

# User Manual



## WebMSM Web Monitoring System Manager 071-1239-01

This document supports software version 2.0 and above.

[www.tektronix.com](http://www.tektronix.com)

Copyright ©Tektronix, Inc. All rights reserved. Licensed software products are owned by Tektronix or its suppliers and are protected by United States copyright laws and international treaty provisions.

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or subparagraphs (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights clause at FAR 52.227-19, as applicable.

Tektronix products are covered by U.S. and foreign patents, issued and pending. Information in this publication supersedes that in all previously published material. Specifications and price change privileges reserved.

Tektronix, Inc., P.O. Box 500, Beaverton, OR 97077

TEKTRONIX and TEK are registered trademarks of Tektronix, Inc.

WebMSM Web Monitoring System Manager User Manual  
TekCamb Document: SI447 Issue 1.1e

Software version: 2.0

## Software Warranty

Tektronix warrants that the media on which this software product is furnished and the encoding of the programs on the media will be free from defects in materials and workmanship for a period of three (3) months from the date of shipment. If a medium or encoding proves defective during the warranty period, Tektronix will provide a replacement in exchange for the defective medium. Except as to the media on which this software product is furnished, this software product is provided "as is" without warranty of any kind, either express or implied. Tektronix does not warrant that the functions contained in this software product will meet Customer's requirements or that the operation of the programs will be uninterrupted or error-free.

In order to obtain service under this warranty, Customer must notify Tektronix of the defect before the expiration of the warranty period. If Tektronix is unable to provide a replacement that is free from defects in materials and workmanship within a reasonable time thereafter, Customer may terminate the license for this software product and return this software product and any associated materials for credit or refund.

THIS WARRANTY IS GIVEN BY TEKTRONIX IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED. TEKTRONIX AND ITS VENDORS DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TEKTRONIX' RESPONSIBILITY TO REPLACE DEFECTIVE MEDIA OR REFUND CUSTOMER'S PAYMENT IS THE SOLE AND EXCLUSIVE REMEDY PROVIDED TO THE CUSTOMER FOR BREACH OF THIS WARRANTY. TEKTRONIX AND ITS VENDORS WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IRRESPECTIVE OF WHETHER TEKTRONIX OR THE VENDOR HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.



# Table of Contents

<b>Preface</b> .....	v
Related Material.....	vi
Manual Conventions .....	vi
Contacting Tektronix .....	vii

## Getting Started

<b>Getting Started</b> .....	<b>1-1</b>
Overview.....	1-1
System Configuration .....	1-3
WebMSM Options .....	1-7
WebMSM Field Upgrade Kits .....	1-7
Licensing.....	1-8
Passwords.....	1-9
Remote User Interface .....	1-10
<b>Installation</b> .....	<b>1-11</b>
Minimum Requirements .....	1-11
User Installation.....	1-13
Administrator Installation .....	1-20
User Documentation .....	1-28
First Use for Monitoring .....	1-29

## WebMSM Reference

<b>WebMSM Reference</b> .....	<b>2-1</b>
User Interface Overview .....	2-1
Opening the WebMSM Control Panel .....	2-4
Menus and Options .....	2-5
Accessing Configuration Lists .....	2-7

## WebMSM Configuration Reference

<b>WebMSM Configuration Editor</b> .....	<b>3-1</b>
Opening the WebMSM Configuration Editor.....	3-2
Menus and Options .....	3-3
Editing an Existing Configuration File .....	3-5
Configuration List.....	3-6
Hot Spot Editor .....	3-11
Stream Editor .....	3-21

Device Editor ..... 3-24  
Event Classification Editor..... 3-26  
Checking the Configuration against the Current License ..... 3-29

**Index**

## List of Figures

Figure 1-1: System Configuration - Example .....	1-2
Figure 1-2: Network Architecture .....	1-4
Figure 1-3: Configuration File Relationships .....	1-5
Figure 1-4: Password Locations .....	1-9
Figure 1-5: WebMSM Control Panel - Initial User screen .....	1-16
Figure 1-6: WebMSM Configuration Editor - Initial Administrator screen .....	1-22
Figure 1-7: WebMSM Control Panel - First Use .....	1-30
Figure 1-8: Configuration Setup - Example .....	1-32
Figure 2-1: WebMSM Control Panel - Open .....	2-4
Figure 3-1: WebMSM Configuration Editor - Open .....	3-2
Figure 3-2: Select Configuration Dialog .....	3-6
Figure 3-3: WebMSM Configuration List Editor .....	3-7
Figure 3-4: Hot Spot Editor .....	3-11
Figure 3-5: Hot Spot Editor - Background .....	3-16
Figure 3-6: Hot Spot Details Dialog .....	3-18
Figure 3-7: Hot Spot Images Dialog .....	3-19
Figure 3-8: Stream Configuration Editor .....	3-21
Figure 3-9: Device Configuration Editor .....	3-24
Figure 3-10: Event Classification Editor .....	3-27
Figure 3-11: License - Example .....	3-30

## List of Tables

Table 1-1: Sample Files .....	1-6
Table 1-2: Standard WebMSM Configuration.....	1-7
Table 1-3: WebMSM Options.....	1-7
Table 1-4: WebMSM Field Upgrade Kits.....	1-7
Table 2-1: Color Coding - Background.....	2-2
Table 2-2: Color Coding - Buttons.....	2-3
Table 2-3: Configurations Menu Commands.....	2-5
Table 2-4: User Menu Commands .....	2-6
Table 2-5: License Menu Commands .....	2-6
Table 2-6: Configurations Menu Commands.....	2-7
Table 3-1: Configurations Menu Commands.....	3-3
Table 3-2: User Menu Commands .....	3-4
Table 3-3: License Menu Commands .....	3-4
Table 3-4: Help Menu Commands .....	3-4
Table 3-5: Configuration List Editor - File Menu Commands.....	3-7
Table 3-6: Hot Spot Editor - File Menu Commands.....	3-13
Table 3-7: Hot Spot Editor - Frame Menu Commands .....	3-14
Table 3-8: Hot Spot Editor - Hot Spots Menu Commands .....	3-14
Table 3-9: Hot Spot Editor - Main Panel Menu Commands.....	3-15
Table 3-10: Hot Spot Editor - Status Banner Menu Commands.....	3-15
Table 3-11: Hot Spot Details Dialog Commands.....	3-18
Table 3-12: Stream Configuration Editor - File Menu Commands.....	3-22
Table 3-13: Device Configuration Editor - File Menu Commands.....	3-24
Table 3-14: Event Classification Editor - File Menu Commands .....	3-28



# Preface

This manual describes the functions and use of the Tektronix WebMSM Web Monitoring System Manager. The manual is organized into the following sections:

- **Getting Started**  
This section describes the WebMSM and provides installation instructions.
- *WebMSM Reference*  
This section provides descriptions and procedures for the WebMSM.
- *WebMSM Configuration Editor Reference*  
This section provides descriptions and procedures for the WebMSM Configuration Editor.

WebMSM will operate with a range of Real Time Monitoring (RTM) devices. Each RTM user interface will inevitably have minor differences, dependent upon the features offered by the RTM device. For this reason each RTM user interface is described in the associated RTM User Manual.

## Related Material

This manual is also provided in portable document format (PDF) on the application CD-ROMs; it is installed with the application. A PDF reader is included on the CD-ROM.

The RTM devices that the WebMSM interacts with are documented separately. The appropriate user manuals are supplied with the RTM devices.

## Manual Conventions

The following formatting conventions are used in this manual:

- **On-screen** buttons.  
Example: Select the **Streams** button.
- **Dialog** box names and **field** names.  
Example: Enter the decimal value in the **Value** field.
- Menu option selections are represented thus: **<menu> → <option>**,  
Example: **File → Save**.
- Mono-spaced text is used where ASCII text is being illustrated.  
Example: `\wsm\config.txt`
- 'Path names' and 'filenames' are contained within single quotes.

# Contacting Tektronix

<b>Phone</b>	1-800-833-9200*
<b>Address</b>	Tektronix, Inc. Department or name (if known) 14200 SW Karl Braun Drive P.O. Box 500 Beaverton, OR 97077 USA
<b>Web site</b>	<a href="http://www.tektronix.com">www.tektronix.com</a>

## Support - N & S America

<b>Sales support</b>	1-800-833-9200, select option 1*
<b>Service support</b>	1-800-833-9200, select option 2*
<b>Technical support</b>	Email: <a href="mailto:techsupport@tektronix.com">techsupport@tektronix.com</a> 1-800-833-9200, select option 3* * - toll free in North America.  6:00 a.m. -- 5:00 p.m. Pacific time After office hours, please leave a voice mail message.

## Sales Support - Europe & the Rest of the World

Telephone: +44 (0)1344 392000

## Service & Technical Support - Europe & the Rest of the World

Telephone +44 (0)1223 200700

Fax +44 (0)1223 200701





# Getting Started



# Getting Started

## Overview

The Web Monitoring Systems Manager (WebMSM) provides complete visibility of the error status of a transmission network.

Real time monitoring (RTM) devices can be placed at strategic points in a transmission network. An RTM device can facilitate one or more probes; a probe corresponds to a monitoring point in a transmission network. WebMSM licensing is carried out on a 'per probe' basis. In addition to the licensed probes, RTM device parameters, such as operating temperature and hard disk status, can be monitored. All of this data can be monitored from a central point.

Transport stream monitoring data is handed from the probe point to the WebMSM; similarly, device data is handed from the RTM device to the WebMSM. Both sets of data will vary from probe to probe and from RTM device to RTM device. For this reason, the Stream and Device sections of the user interface are not described in detail in this user manual; they are described in the relevant RTM device user manual.

The WebMSM Configuration Editor allows a complete multi-layered model of the network to be configured and implemented. It also allows the network manager to identify and monitor specific elements in the network, such as the status of a particular RTM device, or to raise or lower the reporting status of errors in the transport stream.

The WebMSM features are all accessible through the WebMSM Control Panel: configuration selection, password management and license registration.

Configuration of systems may use one or more of the following views: Hot Spot, Stream and Device. Each view is provided by a separate application that handles a different aspect of system management and monitoring.

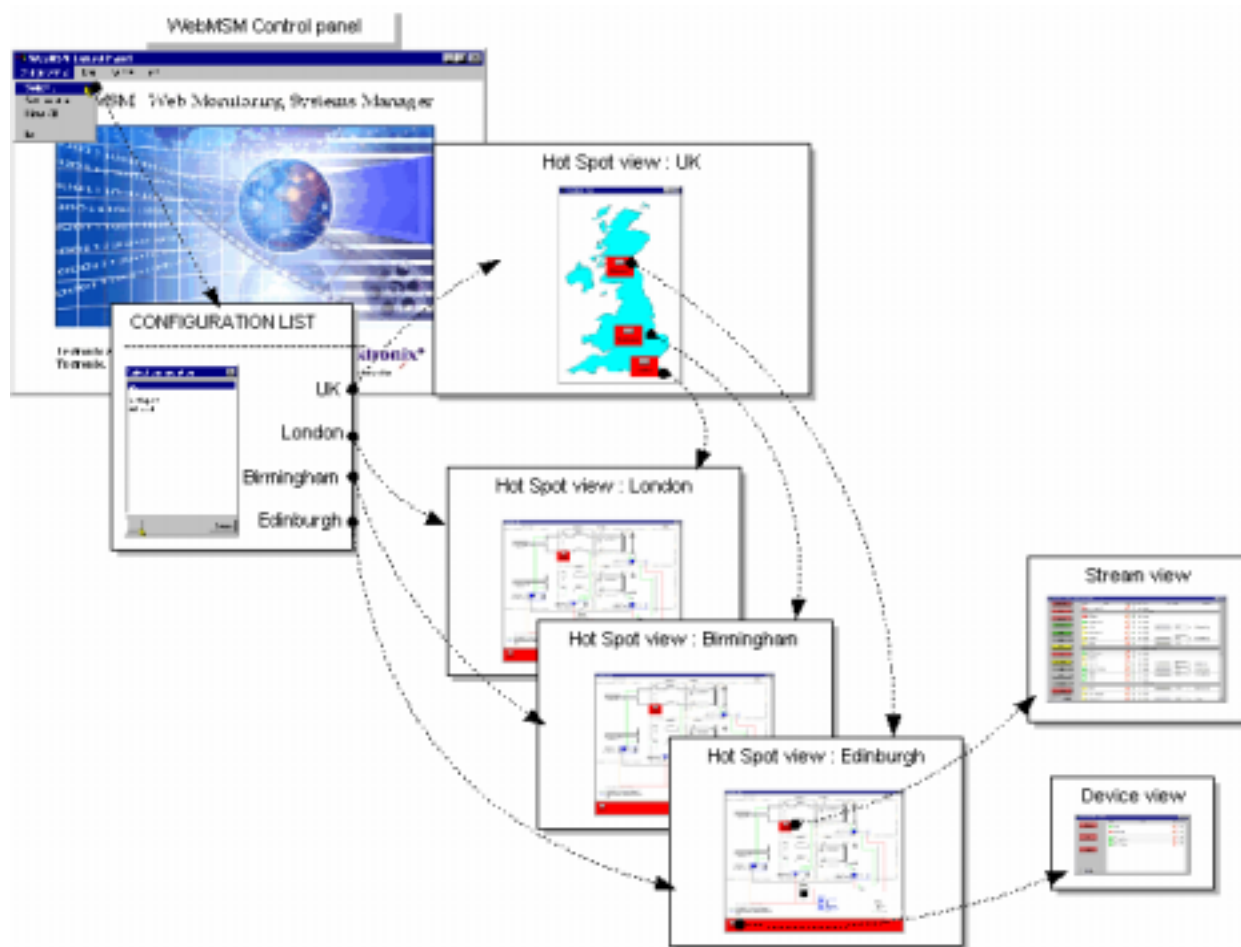


Figure 1-1: System Configuration - Example

The Hot Spot application allows the overall state of streams and RTM devices to be viewed in a graphical environment. Hot spots are icon-like images placed at strategic points on a background image of a map or system diagram and linked to a device, a stream or another hot spot view. Hot Spots also provide an overview of the status of the linked item using color coding.

The Hot Spot views are managed by a set of configuration files that dictate the content and linking of the various views. Any number of configurations can be created using WebMSM Configuration Editor. On starting the WebMSM, the user can make a selection from a configuration list.



The Stream application interprets and displays stream-related information received from the associated RTM device, including:

- Tests
- Programs
- PIDs (packet identities)
- Service information tables:
  - PSI/SI/PSIP - Program Specific Information (MPEG)
  - Service Information (DVB)
  - Program and Specific Information Protocol (ATSC)

The Device application interprets and displays RTM device-related information received from the associated RTM device, including fan status and the device event log.

## System Configuration

A major feature of WebMSM is its versatility with respect to configuration. Although always operating within a client-server architecture, the system components can be centralized or distributed around a system.

A large network may have a dedicated Web server that holds the WebMSM Configuration files. Users of the system would have WebMSM installed on their own personal computer (PC); they may then choose to use either their own local WebMSM configuration files or the WebMSM configuration files held by the dedicated Web server.

System Security is facilitated using password files. These are held on individual RTM devices or on a central Web server.

The monitoring data generated by some RTM devices can also be accessed by a Remote User Interface. It is accessed through a Web browser running on a Client PC.

Although a user can access multiple RTM devices through multiple instances of the Remote User Interface, this is not recommended as a normal working practice.

### Network Architecture

The diagram below illustrates an example of WebMSM network architecture.

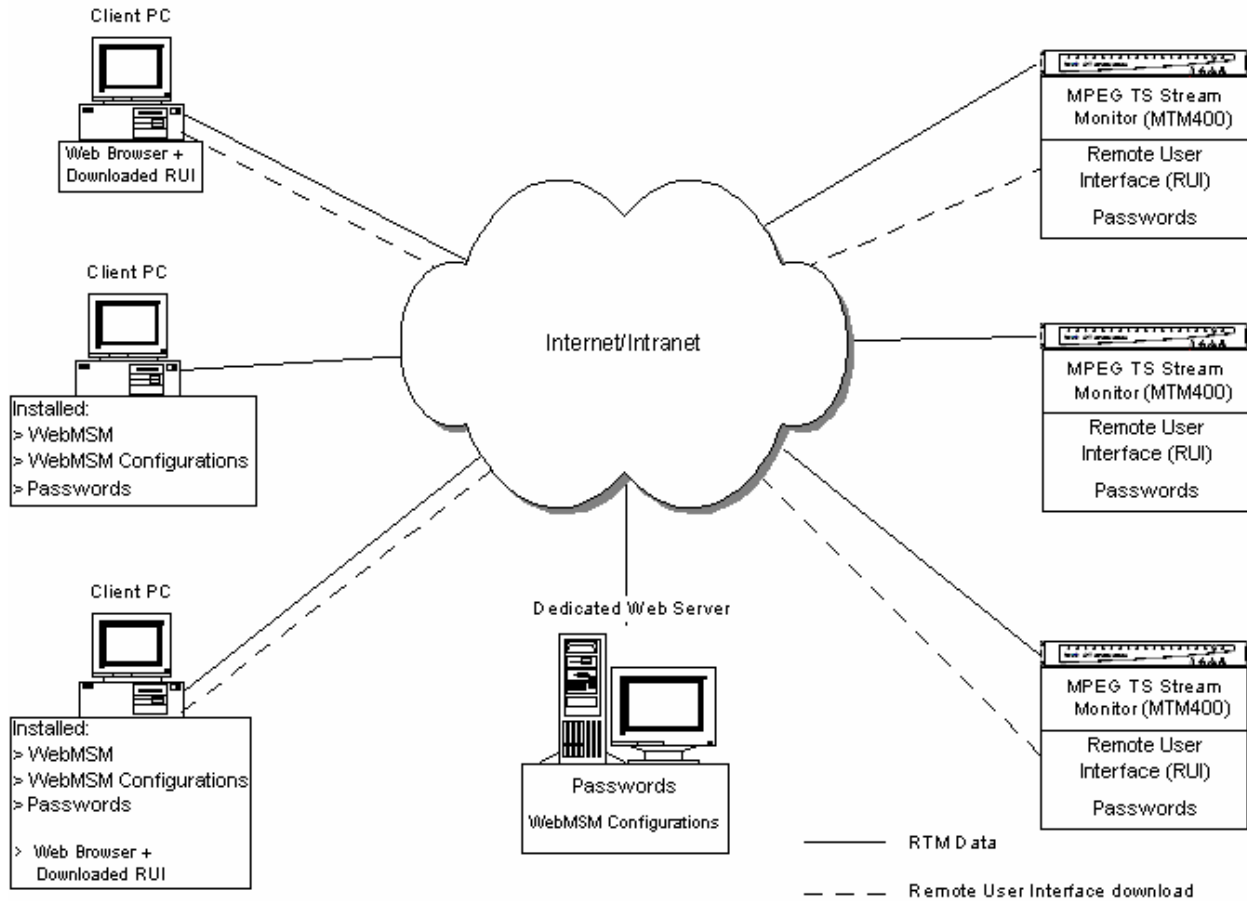


Figure 1-2: Network Architecture

WebMSM configuration files can be stored either on the Web server, on the client PCs, or in both locations. The files stored on the Web server are available to all users of the network (subject to permissions), whereas those stored on client PCs are available to only the user of that PC.

The Passwords can still be installed on a Web Server; this can either be a monitoring device or a dedicated Web server.

**NOTE.** *The Remote User Interface can be used from any networked PC equipped with a Web Browser independently of the WebMSM architecture.*

## WebMSM Configuration

Configuration of the WebMSM for a particular system setup is provided by a hierarchy of configuration files. Each configuration file handles a specific aspect of the system architecture and provides links to other levels. The WebMSM Configuration Editor provides the tools (editors) needed to create and edit the configuration files.

The diagram below illustrates the relationship between the various configuration files.

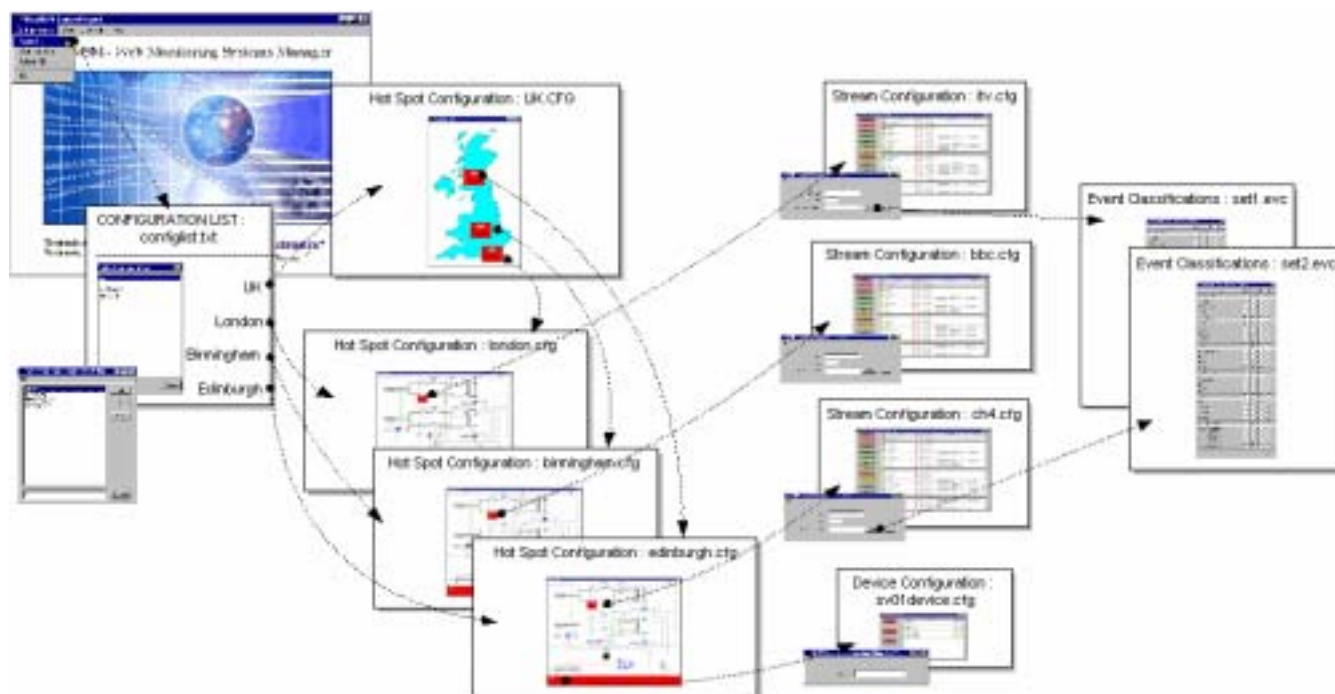


Figure 1-3: Configuration File Relationships

The configuration files are as follows:

- Configuration List.** The WebMSM reads this file (configlist.txt) when **Configurations → Select...** is selected from the WebMSM Control Panel. The configuration list provides content for the **Select Configuration** dialog. Each entry in the Configuration List acts as a pointer to the next level of system configuration files.

Configuration Lists are created and edited using the Configuration List Editor.

- **Hot Spots.** Hotspot views are graphical representations of systems overlaid with active hotspots. Each hot spot provides a link to another hot spot view, a device view or a stream view.

Hotspot configuration files (\*.cfg) are created and edited using the Hot Spot Editor.

- **Stream.** The content for Stream views is received from an RTM device.

Stream configuration files (\*.cfg) indicate which stream is to be used. The file may also be associated with an Event Classification file. Stream configuration files are created and edited using the Stream Configuration Editor.

- **Device.** The content for Device views is received from an RTM device.

Device configuration files (\*.cfg) indicate which device is to be used. Device configuration files are created and edited using the Device Configuration Editor.

- **Event Classifications.** Events in streams can be categorised and grouped.

Event Classification files (\*.evc) contain the error classification data. Each classification file can be associated with one or more streams. Event Classification files are created and edited using the Event Classification Editor.

**Sample Configuration.** A sample configuration has been provided in the SampleConfiguration directory. It may be useful to inspect the sample files.

The directory containing the files should be copied from the CD-ROM to a suitable location on the PC. The sample contains the following files:

**Table 1-1: Sample Files**

Hot Spot views	Stream views	Device views
uk.cfg london.cfg birmingham.cfg edinburgh.cfg	stream1.cfg stream2.cfg stream3.cfg	device1.cfg device2.cfg device3.cfg

Two graphic files: uk.gif and site.gif.

One event classification file: test.evc

The primary configuration list file: configlist.txt

## WebMSM Options

WebMSM options are enabled using licensing. All options are available at installation; no further installation activity is currently required. The License Key enables those options that the customer has purchased.

The options available are given in the following tables:

**Table 1-2: Standard WebMSM Configuration**

Nomenclature	Description	Deliverables
WebMSM	Web-based monitoring management software, installable application with license for monitoring up to 4 monitoring probes.	<ul style="list-style-type: none"> <li>- Web Monitoring Systems Manager installation CD (Tektronix part number: 063-3648-xx).</li> <li>- Web Monitoring Systems Manager Configuration Editor installation CD (Tektronix part number: 063-3649-xx).</li> <li>- Option Key license for up to 4 monitoring probes.</li> </ul>

**Table 1-3: WebMSM Options**

Item	Option	Description
WebMSM	08	Additional license for adding up to eight monitoring probes to WebMSM.
	16	Additional license for adding up to 16 monitoring probes to WebMSM.
	32	Additional license for adding up to 32 monitoring probes to WebMSM.
	64	Additional license for adding up to 64 monitoring probes to WebMSM.
	UL	Additional license for adding unlimited monitoring probes to WebMSM.

## WebMSM Field Upgrade Kits

The field upgrade kits that are available for the WebMSM are listed in the following table:

**Table 1-4: WebMSM Field Upgrade Kits**

Item	Description
WebMSMF16	Additional license for adding up to 16 monitoring probes to WebMSM.
WebMSMF32	Additional license for adding up to 32 monitoring probes to WebMSM.
WebMSMF64	Additional license for adding up to 64 monitoring probes to WebMSM.
WebMSMFUL	Additional license for adding unlimited monitoring probes to WebMSM.

## Licensing

WebMSM uses a licensing scheme to control the number and types of probes that can be accessed and controlled by WebMSM. The license also authorizes use of the WebMSM Configuration Editor.

A serial number and an option key are supplied with WebMSM. The option key is of the form 'nnnnn-nnnnn-nnnnn-nnnnn', where 'n' is any alphanumeric character; the option key is case-sensitive.

Users are required to enter these details in either the WebMSM Client or WebMSM Configuration Editor applications through a dialog box before they can use any of the features. The license details will be stored on the client machine.

## Passwords

Security access is controlled by a combination of user names and passwords. Currently two user names are available:

- 'User' enables monitoring only access to the RTM devices.
- 'Administrator', in addition to monitoring access, allows a range of device parameters to be set.

Each user name may be allocated a password by the Administrator. The user name / password details are stored in a password file, which may be stored locally or on a Web server.

The following diagram shows the possible locations for the password file and the accessibility:

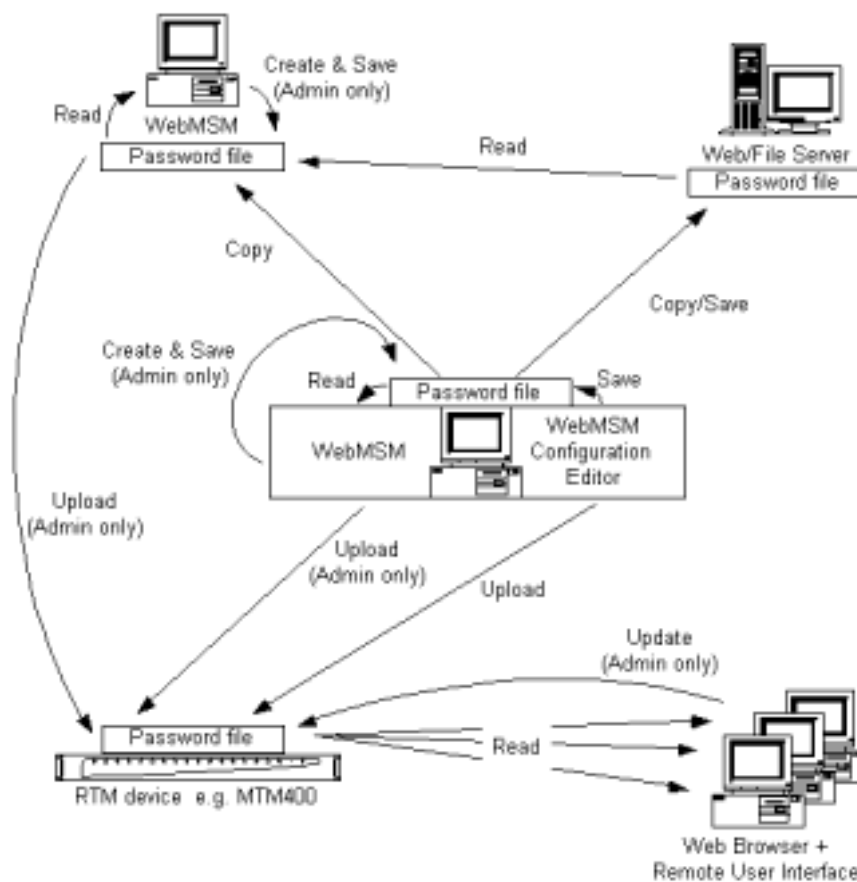


Figure 1-4: Password Locations

From Figure 1-4, note the following points:

- Only a user designated as an Administrator can create and save passwords.
- Passwords for the installed WebMSM can be stored on the local PC or on a Web/File Server.
- Passwords created and edited on an installed WebMSM or WebMSM Configuration Editor can be uploaded to RTM devices for use by those accessing the device through the RUI.

## Remote User Interface

Separate Remote User Interface (RUI) software, based on the WebMSM, is supplied with some RTM devices; it may be preinstalled or supplied as an upgrade kit. The RUI is accessed a Web browser (Microsoft Internet Explorer with Microsoft Virtual Machine installed) of any networked personal computer. The interface initially displays a view similar to the Hot Spot view status bar. The buttons on the Status Bar link to a Device view and Stream view(s).



# Installation

This section describes the procedures for installing the WebMSM and the WebMSM Configuration Editor onto a personal computer. Use these procedures to reinstall the software if it is deleted or becomes corrupted.

Installation is described in two sections:

- **User installation:** Installation of WebMSM, including registration of the serial number and the license key.

A User has access to WebMSM and the monitoring functions that it provides. Security, in the form of passwords, will be advised by the Administrator.

- **Administrator installation:** Installation of WebMSM and the WebMSM Configuration Editor, including registration of the serial number and the license key and password setup.

An Administrator has access to the WebMSM Configuration Editor and WebMSM. The WebMSM Configuration Editor allows the Administrator to configure the system and allocate passwords.

## Minimum Requirements

The minimum requirements for a client PC running the WebMSM applications are as follows:

- 500 MHz Intel Pentium Processor
- 256 MB RAM
- 30 MB free disk space
- Any Microsoft Windows operating system
- Microsoft Internet Explorer, Version 5.0 minimum
- Microsoft Java Virtual Machine installed, Version 5.0 minimum
- 1024 x 768 pixel video monitor with 256 available colors
- Ethernet: 10/100 Base-T; RJ45
- RTM device

It is assumed that the RTM device and the Client PC are incorporated into a network.

Confirm that Internet Explorer, Version 5.0 (minimum), and Microsoft Java Virtual Machine, Version 5.0 (minimum), are present before proceeding with the installation.

### Checking Microsoft Internet Explorer Version

Open Microsoft Internet Explorer. The version number will be displayed on the opening splash screen. Further confirmation is available by selecting **Help → About Internet Explorer**.

### Checking Microsoft Java Virtual Machine Version

Select the Command Prompt from the Start menu:

- WindowsNT: **Start → Programs**
- WindowsXP: **Start → All Programs → Accessories**
- Windows2000: **Start → Programs → Accessories**

Select the **Command Prompt**.

1. Using DOS commands, navigate to the root drive; for example, C:\>.
2. Enter `java`.

The version number of the Microsoft Java Virtual Machine is displayed in the first line of the response thus:

```
Microsoft (R) Command-Line Loader for Java Version 5.00.3802  
...
```

The minimum acceptable version number is 5.00.0000.

If the Java Virtual Machine is not installed, the prompt will be redisplayed with no response.

### Installing the Java Virtual Machine

The user must have Windows NT administrative rights to be able to install the Java Virtual Machine.

1. Locate the following program: MSJAVX86.exe.
2. Run MSJAVX86.exe.

The response will indicate that the installation has been successful.

---

**NOTE.** *If the user does not have Windows NT administrative rights, attempting to install the Java Virtual Machine will elicit an error message and go on to indicate success – this is not the case!*

---

3. Enter `java` at the command prompt to confirm the the Java Virtual Machine has been successfully installed.

## User Installation

Installation for a User includes the following processes:

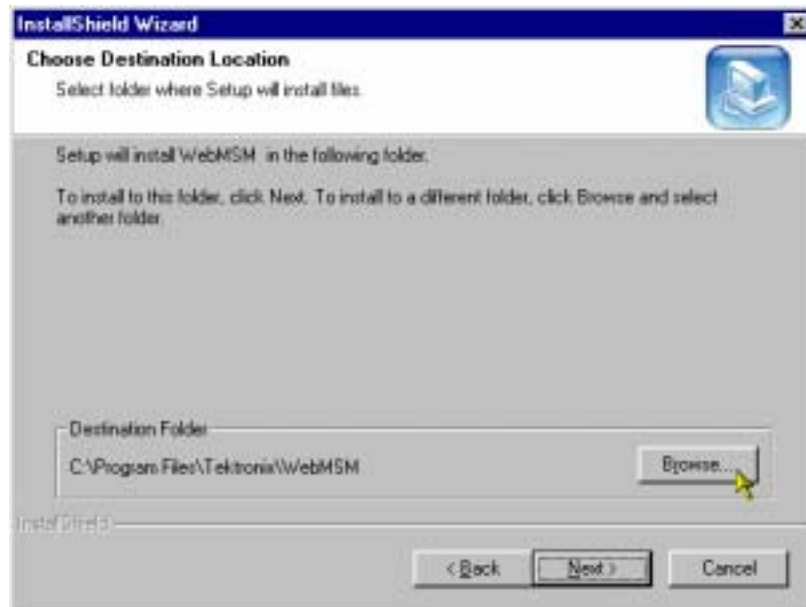
- Installing WebMSM
- Accessing passwords
- Entering the Serial Number and License Key

A WebMSM User must be able to access real-time monitoring devices using the WebMSM interface. For this activity all that is required is a password and the configuration, for example, IP address. The password and configuration is supplied and set up by the WebMSM Administrator. At first use, the User will also need to provide the licensing data (serial number and option key).

### Installing WebMSM

1. Insert the WebMSM Applications installation CD-ROM in the personal computer CD-ROM drive.
2. On the CD-ROM, run `setup.exe` from the root directory.
3. Step through the installation process, following the instructions as necessary.

During the WebMSM installation, the following screen is displayed:

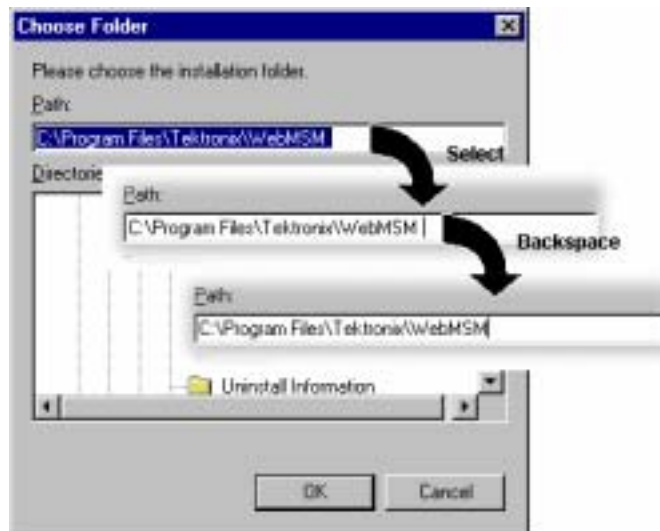


4. At this point select **Browse**.
5. In the **Choose Folder** dialog, if applicable, remove the space at the end of the **Path:** name.

---

**NOTE.** The additional space in the path is not present on all installation disks. However, this check must be made to ensure correct operation.

---



6. Select **OK**.
7. Continue and complete the installation.

## Starting WebMSM

8. Start WebMSM from either the desktop shortcut (created during installation):



or the **Start → Programs → Tektronix WebMSM → WebMSM** option.



The WebMSM cannot be used if a password file cannot be found and the Serial Number and License Key are not registered with the program. The password and license details are stored in separate files.

This will typically occur at first use, but it may also occur if the password or license files are not stored locally; in this case, the user will need to identify the location of the files.

A message is displayed when the file containing passwords cannot be found.



Similarly, a message is displayed when the file containing license details cannot be found.



9. Select **OK** in both cases. The lack of password and license details is explained and rectified in the following steps. The following screen is displayed:



Figure 1-5: WebMSM Control Panel - Initial User screen

---

**NOTE.** *The menu options are limited initially. When the Password and License details have been successfully entered, more menu options will become available.*

---

### Accessing Passwords

Only an operator designated as a WebMSM Administrator can create or edit the password file. From a User's point of view, there are two options:

- The password file must have already been set up and placed in a location accessible from the User's personal computer.
- The file must be supplied to the user by the administrator and copied into the WebMSM installation directory.

If passwords have not been set up, the instructions for the Administrator Installation must be carried out (see page 1-20).

If the WebMSM Administrator accepted the default location for the password file, the password file will be available and the **WebMSM Warning: No password file found** dialog will not be displayed.

If the password file is stored at a location other than the default (c:\program files\tektronix\webmsm\), examples of the path set up by the administrator may be as follows:

Local:

file:c:\program files\tektronix\webmsm\security\

Network:

file:\\server/path/

Web Server:

http://streamview01/

---

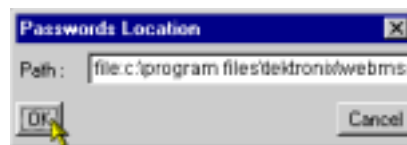
**NOTE.** If the password file is available, the **Login Details** dialog is displayed.

Proceed to Logging On, page 1-19.

---

If the existence and location of the password file is known, the user can locate and use it.

10. Select **User** → **Set Passwords Location...**



11. In the **Passwords Location** dialog, enter the full path to the passwords file.

---

**NOTE.** In all cases, the file name (*passwords*) is omitted.

---

12. Select **OK**.

### Entering the Licensing Data

The serial number and option key are held in a file that is accessible to WebMSM at startup. The user must supply this data at first use of the WebMSM; the file is created at that time and retained for future use. The license data is supplied with the product documentation.

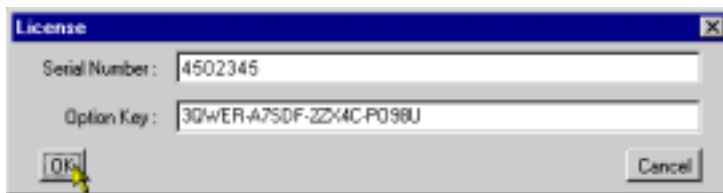
---

**NOTE.** When another license is obtained, to increase the number of probes accessible for example, a new serial number and option key will be supplied. This data should be reentered in order to upgrade the WebMSM application.

**NOTE.** If the Serial Number is preceded by an alpha character (for example, B), omit the alpha character when entering the Serial Number in the **License** dialog.

---

13. Select **License** → **Update....** The **License** dialog is displayed.



14. Enter the **Serial Number** and **Option Key** details.

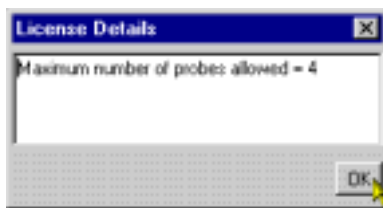
---

**NOTE.** that the data is case sensitive; enter it exactly as given in the product documentation.

---

15. Select **OK**.

The license can be verified by selecting **License** → **View Details....**

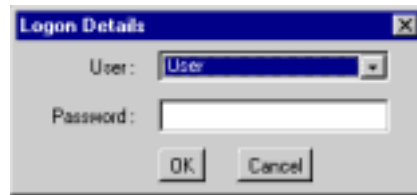


The **License Details** dialog will report the license status.



### Logging On

With the location of the passwords file identified, select **User** → **Logon...** The **Login Details** dialog is displayed.



16. Select **User** from the **User:** drop-down list.
17. Enter a password (if required). The person designated as Administrator is responsible for the allocation of passwords.
18. Select **OK**.

Proceed to *First Use for Monitoring*, page 1-29.

## Administrator Installation

Installation for an Administrator includes the following processes:

- Installing WebMSM Configuration Editor
- Starting WebMSM Configuration Editor
- Entering the Licensing Data
- Setting Passwords
- Saving the Password File
- Uploading the Password File
- Installing WebMSM

---

**NOTE.** *It is the WebMSM Administrator who sets up passwords. Password information must be passed to WebMSM Users before they can successfully access the WebMSM interface.*

---

### Installing WebMSM Configuration Editor

1. Insert the WebMSM Configuration Editor installation CD-ROM in the personal computer CD-ROM drive.
2. On the CD-ROM, run setup.exe from the root directory.
3. Step through the installation process, following the instructions as necessary.

### Starting WebMSM Configuration Editor

4. Start WebMSM Configuration Editor either from the desktop shortcut (created during installation):



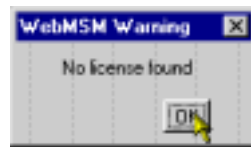
or the **Start → Programs → Tektronix WebMSM → WebMSM Configuration Editor** option.



The WebMSM Configuration Editor cannot be used if the serial number and license key are not registered with the program.

This will typically occur at first use. It may also occur if the license files are not stored locally; in this case, the user will need to identify the location of the files.

A message is displayed when the file containing license details cannot be found.



5. Select **OK**. The lack of license details is explained and rectified in the following steps. The following screen is displayed:



Figure 1-6: WebMSM Configuration Editor - Initial Administrator screen

Only a limited set of menu options is available. When the license details have been successfully entered, more menu options will become available.

### Entering the Licensing Data

The serial number and option key are held in a file that is accessible to WebMSM Configuration Editor at startup. The user must supply this data at first use of the editor; the file is created at that time and retained for future use. The license data is supplied with the product documentation.

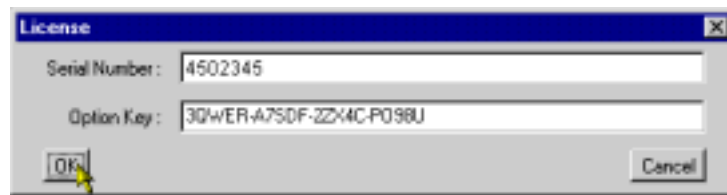
---

**NOTE.** When another license is obtained, to increase the number of probes accessible for example, a new serial number and option key will be supplied. This data should be reentered in order to upgrade the WebMSM application.

**NOTE.** If the Serial Number is preceded by an alpha character (for example, B), omit the alpha character when entering the Serial Number in the **License** dialog.

---

6. Select **License** → **Update....** The **License** dialog is displayed.



7. Enter the **Serial Number** and **Option Key** details.

---

**NOTE.** The data is case sensitive; enter it exactly as given in the product documentation.

---

8. Select **OK**.

## Setting Passwords

Only an operator designated as an Administrator can create or edit a password file for use by the WebMSM. It is assumed the a user accessing the WebMSM Configuration Editor is an Administrator and therefore no password is required to open the application. However, both a User and an Administrator require a password to access the WebMSM.

Passwords must be set for a new installation. A common password file can be used for multiple installations if the file is accessible by either a network or a Web server. For example:

Local:

file:c:\program files\tektronix\webmsm\security\

Network:

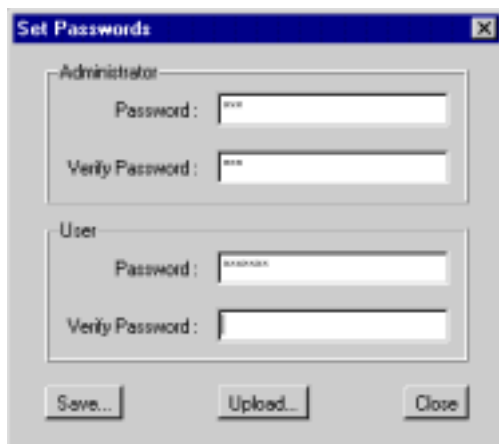
file:\\server/path/

Web Server:

http://streamview01/

Password files can also be uploaded to individual RTM devices (or lists of RTM devices). This allows passwords which will be used to access WebMSM to be administered using the WebMSM Configuration Editor.

9. Select **User** → **Set Passwords....** The Passwords dialog is displayed. This dialog is used to set the User and the Administrator password.



10. Enter the required password in the **Administrator - Password:** field. Repeat the password in the **Administrator - Verify Password:** field.

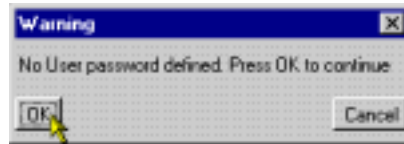
Repeat for the **User** password.

Use **Save...** to save the passwords to the passwords file either locally or on a network. Use **Upload...** to save the passwords file to RTM devices.

### Saving the Password File

11. Select **Save...**.

If a blank password has been set for either user, a message box is displayed.



---

**NOTE.** While a blank password is permissible, for security reasons it may not be advisable.

---

12. The **Password Filename** dialog is displayed.



This is a standard Windows feature. Select the required location and **Save** in the selected directory.

Always name the file `passwords`.

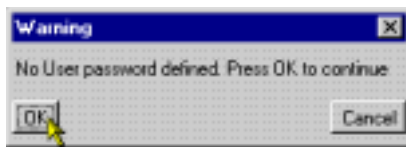
13. Unless the password file is also to be uploaded to individual RTM devices, proceed to install the WebMSM (page 1-27).

### Uploading the Password File

This feature allows the password file to be uploaded to one or more RTM devices and hence set the password for any user accessing the WebMSM through the RUI.

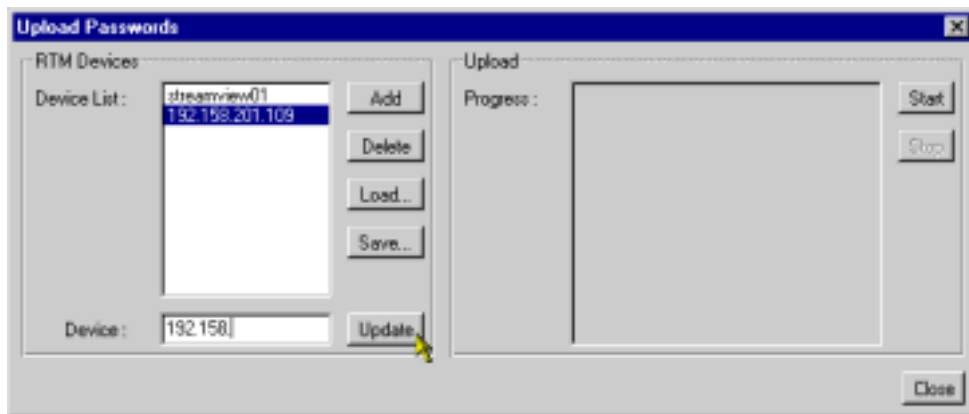
14. Select **Upload...**.

If a blank password has been set for either user, a message box may be displayed.



**NOTE.** While a blank password is permissible, for security reasons it may not be advisable.

15. Select **OK**. The **Upload Passwords** dialog is displayed.



The **RTM Devices** pane displays the addresses of the RTM devices that the Passwords file will be uploaded to when **Start** is selected.

16. To create or add to the Device List, enter the RTM device network identity or IP address in the **Device** field. Select **Add** to add the device to the **Device List**.

Devices can be deleted from the **Device List** using **Delete**. Device lists can be saved using **Save...**. Saved lists of devices can be loaded using the **Load...**.

Device names already in the Device List can be modified by highlighting the device name in the list, modifying it in the **Device** field and selecting **Update**.



17. To upload the Passwords file to the listed devices, select **Start** in the **Upload** panel.

Upload progress will be logged in the **Progress:** window.

18. When the password file has been successfully uploaded, close the dialog using **Close**.

### Installing WebMSM

19. Insert the WebMSM installation CD-ROM in the personal computer CD-ROM drive.
20. On the CD-ROM, run `setup.exe` from the root directory.
21. Step through the installation process, following the instructions as necessary.

It is assumed that the Passwords file and the License key have been correctly set up during installation of the WebMSM Configuration Editor.

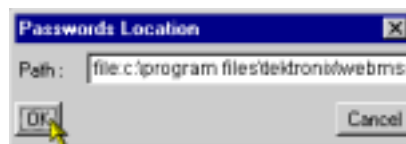
If the password file is not stored locally, on starting WebMSM it will be necessary to set the password location:

22. On start-up, the WebMSM will display the following message (if the password file cannot be found):



If the existence and location of the password file is known, the user can locate and use it.

23. Select **User** → **Set Passwords Location....**



24. In the **Passwords Location** dialog, enter the full path to the passwords file.
25. Select **OK**.

WebMSM and the WebMSM Configuration Editor have now been installed, passwords have been set up and the License Key has been entered and validated.

---

**NOTE.** *The WebMSM and the WebMSM Configuration Editor do not need to be installed on the same personal computer. Configuration creation and setup can be carried out on any PC, provided that the files thus created are made available to the WebMSM*

---

## User Documentation

Documentation, in the form of this manual in PDF (portable document format), is supplied on both installation CDs (WebMSM and WebMSM Configuration Editor) and is automatically installed if not already present. The PDF Reader can be installed by running the program ar40eng.exe; this can be found on either installation CD.

## First Use for Monitoring

This section describes first access to the WebMSM monitoring functions.

(It is assumed that the WebMSM Configuration Editor has been used to configure the system and set up passwords.)

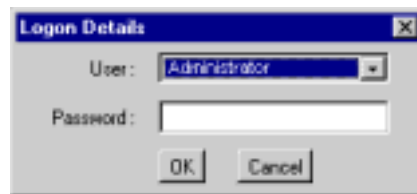
1. Start WebMSM from either the desktop shortcut (created during installation):



or the **Start** → **Programs** → **Tektronix WebMSM** → **WebMSM** option.



2. During the start up, the **Logon Details** dialog will be displayed (if the passwords file is available).



3. Select the user and enter the password (if required).
4. Select **OK**.

The WebMSM Control Panel is displayed.



Figure 1-7: WebMSM Control Panel - First Use

5. Select **Configurations** → **Select...** from the Control Panel menu bar.

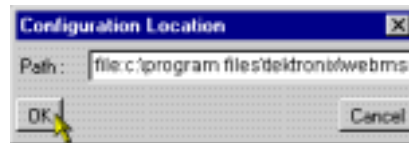
The **Select Configuration** dialog is displayed.



6. Select an opening configuration from the **Configuration List**.

If the configuration files are not available locally, it may be necessary to set their location.

- a. From the Control Panel menu bar, select **Configurations → Set Location....**
- b. The **Configuration Location** dialog is opened.



- c. Enter the configuration files path.
  - d. Select **OK**.
7. From the **Select Configuration** dialog, select the required configuration.

A pictorial example of the process is given in Figure 1-8. Configurations will vary in content and the number of Hot Spot levels.

---

**NOTE.** *When another license is obtained, to increase the number of probes accessible for example, a new Serial Number and Option Key will be supplied. This data should be reentered in order to upgrade the WebMSM application.*

---

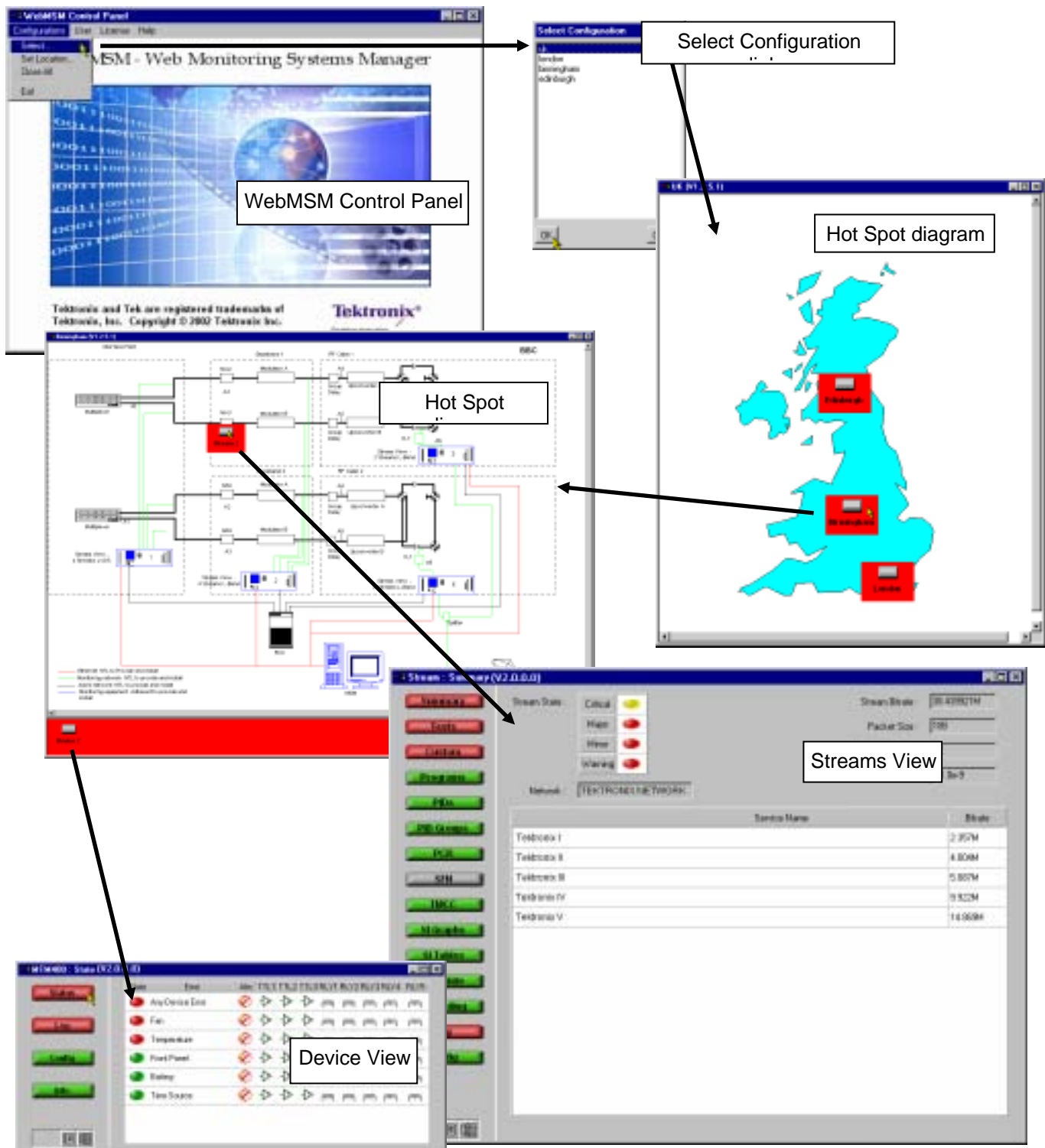


Figure 1-8: Configuration Setup - Example

From the users point of view, the Streams and Device views are the point at which monitoring of a probe or a device starts.

The Streams and Device views are not described here; they will vary depending on the RTM device being monitored. Refer to the RTM device user manual for a detailed description of these views.







# WebMSM Reference



# WebMSM Reference

The WebMSM Control panel provides a gateway to the WebMSM functions (using the Configuration menu) and a means of setting up the licensing and security (password) options.

## User Interface Overview

The main point of entry to the monitoring features provided by WebMSM is through the Configurations menu in the Control Panel - specifically the **Configuration → Select...** option which opens the **Select Configuration** dialog.

The Select Configuration dialog lists the available configuration entry points as defined in the Configuration List. An entry point may be either a Hot Spot view or a Stream or Device view on a specific RTM device; this will depend on the configuration set up using the WebMSM Configuration Editor.

### Hot Spot View

The Hot Spot view allows the overall state of streams and RTM devices to be viewed in a graphical environment. Hot spots are icon-like images placed at strategic points on a background image of a map or system diagram and linked to a device, a stream or another hot spot view.

The Hot Spot window is split into a main panel and a status banner; the latter may be hidden. The main panel can display a background map, a system diagram or similar graphic information. Also visible in the main panel are hot spots; user-defined images and labels can be used for hot spots images.

The Hot Spot color or the Hot Spot background color is dependent on the error status of the item to which it is linked.

In terms of the view that a hot spot links to, the error status of each type of hot spot is determined as follows:

- Device - the highest error state of the RTM device.
- Stream - the highest error state of the stream.
- Hot Spot - the highest error state of any of the hot spots on the linked hot spot view.

Hot spots can also be displayed on the status banner, but in this case the background of the status banner itself will indicate the highest error state of any hot spot (device, stream or other hotspot view). If no errors are present, the status banner background will be green.

If a user clicks on a hot spot with the left mouse button, the linked WebMSM view will be opened. For example, if the hot spot represents a stream, the Stream view will be started for the stream. If the hot spot represents another hot spot view, the linked Hot Spot view will be opened.

The Hot Spot view may also be configured so that clicking the right mouse button on a hot spot highlights a set of hot spots. This may be useful for highlighting stream and RTM device hotspots that relate to the same monitoring unit.

### Color Coding

In setting up the WebMSM User Interface, a choice is offered between changing the button colors and changing the button background color (see Hot Spot Images, page 3-19). Table Table 2-1 shows the color scheme where the background color option is chosen:

Table 2-1: Color Coding - Background









Icon	Background color	Meaning
 Device	White	Operation normal — no error detected.
 Device	Red	Error detected and still present.
 Device	Yellow	Transient error, which has now corrected itself.
 Device	Grey	The corresponding test has been disabled (or is unavailable). All buttons are gray indicates that connection to a device has been lost.

Table 2-2 gives examples of buttons that may be used where the button color is to indicate the error state.

**Table 2-2: Color Coding - Buttons**

Icon	Button color	Meaning
 Device	Green	Operation normal — no error detected.
 Device	Red	Error detected and still present.
 Device	Yellow	Transient error, which has now corrected itself.
 Device	Grey	The corresponding test has been disabled (or is unavailable). All buttons are gray indicates that connection to a device has been lost.

### Stream and Device Views

The Streams and Device views are not described here; they will vary depending on the RTM device being monitored. Refer to the device user manual for a detailed description of these views.

## Opening the WebMSM Control Panel

The **WebMSM** can be started by selecting the **WebMSM** option from the **Start → Programs → Tektronix WebMSM** menu



or by double-clicking the **WebMSM** shortcut on the desktop.



The WebMSM Control Panel is opened, as shown in Figure 2-1.



Figure 2-1: WebMSM Control Panel - Open

### Closing WebMSM

Select **Configurations** → **Exit** to close the WebMSM and all associated windows.

## Menus and Options

The Menu Bar provides access to all WebMSM control options using drop-down menus.

Options displayed in the menus are context sensitive. They may be grayed out depending on the level of access granted to the user (Administrator or User).

### Configurations Menu

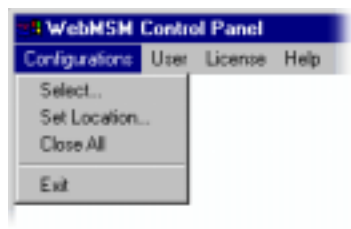


Table 2-3: Configurations Menu Commands

Command	Function
<b>Select...</b>	Opens the <b>Select Configuration</b> dialog.
<b>Set Location...</b>	Allows the location of the configuration files to be set.
<b>Close All</b>	Closes all associated WebMSM windows. The Control Panel remains open.
<b>Exit</b>	Closes the WebMSM Control Panel.

### User Menu



Table 2-4: User Menu Commands

Command	Function
<b>Logon...</b>	Opens the <b>Logon Details</b> dialog.
<b>Set Passwords Location...</b>	Allows the location of the password file to be set.
<b>Set Passwords...</b>	(Administrator only) Allows passwords to be set.

Password setup is described in the Installation section, page 1-24.

### License Menu



Table 2-5: License Menu Commands

Command	Function
<b>View Details...</b>	Opens the <b>License Details</b> dialog and allows license details to be viewed.
<b>Update...</b>	Allows license details to be entered and changed.

License setup is described in the Installation section, page 1-23.



## Help Menu



Table 2-6: Configurations Menu Commands

Command	Function
About	Opens the About WebMSM dialog; this gives program details.

## Accessing Configuration Lists

The list of configurations that is displayed in the **Select Configuration** dialog is derived from the Configuration List stored in the file 'config.txt' created by the WebMSM Configuration Editor. By default configuration files are stored in a 'configuration' directory automatically created at installation under the WebMSM Configuration Editor program files directory.

Configuration files do not need to be stored locally. They can be made accessible by either sharing the default directory on a network or placing them on a Web server. If this is done, the **Configurations** → **Set Location...** option in the Control Panel should be used to indicate the location of the configuration files.



Example: Other directory: file://<drive>:\<path>\webmsm\configuration\  
 Web Server: http://<network id or IP address>/

If the **Path:** field is left blank, the location will be set to the default configuration directory.





# **WebMSM Configuration Reference**



# WebMSM Configuration Editor

The WebMSM Configuration Editor provides access, using a simple Windows dialog, to the tools that are used to create, configure and edit the system-level interface components of WebMSM.

It is intended for use by the System Administrator or the person responsible for configuring the user interface. It will not normally be used by the system operator. It is installed as a separate application.

All configuration files must be filed in a single directory. Since all configuration files use the file extension 'cfg', it is recommended that a naming convention is adopted to enable the different configuration types (Hot Spot, Stream, Device) to be identified. A suitable scheme might be to preface the filenames with 'hotspot\_', 'stream\_' or 'device\_', for example, stream\_sv01.cfg.

For large systems with many levels and probes, it is also recommended that a hierarchical system diagram be drawn before using the Configuration Editor. This will aid the user in visualizing the system configuration requirements. Configuration file names can be allocated from the diagram.

---

**NOTE.** *All configuration files associated with a single configuration must be stored in a single directory; this can be local or remote.*

*Configuration files are stored by default in a 'configuration' directory automatically created at installation under the WebMSM Configuration Editor program files directory.*

---

## Opening the WebMSM Configuration Editor

Start WebMSM Configuration Editor either from the desktop shortcut (created during installation):



or the **Start** → **Programs** → **Tektronix WebMSM** → **WebMSM Configuration Editor** option.



The WebMSM Configuration Editor dialog is opened, as shown in Figure 3-1.



Figure 3-1: WebMSM Configuration Editor - Open

### Closing the WebMSM Configuration Editor

Select **Configurations** → **Exit** to close the WebMSM Configuration Editor and all associated windows. Options will be offered by the various editors to save unsaved configuration data.

## Menus and Options

The initial screen provides access to all WebMSM Configuration Editor control options through the Menu Bar.

### Configurations Menu

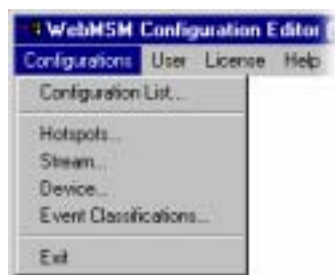


Table 3-1: Configurations Menu Commands

Command	Function
<b>Configuration List...</b>	Opens the Select Configuration dialog.
<b>Hot Spots...</b>	Opens the Hot Spot Configuration Editor.
<b>Stream...</b>	Opens the Stream Configuration Editor.
<b>Device...</b>	Opens the Device Configuration Editor.
<b>Event Classifications...</b>	Opens the Event Classification Editor.
<b>Exit</b>	Closes the WebMSM Configuration editor control panel.

### User Menu



Table 3-2: User Menu Commands

Command	Function
<b>Set Passwords...</b>	Allows passwords to be set.

### License Menu



Table 3-3: License Menu Commands

Command	Function
<b>View Details...</b>	Opens the <b>License Details</b> dialog and allows license details to be viewed.
<b>Update...</b>	Allows license details to be entered and changed.

### Help Menu



Table 3-4: Help Menu Commands

Command	Function
<b>About</b>	Opens the About WebMSM dialog; this gives program details.



## Editing an Existing Configuration File

The procedure for opening an existing configuration file in each editor is similar.

1. Identify the type of configuration file to be opened, i.e. Configuration List, Hotspot, Stream, Device or Event Classifications, and select the appropriate editor from the Configuration menu.



2. In the selected editor, from the File menu, select **File → Open**.
3. A standard File Open dialog will be displayed from which the required configuration file can be selected.
4. The selected configuration file will be opened in the appropriate editor.

If an attempt is made to open a configuration file in the wrong editor, the most likely result is that the fields normally displayed in the editor will be blank.

## Configuration List

The Configuration List is the 'entry point' for the WebMSM to a system configuration. It is the Configuration List that provides the entries in the **Select Configuration** dialog that may be displayed after logging on to WebMSM. Each entry in the Configuration List acts as a pointer to the next level of system configuration.



**Figure 3-2: Select Configuration Dialog**

Only configurations at a higher level that need to be available to a user at WebMSM start up are included in the configuration list.

The Configuration List Editor allows configuration file names to be added, removed and modified to and from the configuration list. Listed files can also be opened and edited by the Configuration List Editor.

To open the Configuration List Editor, select **Configurations** → **Configuration List...**

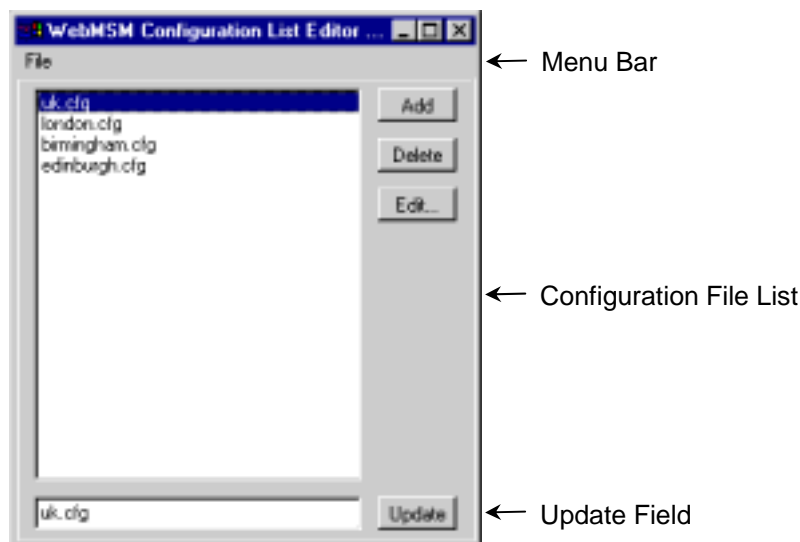


Figure 3-3: WebMSM Configuration List Editor

The Menu Bar contains a **File** menu only. The following options are available in the File menu:



Table 3-5: Configuration List Editor - File Menu Commands

Command	Function
<b>New</b>	Opens new configuration list file.
<b>Open...</b>	Allows an existing configuration list file to be opened.
<b>Save</b>	Saves the current configuration list file.
<b>Save As...</b>	Allows the current configuration list file to be named and saved.
<b>Exit</b>	Closes the Configuration List Editor (and all associated windows).

The buttons operate as follows:

- |                |   |
|----------------|---|
| <b>Add</b>     | Adds a default name (config.cfg) to the configuration list. It is automatically highlighted and displayed in the update field, where it can be renamed and updated. |
| <b>Delete</b>  | Deletes the currently highlighted file name.  |
| <b>Edit...</b> | Opens the currently highlighted file for editing (see below).   |
| <b>Update</b>  | Updates the configuration file list with any changes made in the update field.  |

### Adding a Configuration List File Name

1. Select the **Add** button. The default file name config.cfg is added to the file list.
2. With the file name (config.cfg) highlighted in the file list (and therefore displayed in the update field), rename the file and select the **Update** button.

The file name is updated in the file list. Note also that the file only exists as a name in this list; it is yet to be created (by editing it).

---

**NOTE.** Configuration files must be given their required name in the configuration list before they are edited. If a file is opened in an Editor (**Edit**) and saved under a different filename, the new filename will not appear in the Configuration List until it is specifically added.

---

### Deleting a Configuration List File Name

1. Highlight the file name to be deleted.
2. Select the **Delete** button.

The selected file name is deleted from the file list.

---

**NOTE.** The file referred to is not deleted, only the reference in the configuration list.

---

### Renaming a Configuration List File Entry

1. Highlight the file name to be renamed.
2. In the update field, enter the new file name.
3. Select the **Update** button.

The file name is updated in the file list. The renaming does not affect the source file, only the entry in the file list.

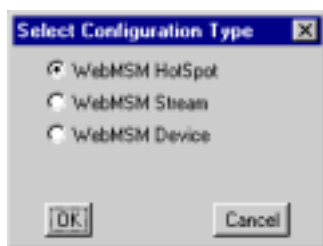
### Editing a Configuration List File

Configuration files named in the file list can be created and/or edited.

The Configuration List file must be saved before it can access existing files named in the list (see below).

1. Highlight the file name to be edited.
2. Select the **Edit...** button.

If the selected configuration file is found (and recognized) in the configuration file directory, the appropriate editor will be opened with the file loaded.



If the selected configuration file is not found in the configuration file directory, the **Select Configuration Type** dialog will be displayed. This allows the user to specify which type of configuration file is to be created. When the selection has been made and the **OK** button is pressed, the appropriate editor will be opened.

The operation of the other Editors is described below.

### Saving the Configuration List

1. From the Menu Bar, select **File → Save**.
2. The name and location of the Configuration List file is dependent on the system configuration. The Configuration List file name is displayed in the editor title bar.

## Hot Spot Editor

The Hot Spot Editor allows Hot Spot configuration files to be created and edited; backgrounds can be added and hot spots can be associated with devices, streams or other hot spot diagrams.

To open the Hot Spot Editor, do one of the following:

- Select **Configurations** → **Hot Spots...** in the main WebMSM Configuration Editor control panel
- Highlight a Hot Spot configuration file in the Configuration List Editor and select the **Edit...** button
- Create a configuration file in the Configuration List Editor, use the **Add** button to create a new entry in the configuration list, rename it if required and when the **Edit...** button is used, select **WebMSM Hot Spot** in the **Select Configuration Type** dialog

A new Hot Spot file will be displayed in the Hot Spot Editor as shown in Figure 3-4:

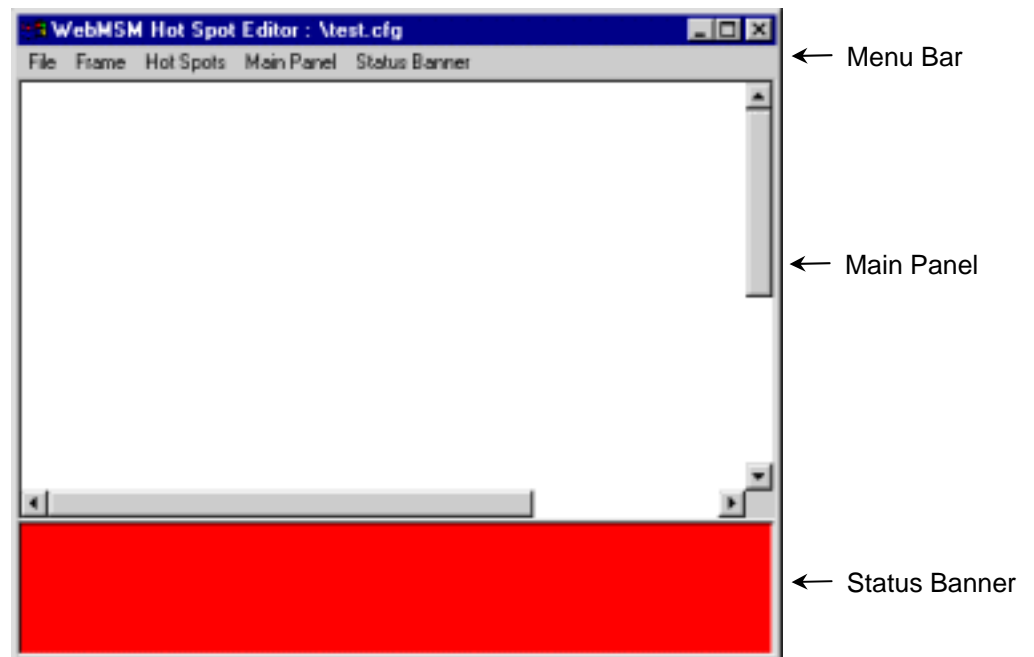


Figure 3-4: Hot Spot Editor

The Hot Spot Editor displays the images that will be visible in the WebMSM Hot Spot view. The main window comprises two panels: the Main Panel and the Status Banner.

The Main Panel will commonly contain a background image of a physical area or a system diagram on which monitoring points are signified by Hot Spot images. The Hot Spots link to Device, Stream or other Hot Spot applications.

The Status Banner is not displayed when the Hot Spot Editor is first opened; select **Status Banner → Display**. The Status Banner provides a means of monitoring a group of devices, for example, the monitoring points from a selected stream.

In the WebMSM application, the background color of each Hot Spot or the Hot Spot image itself in the Main Panel is dependent on the error status of the item that it is linked to. In the Status Banner, the highest error state of any Hot Spot in both panels will be indicated by the overall background color.



## Menu Bar

The Menu Bar provides access to all editor options through the drop-down menus; some options are context sensitive and may be disabled. Also, a number of menu options are available from pop-up menus displayed when the right mouse button is clicked once; these pop-up menu options are also context sensitive.

A check mark (✓) next to a menu option indicates that the feature is currently visible; no check mark means that it is hidden.

## File Menu



Table 3-6: Hot Spot Editor - File Menu Commands

Command	Function
<b>New</b>	Opens a new Hot Spot configuration file.
<b>Open...</b>	Opens an existing Hot Spot configuration file.
<b>Save</b>	Saves the current Hot Spot configuration file.
<b>Save As...</b>	Allows the current Hot Spot configuration file to be named and saved.
<b>Check Against License</b>	Checks the number of probes accessible from the currently selected Hot Spot configuration file (see Checking the Configuration against the Current License, page 3-29).
<b>Exit</b>	Closes the Hot Spot Editor.

Frame Menu



Table 3-7: Hot Spot Editor - Frame Menu Commands

Command	Function
Title...	Allows the name displayed in the title bar of the Hot Spot application to be edited.
Bring to Front On Error	When enabled (✓), indicates that this Hot Spot view should be brought to the front of the displayed views when any of the Hot Spots indicates an error.

Hot Spots



Table 3-8: Hot Spot Editor - Hot Spots Menu Commands

Command	Function
Add to Main Display	Adds a Hot Spot icon to the Main Panel. A sequential hot spot name is allocated; this name can be changed in the Hot Spot Details dialog.
Add to Status Banner	Adds a Hot Spot icon to the Status Banner. A sequential hot spot name is allocated; this name can be changed in the Hot Spot Details dialog.
Delete...	Displays a list dialog from which a Hot Spot can be selected for deletion.

## Main Panel



Table 3-9: Hot Spot Editor - Main Panel Menu Commands

Command	Function
<b>Select Background...</b>	Allows a background to be added to the Main Panel.
<b>Clear Background</b>	Clears the current Main Panel background.
<b>Display Labels</b>	When enabled (✓), displays the Hot Spot labels in the Main Panel.

## Status Banner



Table 3-10: Hot Spot Editor - Status Banner Menu Commands

Command	Function
<b>Display</b>	When enabled (✓), displays the Status Banner.
<b>Display Labels</b>	When enabled (✓), displays the Hot Spot labels in the Status Banner.

## Backgrounds

Backgrounds in the Hot Spot views are simply images; they perform no active function other than to act as a visual reference. If required, a background can be changed without affecting the operation of the Hot Spots. Backgrounds can be in either GIF or JPEG graphics format. Image size is not important except with respect to usability; however, the image cannot be resized in the editor window.



Figure 3-5: Hot Spot Editor - Background

To add a background to the Main Panel, select the **Select Background...** option from the **Main Panel** menu. Use the **Select Background** dialog to locate and select a background.

## Hot Spots

Hot Spots provide links to subsequent layers of a system; they can link to Device, Stream or another Hot Spot application. In the Main Panel Hot Spots can be dragged to any position; each Hot Spot can be specified in one of the following forms:

- The Hot Spot image itself can change color with the error state, in which case an appropriately colored image must be specified for each state.
- The Hot Spot background color can change color for each error state, in which case only a single Hot Spot image need be specified.

Different styles of Hot Spot can be used in a single Hot Spot view.

A set of default Hot Spot images are provided to be used if no other images are specified by the user.

Various properties can be associated with a Hot Spot; these are listed in the description of the Hot Spot properties below.

### Adding a Hot Spot

1. From the **Hot Spots** menu, select the **Add to Main Display** option (or the **Add to Status Banner** option).

A Hot Spot is added to the selected display area.

2. In the Main Panel, drag the Hot Spot to the required location.
3. In either panel, with the cursor over the Hot Spot, select the **Edit...** option from the right-click menu (or double-click the Hot Spot image).
4. Edit the Hot Spot properties (see below).

Hot Spot Properties

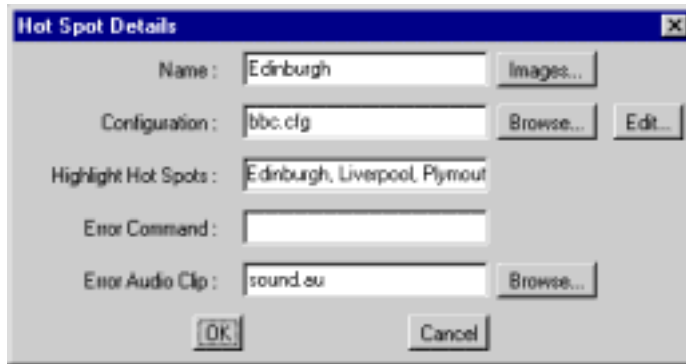


Figure 3-6: Hot Spot Details Dialog

Table 3-11: Hot Spot Details Dialog Commands

Command	Function
<b>Name:*</b>	The name of the Hot Spot; this name is displayed in the Hot Spot label. Up to 11 characters can be used.
<b>Images...</b>	Allows the Hot Spot images (buttons) to be set up (see page 3-19).
<b>Configuration:*</b>	The configuration file that the Hot Spot is linked to; Device, Stream or another Hot Spot. If the named configuration file exists, the <b>Edit...</b> button will open the configuration file in the appropriate editor. If the named configuration file does not exist, the <b>Select Configuration Type</b> dialog will be displayed from which the user can select the configuration type to be created; when <b>OK</b> is selected, the appropriate editor will be opened.
<b>Highlight Hot Spots:</b>	A comma-delimited list of Hot Spot names that will all be highlighted when the user right-clicks any of the named Hot Spots in the WebMSM Hot Spot view.
<b>Error Command:</b>	A command which will be executed on the Client PC if the Hot Spot signals a (red) error state.
<b>Error Audio Clip:</b>	An audio clip file name that will be played if the Hot Spot signals a (red) error state. Audio clips must be provided as .au files in eight-bit, mono $\mu$ -law format.

\* **Name** and **Configuration** are the only required fields.

## Hot Spot Images

(For related information, see also Color Coding, page 2-2.)

This dialog specifies images to be used for Hot Spots. Any GIF or JPEG format image can be used; the maximum recommended image size is 32 pixels x 32 pixels.

The dialog comprises three areas. If the **Button Images** checkbox is selected in the **Hot Spot State Indicator** area, the **Button Images Mode** area is made active. If the **Background Color** checkbox is selected in the **Hot Spot State Indicator** area, the **Background Color Mode** area is made active.

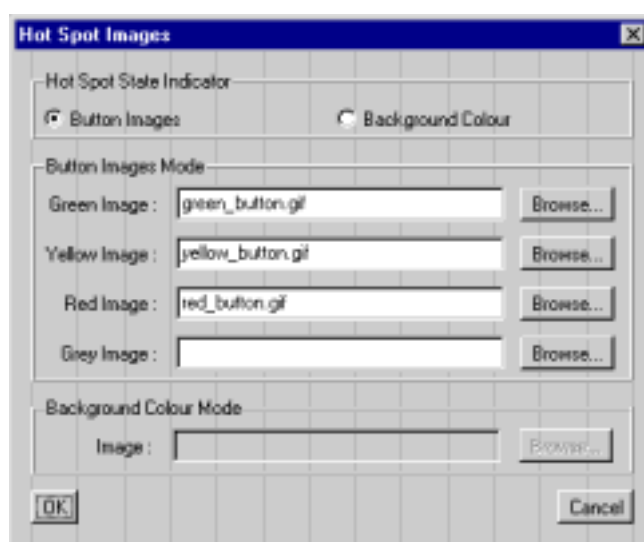


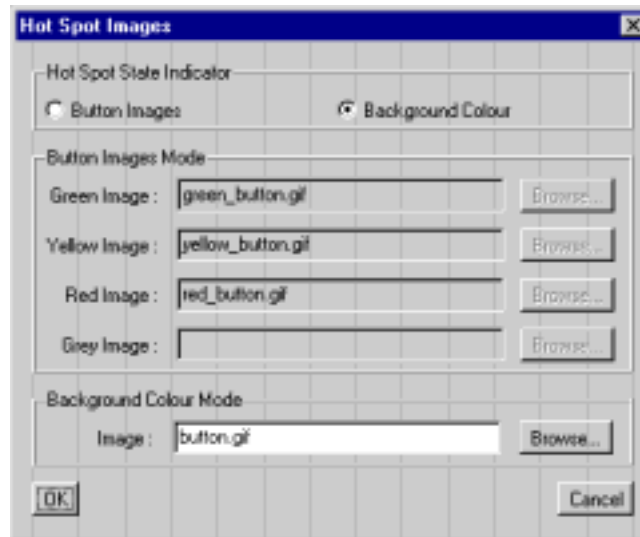
Figure 3-7: Hot Spot Images Dialog

**Selecting Hot Spot State Indicator.** This selection dictates whether the Hot Spot image or the Hot Spot button background indicates the error state of the linked item.

**Selecting Button Images.** With the **Button Images** checkbox selected in the **Hot Spot State Indicator** area, enter or browse and select an image file for each button color. These images will be used to indicate the error state of the associated configuration item.

If images are not specified, default images will be used.

**Selecting Background Color Mode.** With the **Background Color** checkbox selected in the **Hot Spot State Indicator** area, enter or browse and select the image file to be used. The background color of this image will be used to indicate the error state of the associated configuration item.



If no image is specified, a default gray button is used.

### Save Hot Spot View

When editing is complete, the Hot Spot view can be saved using **File → Save**.

When configuration files are saved, the .cfg extension is added automatically, if necessary. Images specified as the Main Panel Background or Hot Spot images are copied to the same directory as the configuration file.



## Stream Editor

The stream configuration file provides a means of identifying a single stream and subsequently opening the Stream view in WebMSM. The stream is identified by its position or number on an RTM device; the RTM device is identified by its IP address or Network identity. An Event Classification file can also be associated with the stream through this dialog.

### Adding a New Stream Configuration File

1. From the WebMSM Configuration Editor control panel, select **Configurations → Stream....**

The Stream Configuration Editor dialog is displayed:



Figure 3-8: Stream Configuration Editor

The File menu comprises the following options:



**Table 3-12: Stream Configuration Editor - File Menu Commands**

Command	Function
<b>New</b>	Opens a new Stream configuration file.
<b>Open...</b>	Opens an existing Stream configuration file to be opened.
<b>Save</b>	Saves the current Stream configuration file.
<b>Save As...</b>	Allows the current Stream configuration file to be named and saved.
<b>Exit</b>	Closes the Stream Configuration Editor.

2. Enter the **Host Name** of the Device; the IP address or the network identity can be used.
3. Enter the **Stream** number on device.
4. Enter the **Event Classification File** name to be associated with the stream (if required).

It is possible to open the named file with the Event Classification Editor using the **Edit...** button - this is described in the following section (see page 3-26).

5. Save the configuration file (**File → Save**), naming it as required.

When configuration files are saved, the .cfg extension is added automatically, if necessary.

To be accessible, the configuration file thus created must be identified in either a configuration list or as a hot spot.

### Editing a Stream Configuration File

1. From the WebMSM Configuration Editor control panel, select **Configurations → Stream....**
2. Select **File → Open...** and select the required Stream Configuration file.
3. Edit the parameters as required.
4. Save the configuration file (**File → Save**).

### Deleting a Stream Configuration File

The appearance of a Stream Configuration File name can be removed from either a configuration list or from a Hot Spot diagram. If the file is to be completely deleted from the system, standard Windows commands must be used.

## Device Editor

The Device configuration file provides a means of locating a single RTM device and subsequently opening the Device view in WebMSM. The device is identified by its IP address or Network identity on the network.

### Adding a New Device Configuration File

1. From the WebMSM Configuration Editor control panel, select **Configurations → Device....**

The Device Configuration Editor dialog is displayed:



Figure 3-9: Device Configuration Editor

The File menu comprises the following options:



Table 3-13: Device Configuration Editor - File Menu Commands

Command	Function
<b>New</b>	Opens a new Device configuration file.
<b>Open...</b>	Opens an existing Device configuration file to be opened.
<b>Save</b>	Saves the current Device configuration file.
<b>Save As...</b>	Allows the current Device configuration file to be named and saved.
<b>Exit</b>	Closes the Device Configuration Editor.

2. Enter the **Host Name:** of the Device; the IP address or the network identity can be used.

3. Save the configuration file (File → Save), naming it as required.

When configuration files are saved, the .cfg extension is added automatically, if necessary.

To be accessible, the configuration file thus created must be identified in either a configuration list or as a hot spot.

#### Editing a Device Configuration File

1. From the WebMSM Configuration Editor control panel, select **Configurations → Device....**
2. Select **File → Open...** and select the required Device Configuration file.
3. Edit the **Host Name:** as required.
4. Save the configuration file (**File → Save**).

#### Deleting a Device Configuration File

The appearance of a Device Configuration File name can be deleted from either a configuration list or removed from a Hot Spot diagram. If the file is to be completely deleted from the system, it must be deleted using standard Windows commands.

## Event Classification Editor

The Event Classification file allows individual tests to be categorized and grouped by the user. Four levels of error classification are available: Critical, Major, Minor and Warning. The classification levels thus allocated are used in the Stream State section of the WebMSM Stream Summary view and the WebMSM Custom view. Tests can be classified in one or more categories.

An Event Classification file is associated with a stream in the Stream Configuration file (see page 3-25).

---

**NOTE.** *Event classifications can be modified directly from the WebMSM user interface. This will only affect the classification of events while the WebMSM application is open. The classifications will revert to those specified in the associated Event Classification file when the application is reopened.*

---

### Adding a New Event Classification File

1. From the WebMSM Configuration Editor control panel, select **Configurations → Event Classifications...**

The Event Classification Editor dialog is displayed:



Figure 3-10: Event Classification Editor

The File menu comprises the following options:



Table 3-14: Event Classification Editor - File Menu Commands

Command	Function
<b>New</b>	Opens a new Event Classification file.
<b>Open...</b>	Opens an existing Event Classification file.
<b>Save</b>	Saves the current Event Classification file.
<b>Save As...</b>	Allows the current Event Classification file to be named and saved.
<b>Exit</b>	Closes the Event Classification Editor.

- Each type of RTM device monitors a unique set of events comprising the DTV Standard events and the associated proprietary events. The events available in the editor are dictated by the selection made in the **Events:** drop-down list.

An Event Classification file must be set up for each device and standard likely to be encountered. The following choices are available from the **Events:** drop-down list:

- **DVB (MTM400)**
- **DVB (SV970)**
- **DVB Proprietary**
- **ATSC (MTM400)**
- **ATSC (AT970)**
- **ATSC Proprietary**

The event classification list displayed in the WebMSM for any given device and standard will comprise a combination of the device list (for example, DVB (MTM400)) and the associated proprietary list (for example, DVB Proprietary).

- Click on the checkboxes to select the event classifications.



4. Select **File → Save** (or **Save As...**) to save the Event Classification file. The file will be saved with the extension '.ecl'.
5. Remember to associate the file with a stream (see page 3-25).

#### Editing an Event Classification File

1. From the WebMSM Configuration Editor control panel, select **Configurations → Event Classifications...**
2. Select **File → Open** and select the required Event Classification file.
3. Edit the checklist as required.
4. Save the configuration file (**File → Save**).

## Checking the Configuration against the Current License

The total number of probes accessible from a configuration level (for example, a Hot Spot view) must not exceed the licensed number of probes. Using **File → Check Against License** in the Hot Spot Editor, the current configuration and the number of probes that it accesses can be checked against the current license. A dialog will show details of the checking process.

It is important that the license is checked using the top level Hot Spot file. Only in this way can all links be checked and hence the number of probes accessible. It also follows that the license should not be checked until the configuration setup is complete. It can, of course, be rechecked if any probes are subsequently added.

For example, with a four probe license and in the system set up below (Figure 3-11), if **Check against License** is applied to one of the second level Hot Spot files (for example, Birmingham), the check will pass because only three probes are accessible through the Birmingham Hot Spot file. However if the same license is applied to the top level Hot Spot diagram (for example, UK), the check will fail because more than four probes (five in this example) are accessible.

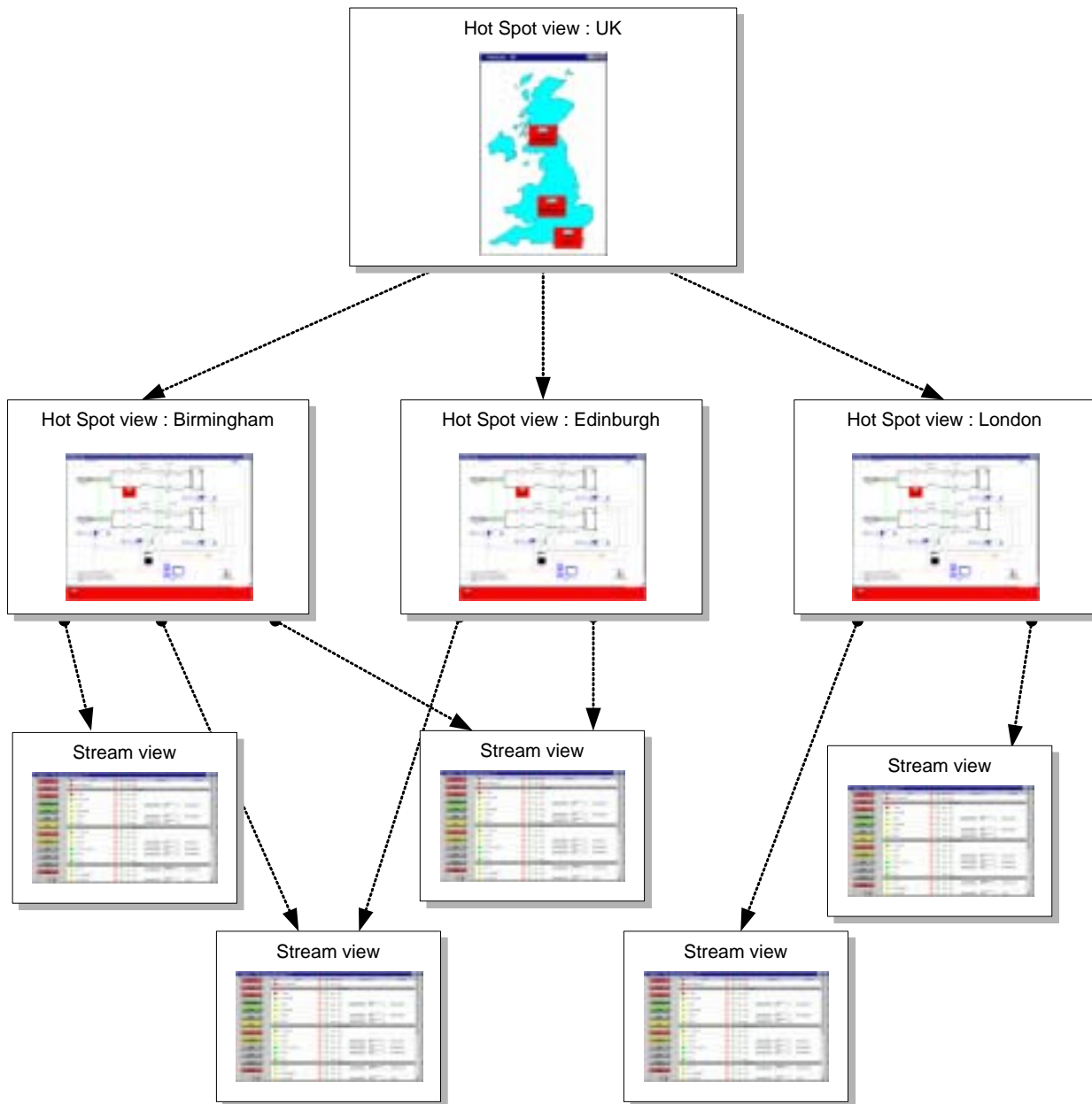


Figure 3-11: License - Example



# Index



# Index

## A

administrator  
passwords, 1-24

## C

configuration files, 1-5  
configuration list  
access, 2-7  
add a file name, 3-8  
delete a file name, 3-8  
open for edit, 3-5  
save, 3-10  
configuration options, 1-7

## D

Device Editor, 3-24  
add configuration file, 3-24  
delete configuration file, 3-25  
edit configuration file, 3-25

## E

Event Classification Editor, 3-26  
add configuration file, 3-27  
edit configuration file, 3-29

## F

first use, 1-29

## H

Hot Spot  
add, 3-17  
Hot Spot Editor, 3-11  
images, 3-19  
select, 3-19  
menus, 3-13  
save, 3-20

hot spot view  
overview, 2-1

## I

installation, 1-11  
administrator, 1-20  
user, 1-13

## L

license  
checking, 3-29  
user, 1-18, 1-23  
licensing, 1-8

## N

network architecture, 1-4

## P

passwords, 1-9  
administrator, 1-24  
save, 1-25  
upload, 1-26  
user, 1-16

PC requirements, 1-11

## R

Remote User Interface, 1-10

## S

security, 1-9  
Stream Editor, 3-21  
add configuration file, 3-21  
delete configuration file, 3-23  
edit configuration file, 3-23  
system configuration, 1-3

## U

- user
  - license, 1-18, 1-23
  - passwords, 1-16
- user interface
  - overview, 2-1

## W

- WebMSM
  - overview, 1-1
- WebMSM CE
  - close, 3-3
  - menus, 3-3
  - start, 3-2
- WebMSM Configuration Editor, *See* WebMSM CE