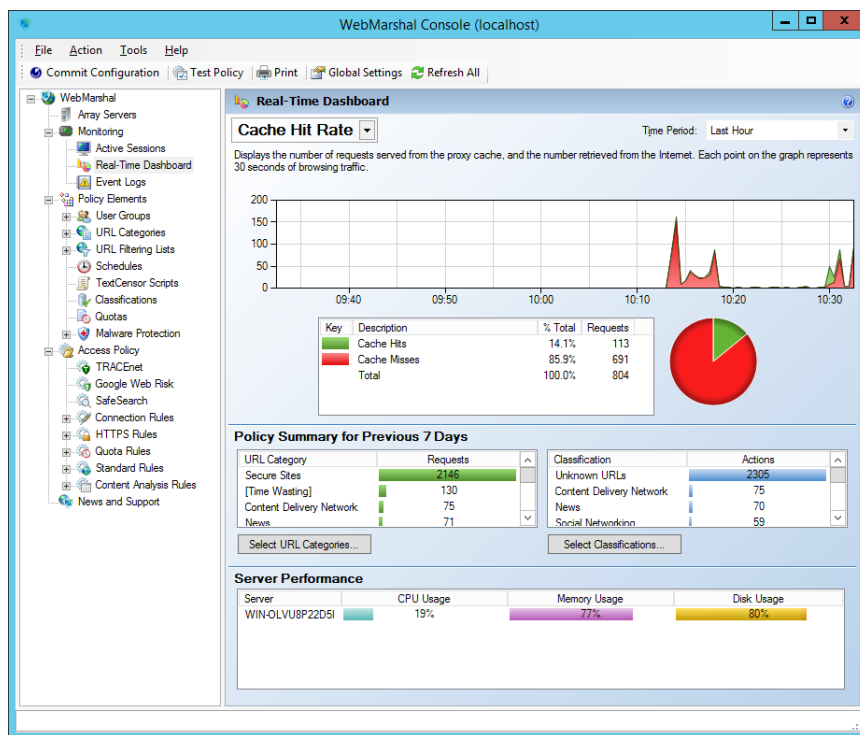
4.1.6 Event Logs

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 164.

4.1.7 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.

4.1.7.1 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 96.

4.1.7.2 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.

4.1.7.3 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 101.

> **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.)

4.1.7.4 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 106.

4.1.7.5 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 107.

4.1.7.6 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 114.

4.1.7.7 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 126.

4.1.7.8 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 109.

4.1.7.9 Malware Protection

Expand this menu branch and select "Virus Scanners" to see a list of third-party virus 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 124. To implement malware scanning, see Chapter 6, "Understanding Web Access Policy, Rule Containers, and Rules."

4.1.8 Access Policy

Expand this menu branch to see its subcategories:

• TRACEnet

• Safe Search

• Connection Rules

• HTTPS Rules

• Quota Rules

• Standard Rules

• Content Analysis Rules

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."

4.1.9 Printing Configuration and Rules

You can view and print WebMarshal configuration, rules and policy 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).
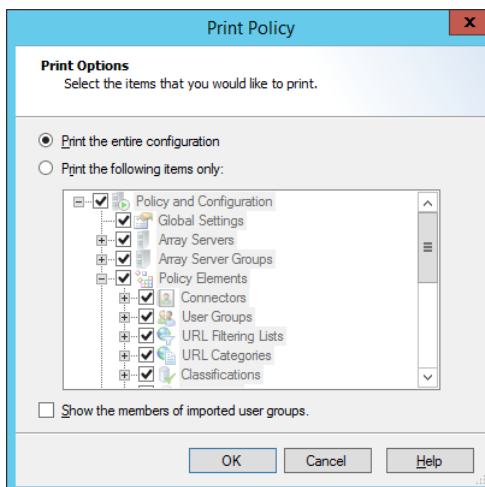
4. Click **OK** to view the information in a new window.

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.**

4.1.10 News and Support

The News And Support item in the console tree presents the support section of the Trustwave 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 Trustwave.

4.2 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.

*   Change some performance related settings.

*   Change locations for log and temporary files.

*   Configure communication between the Processing Server and the WebMarshal Array Manager.

For more information about servers and arrays, see "Managing Array Servers" on page 160. 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 159.

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 158.

The **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 Trustwave support team diagnose support issues. To use the tool select **Tools > Open Support Tool**. You can also run the tool from the Start menu (Apps), or from a command prompt as `MarshalSupportTool.exe` in the WebMarshal installation directory. Each time you run the tool it checks for updates to the support tool application. For more information on how to use the Support Tool, see Trustwave Knowledge Base article Q15024.

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 Trustwave Knowledge Base article Q12724.

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.

5.1 Configuring Web Content Security

When you run the Configuration Wizard, you can install a default set of policies, rules, and policy elements. Trustwave 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 Trustwave 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.

5.1.1 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. The Configuration Wizard attempts to create a connection to the directory service that is used in your environment. To learn about how to create connections to other services, including Active Directory, legacy Windows NT, Novell, and workstation based authentication, see "User Management" on page 96.

The default WebMarshal configuration includes local "WebMarshal groups" and sets of rules that apply to users in these groups.

- You can set the permissions for an imported user by adding the user to the appropriate WebMarshal group.

- You can adjust permissions by enabling or disabling the rules in the default set that apply to each group.

- You can create new rules that apply to any of the groups.

5.1.1.1 Adding User Groups From a Connector

To import User Groups:

1. Within the WebMarshal Console, ensure that User Groups is selected. Click the **Import User Group** icon 👥 in the taskpad to open the Import User Groups window.

2. Choose the connector to use. (You can also create a new connector.).

3. Browse for or 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.

   When browsing you can use ctrl-click and shift-click to multi-select.

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

4. Click **Import** to add the User Group(s) and contained users.

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

5.1.1.2 Adding Imported User Groups to WebMarshal Groups

WebMarshal default configuration includes a number of local WebMarshal groups. To grant permissions to an imported user, you can add the user (or an entire group) to a WebMarshal Group.

To add a group to a WebMarshal group:

1. Within the WebMarshal Console, ensure that User Groups is selected.

2. Drag a group from the right pane over a WebMarshal group in the left pane.

To add individual users, or sub-groups from an imported group:

1. Select the target group in the left pane.

2. At the top of the right pane, click **Insert Existing Group.**

3. Select items from the list, and then click **Insert.**

5.1.2 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 use or enable the default items. You may need to customize some rules to meet your needs. You can monitor policy compliance by using Marshal Reporting Console 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.

5.1.3 Ensuring Appropriate Usage

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

5.1.3.1 TRACEnet

You can help to ensure appropriate usage with 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 59. 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.

TRACEnet is enabled by default and TRACEnet filtering applies to all users and sites by default. You can adjust these settings using the Settings button on the **Access Policy > TRACEnet** page.

5.1.3.2 Rules

The WebMarshal default configuration includes a number of rules that apply to specific WebMarshal groups. To allow appropriate use, add imported groups to the WebMarshal groups *Power Users*, *Standard User*s, and *Restricted Users*. Review the policy to see what rules are enabled for each group.

You can check for appropriate textual content of pages with Content Analysis rules such as *Block Download - Adult and Nudity Content, Block Download - Offensive Content,* and *Block Upload - 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.

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 URL - Adult & Nudity, Block URL - R Rated and Profanity*, *Block URL - Gambling* Sites, and *Block URL - Time Wasting Inside Office Hours*. 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 File - Dangerous File Extensions*, *Block File - Dangerous File*s, *Block File - Multimedia*, and *Block File - 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 151.

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.

5.1.3.3 Enabling rules

To enable a WebMarshal rule (such as *Block URL - Adult & Nudity*):

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 URL - Adult & Nudity*) 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.

5.1.3.4 Exceptions to rules

You may want to allow a few users to use sites or files that are blocked for most users including the default Power Users group. The WebMarshal default rules allow full access to all sites for members of the WebMarshal Group *Unrestricted Site Access*. You could also create additional groups and additional rules to permit specific exceptions.

To implement the exceptions, add the appropriate Users or User Groups to *Unrestricted Site Access* (or another exception group you create)

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

2. Right click and select **Insert Existing**.

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 96.

5.1.4 Protecting Against Malware

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

5.1.4.1 Malware Scanning

WebMarshal can scan for viruses, malware, 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 124.

> **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 Malware 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.

5.1.4.2 File Type and File Name rules

Other types of rules also help to protect against malware downloads. The Standard rules *Block File - Dangerous File Extensions* and *Block File - Dangerous Files* are pre-configured to apply to Standard and Restricted users.

• 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.

5.1.5 Conserving Network Resources

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

5.1.5.1 Proxy caching

You can reduce bandwidth usage by enabling WebMarshal proxy caching. Caching is enabled by default on new installations. For more information about caching, see "Configuring Proxy Caching" on page 141.

5.1.5.2 Connection rules

You can manage connections from many popular Instant Messaging and Streaming Media applications, as well as the WebSocket protocol. Sample blocking rules are provided in the default configuration. To quickly apply these rules to a user, add the user to the pre-defined WebMarshal Group *Restricted Users*. For more information about how to enable and use connection rules, see "Connection Rules" on page 62.

5.1.5.3 Quota rules

You can limit each user to a quota of browsing time and/or bandwidth. Sample quotas are configured in the default rules, but all quota rules are disabled by default. Enable the pre-configured rules "Enabling rules" on page 56. If quota rules are enabled, Trustwave recommends you also enable the Standard rule *Global Policy > Display Quota Limits Policy*.

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 63.

5.1.5.4 Standard rules

WebMarshal can stop the download of oversized files by a Standard rule. The rule *Block Download - Files Larger than 20MB* stops large files from being accessed.

WebMarshal can also stop uploading of oversized files by a Standard rule. The rule *Block Upload - Files Larger than 5MB* stops large files from being uploaded.

These file size rules are enabled by default for the Restricted Users group. 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 move them to a group with greater default permissions. You can also apply limits for specific users, file types, or other custom criteria. For complete information, see Chapter 6, "Understanding Web Access Policy, Rule Containers, and Rules."

Blocking of multimedia files also helps save network resources.

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 Safe Search features.

6.1 Understanding TRACEnet

The TRACEnet feature is a "zero day" protection framework supported by the Trustwave Security Labs team. TRACEnet identifies malicious URLs and allows you to block access to these sites. The Security Labs 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 Trustwave. The TRACEnet digest collator reports summary data about blocked threats to Trustwave over a secure Web connection. The Security Labs 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)

Trustwave 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.

Figure 19: WebMarshal Console, TRACEnet window
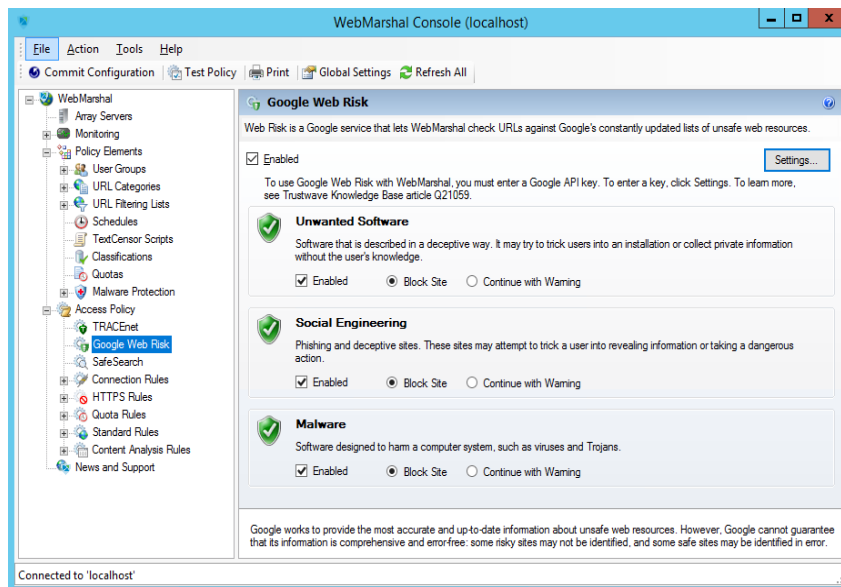
To configure TRACEnet, in the left pane of the WebMarshal Console expand **Access Policy** and select **TRACEnet.**

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.

6.2 Understanding Google Web Risk Integration

Web Risk is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources. To configure Web Risk integration, in the left pane of the WebMarshal Console expand **Access Policy** and select **Google Web Risk.** For full information about the options, see Help.

To enable or disable the feature, check or clear the box on the main Google Web Risk page. To enable or disable the individual categories, check or clear the box for each. You can also choose to allow users to continue with a warning.

Note: Google Web Risk is only enabled after you enter a Google API Key. To check or enter the key, on the main Google Web Risk page click **Settings**.

 You can configure advanced settings for Google Web Risk integration, including User Group and URL exclusions. To configure advanced settings, at the top right of the main Google Web Risk page click **Settings**.

Figure 20: WebMarshal Console, Google Web Risk window
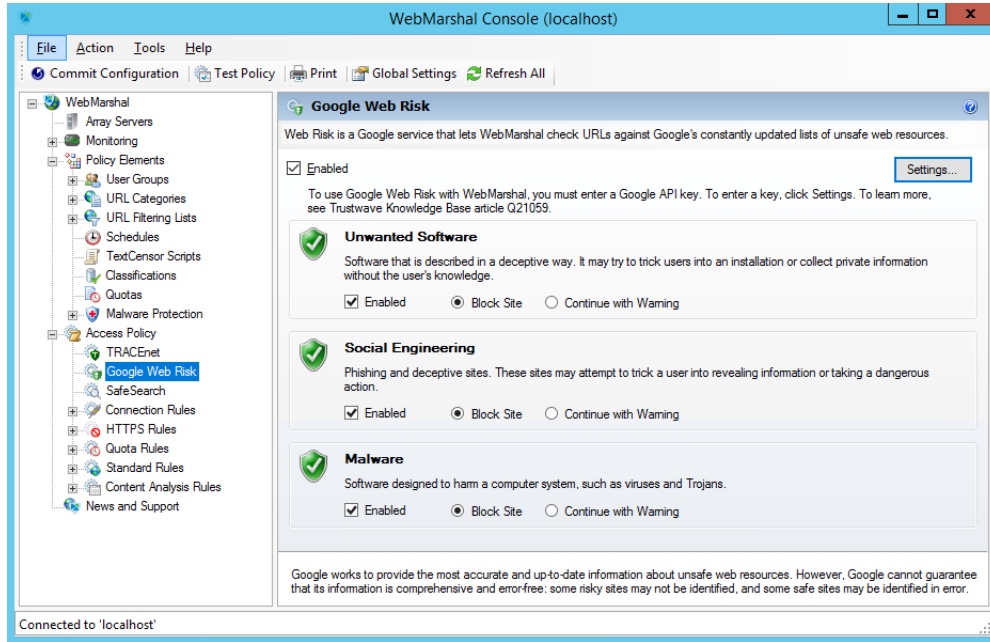
6.3 Enforcing SafeSearch

WebMarshal allows you to enforce use of the "Strict Safe Search" function that some search engines provide. At this release, WebMarshal Safe Search supports Google, Yahoo!, and Bing safe search, as well as YouTube Safety Mode. This feature adds the "safe search" parameter to each request that a user makes to the supported search engines or sites.

> **Note:** The search filtering provided when WebMarshal Safe Search 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 Safe Search, 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 Safe Search 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 Safe Search page click **Settings**. For more information, see Help.

6.4 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.

6.5 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.

6.5.1 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, as well as the WebSocket protocol.

> **Note:** 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 Trustwave Knowledge Base article Q12021.
>
> • Before you can use Connection Rules, you must enable this functionality in the WebMarshal Global Settings. For more information, see "Configuring Connection Rule Processing" on page 155.

6.5.2 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. HTTPS traffic to be scanned is decrypted, and then re-encrypted for transfer to the destination.

> **Note:** Before you can use HTTPS rules, you must configure the HTTPS functionality. See "Configuring HTTPS Content Inspection" on page 151.
>
> • When HTTPS rules are enabled, content is always secured when transmitted over the network.
>
> • HTTPS traffic that does not match a rule requiring scanning is not decrypted.

6.5.3 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 109. For a full list of conditions and actions, see Help for the Quota Rules window in the WebMarshal Console.

6.5.4 Standard Rules

Standard rules are evaluated when WebMarshal receives a request from a browser session. Standard rules allow you to permit or deny access to URL categories by user groups. Standard rules also allow you to match or rewrite the headers of a web request or response.

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.

Understanding Web Access Policy, Rule Containers, and Rules

6.5.5 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 use a standard rule to block future requests for the URL quickly, using a Standard rule.
>
> • To reduce the delay due to processing, in some cases WebMarshal begins to return a file to the user. A small part of the file is held back from the user until WebMarshal has completely received and processed the file. If the page triggers the rule, the download is aborted. For information about configuring this feature, see "Configuring Download Options" on page 144.

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

6.6 Working With Access Policy

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

6.6.1 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.
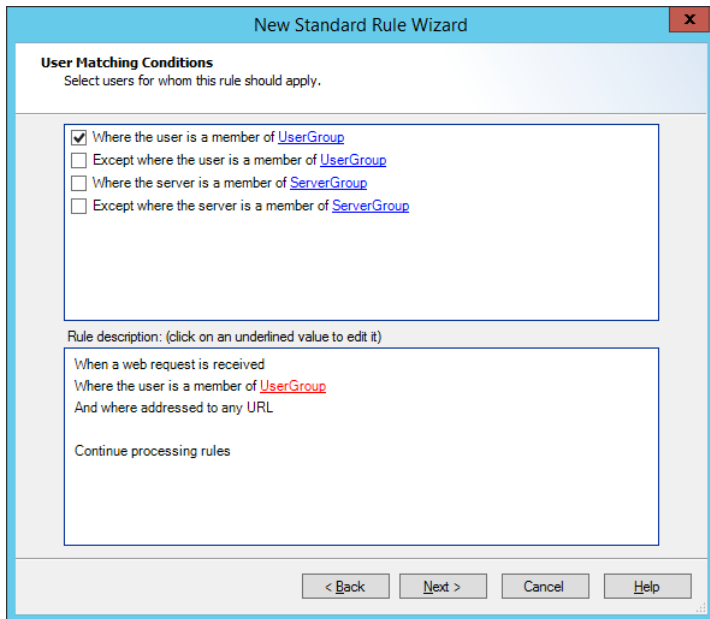
5. On the User Matching Conditions page, check the boxes in the top pane to select the conditions you want to include in the rule. The items you select items display in the rule description pane, at the bottom of the page.

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 68.

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.
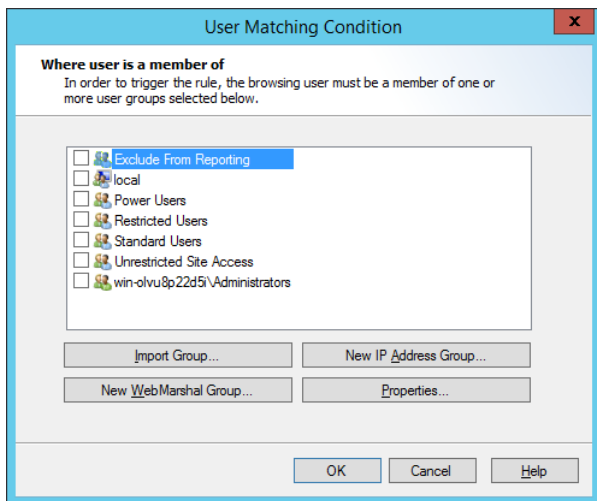
In this window, you can select an existing user group. You can also create or import a new group. If you create or import a group, it is selected for use when you return to the Select User Groups window.

> **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.

9. Select conditions and enter details on this page in the same way as for 5.. See "Rule Conditions" on page 70 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.

11. Select actions and enter details on this page in the same way as for 5.. The actions that you can select vary depending on the type of rule. See "Rule Actions" on page 86 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.
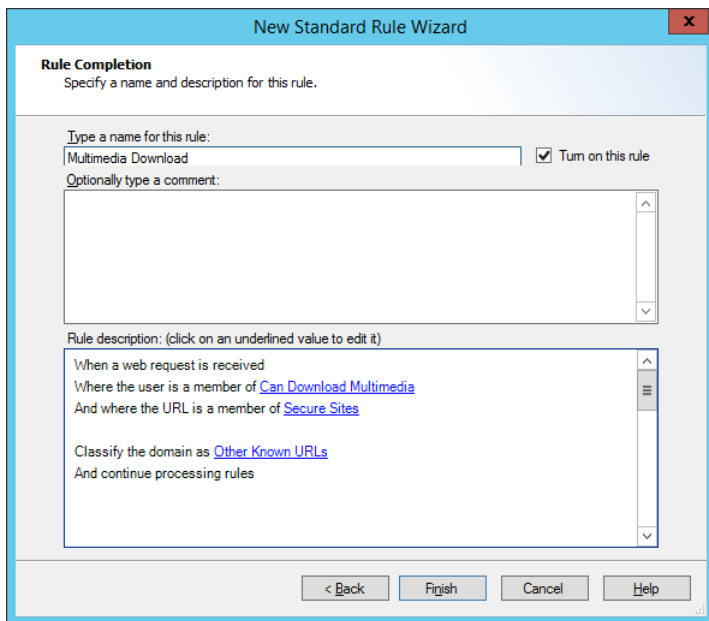
13. Enter a name for the rule.

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.

> **Note:** 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 92.
>
> **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.

6.6.2 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**.

6.6.3 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).

Figure 21: WebMarshal Console, Rules window
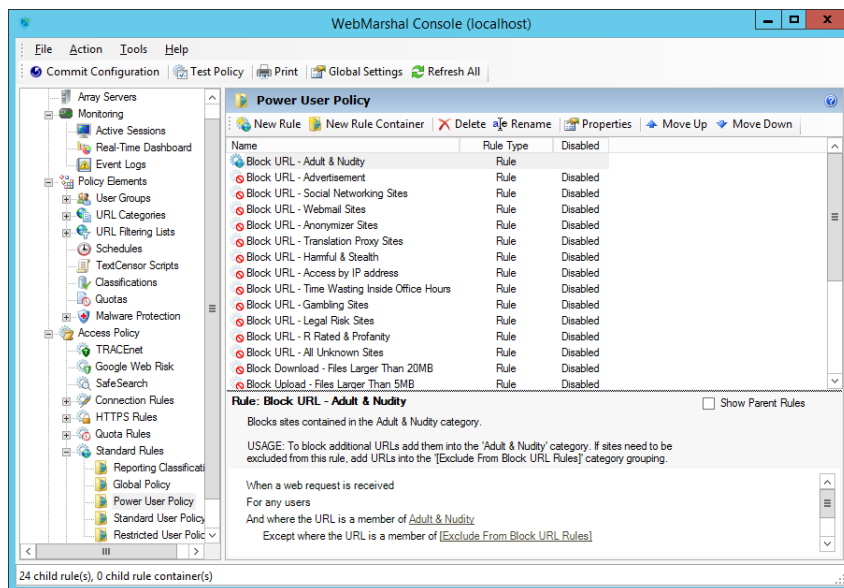
1. Expand Access Policy, and select a rule type in the left pane.

2. Double-click a particular rule or rule container in the right pane.

3. On the Rule Wizard page, check or uncheck **Turn on this rule**.

4. 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.

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

6.7 Understanding User Matching

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

6.7.1 User Matching Conditions

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

6.7.1.1 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 create or import a new group. If you create or import a 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.

6.7.1.2 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.
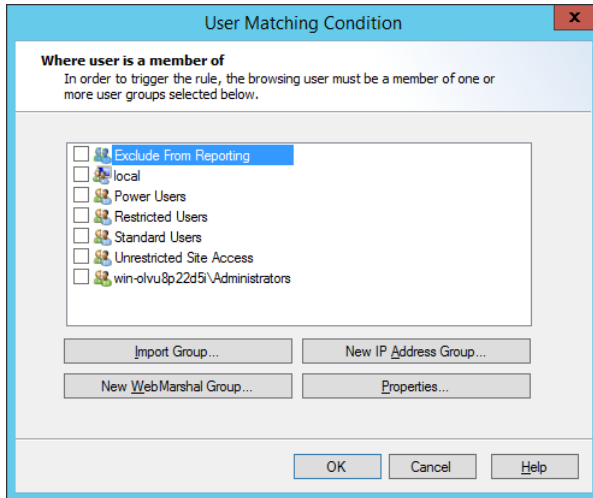
This condition overrides the previous condition. For instance, a Rule might start:

```
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*).

6.7.1.3 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 162. If you create a new server group, it is selected for use when you return to the Server Matching Condition window.

6.7.1.4 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.

6.8 Understanding Rule Conditions

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

6.8.1 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 header(s) match

- 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

6.8.1.1 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.

6.8.1.2 Where the protocol/application is of type

If this condition is selected, the Rule will apply for requests from specific Instant Messaging, Streaming Media, and WebSocket applications. Click **Protocol/Application** to open the Select Application window.
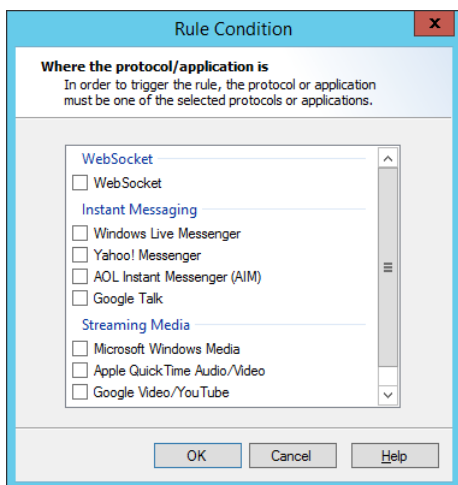
1. Select one or more applications to match by checking the boxes. To view the detailed description of the protocol, hover over an item.

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**.

6.8.1.3 Except where the protocol/application is of type

If this condition is selected, the Rule will not apply for requests from specific Instant Messaging, Streaming Media, and WebSocket 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.**

6.8.1.4 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.

Note: URL matching is not case sensitive.

Click **Category** to open the Select URL Categories window.
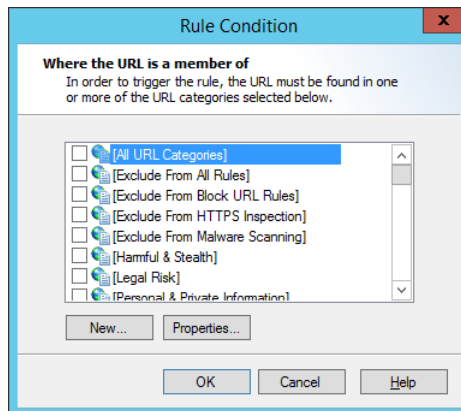
1. Select one or more URL Categories to match by checking the boxes. To view the detailed description of a category and the number of URLs it includes, select the category name and then click **Properties**.

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**.

6.8.1.5 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.`)

6.8.1.6 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.
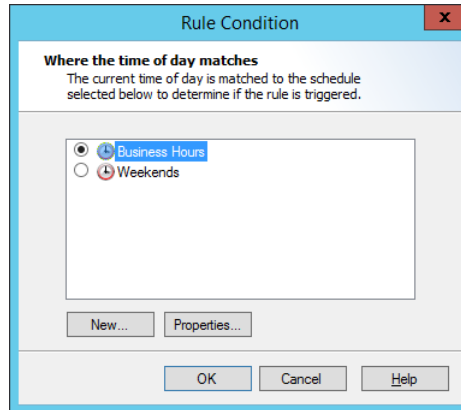
1. Select a Schedule to match using the radio buttons. To view or edit the details of a schedule, select the schedule name and then click **Properties**.

2. Optionally click **New** to create a new Schedule, as described in "Configuring Access Using Schedules" on page 107.

3. Schedule conditions normally match times within the schedule (blue area in the schedule policy 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.

6.8.1.7 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 used to authenticate a website (typically due to usage constraints encoded in the certificate).

    •   **Certificate is revoked**: The certificate is marked as revoked by the issuer.

- **Certificate revocation check failed**: WebMarshal could not check the certificate revocation status. For more information about possible reasons see Help.

Note: Before you can use the two revocation options you must enable certificate revocation checking. See **"Enabling Certificate Revocation Checking" on page 154**.

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

6.8.1.8 Where the security protocol is protocol

This condition allows you to check for the specific security protocol that was used for a HTTPS connection. The available protocols are distinguished by the difference in their cipher strength. The minimum protocol strength recommended is TLSv1.0.

Note: WebMarshal uses only TLSv1.0, TLSv1.1, TLSv1.2, or TLSv1.3 by default. SSLv2 connections are never allowed by the WebMarshal Proxy. SSLv3 connections are not allowed by default, but can be allowed. For information about how to change this default, see Trustwave Knowledge Base article Q20067.

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 use for a connection is selected automatically from the available protocols. 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. You could also use this condition to create rule-based exceptions for sites that are required by your business but do not support best practice cipher strength.

6.8.1.9 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.

6.8.1.10 Where SSL/TLS could not be negotiated

This condition allows you to take action when the user enters a HTTPS URL, but WebMarshal and the server cannot agree a security protocol.

Caution: If WebMarshal and the remote server cannot negotiate a protocol, traffic could be passed through uninspected. By default, this situation should be very rare since WebMarshal first negotiates any protocol and then checks the result to determine if the connection should be allowed.

Best practice is to **block** all HTTPS connections where SSL/TLS could not be negotiated.

6.8.1.11 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 Web-Marshal.

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

6.8.1.12 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).

6.8.1.13 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 including IPv4 and IPv6 addresses.

> **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).

6.8.1.14 Where the header(s) match

This Condition, available in Standard rules, allows you to check the existence and content of HTTP headers. Header matching can apply to request headers (sent by the client), response headers (sent by the server), or both. You can include one or more Header Match conditions in a single rule condition.

Click **matches** to open the Header Match Conditions window.

Understanding Web Access Policy, Rule Containers, and Rules
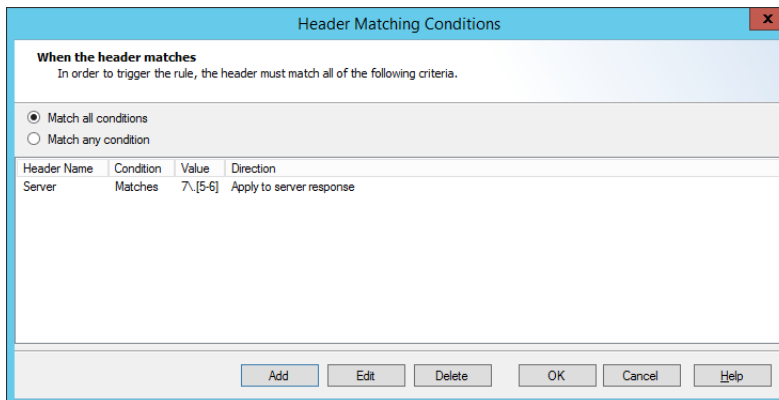
To begin choosing headers for matching, click **Add.** On the Add Item window, select the header name and define the action to perform.
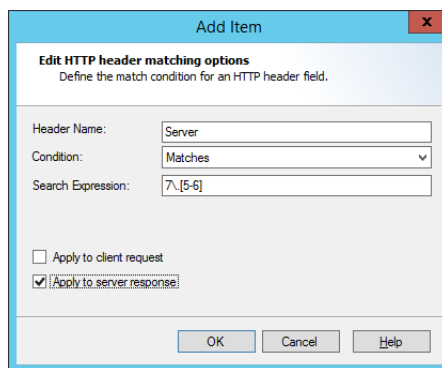
To change or remove the header matching actions, on the Rule Action window select an item and then click **Edit** or **Delete**. For more information, see Help.

6.8.1.15 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.
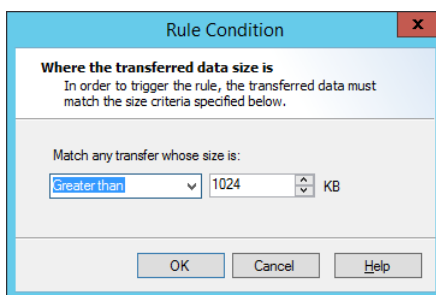
1. Choose whether to trigger on file transfers greater than or less than a specified size, or between two sizes.

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.

6.8.1.16 Where the result of a malware scan by scanner is

This condition invokes the scanners you select to check for viruses and other malware.

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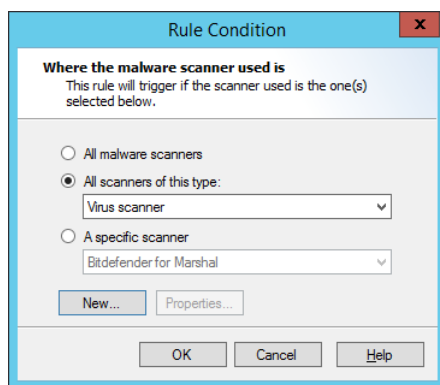
1. Choose which scanners to use. You can only select scanners you have configured in WebMarshal.

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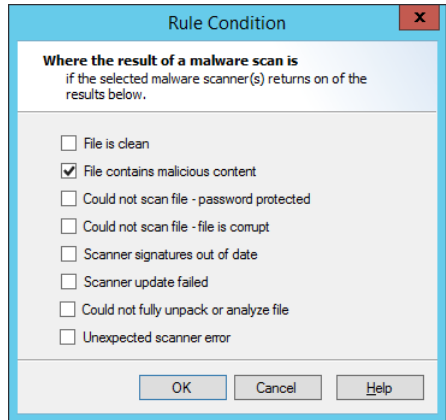
1. Check the boxes to select the desired conditions. In general, the more boxes selected, the more restrictive the conditions on downloads or uploads.

   • **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.

6.8.1.17 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.
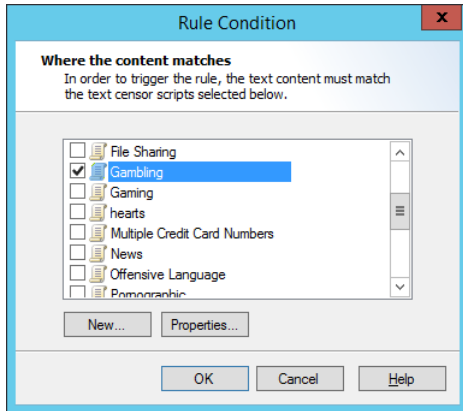
2. To create a new TextCensor Script, click **New**. For more information see "Identifying Web Content Using TextCensor Scripts" on page 114.

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.

6.8.1.18 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.

Caution: Although this condition is available in both Standard and Content Analysis rules, Trustwave 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 Trustwave 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.
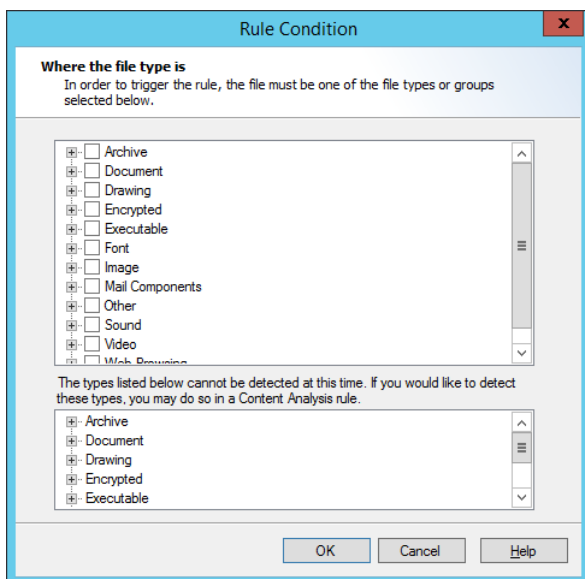
2. Expand any category to see the particular types available.

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.

6.8.1.19 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 79.

- 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.

6.8.1.20 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.

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

   Tip: 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.

6.8.1.21 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.

> **Tip:** 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`.

6.8.1.22 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.

6.8.1.23 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.

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.
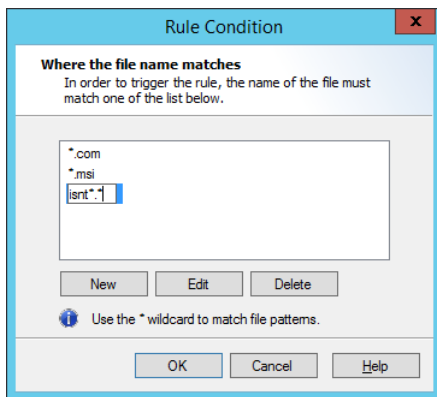
2. To edit an existing name, select it and then click **Edit**.

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.

Understanding Web Access Policy, Rule Containers, and Rules

6.8.1.24 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`.

6.8.1.25 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.

6.8.1.26 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.
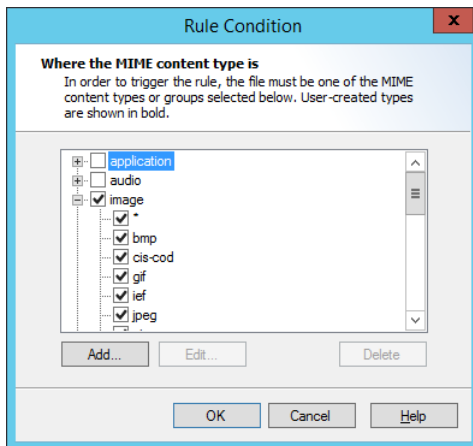
1. Expand any category to see the particular types available.

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.

6.8.1.27 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.

6.8.1.28 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.

6.9 Understanding Rule Actions

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

6.9.1 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

- Rewrite headers

- 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

6.9.1.1 Permit access

The web page, download, or upload is delivered.

6.9.1.2 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 128.

6.9.1.3 Permit access and inspect content

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

Tip: Use of this action in Connection rules is intended to support inspection of WebSocket content.

6.9.1.4 Permit access and do not inspect content

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

6.9.1.5 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.
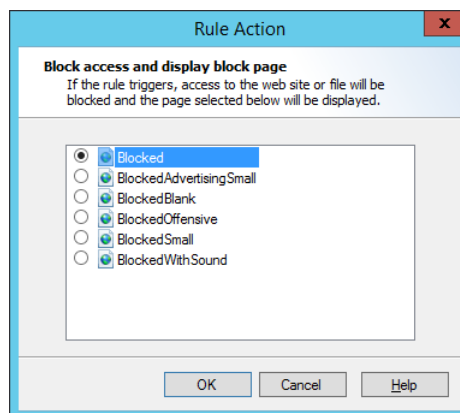
1. Select a web page to display from the list

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 only displays if WebMarshal begins to return the download and then stops it due to a rule 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.

6.9.1.6 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, Streaming Media, or WebSocket application to connect through WebMarshal.

6.9.1.7 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.
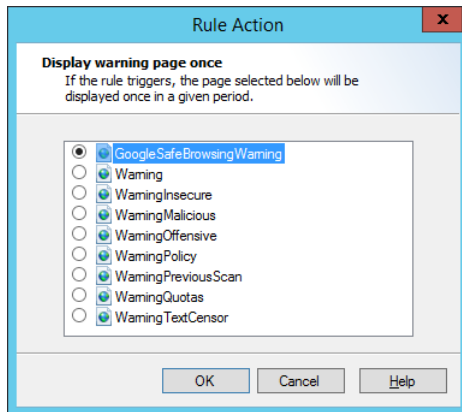
1. Select a web page to display from the list.

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.

6.9.1.8 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.

6.9.1.9 Rewrite headers

One or more HTTP headers are added, deleted, replaced, or modified using Regular Expressions. Header rewriting can apply to request headers (sent by the client), response headers (sent by the server), or both.

> **Notes:**
>
> • Header rewriting is not available for HTTPS CONNECT.
>
> • Header rewriting is not available for response headers in the Websocket protocol.
>
> • Some rule conditions do not affect request header rewriting, because the required information is not available at the time this action is applied. See Help for details.

Click **headers** to open the Rewrite Headers window.
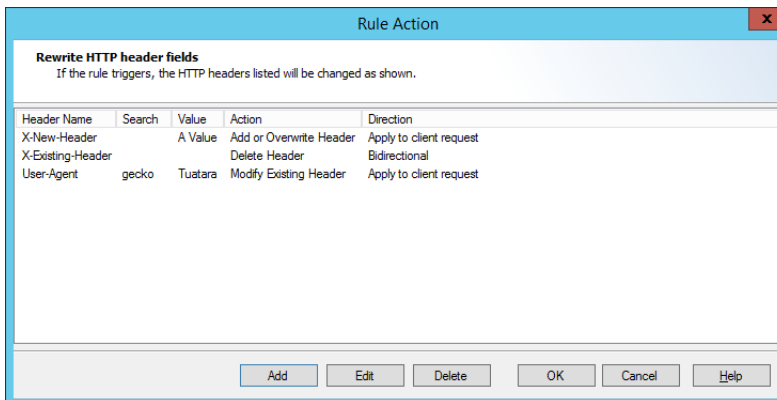
To begin choosing headers for rewriting, click **Add.** On the Add Item window, select the header name and define the action to perform.
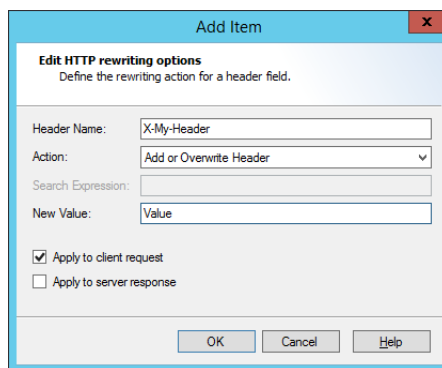
To change or remove the header rewriting actions, on the Rule Action window select an item and then click **Edit** or **Delete**. For more information, see Help.

6.9.1.10 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.
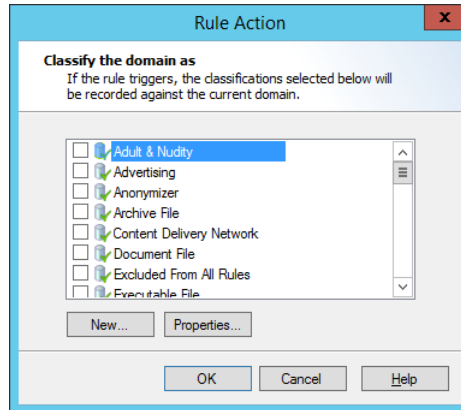
To create a new classification, click **New**. To review and edit an existing classification, click **Properties**.

For more information about adding and editing classifications, see "Logging Activity with Classifications" on page 126.

6.9.1.11 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 126.

6.9.1.12 Add the user to a user group

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

Select an existing WebMarshal Group or new WebMarshal 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 96 for more information on User Groups.

6.9.1.13 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.
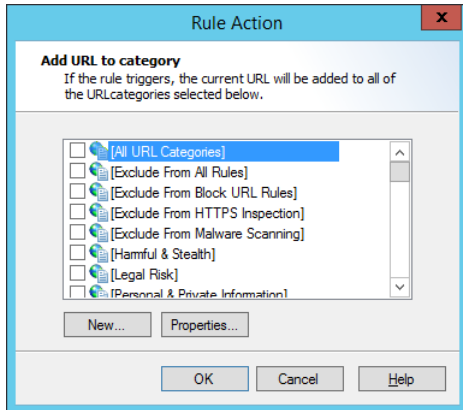
2. Choose one or more categories into which this site should be placed by checking the boxes.

3. To create a new category, click **New**. To review and edit an existing category, click **Properties**. See "Understanding URL Categories" on page 101 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.

> **Note:** You cannot add filename or query string parts automatically. You can add URLs containing these parts manually. See "Adding URLs to a URL Category" on page 103.
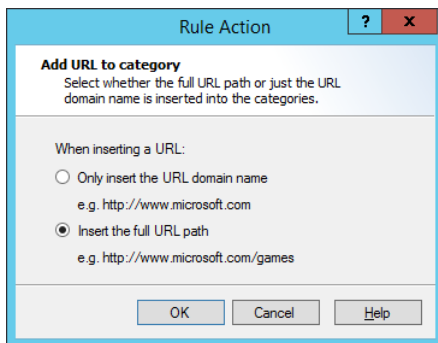
6.9.1.14 Send a notification to the administrator

A notification email is sent to the administrator email address as configured on the Email Notifications page of Global Settings.

> **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.

6.9.1.15 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.

> **Note:** 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,** Trustwave 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.

6.9.1.16 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.
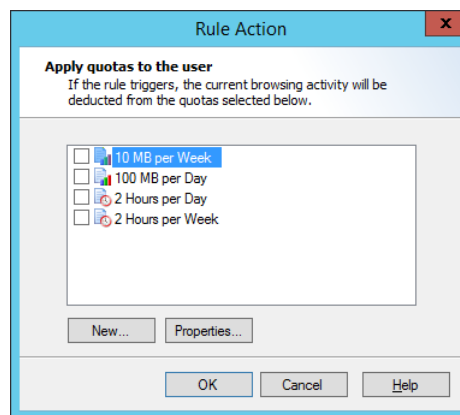
To create a new quota, in the window click **New** to start the Quota Wizard. To review and edit an existing quota, click **Properties**. For more information on Quotas and the New Quota Wizard, see "Configuring Access Using Quotas" on page 109.

6.9.1.17 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.

6.9.1.18 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.

6.10 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.

6.11 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.

   • 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)

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

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

4. Choose whether to test download or upload processing.
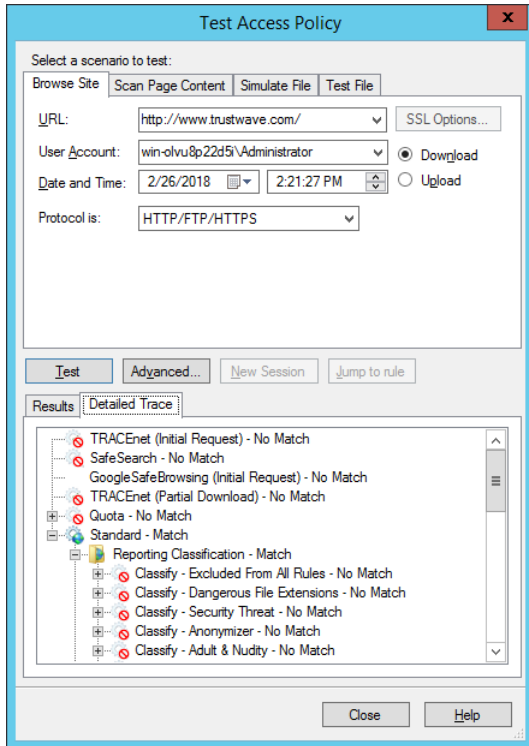
5. For the Scan Page Content tab, which applies TextCensor scripts to text and HTML documents, enter text in the box.

   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**).

6. 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.

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

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

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

10. 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.

11. If an Alternate Upstream Proxy would be used for the URL, this information is shown following the rule results.

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.

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.

> **Tip:** You can see how WebMarshal uses any item by viewing the properties of the item. For example, a User could be included in User Groups and used in Rules. A URL Category could be included in other Categories and used in Rules.
>
> - To view the properties of an item, select it and click the **Properties** icon in the toolbar, or use the right-click menu.
>
> - To open a rule or category that uses an item, select it in the properties window and then click **Jump To.**
>
> - For details of the available options, see Help for each Properties window.

WebMarshal provides the following types of elements:

User Groups

Allow you to apply policy based on user accounts or workstation IP addresses. For more information, see "User Groups" on page 96.

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 101.

URL Filtering Lists

Allow you to configure external lists sources for URL categories, including text based imports, DNS Blacklists, and the Trustwave Web Filter Database. For more information, see "Configuring URL Filtering Lists" on page 106.

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 107.

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 114.

Classifications

Allow you to classify files and requests based on rule criteria. For more information, see "Logging Activity with Classifications" on page 126.

Quotas

Allow you to limit browsing activity by time and bandwidth. For more information, see "Configuring Access Using Quotas" on page 109.

Malware Protection

Allows you to check downloads and uploads for viruses, malware, and other malicious content using third party scanners. For more information, see "Scanning Overview" on page 124.

7.1 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.

> **Note:** Connectors, previously covered in detail here, are now covered under Global Settings. See "Configuring Connectors" on page 149. You can choose to create a new connector any time you import a User Group.

7.1.1 User Groups

7.1.1.1 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**. This action does not affect logging records.

7.1.1.2 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 **User Groups** tab shows all user groups that this user belongs to. Highlight a group and click **Jump to User Group** to view the details of that group.

- 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 110.

7.1.1.3 User groups

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

- **WebMarshal** groups 👤 (user folder).

- **Windows 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).

- **IP address range** groups 👥 (users with workstation).

Typically, WebMarshal 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 quickly enable the default policy, you can import groups from connectors, or create computer groups, and then insert these new groups into the default WebMarshal groups.

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

Figure 22: WebMarshal Console, User Groups window
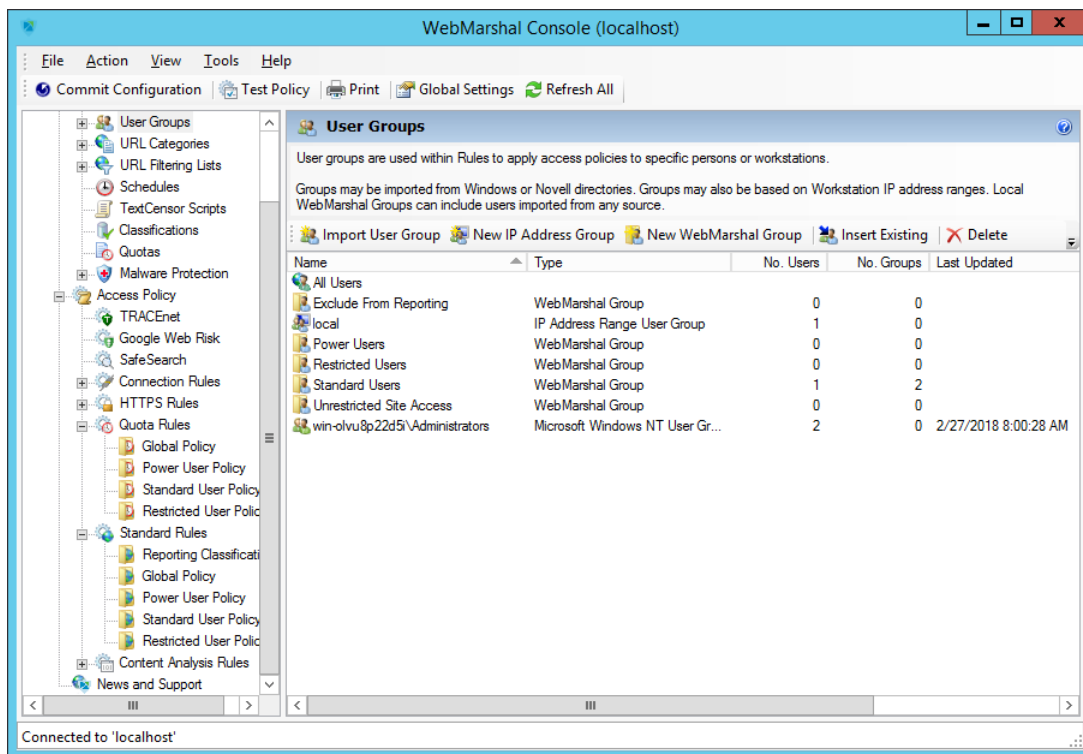
To edit the group description, and/or to reload the group (for Windows and NDS directory groups), right-click the group and click **Properties**.

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).

7.1.1.4 Adding a user group

1. In the WebMarshal Console, expand **User Groups** or a specific group.

2. From the Action menu or the right pane menu bar, choose one of the following actions:

    *   Import User Group

    *   New IP Address Group

    *   New WebMarshal Group

3. **Import User Group(s) from a Connector:** On the Import User Groups window, find and select 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.
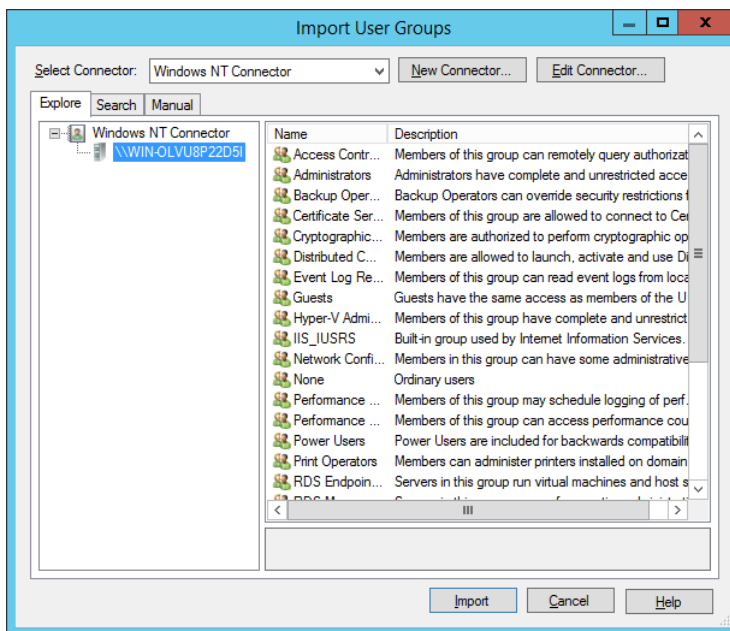
    You can explore or search for groups. You can also enter group names manually.

    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 Trustwave Knowledge Base article Q11870.

4. Click **Import** to add the User Group.

5. **New IP Address Range Group:** Enter a name and optionally a description.
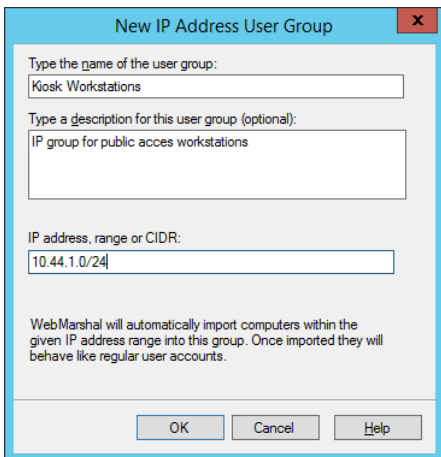
Enter an IP address, a range (starting and ending addresses separated by -) or a CIDR specification. Any user or process on a computer with an IP address in the specified range can browse through WebMarshal, subject to any Rules applied to the group.

> **Note:** A range can be in the IPv4 or IPv6 address space.
>
> 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 Group" on page 100.

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. (As a consequence, you cannot specify different permissions for the IPv4 and IPv6 interfaces of the same computer.)

6. **New WebMarshal Group:** Enter a name and optionally a description. This type of group is internal to WebMarshal. You can use WebMarshal groups to quickly apply policy to multiple groups and users.

7.1.1.5 Inserting existing groups to a WebMarshal Group

1. In the WebMarshal Console, expand a specific group within User Groups.

2. Click the **Insert Existing** 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)
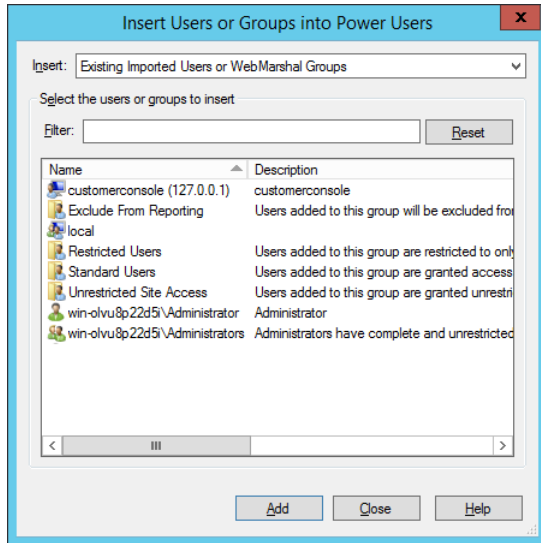
3. Within the Insert Users or Groups window, select **Existing Imported Users or WebMarshal Groups**. Select one or more users or groups with the mouse, or type the beginning of a name to select it.

4. Use the **Enter** key or click **Add** 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.

7.1.1.6 Adding computers or IP addresses to a Group

1. In the WebMarshal Console, expand a specific group within User Groups.

2. Click the **Insert Existing** icon in the tool bar.

3. Select **New Computer Accounts by IP Address** or **New Computer Accounts by Computer Name**. In the text box, enter computer names, or IP addresses, one per line. 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 IPv4 or IPv6 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.

7.1.1.7 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**.

7.2 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).

7.2.1 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 Trustwave Web Filter Database or WebMarshal's FileFilter). 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.

7.2.2 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, a particular sub-directory (path) at a site, or a specific path and file name. The * wildcard character can be placed at the beginning or the end of the site name part of the URL to match multiple similar sites.

Notes:

Matching of URLs is not case sensitive.

The path, file, and query string parts 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.

To see a list of the URLs and Categories included in a Category, expand it in the Console tree. To view more information about a category, including a list of the Rules and other Categories that use it, view the Properties of the Category. For details of the available information, see Help.

If a URL was placed in a Category by WebMarshal Rule action, the URL listing includes the date and time when it was appended. To see a report of the WebMarshal Rule action that added a URL, double-click it. (If the URL was added manually, no information is available and double-clicking will have no effect.)

Figure 23: WebMarshal Console, URL Categories window
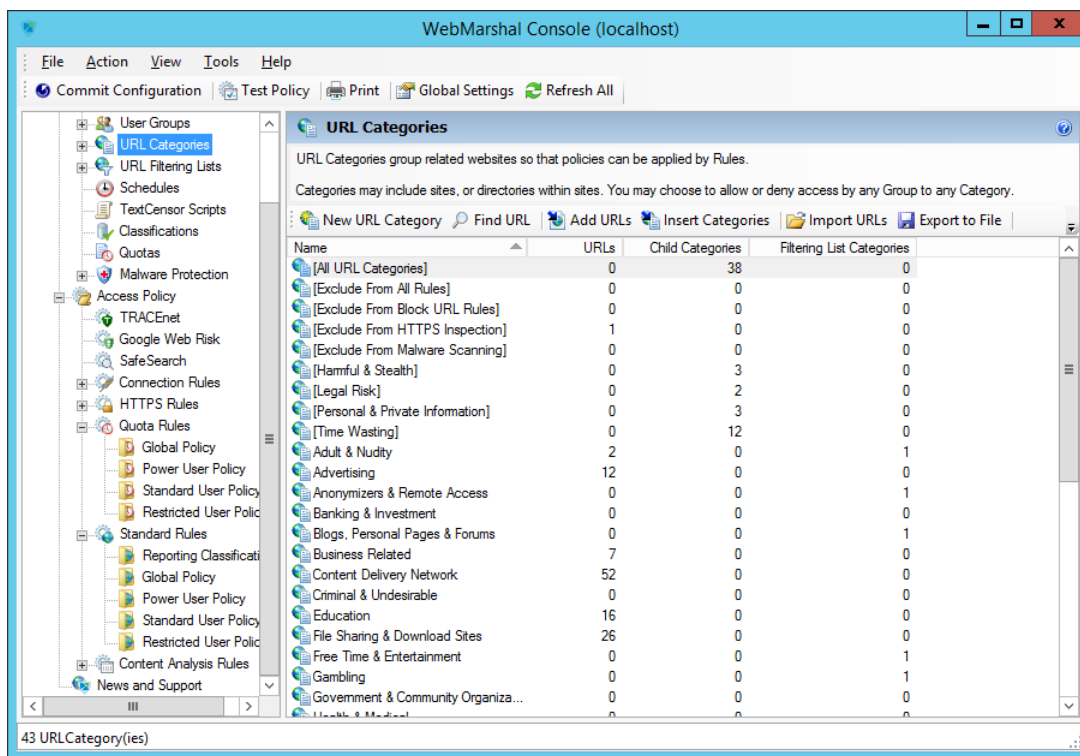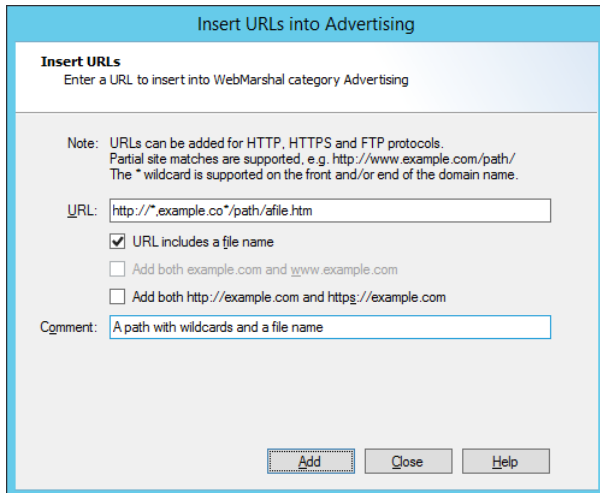
7.2.3 Adding a URL Category

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.

7.2.4 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 ![icon] in the tool bar to open the Insert URLs window.

4. To add a new URL to this category, enter the URL. You can enter any of the following:

    - A full site name or IP address literal, and optionally a port, such as:

        - `http://www.trustwave.com/`

        - `http://198.51.100.25/`

        - `http://[2001:db8:8:4::6]:81`

    - A specific sub-directory, such as
      `http://www.trustwave.com/webmarshal/`

    - A specific full path including file name, such as
      `http://www.trustwave.com/webmarshal/documentation.asp`

    - A string with an asterisk as a wildcard at the beginning and/or the end of the site part of the URL, such as `http://*.wave*` (not available with IPv6 literals)

    - Any of the above, with a query string. For details of query string matching rules, see "URL Query String Matching" on page 104.

5. To clarify that the entry includes a file name, check the box **URL includes a file name**. This box is disabled when the last character of the URL entered is / (slash). (URLs with a file name do not have a slash at the end of the resulting URL.)

6. Optionally select the variations of the URL that you want to add (such as the www. prefix or HTTPS and HTTP protocols).

7. Click **Add** (or press **Enter**) to add the URL to this category.

8. The window remains open so you can add additional URLs.

9. Click **Close** when done.

7.2.5 URL Query String Matching

When you manually add a URL to a URL Category, you can include a query string part. WebMarshal will match URLs that contain the query string text you enter.

Like all URL matching, query string matching is not case sensitive. You cannot use wildcards in the query string part.

- Begin the query string part of the URL with ?

  - For example, `http://example.com/?query=1`

- The query string can contain one or two strings to match exactly. Separate the strings using &

  - For example, `http://example.com/path/file.htm?this=1&that=text`

- If you include two strings, both must be present for the URL to be matched.

  - `http://example.com/?this&that` does not match `http://example.com/?this`

- The strings will be matched in any order, and will match a URL with additional query parts.

  - `http://example.co*/?this&that` matches `http://example.com/?that&more&this`

- If you add query strings to an entry, they match on any deeper path.

  - `http://*.com/?this&that` matches
    `http://example.com/path/file.htm?that&this&more`

- Strings must match exactly.

  - `http://example.com/?attach` does not match `http://example.com/?attached`

- To match a key-value pair you must enter the exact key=value string.

  - `http://example.com/?true` does not match `http://example.com/?this=true`

> **Tip:** Characters in the query string should be urlencoded. For example, a literal ampersand (&) in a string should appear as `%26` (but the & used as a separator for parameters must not be encoded).
>
> To be sure of matching spaces you may need to match both `+` and `%20` (for example, `http://example.com/?a+space&a%20space`).

7.2.6 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 ![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).
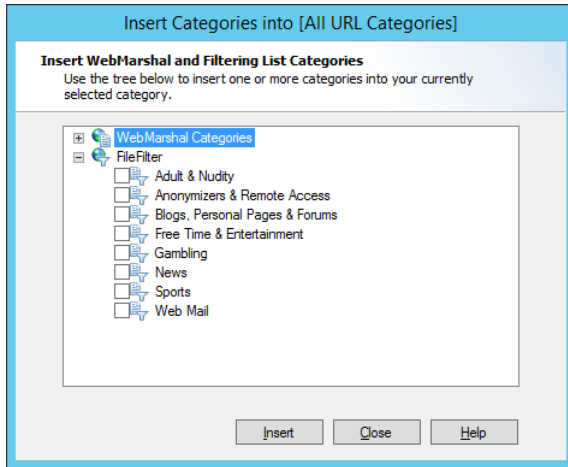
4. To include one or more URL categories in this category, expand the tree and select the desired categories.

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.

7.2.7 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 174.

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.

7.2.8 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**.

7.2.9 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.

7.3 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 174.

*   **URLCensor:** A real-time facility that categorizes IP addresses through DNS Blacklist lookup. For more details about URLCensor please see "URLCensor" on page 175.

*   **Trustwave Web Filter Database**: A URL list provided by Trustwave and licensed separately. The list consists of 116 categories. For more information on the Trustwave Web Filter Database including trial license information, please see "Trustwave Web Filter Database" on page 176

7.3.1 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, or to initiate an update for all servers, right-click a list name in the left pane. Click **Update All Servers** to force an immediate check for Filtering List updates (where internet updates are provided).

    🔍 **Note:** 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 for the server.

7.3.2 Adding Filtering Lists

You can add one or more filtering lists to the WebMarshal configuration. For additional details, see Help.

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. Click **Next**.

4. For the Trustwave Web Filter Database, to allow WebMarshal to validate the license (one time requirement), select an Internet connection method that is valid from the WebMarshal Array Manager server, and then click **Next**.

5. Click **Finish** to validate the license (if required) and 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 104.

> **Note:** WebMarshal will use the categories for filtering as soon as the list is available on processing servers. For the Trustwave Web Filter Database, the initial population of categories can take half an hour or longer, depending on Web connection speed.

7.3.3 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.

7.3.4 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.

7.4 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.

> **Note:** Schedule times are calculated in local time on the processing server that handles a request.

You can apply different schedules for different user groups.

To list the rules that use a schedule, view the properties of the schedule.

7.4.1 Adding a Schedule

1. Select **Schedules** in the left pane.

2. Click the **New Schedule** icon ![icon] in the tool bar to start the New Schedule wizard.
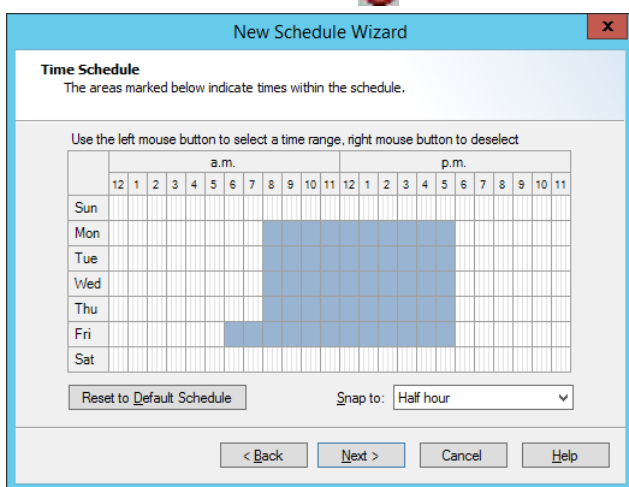
3. On the Time Schedule page of the wizard, drag with the left mouse button to add to the blue "inside" area. Drag with the right mouse button to erase from the blue "inside" area.

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 menu.

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.

7.4.2 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 menu.

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.

7.4.3 Duplicating a Schedule

To duplicate a schedule:

1. Right-click the Schedule name in the right pane.

2. Select **Duplicate**.

7.4.4 Deleting a Schedule

To delete a Schedule:

1. Right-click the Schedule name in the right pane.

2. Select **Delete.**

7.5 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. To list the rules that use a quota, and the quota usage for each user, view the properties of the quota.

7.5.1 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). Choose whether to apply the quota to pages served from the WebMarshal Proxy Cache.

7. Click **Next** to continue.

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 128.)

    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.

7.5.2 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.
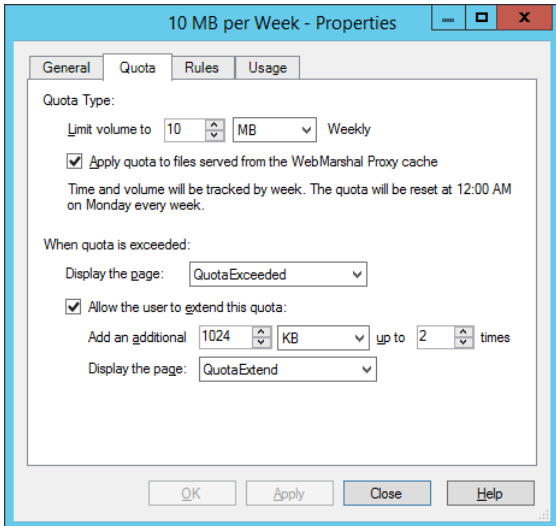
5. On the Rules tab, you can see a list of rules that apply to this quota. Highlight a rule and click **Jump to Rule** to view the details of that rule.

6. On the Usage tab, you can see the quota usage for a selectable period 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.
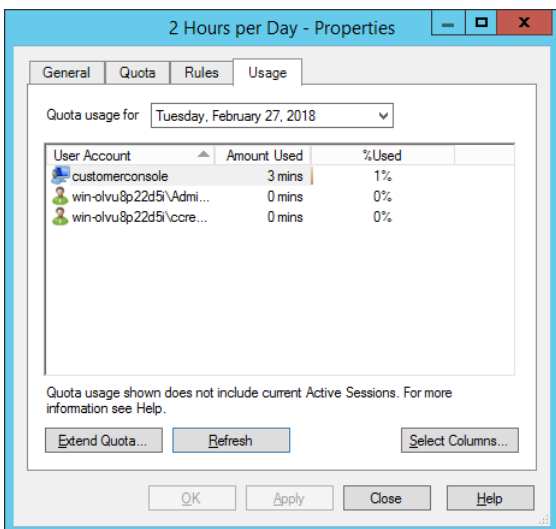
7. To extend the quota for a specific user, select that user from the list then click **Extend Quota** to open the Extend Quota window.
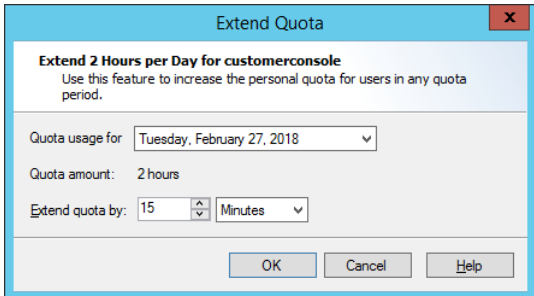
- The window shows the user's default allocation. Enter the desired extension as a number of minutes, hours, KB, MB, or GB. Click **OK** to apply the change and return to the Quota Properties window.

Note: Changes made here only affect the selected 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 113.

8. Click **OK** to save the changes to the Quota, or **Cancel** to lose any changes.

7.5.3 Duplicating a Quota

To duplicate a Quota:

1. Right-click its name in the right pane.

2. Select **Duplicate.**

7.5.4 Deleting a Quota

To delete a Quota:

1. Right-click its name in the right pane.

2. Select **Delete.**

7.5.5 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.

Figure 24: WebMarshal User Quota page
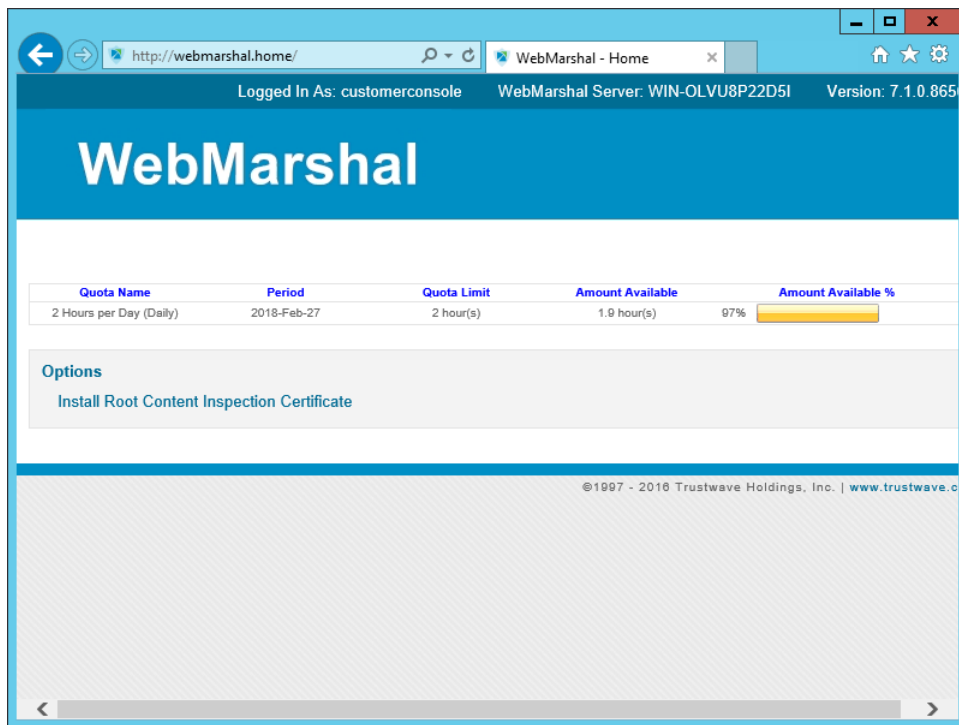
Each quota for that user is displayed. The quota limit (including extensions used if any), amount remaining, and percentage remaining are shown.

7.5.6 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 108).

7.5.7 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 135. For additional details see Trustwave 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.

7.6 Identifying Web Content Using TextCensor Scripts

TextCensor scripts allow you to check for the presence of particular content in a file or text. You can apply TextCensor to any text, including web pages, plain text files, and text extracted from PDF or Office documents.

TextCensor supports Unicode and wide characters, and is designed to work intuitively with a wide variety of languages.

A script can include many conditions based on text combined using logical and positional operators. Triggering of the script is based on the weighted result of all conditions.

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. To see a list of rules that use a script, view the properties of the script.

7.6.1 TextCensor Elements

TextCensor scripts contain one or more expressions, each consisting of a word or phrase.

You can use two wildcard characters, anywhere in a word or phrase.

- * matches zero or more letter or digit characters.

- ? matches one letter or digit.

Wildcards match only letters and digits, and apostrophes or hyphens that are treated as part of words (see "Word Breaks" on page 118). Wildcards do not match other symbol characters.

If you want to set the order of evaluation of a complex expression that uses more than one operator, use parentheses ( ).

Each TextCensor expression can include logical and positional operators. The operators must be entered in UPPERCASE.

7.6.1.1 Positional Operators

TextCensor works with the positions of words or phrases within a file. For example, in the sentence "The quick brown fox jumps over the lazy dog" the word "quick" starts and ends at position 2, and the phrase "jumps over" starts at position 5 and ends at position 6.

A positional operator works with expressions that evaluate to sets of positions. It takes two sets of positions as parameters, and returns a new set of positions.

> **Tip:** In a simple TextCensor expression, you can think of the expression result as "true" or "matched" if the word or phrase is found in any position in the text. When the word or phrase is found in more than one position, this counts as more than one match of the expression.
>
> When you combine positional operators to make a complex expression, note the explanations of the sets returned by each operator (see below). Test your script before applying it in production.

You can specify a distance for many positional operators. The default distance (if you do not specify a value) is 4.

Table 5: TextCensor Positional Operators

Operator and Syntax	Matching Results
FOLLOWEDBY `A FOLLOWEDBY[=distance] B`	The start of B occurs within *distance* words from the end of A. Returns a set of positions spanning from the start of A to the end of B. `dog FOLLOWEDBY hous*` matches `Dog in the house`
NOT FOLLOWEDBY `A NOT FOLLOWEDBY[=distance] B`	The start of B does not occur within *distance* words from the end of A. Returns a set containing the positions in A that are not followed by B. `dog NOT FOLLOWEDBY=1 hous*` matches `Dog in the house`
PRECEDEDBY `A PRECEDEDBY[=distance] B`	The end of B occurs within *distance* words from the start of A. Returns a set of positions spanning from the start of B to the end of A. `dog PRECEDEDBY cat` matches `Cat chasing dog`
NOT PRECEDEDBY `A NOT PRECEDEDBY[=distance] B`	The end of B does not occurs within *distance* words from the start of A. Returns a set containing the positions in A that are not preceded by B. `dog NOT PRECEDEDBY=2 cat` matches `Cat was not chasing dog`
NEAR `A NEAR[=distance] B`	If A occurs within *distance* words before B the resulting position spans from the start of A to the end of B. If B occurs within *distance* words before A the resulting position spans from the start of B to the end of A. `dog NEAR cat` matches `Cat chasing dog` and also matches `Dog chasing cat`
NOT NEAR `A NOT NEAR[=distance] B`	Returns the positions of all instances of A where B is not found within *distance* words from A `dog NOT NEAR=2 cat` matches `Cat was not chasing dog` and also matches `Dog was not chasing cat`
OR `A OR B`	This form of the OR operator is applied when both A and B are sets of positions, even if one or both are empty sets. It returns the union of position sets A and B. For the sentence "A rose is a rose", the expression (`rose OR is`) returns the position set 2,3,5.

7.6.1.2 Logical (Boolean) and Special Operators

A logical operator takes Boolean (true/false) values as input, and returns a Boolean result. These results cannot be used as parameters of a positional operator.

When one of the parameters to a logical operator is an expression that returns a position set, the parameter is treated as a logical value. A set with at least one position match is treated as true. A set that has no matches is treated as false.

TextCensor also supports the special operator INSTANCES.

Table 6: TextCensor Logical and Special Operators

Operator and Syntax	Matching Results
OR `A OR B`	Returns true if A or B (or both) is true. This form of the OR operator is applied when either A or B (or both) are logical expressions. If both A and B are position sets then the positional OR operator is used instead.
AND `A AND B`	Returns true if both A and B are true.
NOT `NOT A`	Returns the opposite of A (true if A is false).
INSTANCES `A INSTANCES=count`	A must be an expression that returns a position set. The result is true if A contains *count* or more word positions; otherwise the result is false.

7.6.1.3 Anchored Regular Expressions

TextCensor supports use of Regular Expressions through the ARX operator.

An anchored regular expression is a regular expression (regex) which must be preceded by a word on the left hand side of the ARX operator. Matching of the regex begins at the next character following the word. **Regex patterns must always begin by matching one or more non-word characters.** In most cases you can start the regex pattern with \W to match non-word characters..

Notes:

- ARX is based on Google RE2. The syntax generally follows well known Regular Expression syntax.

- Distance parameters for ARX operators are specified in characters.

- Regular expressions are case insensitive by default. You can force case sensitive matching with the operator `?-i`

- ARX does not support lookahead or lookbehind.

- ARX does not support capture groups. Capture groups will be ignored or converted to non-capturing sequences.

- ARX does not support `\Q...\E` literal text.

- For further details of the ARX syntax, see the [RE2 wiki](#).

Table 7: TextCensor Regular Expression Operators

Operator and Syntax	Matching Results
ARX `A ARX[=distance] /pattern/`	Locates instances of A where it is followed by text matching the regex pattern within *distance* characters of the end of A. The entire pattern must occur within the specified distance. The resulting position list spans from the beginning of A to any content matched by the regex. `dog chasing ARX /\W(one|two|10) cat(s*)/`
NOT ARX `A NOT ARX[=distance] /pattern/`	Locates instances of A where text matching the regex pattern does not occur within *distance* characters of the end of A. When this expression matches, the resulting position list is the position list of A.

Multiple anchored regular expressions can be combined with other expressions and operators to create complex statements. For example,

```
((dog OR boy) FOLLOWEDBY=1 ((chasing OR leading) ARX /\W(one|two|10)/) NEAR
big) FOLLOWEDBY (white ARX /\W(horse|cat)s*/)
```

matches the phrase: *dog chasing one or more big white cats.*

7.6.2 TextCensor Concepts

The following concepts clarify how TextCensor expressions are evaluated.

Note: This section does not apply to Regular Expression patterns.

7.6.2.1 Words

A word is made up of one or more letters and digits, and sometimes symbols.

- In alphabetic languages, a word is a group of letters or digits separated by other characters (such as punctuation, other symbols, and white space).

- In Chinese, or Japanese kanji, a word or "token" may be composed of one or more characters (ideo-graphs).

7.6.2.2 Phrases

A phrase is made up of a series of words separated by word break characters.

7.6.2.3 Symbols and Punctuation

Symbols other than letters and digits are not treated as part of a word unless they appear in the specific statement being evaluated. A group of symbols is not treated as a word.

> **Tip:**
> - The text `word$deed` is matched as two words by the expression `word FOLLOWEDBY deed`, and also by the exact expression `word$deed`
> - The text `$word$` is matched by any of `word`, `$word`, `word$`, or `$word$`
> - The text `Save $$$ Now` is matched by `save FOLLOWEDBY=1 now`

7.6.2.4 Word Breaks

The sets of characters that are treated as word and number break characters generally follow Unicode standards.

A word break character can also be matched exactly or by a wildcard.

> **Tip:**
> - Each of the following strings is treated as one word:
>   ```
>   John's
>   3.14159
>   1,234.56
>   3a
>   REV.B (the full stop between letters with no surrounding spaces is not a word break)
>   ```
> - The text `half-baked` is treated as two words and is matched by any of the following expressions:
>   ```
>   half FOLLOWEDBY=1 baked
>   half-baked
>   half?baked
>   ```

7.6.2.5 Accented Letters

TextCensor treats each accented character as a single letter. A letter with additional composed accent characters is normalized to a single character before the text is evaluated.

7.6.2.6 Escape Characters

Some characters have special meanings in TextCensor. These characters are parentheses, square braces, the asterisk, the equal sign, the double quote character, and the question mark. You can place a backslash character ('\') before any of these characters in order to use the character's normal meaning. To use a normal backslash character, place two of them together ("\\").

Within ARX expressions, the Regular Expression reserved characters apply (in particular the forward slash '/' which marks the start and end of the regex pattern).

7.6.2.7 Case Sensitivity

TextCensor evaluation is NOT case sensitive by default. To perform a case sensitive match, quote the content using double quote characters. All special characters and escape characters retain their meaning within double quotes.

7.6.2.8 Classes

You can use TextCensor Classes to match specific types of characters inside a word, or special types of words.

Table 8: TextCensor Classes

Operator and Syntax	Matching Results
[LETTER]	Matches any single letter inside a word.
[DIGIT]	Matches any single digit inside a word.
	For example, `A[LETTER]B[DIGIT]C` would match both "axb0c" and "aab9c".
[NUM]	Use in place of a word to match any number made up of one or more digits. This class does not match numbers with a decimal point, or Asian language numbers that use words between characters
[CCARD]	Use in place of a word to match a series of digits that look like credit/payment card numbers. These numbers consist of up to 5 groups of digits, are up to 19 digits in length, and must pass checksum validation (using the Luhn algorithm). This class should match most card numbers.
[US-SSN]	Use in place of a word to match series of digits that look like US Social Security Numbers. Valid numbers must follow a specific format. However, the format is loosely defined and it is not possible to prevent accidental matching of other numbers.
[CAN-SIN]	Use in place of a word to match a series of digits that looks like a Canadian Social Insurance Number. Valid numbers must follow a specific format and pass a Luhn check.

7.6.2.9 Named Statements

You can give a TextCensor statement a name. When a named statement is executed, the result is stored. You can reference it in later statements within the same script.

If a statement contains only words or only uses positional operators, the stored result is the set of word positions found by that statement. If the statement uses any other operators then the result is logical.

You can reference the result of a statement by using `[@name]` inside a statement. This can be used anywhere that you would otherwise use the bracketed result of an operator.

Note: Naming a statement does not affect the statement's score. To use a named statement as a macro expression, in most cases you should set the statement's score to zero.

When using named statements within other expressions, remember that the result must match the required parameter type. If a statement returns a logical result you cannot use it as a parameter to a positional operator. Test your scripts before applying them in production.

7.6.3 Scoring a TextCensor Script

Each script is given a trigger threshold, expressed as a number. Each expression in a script is given a positive or negative score. If the total score of the content being checked reaches or exceeds the trigger threshold, the script is triggered.

The total score is determined by summing the scores resulting from evaluation of the individual expressions in the script.

For each expression, if the result is a true logical value, the expression score is the base score.

If the expression result is a position set (the word or phrase was found one or more times in the text), by default the final score of the expression is the base score. You can choose how to add the score when the expression is matched more than once. The options are:

Table 9: Cumulative scoring options

Option	Description
Every time	Each match of the words or phrases adds the score to the total.
First Match Only	Only the first match of the words or phrases adds the score to the total.
First N Matches	Each match, up to the number you set, adds the score to the total. For instance if the expression score is 5 and you select "first 3 matches," then the expression can contribute up to 15 to the total score, but never more than 15.

Negative scores and trigger levels allow you to compensate for the number of times a word could be used in text that you do not want to match. For instance: if `breast` is given a positive score in an "offensive words" script, `cancer` could be assigned a negative score (since the presence of this word suggests the use of `breast` is medical/descriptive).

Note: Script evaluation always checks all expressions to obtain the final score. The order of expressions in a script is not significant. This is a change from earlier versions.

7.6.4 Adding a TextCensor Script

1. Select **Policy Elements > TextCensor Scripts**.

2. Click the **New TextCensor Script** icon in the tool bar to open the New TextCensor Script wizard. If necessary click Next to continue to the TextCensor Expressions window.
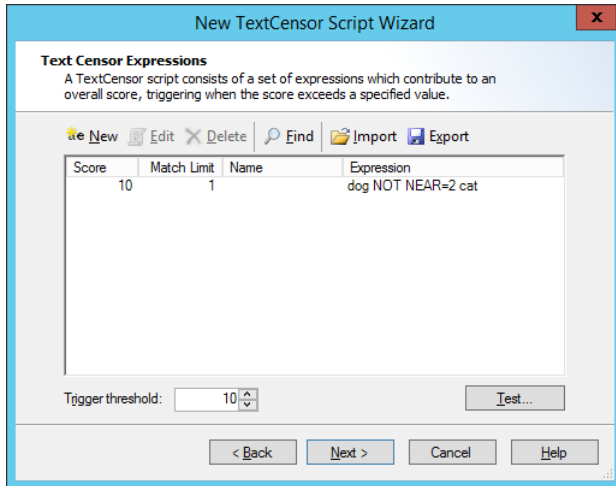
3. Click **New** to open the Add TextCensor expression window.
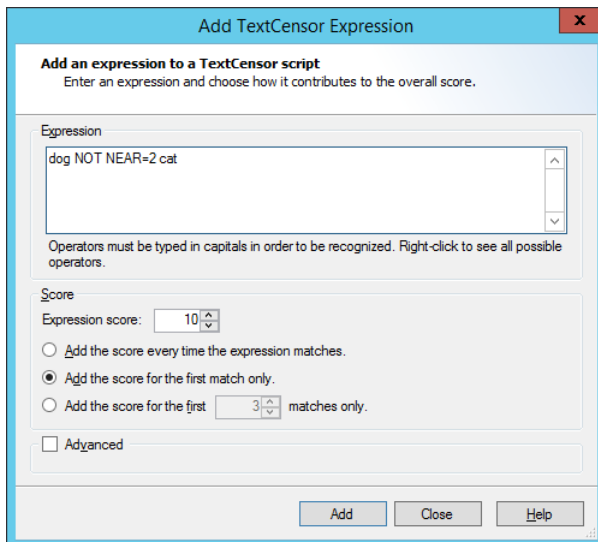
4. Enter the expression, optionally using the operators described earlier. For example:

       (Dog FOLLOWEDBY hous*) AND NOT cat

   In this example the expression score 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 expressions are **not** case sensitive by default. However, quoted content is case sensitive. So textcensor would match TextCensor, but "textcensor" would not.

5. Select a score and contribution method for this expression (see "Scoring a TextCensor Script" on page 120 for more information).

6. Click **Add** (or press **Enter**) to add the expression to this script. The window remains open so you can create additional expressions.

7. When all expressions have been entered, click **Close** to return to the New TextCensor Script window.

8. Select a trigger threshold. If the total score of the script reaches or exceeds this level, the script is triggered. The total score is determined by evaluation of all expressions in the script.

9. Click **Next**

10. On the TextCensor Script Information page, enter a name and optional description for the script.

11. Click **Next,** then **Finish,** to add the script.

7.6.5 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 script properties window.

3. Double-click an expression to edit it.

4. To delete a line, select it and click **Delete**.

5. Change the script name and trigger level as necessary.

6. Click **OK** to accept changes or **Cancel** to revert to the stored script.

7.6.6 Importing a TextCensor Script

You can import TextCensor scripts from files.

> **Note:** You can import scripts in the format used by WebMarshal 6.9.5 and above, as well as scripts in the format used by earlier versions. The earlier version scripts will be upgraded to the new format automatically. Any problems with upgrading will be reported.

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.

7.6.7 Exporting a TextCensor Script

You can export TextCensor scripts to XML or text 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 script properties window.

3. Click **Export**.

4. Enter the name of the file you want to create, and click **Save**.

5. In the script properties window, click **OK**.

7.6.8 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.

7.6.8.1 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 score 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 score (that is, promoting earlier triggering) than, for example, `college sports`.

7.6.8.2 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 score 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.

7.6.9 Testing TextCensor Scripts

To test the operation of a TextCensor script:

1. Click **Test** on the New TextCensor Script or script properties window to open the Test TextCensor window.
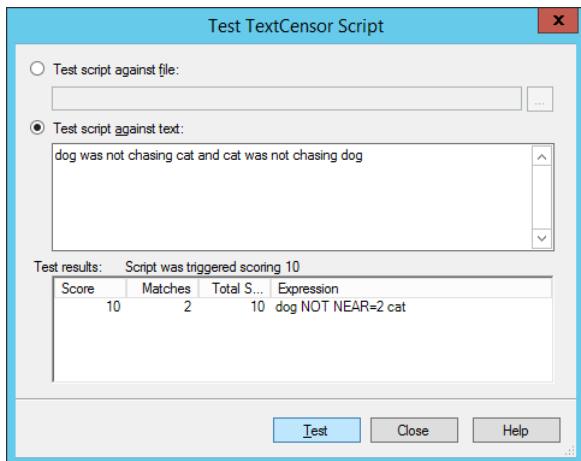
2. In the Test TextCensor window, enter the sample text you want to test using one of two methods.

    •   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 expressions which triggered and their scores) 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 93 for detailed information on Rule testing.

7.7 Using Malware Scanning

WebMarshal can invoke third-party scanners to check file uploads and downloads for malware, including viruses and other malware. Before you enable scanning Rules, you must install at least one supported scanner *on each processing server*, and configure the scanners within WebMarshal.

7.7.1 Scanning Overview

WebMarshal currently supports only specific malware scanners that have licensed DLL interfaces.

Supported scanners include Bitdefender for Marshal, McAfee for Marshal, and Sophos for Marshal.

> **Note:** The Sophos (SAVI interface) and Symantec scanners that were previously supported are not supported in this release, as the required 64-bit integration is not currently available. These scanners may be available in a future release depending on the availability of the third party integration.
>
> Customers using Sophos Anti-Virus (SAVI interface) can move to Sophos for Marshal and should contact Trustwave for details.
>
> Kaspersky for Marshal is no longer sold and signature updates end December 31, 2023.

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 malware, 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 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.

7.7.2 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.

2. Click the **New Malware Scanner** icon 🐞 in the tool bar to start the New Virus Scanner Wizard.
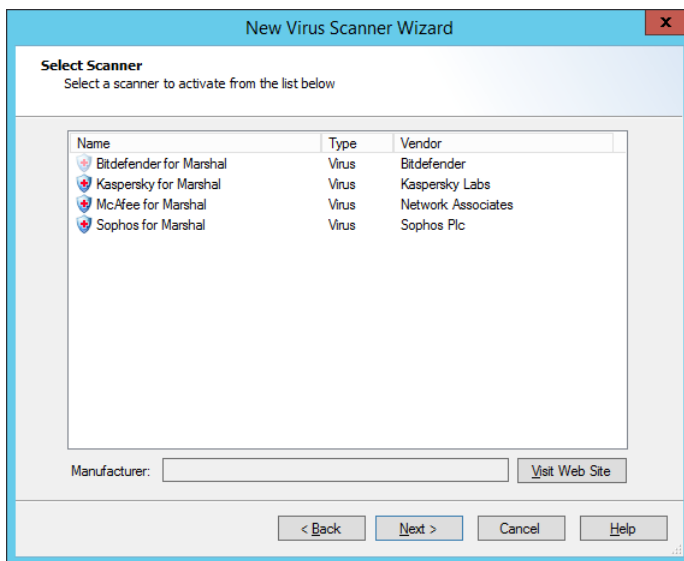
3. The Select Scanner page of this Wizard shows a list of scanners WebMarshal can use.

   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.

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:** Bitdefender for Marshal, McAfee for Marshal, and Sophos for Marshal each require installation of a configuration Console, available in separate downloads from Trustwave (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 Trustwave supplier. If you are a customer with a permanent WebMarshal key and you want to try one of these scanner products, contact your Trustwave supplier for a special time-limited key.

7.7.3 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.

> **Note:** 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.

7.7.4 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.

7.8 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.

7.8.1 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. For details see Chapter 8, "Reporting on Browsing Activity".
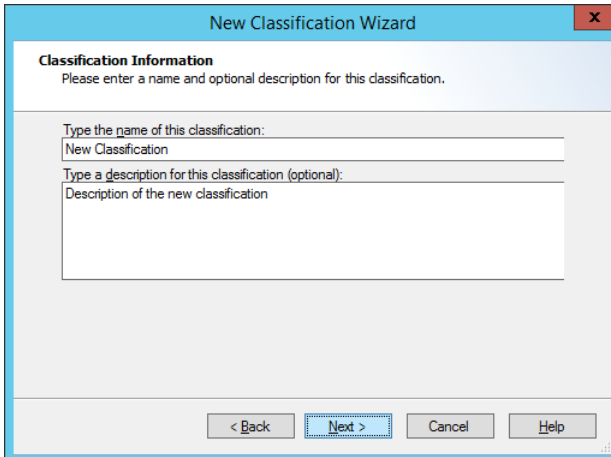
In addition, when any filtering list integration is enabled, every browsing request returns a categorization as provided by the filtering list. These categorizations are recorded regardless of whether they are used within rules to filter requests. This process is separate from the logging of classifications. You can generate reports based on the categorizations.

To see a list of rules that use a classification, view the properties of the classification.

7.8.2 Adding a Logging Classification

To add a classification:

1. Select **Classifications** in the left pane of the console.

2. Click the **New Classification** icon ![icon] in the tool bar to open the New Classification wizard.

In the New Classification window, enter a name and optionally a description for the classification.

3. Complete the wizard to add the classification.

7.8.3 Editing a Logging Classification

To edit a classification:

1. Double-click the classification name in the Console to open the Edit Classification window.

2. Make any required changes.

3. Click **OK**.

7.8.4 Deleting a Logging Classification

To delete a Classification:

1. Right-click the classification name in the Console.

2. Select **Delete**.

7.9 Notifying Users with Notification Pages

WebMarshal uses web pages to provide pre-configured notification messages to users. The notifications can also be customized.

7.9.1 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.

7.9.2 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` sub-directory 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.
>
> You can store small helper files in this location, but any large content should be served from another location.

- **Page Blocked–**for denied web pages and other items where no part of the file was returned to the browser.

    - 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 returned to the browser.

    - Standard

    - Malicious (Malware content)

    - Virus (virus content)

- **File Blocked–**for denied file type or size.

- Standard

- Malicious (Malware content)

- TextCensor (lexical scan found denied content)

- TextCensor Offensive (lexical scan found offensive content)

- Virus (virus content)

- **GoogleWebRisk–**used by the Google Web Risk policy. Any custom versions of these pages must include the Google disclaimer.

  - GoogleWebRiskBlocked

  - GoogleWebRiskWarning

- **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)

  - 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)

7.9.3 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 returned 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">`

- Files over 32KB in size (such as a company policy document) should not be served from the Templates sub-directory, to avoid deadlock problems with configuration updates. Host large files on another server/site.

- 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 Trustwave Knowledge Base article Q10318 for more details.

8 Reporting on Browsing Activity

WebMarshal can log web request activity in a Microsoft SQL database (using either SQL Server or SQL Express). The Marshal Reporting Console application allows you to generate reports based on this information.

WebMarshal can also send records of activity to a Syslog server.

8.1 Marshal Reporting Console

The Marshal Reporting Console is based on SQL Server Reporting Services, and offers scheduled generation and automatic delivery of reports. For more information about this application, see the Trustwave website or contact Trustwave.

> **Note:** You can set up a link from the Console to the MRC application. To enter the URL for the link, see Global Settings > Reporting Database.

The reports provided by MRC allow you to examine browsing behavior, successful and denied requests over time. Available reports include bandwidth, URL, and quota information.

> **Note:** The workstation based WebMarshal Reports application, previously included with WebMarshal, is no longer available. Earlier versions of the Reports application cannot be used with current versions of WebMarshal. The Marshal Reporting Console provides many of the same reports that were previously available.

For more information about creating the database, see "Reporting Database" on page 38.

8.1.1 Configuring WebMarshal for Accurate Reporting

When configuring WebMarshal and Marshal Reporting Console, keep the following points in mind:

- 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 126.

- WebMarshal logs activity to the reporting database in UTC. When you run reports, the periods and times shown are adjusted for a time zone selected by the Marshal Reporting Console user.

- WebMarshal Proxy Caching does not affect the data reported. A request that is fulfilled from the cache is reported to be the same size 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 Trustwave 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.

8.2 Syslog Logging

Each WebMarshal node can send details of activity using the Syslog protocol. This information can be used by an enterprise SIEM application for monitoring and reporting.

Syslog configuration is through the proxy configuration file on each node. For more information, see Trustwave Knowledge base article Q21116.

9 Managing WebMarshal Configuration

The WebMarshal Console allows you to manage your product license, and control advanced product 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

- Alternate upstream connections

- 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.

9.1 Configuring Global Settings

The Global Settings window (previously known as Server and Array Properties) allows the administrator to modify settings that affect server operation for the entire installation. These are divided into a number of categories.

> **Note:** Licensing information, previously located in Server and Array Properties, is now accessed from the **Tools** menu of the main Console window. See "Managing Licensing Information" on page 163.

9.1.1 System Settings

These items are related to administration of the installation.

- **General:** View information about the WebMarshal version and the latest committed configuration; set session timeouts.

- **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.

- **Remote Console:** Configure access to a web-accessible WebMarshal Console.

- **Reporting Database:** Set up activity logging in the SQL database.

- **Traffic Logging:** Set up activity logging in text files.

- **Customer Feedback:** Anonymously send browsing history through WebMarshal back to Trustwave to improve product quality and functionality.

- **Security Permissions:** Run the WebMarshal Security Tool to configure console access.

9.1.2 Proxy Settings

These items affect client connections to the WebMarshal processing nodes, and connections from WebMarshal to the Internet. Some of these settings can be customized for each Server Group.

- **Proxy Caching:** Activate and configure the Proxy Cache feature

- **Local Address Table:** Edit the list of IP addresses allowed to make client connections.

- **Ports and Authentication:** Edit the list of ports WebMarshal uses for client connections, and the authentication methods accepted.

- **Download Options:** Configure thresholds for scanning-related delays.

- **Internet Connection:** Set the method used by WebMarshal to retrieve requested items from the Internet.

- **Proxy Bypass List:** Configure a list of sites that are excluded from all WebMarshal processing.

9.1.3 Engine Settings

This item affects unpacking of files by the WebMarshal Engine.

- **Unpacking:** Configure a list of URL Categories that might be the source of large files that should not be unpacked and scanned.

9.1.4 Policy Element Settings

These items affect elements used in Rules.

- **Connectors:** Configure directory services used to import users into WebMarshal.

- **HTTPS Content Inspection:** Create the Certificate required for HTTPS inspection, and enable or disable this feature.

- **Filtering List Schedule:** Configure update schedules for URL lists.

- **Connection Rules:** Enable or disable processing of this type of rule.

9.1.5 Advanced Settings

- **General:** Configure logging level for WebMarshal services and other minor items.

- **HTTPS Connection Restrictions:** Configure settings that affect access for non-browser HTTPS applications.

To access the Global Settings window, select **Tools > Global Settings.** 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 162.

9.1.6 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.

Figure 25: WebMarshal Properties, General window
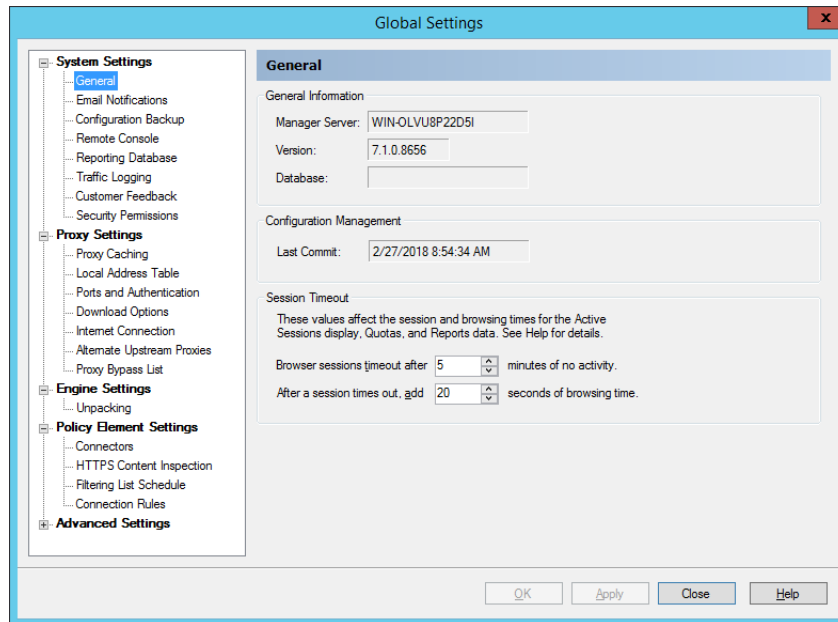
You can commit and revert configuration changes from the Console **Action** menu. You can back up and restore configuration from the Console **File** menu. See "Configuring Configuration Backup" on page 136 and "Working with Configuration" on page 157.

9.1.6.1 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 Trustwave Knowledge Base article Q11755.

9.1.7 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.

Figure 26: WebMarshal Properties, Email Notifications window
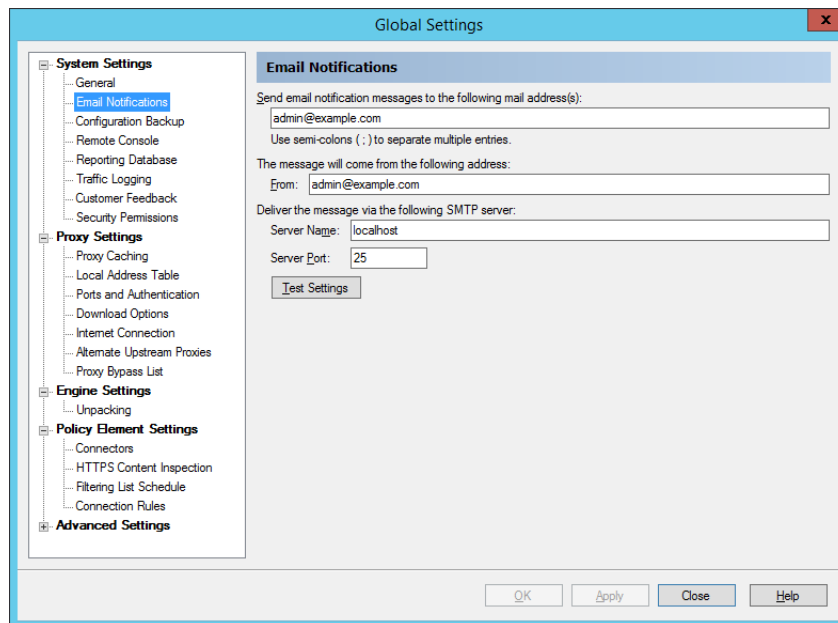
To configure notifications:

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.

9.1.8 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 158.

You can also choose to back up configuration every time configuration is committed.

Figure 27: WebMarshal Properties, Configuration Backup window
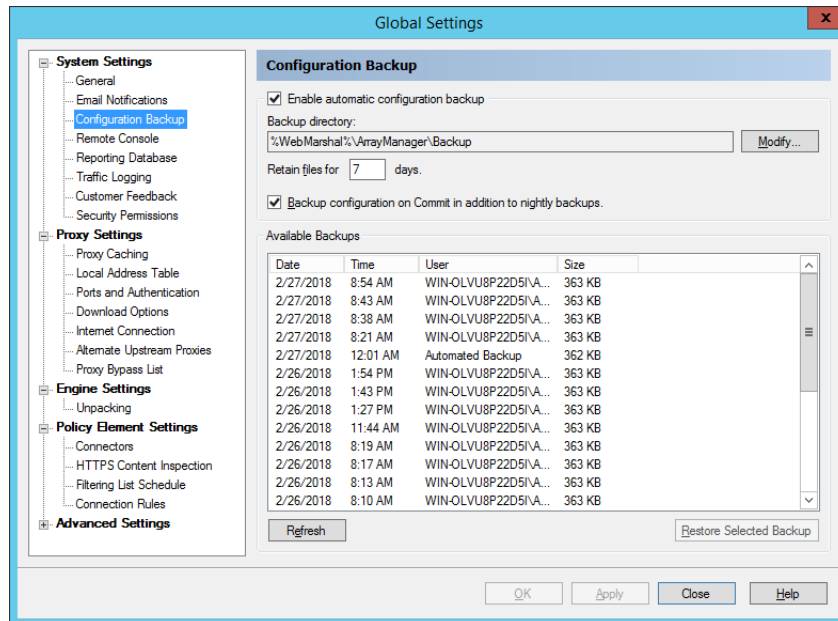
To configure Backup:

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. This can be a local or network location. For details, see Help and Trustwave Knowledge Base article Q12959.

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**.

9.1.9 Configuring Remote Console Access

The Remote Console window allows you to configure access to the WebMarshal Console from any location that can access the WebMarshal proxy as a client (addresses in the Local Address Table). Users can start the Console from a link on the WebMarshal Home page. Remote Console access uses the Microsoft "Click Once" functionality to install a temporary copy of the Console.

Figure 28: WebMarshal Properties, Remote Console window
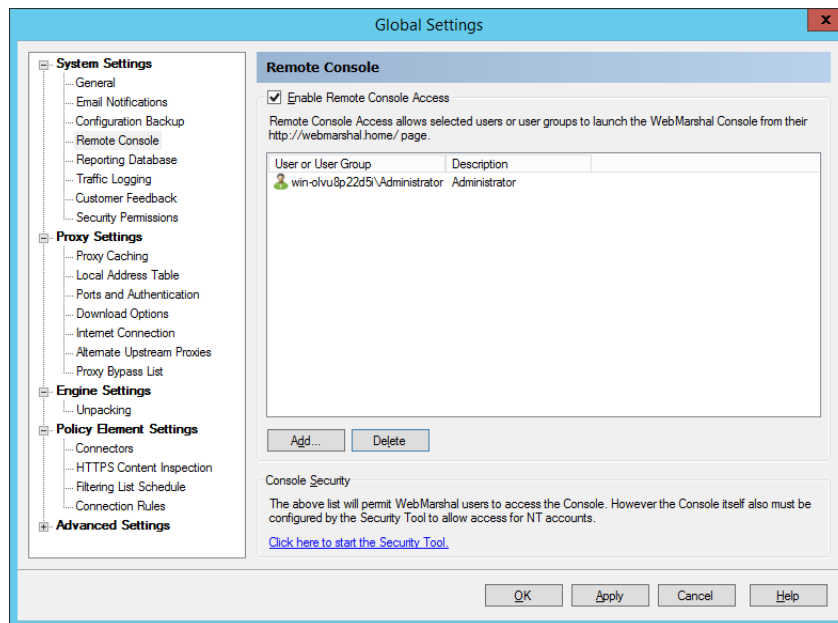
To enable Remote Console:

1. Select **Enable Remote Console Access**.

2. Edit the list of users and groups that are permitted access. These users will see a link to the Console on their WebMarshal Home page.

3. Use the WebMarshal Security Tool to configure access to the Console and individual Console features for specific Windows accounts. By default, members of the Administrators group on the Array Manager server have full access.

For more information about the Remote Console feature and configuration, see Help.

> **Note:** .NET 4.6.2 must be installed on the client workstation. For more tips about client requirements, see Trustwave Knowledge Base article Q13709.

9.1.10 Configuring the Reporting Database

The Reporting Database window allows you to view and change the location of the optional WebMarshal reporting database, as well as data retention settings. You can also enter the URL of the Marshal Reporting Console, if installed.

Figure 29: WebMarshal Properties, Reporting Database window
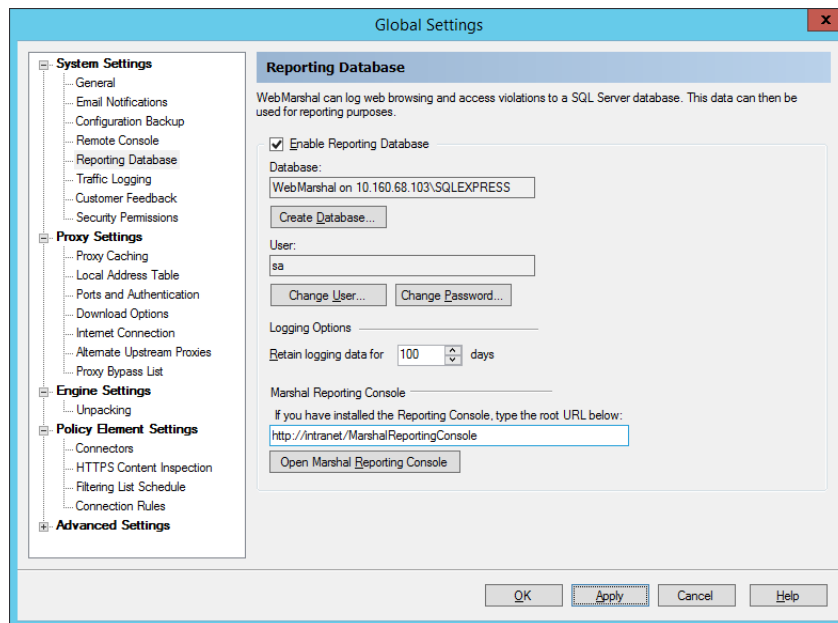
To enable logging:

1. Check the box **Enable Reporting Database.**

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:

- **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.

To configure the Marshal Reporting Console link:

- **Marshal Reporting Console:** Enter the URL of your Marshal Reporting Console installation. Entering a URL enables context menu links on the Active Sessions, User Groups, and Users lists, as well as the Open Marshal Reporting Console button on this page.

9.1.11 Configuring Traffic Logging

The Traffic Logging window allows you to configure logging of Web requests to text files, for processing by external analysis software. WebMarshal supports both W3C and WebTrends Extended Logging Format (WELF). Text logs primarily include information about each file request, and the rule that blocked the request if any.

Figure 30: WebMarshal Properties, Traffic Logging window
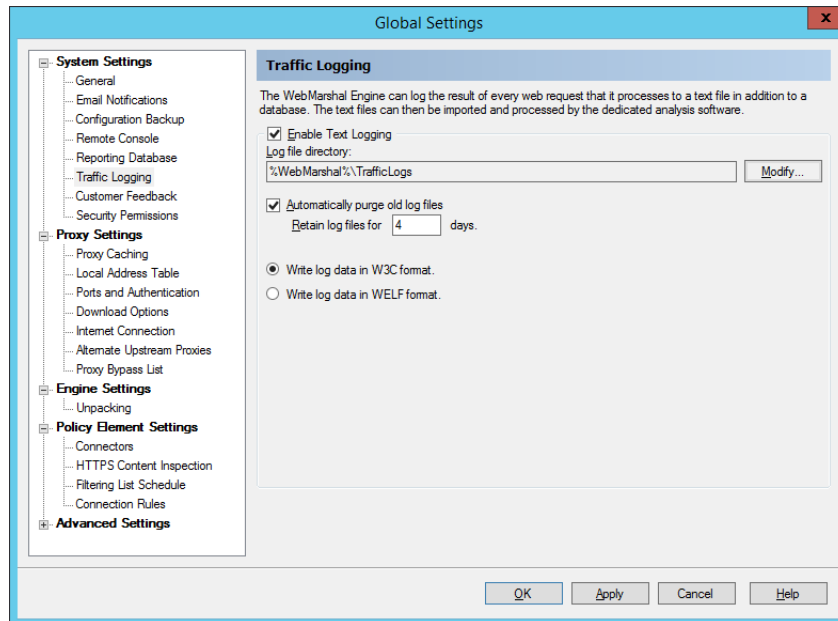
To configure traffic logging:

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, and 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. Select W3C or WELF format.

5. 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 Help.

9.1.12 Configuring Customer Feedback

The Customer Feedback window allows you to configure WebMarshal to send anonymous summarized information about browsing history to Trustwave. Trustwave uses this data to improve product quality and functionality. You can view additional information about this function by clicking the **View Privacy Policy** button.

Figure 31: WebMarshal Properties, Customer Feedback window
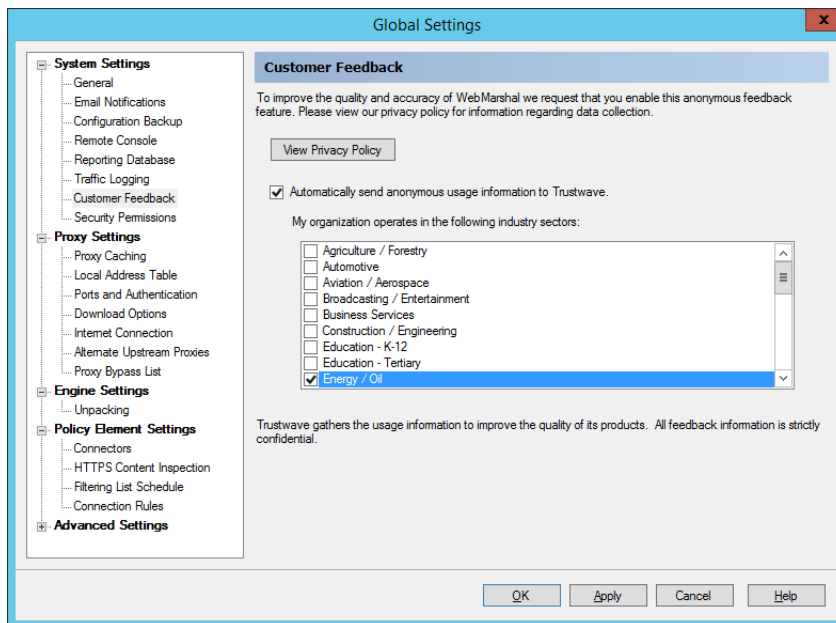
To configure feedback:

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 Trustwave 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.

9.1.13 Configuring Proxy Caching

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 Trustwave Knowledge Base article Q12720, *Proxy Caching Recommendations.*

To review statistics for the cache, see the Cache Statistics section of the Real-Time Dashboard.

Figure 32: WebMarshal Properties, Proxy Caching window
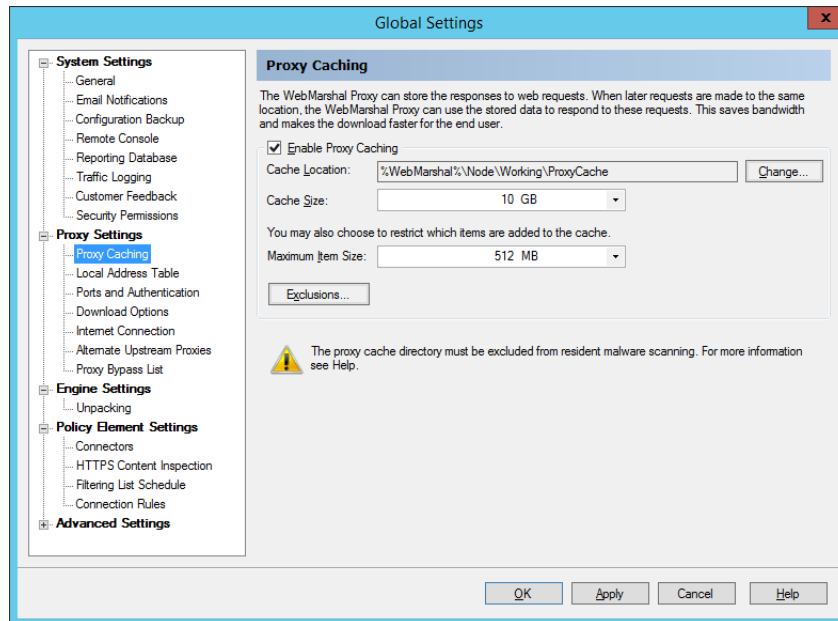
To enable caching, check the box. Then configure the following options:

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.

Optionally click **Exclusions** to open a window that allows you to enter a list of URLs that should never be cached.

> **Note:** Caching is available for HTTP and HTTPS requests only (never for FTP). You can disable caching of content delivered over HTTPS, For more information see Trustwave Knowledge Base article Q21204.

- 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.

9.1.14 Configuring the Local Address Table

This window allows you to specify the range(s) of IPv4 and/or IPv6 addresses that are assigned to computers on your local network. By default, the LAT includes address ranges that are always reserved for

local use, as well as any local ranges detected by WebMarshal auto-detection. 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.

Figure 33: WebMarshal Properties, Local Address Table window
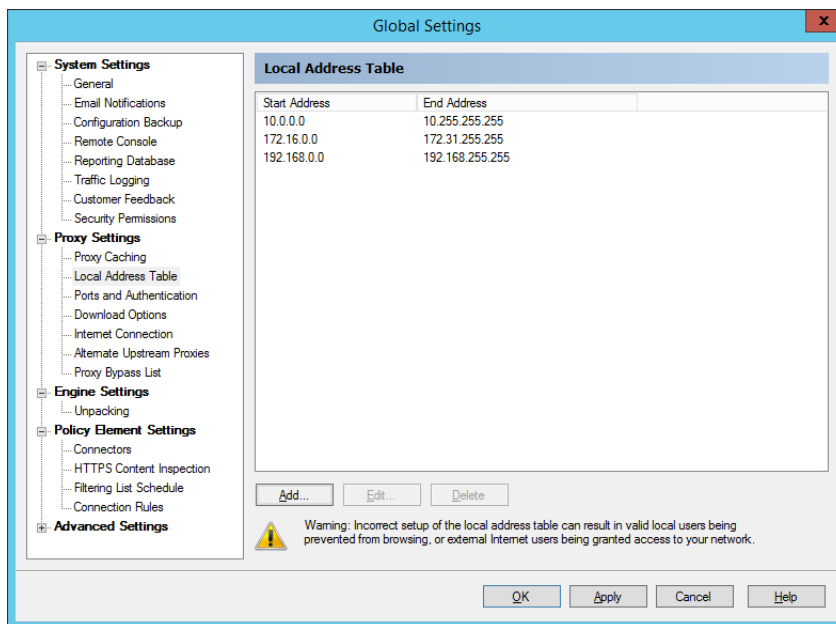
To enter a new LAT range:

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**.

9.1.15 Configuring Ports and Authentication

The Ports and Authentication window allows you to view and change the ports that WebMarshal uses to listen for client connections, and the authentication methods it accepts for each port.

Note: By default WebMarshal monitors each port on all available IPv4 and IPv6 Addresses. If the server has multiple interfaces, you can specify IP Address:port combinations (for example, `10.1.2.3:8085`). You can also limit connections to IPv4 or IPv6 addresses only.

Figure 34: WebMarshal Properties, Ports and Authentication window
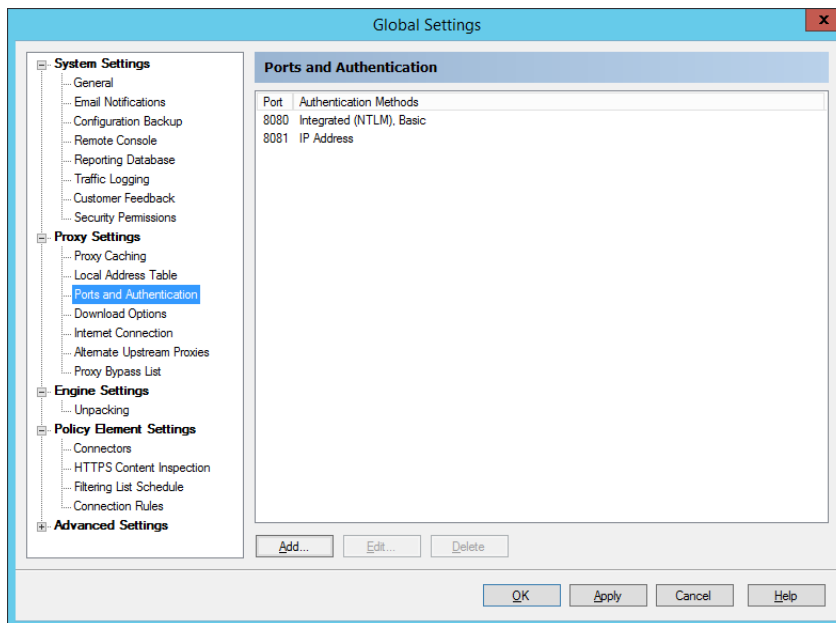
To add or edit listings, use the buttons below the list. For more information, see Help.

9.1.16 Configuring Download Options

The Download Options window allows you to configure the behavior of WebMarshal during Content Analysis scanning.

Figure 35: WebMarshal Properties, Download Options window
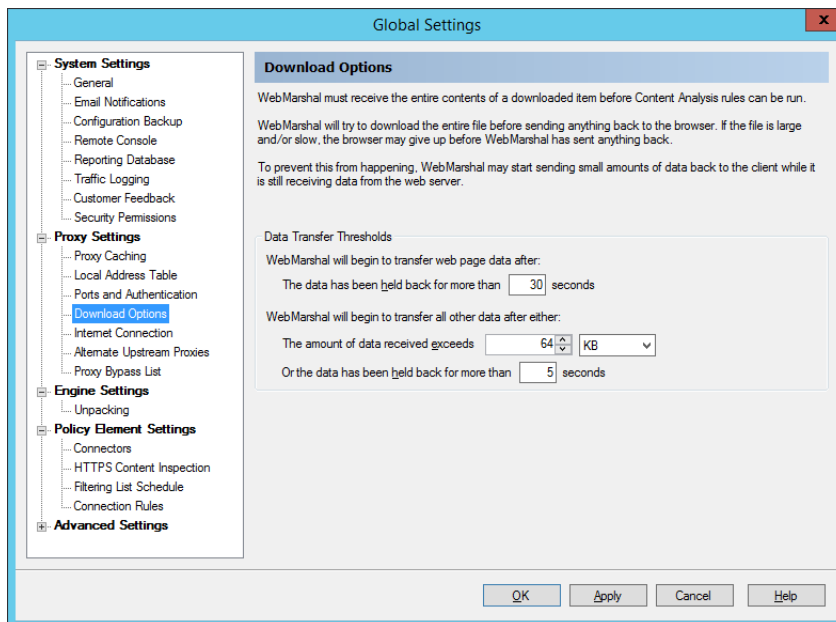
WebMarshal must receive the entire contents of a particular file before evaluating the Content Analysis rules. For large files or slow connections, this delay could affect the user's experience. In some cases the browser software could abort the attempt.

To avoid these issues, WebMarshal can begin returning the file to the user before receiving the complete file. (WebMarshal only returns the final data from the file after scanning is complete.)

You can configure when data transfer will start.

Note: Because the partial text might be offensive or might violate policy, by default WebMarshal holds text data back as long as is practical while minimizing the chance that the web browser application will time out.

- Binary data is returned in near real time. Full file scanning does not substantially increase total download times.

- If a content analysis rule triggers to block a file after data 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.

Because WebMarshal now returns binary data in near real time and does not "trickle" a percentage of binary files, the "streaming content types" configuration used in previous versions is no longer required. You can still apply the "trickle transfer" and streaming content types settings if you wish. For more information about the change and optional configuration settings, see Trustwave Knowledge Base article Q12925.

To configure Data Transfer Options:

1. Enter the minimum time WebMarshal will wait before starting to return text Web files.

2. Enter the minimum time WebMarshal will wait and the minimum amount of data WebMarshal must receive before starting to return non-text files.

Note: For non-text files, the transfer will start if either of these thresholds is reached.

For more details of the settings, see Help.

9.1.17 Configuring Internet Connection

The Internet Connection window allows you to select the method WebMarshal will use to request material from the Web.

- Software updates (such as filtering list and TRACEnet updates) always use the method selected here.

- When WebMarshal is configured as a standalone proxy server (including chained installations), web requests from clients also use this method.

Figure 36: WebMarshal Properties, Internet Connection window
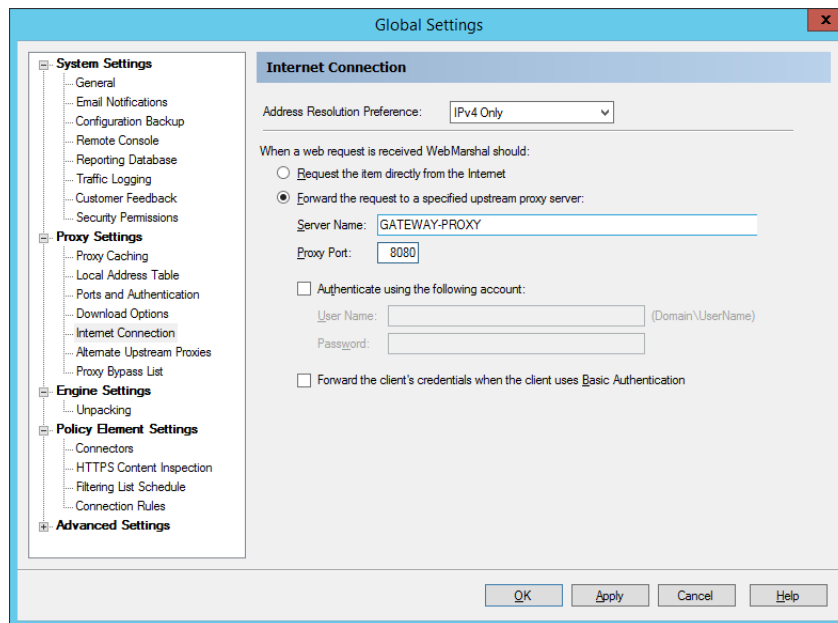
1. Choose the address resolution preference (IP protocol version to use when resolving outbound connections). This setting applies when WebMarshal resolves external websites or forward proxy names. *IPv4 only* is the default setting. For details of all options, see Help.

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

3. If WebMarshal will pass requests on to another proxy server, select 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).

4. 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.

5. If WebMarshal is installed as a standalone proxy, WebMarshal can also forward client credentials. See Help for details.

6. 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.

9.1.18 Configuring Alternate Upstream Proxies

The Alternate Upstream Proxies window allows you to set different methods for connection to the Web for certain URL Categories.

The purpose of this feature is to allow WebMarshal to direct requests for special sites to the proxy or direct connection that can fulfil them.

Notes:

- Alternate Upstream Proxy settings override any settings configured for a Server Group. If a URL is in a category that is assigned to an Alternate Upstream Proxy, requests for this URL will always use the specified alternate proxy.

- Alternate Upstream Proxies use the global Address Resolution Preference setting (IPv4 and/or IPv6) to resolve the proxy name, if required.

- You can check the alternate proxy usage for any URL using the Policy Tester. For more information, see "Testing Access Policy" on page 93.

- Each Alternate Proxy entry can be configured with the same settings as the main internet connection, including port, authentication, credential forwarding, and direct connection.

Figure 37: WebMarshal Properties, Alternate Upstream Proxies window
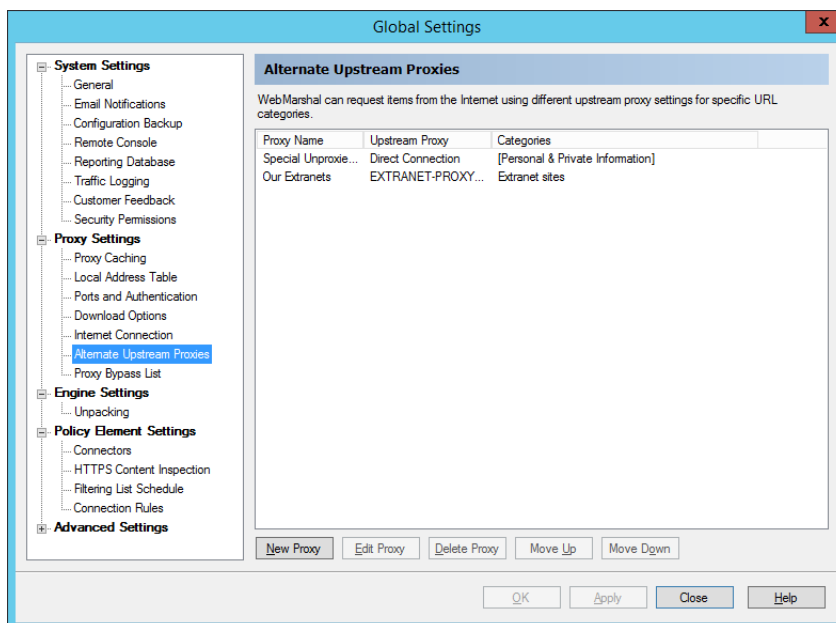
For full details of this feature, see Help.

9.1.19 Configuring the Proxy Bypass List

On this window, you can enter a list of web sites that you want to completely exclude from all WebMarshal Rules.

Caution: 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.

Figure 38: WebMarshal Properties, Proxy Bypass List window
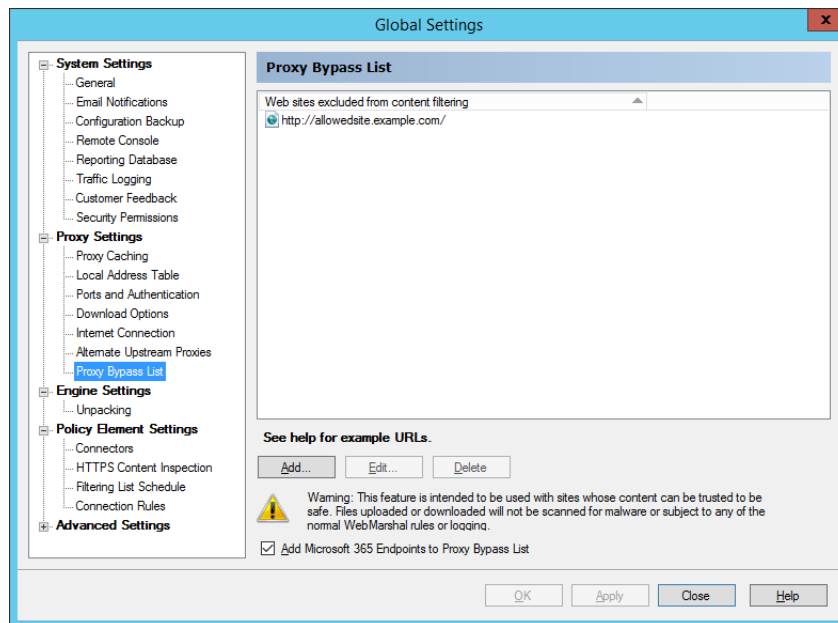
To add a new site:

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://*.trustwave.com/`

     - `http://www.microsoft.*/`

     - `http://203.0.113.*/`

   - Only one wildcard character per entry is allowed.

   - Wildcards cannot be used in IPv6 literals.

   - Wildcards in IPv4 literals only apply to browsing by IP address (not to sites in a network range).

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.**

6. You can also include Office 365 endpoints, based on the Office 365 URLs and IP address ranges service provided by Microsoft. WebMarshal automatically updates this list daily. To include this list, check the box at the bottom of the page.

9.1.20 Configuring Unpacking

The Unpacking window allows you to set up a list of URL Categories containing URLs that might host files larger than a specified size. You can choose to skip unpacking and scanning for URLs in these categories.

The purpose of this setting is to enhance performance or allow download of extremely large files that cannot be unpacked due to size, or that result in a client browser timeout while unpacking.

> ⚠️ **Caution:** This setting results in the affected files being passed through with reduced malware scanning and other policy checks, because any files included in an archive or document will not be separately scanned. It should only be used for locations hosting business critical files that are routinely downloaded, where experience shows that unpacking fails. For example some very large software images meet this definition.
>
> You should set the size limit as high as possible, and include only a few very specific URL paths in the categories.

To configure this feature:

1. Create a URL Category and include the URL paths required.

2. On the Unpacking window, click **Add**.

3. Enter a size limit. Files larger than the limit will not be unpacked. You can enter 0 (zero) to exclude all files.

4. Select a category that the limit should apply to. Click **OK**.

5. Repeat the above steps to create entries with different size limits. If a URL is included in multiple categories, the smallest limit will apply.

Figure 39: WebMarshal Properties, Engine Unpacking window
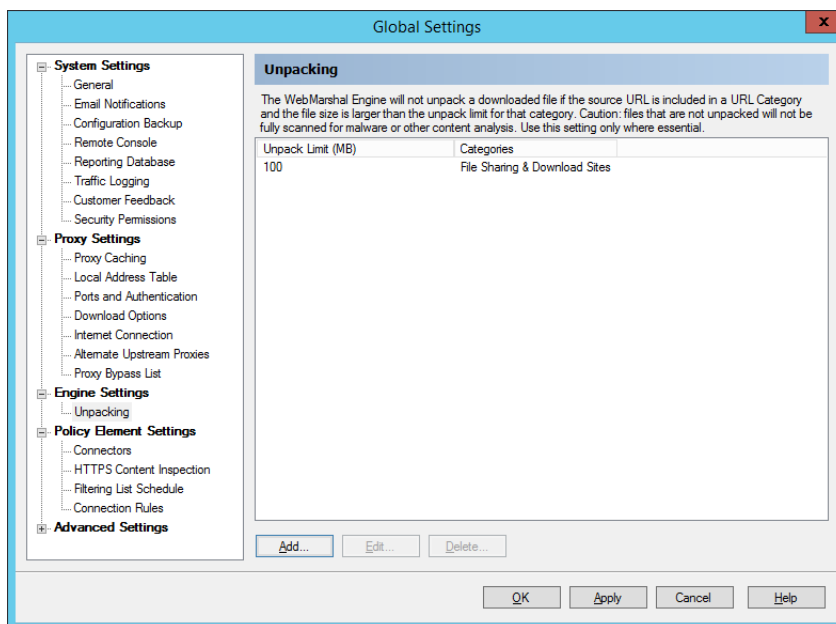
9.1.21 Configuring Connectors

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

Figure 40: WebMarshal Properties, Connectors window
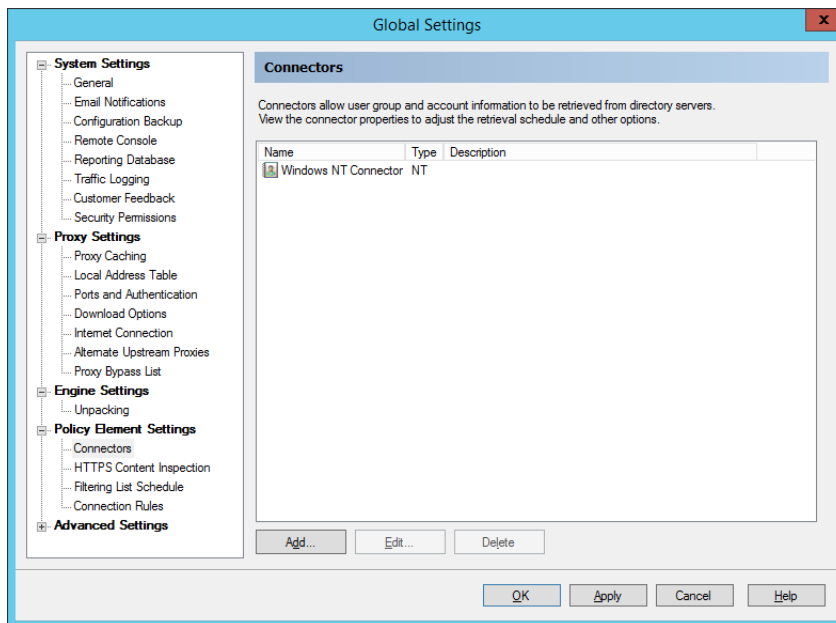
You can install connectors for Active Directory, legacy Windows NT, and Novell (NDS). You can only have one connector of each type at a time.

> **Note:** 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 (Kerberos/NTLM),* Trustwave recommends that you configure separate ports for the two authentication types. For more information, see "Configuring Ports and Authentication" on page 143 and "Proxy Ports and Authentication" on page 34.

To install a new connector:

1. Click **Add**.

2. Select the type of connector.
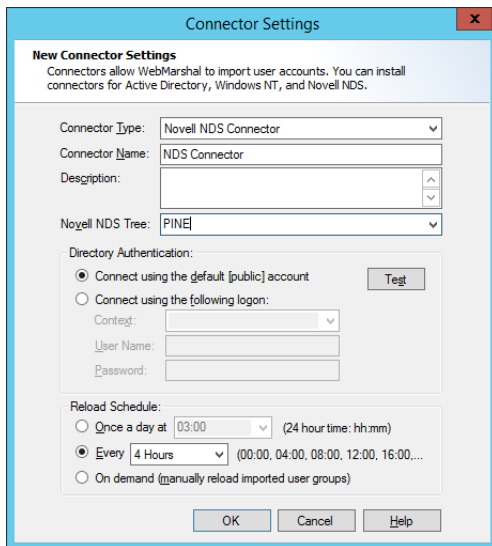
3. If you selected a NDS connector, enter or select a NDS Tree from which to import information. Choose whether you want to use the `[public]` account or a specific user account.

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

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

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

7. In the Reload Schedule area, 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.

8. Click **OK** to add the connector.

9. To import users or groups through this Connector, see the User Groups section in the main Console menu tree.

To delete a connector, select the 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).

To edit the properties of an existing connector, select it and then click **Edit** to open the Connector Properties window.

9.1.22 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.

9.1.22.1 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.

    •   WebMarshal can validate the revocation status of the presented certificate. See "Enabling Certificate Revocation Checking" on page 154.

5. **All communications are encrypted and secured**, but WebMarshal can inspect the content.

6. WebMarshal cannot inspect and by default does not allow connections that use the obsolete SSLv2 protocol. By default, WebMarshal does not permit connections that use SSLv3, which is considered an insecure protocol. You can choose to allow SSLv3 connections. For more information, see Trustwave Knowledge Base article Q20067.

> **Caution:** 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.

9.1.22.2 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**.

Figure 41: WebMarshal Properties, HTTPS Content Inspection window
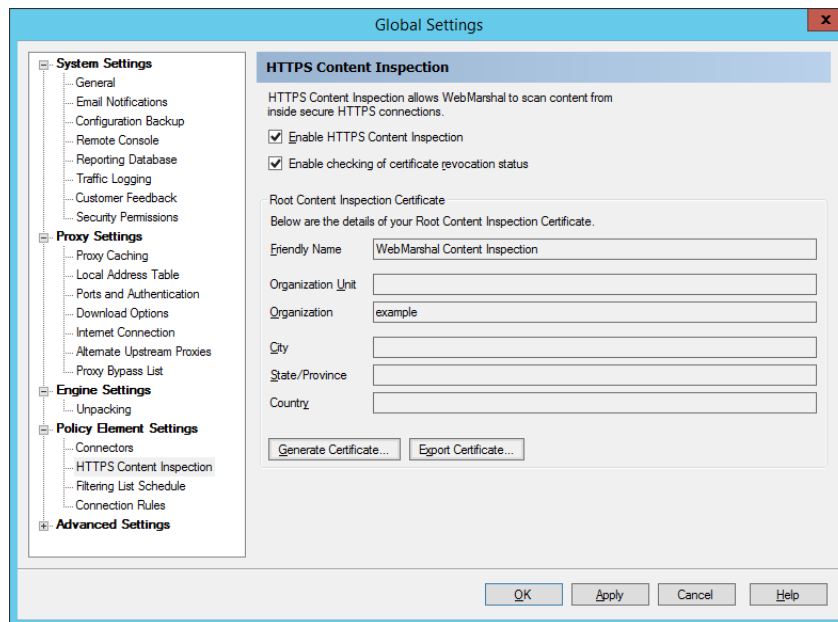
2. On the **Generate Certificate** window, enter information in the fields, and then click **Generate Certificate**. If you have already generated a certificate you will be asked if you want to overwrite it.

    Most of the fields on this window are optional and all required fields are populated by default. You can enter additional information to further identify the certificate. The information you entered displays on the Global Settings page.

    > **Caution:** 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 compliant browsers 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 Trustwave Knowledge Base articles Q12014 and Q12015.

9.1.22.3 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."

9.1.22.4 Enabling Certificate Revocation Checking

WebMarshal can validate the certificate presented by a website. Validation uses Online Certificate Status Protocol (OCSP) stapling or Certificate Revocation List (CRL) information encoded in the certificate. When this feature is enabled, WebMarshal checks the revocation status of the site certificate only. WebMarshal does not currently check for revocation of the root certificate or any intermediate certificates. WebMarshal checks OCSP stapling first for efficiency, and attempts to retrieve CRLs if the OCSP response does not return the required information. For more information about this feature, see Knowledge Base article Q20605.

To enable revocation checking, and to enable the processing of rule conditions that validate certificate revocation, check the box *Enable Checking of certificate revocation status.*

To disable revocation checking, clear the box.

9.1.23 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 and Trustwave Web Filter Database, but not URLCensor.

For more information about Filtering Lists and prerequisites for updates, see "Configuring URL Filtering Lists" on page 106.

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.

9.1.24 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 as well as connections using the WebSocket protocol.

> **Note:** 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 Trustwave Knowledge Base article Q12021.

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."

9.1.25 Configuring Advanced Settings

The Advanced Settings (General) 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

- Set detailed logging for specific workstations

- Control how often the processing servers check for updated policy

- Configure automatic purging of the WebMarshal "All Users" list

9.1.25.1 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.

Figure 42: WebMarshal Advanced Properties, General window
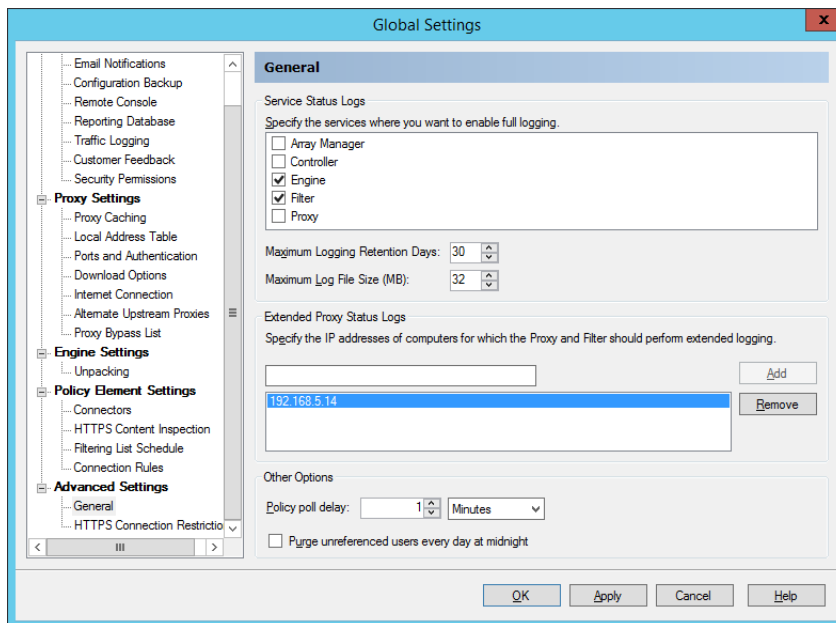
To configure logging retention and size options, use the logging retention days and log file size fields. For more information, see Help.

9.1.25.2 Extended Proxy Status Logs

You can choose to log full connection information for selected workstations if you need to investigate a specific issue. This option makes the desired information easier to find than with full logging.

To configure logging for specific workstations, use the fields and buttons in this section. For more information, see Help.

9.1.25.3 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.

9.1.25.4 Purge Unreferenced Users

This setting allows you to automatically remove users from the WebMarshal **All Users** list daily at midnight. By default user names are retained on this list indefinitely, even if they do not currently appear in any User Group visible within WebMarshal.

> **Note:** If you purge a user and the same user is later re-imported, the new instance will have a new unique identifier. The two instances will be treated as different users in for purposes of reporting.

To enable daily purging, check the box. This action does not affect logging records.

9.1.26 HTTPS Connection Restrictions

On this window, you can choose to allow HTTPS connections with non-standard settings. Non-standard settings include:

• Ports other than the default 443

• Connections from software that does not identify itself with a User Agent header

These settings do not apply to any Web request that is processed by WebMarshal HTTPS Content Inspection. All inspected HTTPS connections are allowed, subject to the applicable WebMarshal Rules.

For more information about this feature, see Help.

> **Tip:** These settings can be used only to provide access to business-related secure sites that would otherwise be blocked. Caution is required as no virus scanning or filtering will be performed on the sites in this list. To learn more about the security implications of the settings, see Help for this page.

9.2 Working with Servers

Right-click the **WebMarshal** server icon in the left pane (or use the **Action** menu) to access the following functions:

9.2.1 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.

9.3 Working with Configuration

You can use the WebMarshal Console to commit and revert configuration changes. You can also use the console to export (back up) and import (restore) configuration files.

9.3.1 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.

> **Note:** You can only revert once. Selecting **Revert Configuration** more than once has no effect.
>
> • You cannot use **Revert Configuration** to undo committed changes.

9.3.2 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.

> **Note:** 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 136.

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.

9.3.2.1 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 4.6.2, and the following files from the WebMarshal installation folder:
>
> • ConfigBackup.exe
>
> • Marshal.Remoting.dll
>
> • WMRemoting.dll

9.4 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 93

Enable Rule Processing

Begins applying the configured filtering rules to Web requests processed by the WebMarshal Server.

Disable Rule Processing

Ceases applying the configured list of rules to Web requests processed by the WebMarshal Server. This option will normally be selected only for troubleshooting purposes.

9.5 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. You can launch the Tool from **Global Settings > Security Permissions**, or from 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.

> **Note:** When installing WebMarshal on a system with User Account Control (UAC) enabled, additional security restrictions apply. For more information see Trustwave 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 Web-Marshal Array.

*   **Modify Security:** Allows the user to change security settings as described here.

*   **View Active Sessions:** Allows the user to see details of current browsing activity in the Active Sessions section of the Console.

9.6 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).

9.6.1 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.

9.6.2 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.

9.6.2.1 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.

9.6.2.2 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.

9.6.3 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.**

9.7 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

• Internet Connection

• Proxy Bypass List

• Proxy Caching

• Email Notification settings

• Advanced settings (service logging and policy polling)

For more information about the purpose of these settings, see "Configuring Global Settings" on page 133. 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 details of the specific settings and fields, see 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.
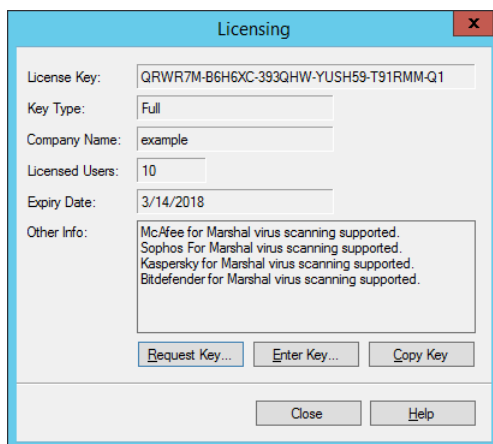
5. Click **OK.**

9.8 Managing Licensing Information

To view licensing information, on the toolbar click **Tools > Licensing**. The Licensing window displays information on the currently installed product key, including type, number of users licensed, 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.

Figure 43: Licensing window

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.

2. Enter the appropriate contact information in the form. WebMarshal automatically appends the current key details. For a quicker response, include the Customer Reference as found on order confirmations.

3. Enter any additional comments in the **Additional Information** field. This could include the number of new user licenses desired.

4. Click **Send Request** to send the data to Trustwave.

> **Tip:** A HTTP connection to the Internet is required to send the data. This function does not depend on an e-mail server connection.

9.9 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.

Figure 44: WebMarshal Console, Event Logs window
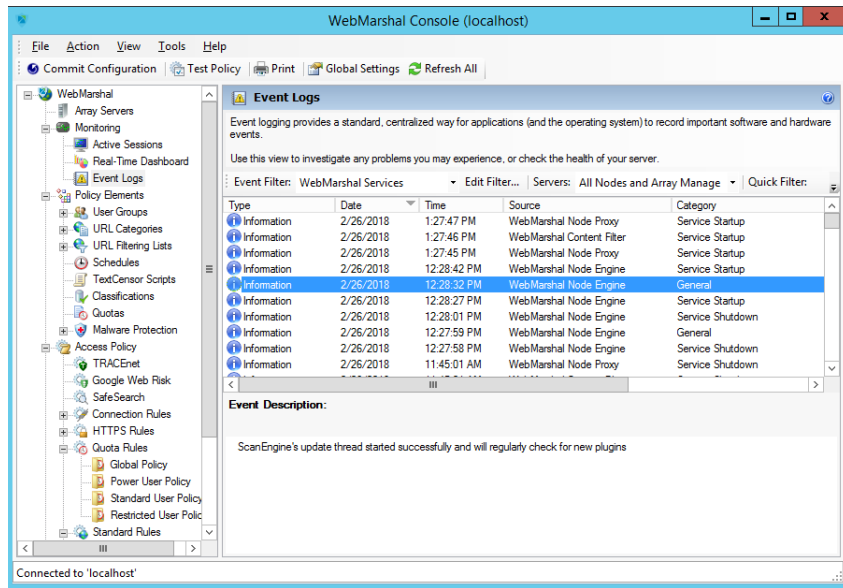
9.9.1 Event Log Filters

The WebMarshal 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.

- **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.

9.10 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 Trustwave 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, select Performance monitor from the menu tree and then click the **+** icon in the tool bar to open the Add Counters window.

Figure 45: Performance Monitor, Add Counters window
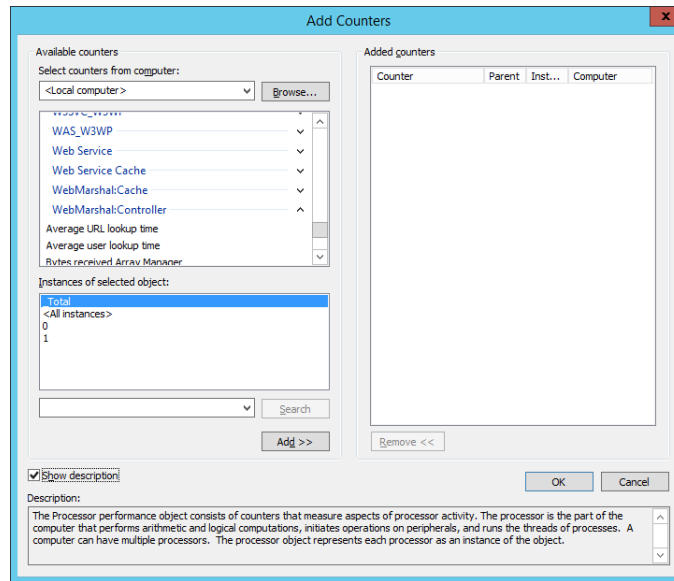
You can choose to add counters from the local computer, or any other computer in the local network.

Tip: The organization of this window depends on the Windows version, but the same fields are available in all versions.

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.

Figure 46: Performance Monitor window
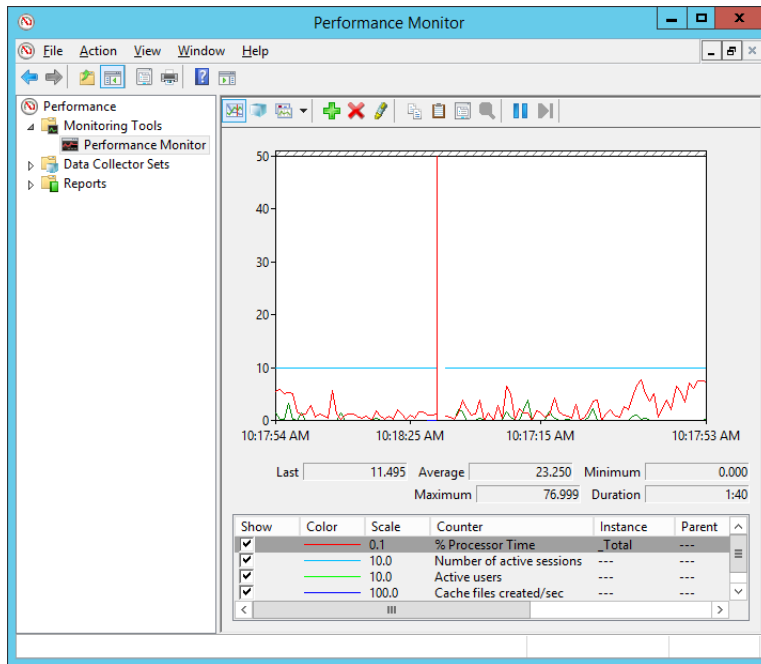
Please see the Performance Monitor documentation for full information on its capabilities, including monitoring of other computers.

10 Troubleshooting

This chapter provides a list of resources you can use when analyzing problems with WebMarshal.

10.1 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 164 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.

10.2 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 155.

Note: To save disk space, the WebMarshal logging folders are compressed.

10.3 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 Trustwave to resolve the issue. The file names have the extension `.mdmp`.

If a file of this type is present, contact Trustwave Technical Support for assistance.

10.4 Support Tool

This tool gathers information about the WebMarshal installation and the server WebMarshal is installed on. Its purpose is to help the Trustwave support team diagnose support issues. To use the tool, run `MarshalSupportTool.exe`, found in the WebMarshal installation directory. For more information on how to use the tool, see Trustwave Knowledge Base article Q15024.

10.5 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

10.5.1 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 93 for details.

- Check that rule processing is enabled. Right-click **Access Policy** in the Console and select **Enable Rule Processing**.

10.5.2 Problems Using Web Browsers

10.5.2.1 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 Windows Authentication or Basic Authentication. Windows Authentication negotiates the strongest available protocol from Kerberos or NTLM.

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 Edge or most current major browsers.

10.5.2.2 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 Windows Authentication, such as Firefox or Microsoft Edge

- On the WebMarshal Server computer, grant the Windows NT permission "log on locally" to all accounts used for browsing

10.5.3 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 Ports and Authentication" on page 143).

10.5.4 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.

10.5.5 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).

10.6 Further Help

For any problems not listed here, please see the Knowledge Base and Forum on the Trustwave Website. If these resources do not resolve the issue please contact your Trustwave supplier or Trustwave Technical Support. To access the support resources or to contact Technical Support, please visit www.trustwave.com/support/.

11 WebMarshal and NDS

WebMarshal can import users and groups for authentication from Novell NDS.

11.1 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 96. 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.

11.2 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/).

11.2.1 Public Access

Experience with the version of NDS included with NetWare has shown the following:

11.2.1.1 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).

11.2.1.2 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.

11.2.2 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.

11.2.3 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).

11.2.4 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=.

11.2.5 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.

11.3 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.

11.3.1 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 172.

*   Most web browser software provides a way to remember your user name and password so you only have to click **OK**.

11.3.2 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 system proxy settings so if proxy settings are not properly configured the logon procedure will not work. To override these settings see *Options* below.

11.3.2.1 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.

11.3.2.2 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.

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 that you maintain.

- **URLCensor** allows you to use a DNS Blacklist lookup as a source for URL categorization.

WebMarshal also supports the **Trustwave Web Filter Database**. This List is licensed separately. Contact Trustwave for licensing information.

12.0.1 Technical Support

Technical support for all WebMarshal Filtering Lists is available from Trustwave. Contact your Trustwave partner or see the Trustwave website for more information.

12.1 FileFilter

FileFilter retrieves URL categorizations from files that you maintain. 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`).

WebMarshal also automatically populates FileFilter files for Office 365 endpoints, based on the [Office 365 URLs and IP address ranges](#) service provided by Microsoft.

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 that will appear in user interfaces and reports, such as: `Porn`

- `<Url>` is a domain name, and optionally includes a path, file name, and query string.

> **Notes:**
>
> If the URL (domain/path part) ends with a trailing `/` it is matched as a path.
>
> If the URL ends with a character other than `/` it is matched as a specific file name.
>
> The URL can include a query string of one or two parameters after the domain/path part. For details, see "URL Query String Matching" on page 104.
>
> If the URL includes other parts such as a port number, user credentials, or protocol (HTTP, HTTPS, FTP), these additional parts are ignored when matching the URL.

A domain entry matches all subdomains.

A path entry matches all deeper paths and files.

For instance, `https://trustwave.com/` also matches `https://www.trustwave.com/` and `https://login.trustwave.com/path/`

You can use the wildcard * at the beginning and/ or end of the domain part. For instance, `*.trustwave.*` matches `https://www.trustwave.com/` and `https://login.trustwave.co.uk/path/`

> **Caution:**
> - Items with query string parts containing more than two items will be imported, but only the first two items will be matched.

Examples:

```
ftp://ftp.microsoft.com/
google.com/
http://example.com/samples/test/
example.com/myfile.htm
*.microsoft.c*/support/
```

Several sample files are included with the WebMarshal distribution. These files demonstrate the functionality. Trustwave does not provide updates for these files.

> **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.

12.2 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).

12.3 Trustwave Web Filter Database

WebMarshal includes support for the Trustwave Web Filter Database (previously known as the M86 Filter List). The list contains 116 categories and is licensed from Trustwave under the WebMarshal license key for the installation. A 30 day trial is provided with all trial installations of WebMarshal. Customers who have

never used a trial of the Web Filter Database can also start a 30 day trial at any time. For information on how to purchase the filter list contact Trustwave.

12.3.0.1 Expiration and Re-activation

If your installation is using a WebMarshal trial key, when it expires the Web Filter Database will no longer update and will stop categorizing. If your installation is using a full Web Filter Database 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 Trustwave.

12.3.1 Integration Information

Information on using the Web Filter Database within WebMarshal is provided in "Understanding URL Categories" on page 101. Enabling and disabling Filtering List integration is covered in "Configuring Filtering List Updates" on page 154.

12.3.2 Prerequisites

The Trustwave Web Filter Database has the following prerequisites:

- 800 MB of available disk space on each processing node (allowing for multiple copies of the database while updating).

- Internet access (HTTP and HTTPS) from all processing servers (to download updates), and from the Array Manager (for initial license validation only, required only when you first set up the list).

12.3.3 Checking and Reviewing Trustwave Web Filter URL Listings

Trustwave provides a web based service that allows you to check a specific URL against the most current categorizations in the master Web Filter 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 Trustwave website.

You can also check a URL with 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 Trustwave website.

If you want to allow some users access to a particular URL that would normally be blocked due to Web Filter 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 than 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.

Certificate Revocation List.

A web response that lists SSL certificates marked as "revoked" or untrusted by the issuer.

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.

CRL

See Certificate Revocation List.

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 example.com, might be represented as follows:

`CN=JDoe,OU=Users,DC=example,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.

Glossary
179

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.

Forefront TMG

See Microsoft Internet Security and Acceleration Server.

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. The 2010 version of this application is known as Forefront Threat Management Gateway (TMG).

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.

OCSP

See Online Certificate Status Protocol.

Online Certificate Status Protocol

An Internet protocol used to obtain the revocation status of a digital certificate. OCSP responses can also be "stapled" to the TLS handshake that establishes a secure connection.

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 Internet 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 logical and positional operators and numerical scores.

TRACEnet

A proprietary service of Trustwave 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.

WebSocket

A standard for client-server communication over web connections.

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

About Trustwave®

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave Fusion® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.