

# **QUICK START GUIDE**

**v6**



# **Web Inspector™**

Copyright © 1998 - 2002 by Elron Software, Inc. All rights reserved worldwide. This manual has been provided pursuant to an agreement containing restrictions on its use. This manual is also protected by United States and worldwide copyright laws. No part of this manual may be reproduced or distributed, transcribed, stored in a retrieval system, translated into any spoken or computer language or transmitted in any form or by any means whatsoever without the prior written consent of:

Elron Software, Inc.  
7 New England Executive Park  
Burlington, Massachusetts 01803  
United States of America  
Telephone: (800) 767-6683  
Fax: (800) 668-6083

## ***Trademarks***

Internet Manager and Message Inspector are registered trademarks, and Elron, the Elron logo, the Message Inspector logo, SmartBlock, SmartList, and Web Inspector are trademarks of Elron Software, Inc.

Other trademarks, registered trademarks and servicemarks mentioned in this software or its documentation are property of their respective owners. The products described anywhere in this software or its documentation may be protected by one or more U.S. patents, foreign patents, or pending applications.

## ***Warranty; Liability***

Reference is made to the Elron Software Program License Agreement and Limited Warranty for the limitations and exclusions of warranty and liability applicable to this documentation and the related software.

## ***U.S. Government Restricted Rights (Applicable to U.S. Users Only):***

This software and documentation is provided with RESTRICTED RIGHTS. The use, duplication, or disclosure by the government is subject to restrictions as set forth in paragraph (c)(1)(ii) of the Rights in Technical Data Computer Software clause at 32.227-7013. The manufacturer of this software is Elron Software, Inc., 7 New England Executive Park, Burlington, MA 01803, USA. Tel: (800) 767-6683. Fax (800) 668-6083.

Revision Date: November 2002.

# Contents

<b>System Requirements .....</b>	<b>1</b>
<b>Logging In Using the WI Console .....</b>	<b>4</b>
<b>Configuring WI Services .....</b>	<b>5</b>
<b>How to Check for Traffic .....</b>	<b>5</b>
<b>Policy Screen .....</b>	<b>7</b>
<b>Classifying Sites .....</b>	<b>12</b>
<b>Blocking and Unblocking .....</b>	<b>12</b>
<b>Unmonitored or Unrestricted Groups .....</b>	<b>12</b>
<b>Opening the Real-Time Monitor .....</b>	<b>13</b>
<b>Licensing Web Inspector v.6 .....</b>	<b>15</b>



# A Quick Start to Web Inspector v6

## System Requirements

### WI Collector

Web Inspector (WI) can be deployed in a variety of network environments, from 25 users at a single site to thousands of users at multiple sites. The following table gives recommended configurations for three representative environments.

Environment	CPU	RAM	Disk	Database
Up to 1,000 users and up to 1.5 Mb/s (T1) line speed	Dual 450 MHz or single 733 MHz	512 MB	1 GB	MSDE or SQL Server
Up to 2,000 users and up to 3 Mb/s line speed	Dual 667 MHz	768 MB	2 GB	SQL Server
Up to 3,000 users and up to 4.5 Mb/s line speed	Dual 900 MHz	1 GB	3 GB	SQL Server

Actual requirements will depend on your particular network size and topology. Please consult Elron Software Technical Support for guidance on system requirements for your environment.

**Note:** *MSDE is included with WI.*

## **A Dedicated Computer**

The host for a WI collector should be a dedicated computer, running as few other services or applications as possible. Of course, a WI collector using the MS Proxy plug-in must be installed on a computer that runs MS Proxy Server 2.0.

**Important:***The presence of other Internet related services on the computer may prevent WI from installing or functioning properly, and other applications on the computer may limit the performance of WI. This includes, but is not limited to, firewalls, proxy servers, mail servers, Microsoft Internet Information Server (IIS), Lotus Notes server, RAS, and Microsoft Exchange .*

## **Operating System**

- Windows NT 4.0 Workstation or Server, with Service Pack 6a or higher
- Windows 2000 Professional or Server, with Service Pack 1 or higher

## **Ethernet Network Interface Card (NIC)**

A 10 Mb, 10/100 Mb, or 100 Mb Ethernet NIC.

## **A Static IP Address**

The NIC must have a static IP Address. If you use CGS, this address is usually on the same subnet as the Internet feed router.

## **WI Administration Console**

The WI Administration Console is a Java application that allows for local or remote administration of WI, including policy management, system management, and reporting. The WI Console can be standalone or run through a browser. For best performance, run it on a computer other than the WI server, with network access to the WI server.

## **Minimum Hardware Requirements**

- Pentium 500 MHz PC or faster
- 256 MB RAM

## **Display Settings**

**Important:** *Set the color palette to 65536 colors or True Color. A setting of 256 colors or below will not support the full WI Console. Set the resolution to 800x600 or greater.*

To change settings click **Start**→**Settings**→**Control Panel**→**Display**→**Settings**.

- In NT, choose the color setting from the *Color Palette* menu. Use the *Desktop Area* slide to choose resolution.
- In Windows 2000, choose the setting from the *Colors* menu, and use the *Screen Area* slide to choose resolution.
- The WI Console will display at any refresh frequency from 56 to 85 Hz, displayed below *Desktop Area* in NT. To find the refresh frequency in Windows 2000, click *Advanced* and choose *Monitor*.

## **Operating System (WI Console)**

- Windows 95
- WI Windows 98
- Windows NT 4.0 Workstation or Server with Service Pack 6a or higher
- Windows 2000 Professional or Server
- Windows XP

## **Browser Requirements (Browser Access)**

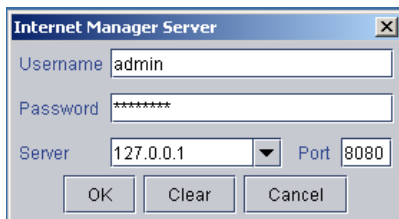
- Internet Explorer 5.5 or later
- Netscape Communicator/Netscape 6.0 or later

## Logging In Using the WI Console

You can connect to the WI interface through a standard Web browser or the WI Administration Console. We recommend using the WI Administration Console. See the Administrator's Guide for instructions on logging in through any Java-enabled Web browser.

**Important:** *Only one administrator at a time should log in and manage WI Policy or System data, whether through the WI Console or through a Web browser. Simultaneous editing of Policy or System data from multiple consoles or browsers may produce unpredictable results, and WI does not support it.*

1. Double-click the **WI Console** icon on your desktop.



2. Enter a user name and password. The first time you log in, use **admin** as the user name and **password** as the password. The username and the password are case sensitive. We recommend changing the password as soon as possible.
3. Enter the IP address for the primary WI collector and the port number it uses. If the WI collector is on the computer you are connecting from, the loopback address of *127.0.0.1* will also work. Port *8080* is the default.

## ***Configuring WI Services***

If you are deploying a WI collector in CGS mode, the WI installation configures the IM Web Inspector Filter service for manual startup. All other WI services are Automatic and start on reboot. The WI Filter is initially manual because some network cards that do not support promiscuous mode can prevent the WI Filter from starting successfully and, if the service were automatic, could prevent the computer from booting successfully.

After you have installed WI and rebooted and are ready to begin monitoring web activity, use the Service Control Manager to start the WI Filter. If the WI Filter runs successfully, it will configure itself for automatic startup on subsequent reboots.

## ***How to Check for Traffic***

Wait five minutes for initialization to complete before checking for traffic. You can check either using the Real-Time Monitor, the Policy Screen, or Reports.

### ***In Real-Time Monitor***

1. Log into the WI Server as Administrator or as a user with administrative privileges.
2. Click **Start → Programs → Internet Manager → Web Inspector → Real-Time Monitor**. The monitor should display entries.

### ***From Policy***

1. Go to **Groups → All Workstations**.
2. Click **All Workstations** to expand. Workstations WI detects should appear.

## ***From Reports***

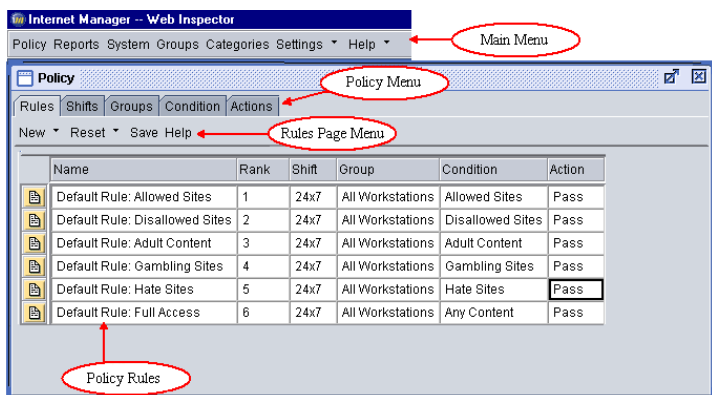
1. Go to **Reports**→**Workstation Reports**→**All Workstations**.
2. Select any report type under **All Workstations** and choose **All Activity**.
3. Accept the defaults on the options screen that appears and click **OK**.
4. The resulting report should show workstation data.

If you are not seeing data, let the product run another five minutes, then run the report again. If you still cannot see traffic, check the placement and hardware.

**Note:** If you have installed WI on an ISA Server and do not see traffic, go to the Control Panel Services menu and cycle— stop and restart—the Web Proxy Service.

## Policy Screen

Click **Policy** on the IM Console menu bar, then click the *Rules* tab. For a complete description of WI policies and their components, see “Policy” in the *WI Administrator’s Guide*.



The *Policy* page displays all the *rules* currently in effect and lets you create new ones. All the tools you need to make a policy are available on this page. You can manage users, workstations, and groups from *Groups*. Use *Categories* to manage categories, sites, and make changes to the SmartList dictionary.


WI comes with six default rules, which are set to *Pass* by default

- **Allowed Sites** Sites defined by the Administrator to which your organization allows unfiltered access.
- **Disallowed Sites** Sites designated by the Administrator for restricted access that are not blocked in another rule.
- **Adult Content** Sites that WI classifies as *Adult*, *Nudity*, or *Sexually Explicit* trigger this rule.
- **Gambling Sites** Sites that WI classifies as *Gambling* trigger this rule.
  - **Hate Sites** Sites that WI classifies as *Hate* trigger this rule.
  - **Full Access** Covers all accessed Web sites. An organization can restrict Web access altogether by setting the Action in this rule to *Block*.

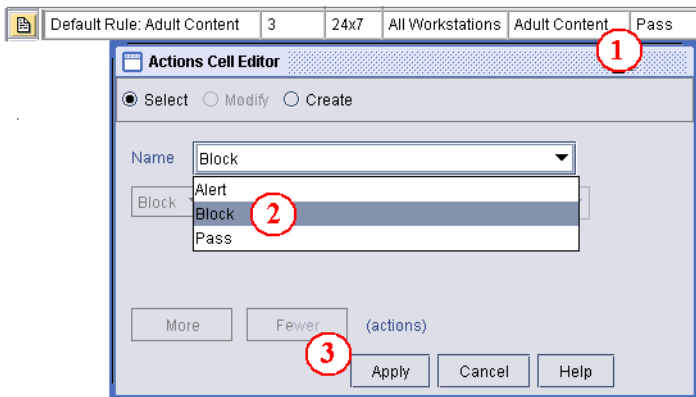
The defaults cover most basic Web accesses. Follow the steps below to make simple changes to the default rules. For detailed descriptions of building rules, see the *WI Administrator's Guide*.

## ***Modifying a Default Rule***

Click the field to modify. You can edit the *Name* and *Rank* fields on-screen:

1. Click the cell.
2. Type in the new information.
3. Press **Enter** on the keyboard (or tab out of the cell).
4. After you change an existing rule, the icon to the left of the row shows that the rule has unsaved changes. Click  the icon if you need to undo the changes, or click **Save** on the menu bar to complete the changes.

WI passes all traffic by default. To change the action on a rule (in this case, *Adult Content*) from *Pass* to *Block*:



1. Click in the *Action* cell of the rule.
2. When the *Actions Cell Editor* appears, click in the *Name* field and select **Block** from the menu.
3. Click **Apply**. Accesses to which the *Adult Content* rule applies are now blocked.

### **Deleting a Rule**

Click the icon on the left of the rule to delete and select **Mark for Removal**. When you see the scissors icon, select **Save** on the menu bar. The marked rule is now deleted from the policy. Repeat these actions to delete other rules.

To cancel the Delete action, again click the icon to the left of the line and select **Undo Mark for Removal**.

### **Saving a Rule**

A new rule is saved automatically when you apply the last parameter. Click **Save** to keep any changes you have made. To

display the current state of the Policy, click **Save**, then click **Reset** → **Reload From Server**.

### **How WI v6 Controls Web Access**

The primary access control tool in Web Inspector 6.0 is the *rule*. You can create rules from elements packaged with WI, from elements you create, or both. You build and rank rules on the *Policy* page, and the entire collection of rules represents your Internet Usage Policy.

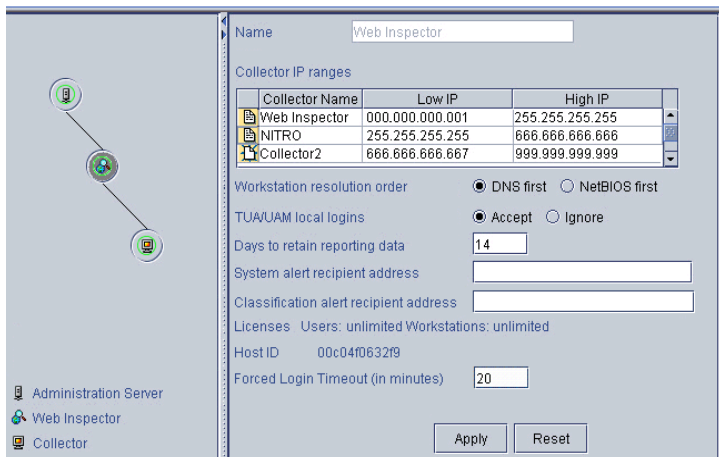
When WI detects any Web access, it applies the rules in rank order, from top to bottom, to any access that meets the *conditions*. The access triggers the *highest ranked* rule that matches the conditions in the access, and WI executes the *action* (*pass, block, or alert*) from the matching rule.

Once WI has matched a rule, it stops searching for others to execute. Rank the most critical or sensitive rules highest. When you create a policy, give the highest rank to rules that block sexually explicit sites, those relevant to illegal activity, or those blocking particular groups of users or workstations. The WI default rule, *Full Access*, should become the lowest-ranked rule: WI would never trigger any rule with a lower rank than *Full Access*.

### **System Screen**

The *System* screen lets you view and manage configuration parameters, including workstation name resolution. The individual nodes, displayed graphically in the left pane, represent the Administration Server, WI global settings, and WI Collector

computers. Click on a node to open the screen for each respective level. You can perform most configuration tasks on the *System* screen.



### **Configuring IP Address Ranges**

If you are installing a WI collector in CGS mode, configure the IP address ranges that the collector will monitor. By default, a primary WI collector monitors Web accesses from all workstations that it detects, and secondary WI collectors monitor no workstations. If you are running multiple WI collectors, you must configure IP address ranges for the collectors, so that each monitors its own range. If you are running a single WI collector, you can configure its IP address ranges to prevent WI from monitoring hosts that are outside your network or in certain portions of your internal network.

1. Click **System** in the top menu bar and select the middle node.
2. Enter the collector name and IP range covered in the format *255.255.255.255*.
3. Click **Apply**.

## **Classifying Sites**

WI categorizes each Web access that it monitors. A site belongs to one or more categories, based on its content, and those categories apply to all accesses to that site. You can use categories when defining access control policy and generating reports.

WI installs with a set of categories and a set of known sites in each category. When a user accesses an unknown site, the WI Classification Server uses SmartList to analyze and categorize it. If the content of a site does not match any specific category, SmartList places the site in the category *Other*. Find a complete description in the *Administrator's Guide*.

## **Blocking and Unblocking**

With WI v6, you will not need to worry about unblocking legitimate sites. The rules you create determine what content to block, rather than relying on block lists. Further, WI v6 blocks by domain, not IP address. For example, if your office supplies vendor shares web hosting with a gambling site and you have blocked all gambling sites, WI passes the vendor and blocks the gambling.

## **Unmonitored or Unrestricted Groups**

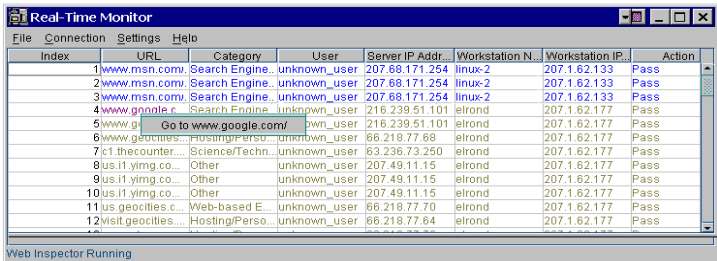
1. If you do not want to monitor some users or workstations on your network, place them in the special groups *Unmonitored Users* or *Unmonitored Workstations*.
2. If you do not want to restrict the Web access of some users or workstations on your network, place them in the groups *Unrestricted Users* or *Unrestricted Workstations*.

**Important:** *Membership in Unrestricted Users or Unrestricted Workstations takes precedence over any rules in access control policy that might otherwise affect the user or workstation.*

For details, see the *WI Administrator's Guide*.

## Opening the Real-Time Monitor

1. Log into the WI Server as Administrator or as a user with administrative privileges.
2. From the *Start* button, select **Programs → Internet Manager → Web Inspector → Real-Time Monitor**.



The screenshot shows the 'Real-Time Monitor' window with a menu bar (File, Connection, Settings, Help) and a table of active connections. The table has columns for Index, URL, Category, User, Server IP Address, Workstation Name, Workstation IP, and Action. Row 6 is highlighted, showing a connection to 'www.google.com' with the category 'Search Engine' and user 'unknown\_user'. A tooltip is visible over the URL, displaying 'Go to www.google.com/'. The status bar at the bottom indicates 'Web Inspector Running'.

Index	URL	Category	User	Server IP Addr...	Workstation N...	Workstation IP...	Action
1	www.msn.com	Search Engine...	unknown_user	207.68.171.254	linux-2	207.1.62.133	Pass
2	www.msn.com	Search Engine...	unknown_user	207.68.171.254	linux-2	207.1.62.133	Pass
3	www.msn.com	Search Engine...	unknown_user	207.68.171.254	linux-2	207.1.62.133	Pass
4	www.google.c...	Search Engine...	unknown_user	216.239.51.101	elrond	207.1.62.177	Pass
5	www.google.c...	Search Engine...	unknown_user	216.239.51.101	elrond	207.1.62.177	Pass
6	www.geocities... Go to www.google.com/	Hosting/Perso...	unknown_user	66.218.77.68	elrond	207.1.62.177	Pass
7	c1.thecounter...	Science/Techn...	unknown_user	63.236.73.250	elrond	207.1.62.177	Pass
8	us.i1.yimg.co...	Other	unknown_user	207.49.11.15	elrond	207.1.62.177	Pass
9	us.i1.yimg.co...	Other	unknown_user	207.49.11.15	elrond	207.1.62.177	Pass
10	us.i1.yimg.co...	Other	unknown_user	207.49.11.15	elrond	207.1.62.177	Pass
11	us.geocities.c...	Web-based E...	unknown_user	66.218.77.70	elrond	207.1.62.177	Pass
12	visit.geocities...	Hosting/Perso...	unknown_user	66.218.77.64	elrond	207.1.62.177	Pass

You can click on any URL in the Monitor to go directly to the site and evaluate it for yourself. By clicking **Settings → Category**, you reach a window that enables you to customize display details for any or all categories.

For configuration details, see the *WI Administrator's Guide*.

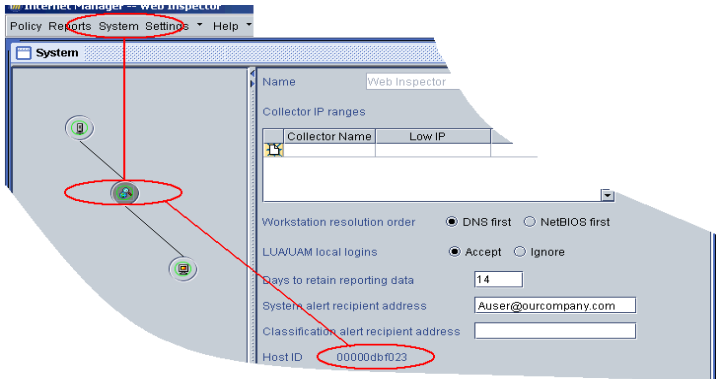


## Licensing Web Inspector v.6

Your initial trial entitles you to install WI v. 6 and monitor Web accesses from an unlimited number of workstations for 15 days. After that, WI stops collecting information until you purchase and register it, although you can run reports on the collected data for another 75 days.

Licensing WI is a short, online process. When you place an order, the information goes to the Elron database. At the end, we send you a license-authorization email with a key.

Install WI before beginning the process. Click **System** in the WI Console menu bar and open the WI page by selecting the middle node in the left pane. In the right pane of the WI page, you can check the licensing status and find the host ID of the WI computer. (This is the MAC address of the WI computer's NIC, with no hyphens.)

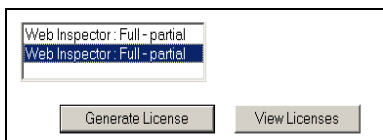


To license WI:

1. Click on the URL in the email.

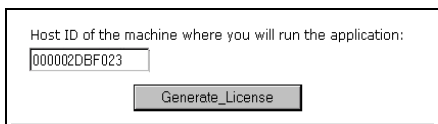
**Note:** *Record this URL or save the email in case you want to move the license to another computer or change the NIC.*

2. On the first screen, enter the authorization code from the email and click **Submit**.
3. Select your WI order in the field and click **Generate License**.



A screenshot of a web form. At the top, there is a dropdown menu with two items, both labeled 'Web Inspector: Full - partial'. Below the dropdown are two buttons: 'Generate License' and 'View Licenses'.

4. On the next screen, enter your host ID and click **Generate License**.



A screenshot of a web form. It contains a text input field with the value '000002DBF023'. Above the field is the label 'Host ID of the machine where you will run the application:'. Below the field is a button labeled 'Generate\_License'.

5. On the *License Certificate* page, right-click the **here** link in the *Save License* area. Then select either **Save Target As** or **Save Link As**, depending on your browser.

### **Save License**

To Complete the fulfillment process, save the license certificate above as a license file on the Web Inspector administration server.

To save the license to a file, right-click [here](#) and select 'Save Target As' option

If you are working from the WI computer, save the file as *im.lic* directly to WI's installation folder. By default, this is

the *C:\Program Files\Internet Manager\bin* folder. If you are at another computer, save *im.lic* locally or on a diskette. Then copy it to the WI computer.

**Important:** *In the Save dialog, save to file type All Files rather than the default .txt.*

**Note:** *We recommend saving a backup copy of the license file in case of hard-drive problems on the server. This will save you time if you have to reinstall WI from scratch.*

6. Click **Exit the System**.

7. After you save *im.lic* to the administration server, stop and start the *IM Administration Server* service through **Control Panel** → **Services**.

Congratulations. You have licensed your WI software.

If you need to re-host a license, see the *WI Administrator's Guide* for instructions.

