

User Manual



MLM1000

Multi-Layer Monitoring Software

071-1433-00

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 supercedes that in all previously published material. Specifications and price change privileges reserved.

Tektronix, Inc., 14200 SW Karl Braun Drive, Beaverton, OR 97077

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

Getting Started

Getting Started	1-1
Minimum System Requirements	1-1
Licensing	1-2
Device Types	1-2
Users and Passwords	1-2
Remote User Interface	1-2
Multi-lingual Support	1-3
Launch Modes	1-3
Terms and Definitions	1-4
Installing the Application	1-5
Starting the Application	1-15
Launching the Server	1-15
Launching the Client Locally	1-15
Launching the Client Remotely	1-15
Logging In	1-17
Setting Up the License	1-18
Walking through the Initialization Wizard	1-19

Operating Basics

Operating Basics	2-1
MLM1000 Desktop	2-2
Hotspot Tree	2-3
Hotspot Preview	2-3
Menu Bar	2-4
Toolbar	2-8
Dialog Boxes or Windows	2-9

Using the MLM1000

Managing the Maps	3-1
Adding a Map	3-1
Modifying Map Properties	3-2
Removing a Map	3-3
Renaming a Map	3-3
Locking or Unlocking a Map	3-3
Monitoring or Stopping a Map from Being Monitored	3-4
Setting the Map Background	3-4
Setting the Map Icon	3-5
Moving a Map to Another Map	3-5
Moving a Map Within the Map Window	3-5
Managing the Devices	3-7
Adding a Device Manually	3-7
Adding a Discovered Device to a Map	3-8
Moving Devices to Another Map	3-8

Moving Devices Within the Map Window	3-9
Monitoring or Stopping a Device From Being Monitored	3-9
Changing the Device Icon	3-9
Managing Default Icons for All Devices	3-9
Removing a Device from the Map	3-10
Removing Devices from the New Devices Window	3-11
Launching Device RUI	3-11
Discovering the Devices	3-13
Foreground Scanning	3-13
Background Scanning	3-14
Adding an IP Address Range to the Device Discovery Settings	3-15
Removing an IP Address Range from the Device Discovery Settings	3-15
Scanning for a Device in an IP Address Range	3-15
Scanning for a Specific Device Type	3-16
Scanning for Devices with Community Strings	3-16
Setting Up Auto Discovery	3-18
Saving Device Discovery Settings	3-19
Managing the User Accounts	3-21
Adding a User Account	3-21
Modifying a User Profile	3-23
Changing Your Password	3-24
Changing the Password of Another User	3-24
Setting the Expiration Date	3-25
Changing the Role of a User	3-25
Removing a User	3-25
Removing an Administrator	3-26
Managing the Event Logs	3-27
Exporting an Event Log	3-27
Removing Event Logs	3-28
Setting the Maximum Event Log Size	3-28
Managing the Application User Interface	3-31
Managing the Alarms	3-33
Acknowledging Alarms	3-33
Setting the Map Window to Pop Up on an Alarm	3-34
Setting Hotspot Tree to Expand on Alarm	3-34
Setting a Beep on Alarm for a Specific Device	3-35
Setting an Action on Alarm for a Specific Device	3-36
Setting an Action on Alarm Recovery for a Specific Device	3-36
Changing the Alarm Indicator Sound	3-36
Viewing an Alarm Occurrence Graph	3-37
Setting the Legend Properties for the Alarm Occurrence Graph	3-37
Setting Up Plot Properties for Alarm Occurrence Graph	3-40
Setting Up Other Properties for Alarm Occurrence Graph	3-44
Saving an Alarm Occurrence Graph	3-45
Printing an Alarm Occurrence Graph	3-45
Zooming In and Out	3-46
Viewing an Alarm Distribution Graph	3-46

Setting the Legend Properties for the Alarm Distribution Graph	3-47
Setting the Plot Properties for the Alarm Distribution Graph	3-48
Setting Other Properties for the Alarm Distribution Graph	3-50
Saving an Alarm Distribution Graph	3-51
Printing an Alarm Distribution Graph	3-52
Setting the Options	3-53
Configuring Server Options	3-53
Configuring Alarm Options	3-55
Configuring Display Options	3-56
Resetting the Default Options	3-57
Generating the Reports	3-59
Saving Reports	3-60
Exporting Reports	3-62
Changing the Page Setup	3-65
Printing Reports	3-66
Navigating the Report	3-66
Zooming In or Out	3-66

Appendices

Appendix A: Error Messages	A-1
Appendix B: Device Types	B-1
About the MTM400	B-1
About the RFM210	B-2
About the WFM700	B-3
About the WVR6XX	B-4
Appendix C: Troubleshooting	C-1
Appendix D: Shortcut Keys and Default Values	D-1

Index

List of Figures

Figure 1-1: Splash Screen of InstallAnywhere Wizard	1-5
Figure 1-2: InstallAnywhere Wizard Introduction window	1-6
Figure 1-3: InstallAnywhere Wizard License Agreement window	1-7
Figure 1-4: InstallAnywhere Wizard Choose Install Folder window	1-8
Figure 1-5: InstallAnywhere Wizard Choose Install Set window ..	1-9
Figure 1-6: InstallAnywhere Wizard Choose Java Virtual Machine window	1-10
Figure 1-7: InstallAnywhere Wizard Choose Shortcut Folder window	1-11
Figure 1-8: InstallAnywhere Wizard Pre-installation Summary window	1-12
Figure 1-9: MLM1000 web page	1-16
Figure 1-10: Login dialog box	1-17
Figure 1-11: Initialization Wizard User Management window	1-19
Figure 1-12: Initialization Wizard License Management window ..	1-20
Figure 1-13: Initialization Wizard Discovery Settings window	1-21
Figure 2-1: Application window	2-1
Figure 2-2: MLM1000 desktop	2-2
Figure 2-3: Hotspot tree	2-3
Figure 2-4: Map preview	2-3
Figure 2-5: Device preview	2-4
Figure 2-6: Toolbar	2-8
Figure 2-7: Login dialog box	2-9
Figure 2-8: Add Map dialog box	2-10
Figure 2-9: Add Device dialog box	2-11
Figure 2-10: Search dialog box	2-12
Figure 2-11: Alarm Distribution Graph window	2-13
Figure 2-12: Alarm Occurrence Graph window	2-14
Figure 2-13: Map Properties dialog box	2-15
Figure 2-14: Device Properties dialog box	2-16
Figure 2-15: Event Viewer window	2-17
Figure 2-16: Discovery Settings window	2-18
Figure 2-17: New Devices window	2-19

Figure 2-18: Change Password dialog box	2-20
Figure 2-19: User Management window	2-20
Figure 2-20: License Management window	2-21
Figure 2-21: Icon Management window	2-22
Figure 3-1: Add Mapdialog box	3-1
Figure 3-2: Map Properties dialog box	3-2
Figure 3-3: Add Device dialog box	3-7
Figure 3-4: Icon Management window	3-10
Figure 3-5: Server Settings tab of Options dialog box	3-18
Figure 3-6: User Management window	3-21
Figure 3-7: User Profile dialog box	3-22
Figure 3-8: Choose a date dialog box	3-23
Figure 3-9: Change Password dialog box	3-24
Figure 3-10: Event Viewer window	3-27
Figure 3-11: Server Settings tab of Options dialog box	3-29
Figure 3-12: Alarm Settings of Options dialog box	3-34
Figure 3-13: Device Properties dialog box	3-35
Figure 3-14: Alarm Occurrence Graph window	3-37
Figure 3-15: Legend tab of Alarm Occurrence graph	3-38
Figure 3-16: Pen/Stroke Selection dialog box	3-39
Figure 3-17: Outline Color dialog box	3-39
Figure 3-18: Plot properties tab of Alarm Occurrence graph	3-41
Figure 3-19: Edit Insets dialog box	3-42
Figure 3-20: Other tab of Alarm Occurrence graph	3-44
Figure 3-21: Alarm Distribution Graph window	3-47
Figure 3-22: Legend tab of Chart Properties dialog box	3-48
Figure 3-23: Plot properties tab of Chart Properties dialog box	3-49
Figure 3-24: Other tab of Chart Properties dialog box	3-51
Figure 3-25: Server Settings tab of Options dialog box	3-53
Figure 3-26: Alarm Settings tab of Options dialog box	3-55
Figure 3-27: Display tab of Options dialog box	3-56
Figure 3-28: Report Preview	3-59
Figure 3-29: Saving Report into PDF file dialog box	3-60
Figure 3-30: Export Report into a Plain Text File dialog box	3-62
Figure 3-31: Export Report into an Excel File dialog box	3-63
Figure 3-32: Export Report into an HTML File dialog box	3-63
Figure 3-33: Export Report into a CSV File dialog box	3-64
Figure 3-34: Page Setup dialog box	3-65

List of Tables

Table 1-1: Minimum system requirements	1-1
Table 2-1: Hotspot Preview interface elements	2-4
Table 2-2: Dynamic menus	2-5
Table 2-3: Hotspots menu	2-5
Table 2-4: View menu	2-5
Table 2-5: Tools menu	2-6
Table 2-6: New Devices menu	2-6
Table 2-7: Event Viewer menu	2-7
Table 2-8: Window menu	2-7
Table 2-9: Help menu	2-7
Table 2-10: Toolbar buttons	2-8
Table 2-11: Mapbackground and icon	2-11
Table 3-1: Color representation	3-33
Table A-1: Error messages	A-1
Table C-1: Troubleshooting	C-1
Table D-1: Shortcut keys	D-1
Table D-2: Default values	D-2



Getting Started

Getting Started

The Multi-layer Monitoring Software remotely monitors the video monitoring equipment in the network.

You can use this software with Tektronix products that monitor video signals at the Baseband, MPEG and RF layers. Using this software, throughout the network you can:

- Monitor Tektronix video devices
- Launch the Remote User Interface (RUI) for devices that you want to configure
- Generate consolidated reports of monitored devices and save historical information

Minimum System Requirements

Table 1-1 lists the minimum system requirements for the MLM1000 software:

Table 1-1: Minimum system requirements

System	Minimum Requirements
Windows 2000 Service Pack 4 and above	1.5 GHz Intel Pentium IV Processor 512 MB RAM 100 MB Free Disk Space*
OR	Ethernet - 10/100-baseT; RJ45
Windows XP Service Pack 1 and above	Microsoft Internet Explorer, version 5.5 minimum/Netscape 4.7; Java Plugin (from Sun Microsystems) version 1.4.2 and higher 8x CD-ROM drive Sound card 1024x768 pixel video monitor with 65535 colors

* Ensure that you have additional disk space for Event logs.

Licensing

The MLM1000 software uses a licensing scheme to control the number and devices that can be accessed and controlled.

An Option Key is supplied with the application. The option key is of the form 'nnnnn-nnnnn-nnnnn-nnnnn', where 'n' is any alphanumeric character; the Option Key is case-sensitive.

The License information is available in a white envelope containing the important documents that are shipped along with the product. Enter the License key while installing the MLM1000 software.

Device Types

The MLM1000 software supports the following Tektronix products:

- WVR6xx
- WFM700
- MTM400
- RFM210

Users and Passwords

Access to the MLM1000 software is controlled by a combination of user names and associated passwords. The two types of users supported are:

- A **User** who can monitor devices in the network
- An **Administrator** who can set up and configure devices, add users, and manage the MLM1000 system. Only an Administrator can allocate a password to the user.

Remote User Interface

You can launch the Remote User Interface (RUI) of a specific device using the MLM1000 to manage the device at any time.

Multi-lingual Support

Using the Options dialog box, you can specify the language in which the MLM1000 application will launch at the next login.

The default MLM1000 language is English; the login dialog box is always in English, no matter which language you specify. All data inputs are restricted to English.

Launch Modes

To launch the MLM1000 software, you need to specify the MLM1000 Server URL (Ex. `http://<MLM1000 Server>:<HTTP port number>`) in the browser.

You can launch the MLM1000 software in two modes:

- Applet
- Webstart

In the Applet mode, you can launch or run the MLM1000 software without installing it on your machine.

In the Webstart mode, the application is initially downloaded and installed on your machine. The next time you login you can launch the application using the icon added to the desktop.

In subsequent launches, the application is installed only when the version is old.

In the Webstart mode, you should enter the MLM1000 Server URL during login using the following format:

`<MLM1000 Server>:<HTTP port number>`

The default HTTP port number is **9999**.

You can use the Options dialog box to change the default HTTP port number.

Terms and Definitions

Map. The Map is the way in which devices are organized hierarchically. A map contains a set of devices and maps.

Device. The Devices are the Tektronix Video Devices that will be monitored by the MLM1000 software.

Hotspot. The Hotspot is the entity which shows its states by means of color changes. Both map and device are referred to as hotspots.

Hotspot Tree. The Hotspot Tree is the tree representation of hotspots.

Hotspot Panel. The Hotspot Panel is the panel where hotspots in a map are displayed.

Monitored mode. A hotspot is said to be in Monitored mode if it is getting monitored actively by the MLM1000 software.

Unmonitored mode. A hotspot is said to be in Unmonitored mode if it is not getting monitored by the MLM1000 software.

Locked Placement. If you lock the placement of a map, any hotspots in that map cannot be modified and you cannot add or remove the hotspots to or from that map. Also you cannot move that map or the hotspots inside the map.

Unlocked Placement. You can do all the operations on a hotspot in a map if the map placement is unlocked.

Installing the Application

This section describes how to install the application using the InstallAnywhere Wizard. The installation program **install.exe** installs the MLM1000 Local Client and MLM1000 Server. Do the following to install the MLM1000 Server:

1. Insert the MLM1000 CD-ROM into the CD-ROM drive.
2. If the installation program does not automatically start, find the **install.exe** on the CD-ROM and double-click it. The InstallAnywhere wizard displays the Splash Screen as shown by the next figure.



Figure 1-1: Splash Screen of InstallAnywhere Wizard

3. Follow the instructions given by the InstallAnywhere wizard.

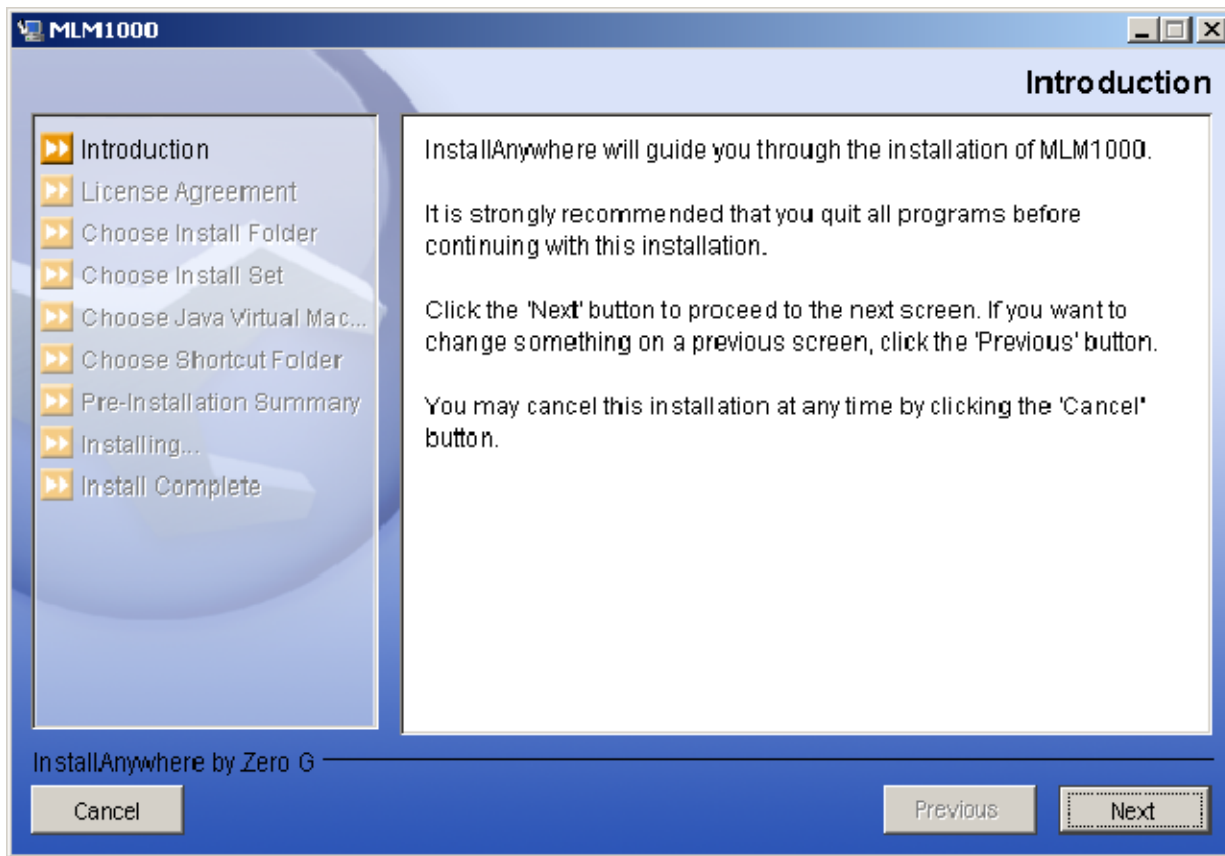


Figure 1-2: InstallAnywhere Wizard Introduction window

4. The installation is a seven-step procedure: Introduction, License Agreement, Choose Install Folder, Choose Install Set, Choose Java Virtual Machine, Choose Shortcut Folder, and Preinstallation Summary.
 - Click **Next** to continue and navigate through the InstallAnywhere wizard.
 - Click **Previous** if you want to change the settings in the previous window.

5. In the Introduction window, click **Next** to display License Agreement window.

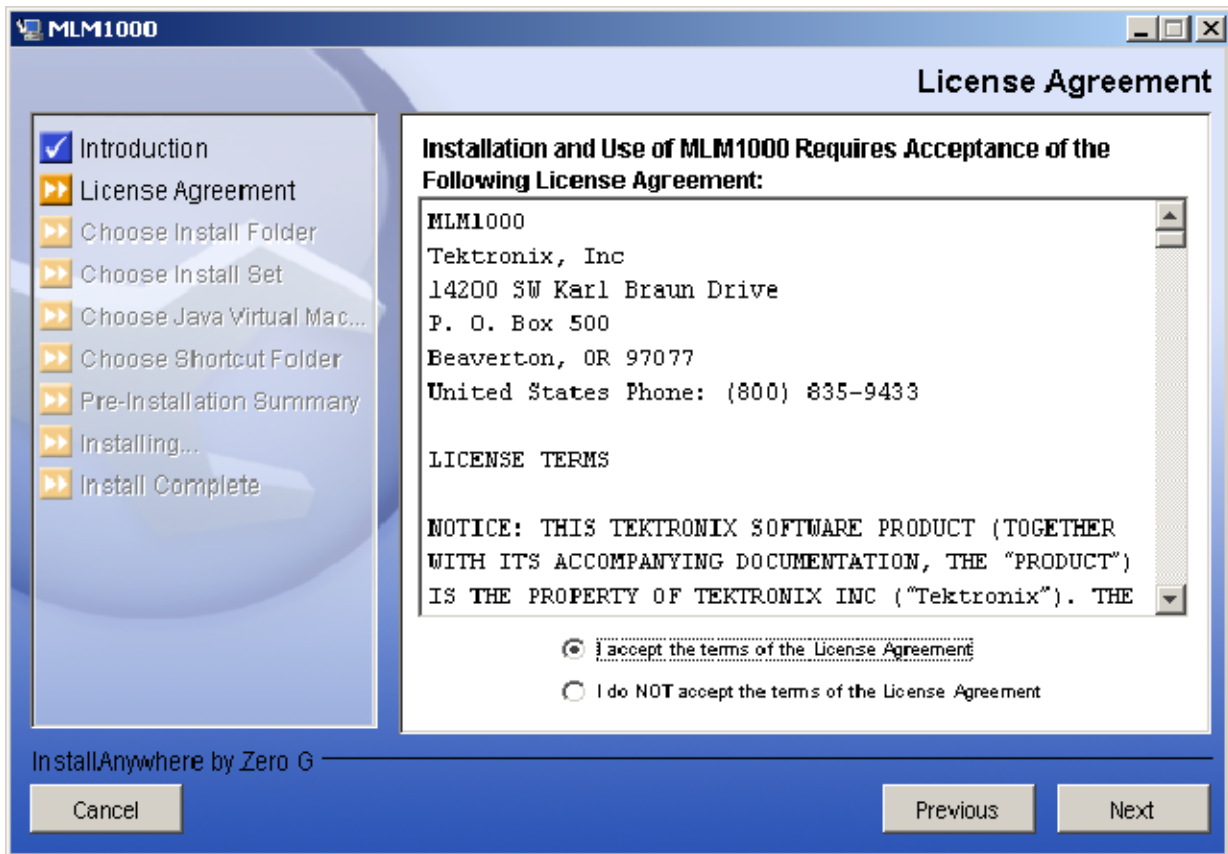


Figure 1-3: InstallAnywhere Wizard License Agreement window

6. In the License Agreement window, do the following:
 - Read the License Agreement carefully.
 - Select the **I accept the terms of the License agreement** option to continue.

7. If you have selected the **I accept the terms of the License agreement** option, then click **Next** to display Choose Install Folder window.

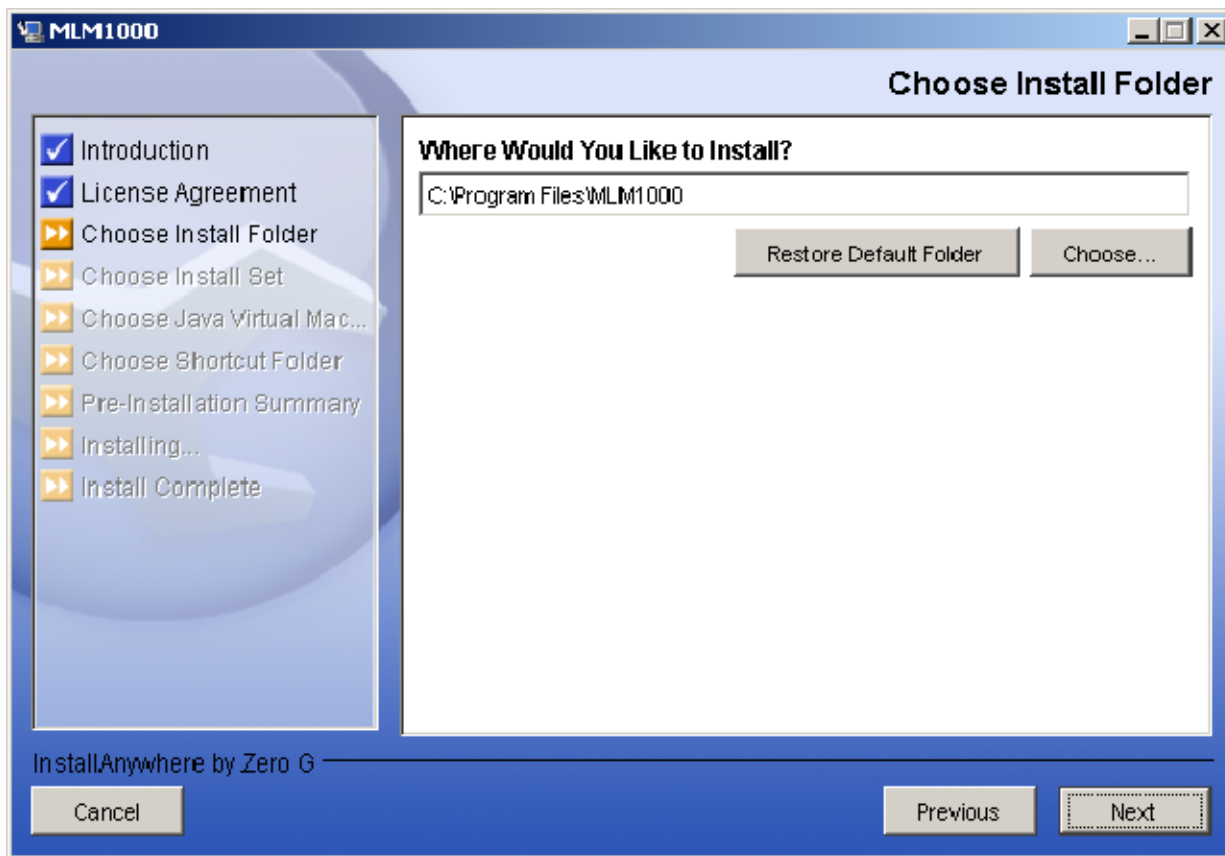


Figure 1-4: InstallAnywhere Wizard Choose Install Folder window

8. In the Choose Install Folder window, do one of the following:
 - To change the location where you would like to install MLM1000, either enter the path in the field or click **Choose** and browse to the location.
 - To restore the default location, click **Restore Default Folder**.
9. Click **Next** to display the Choose Install Set window.

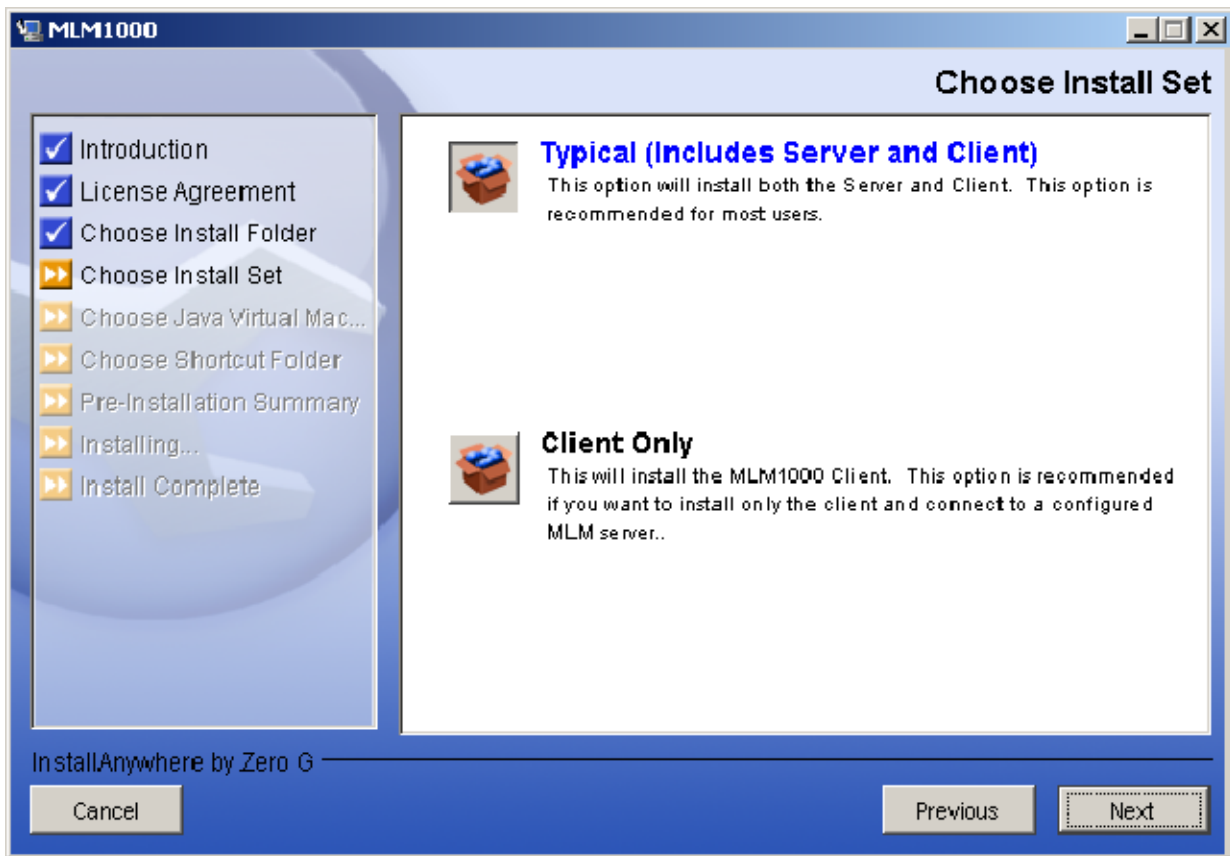


Figure 1-5: InstallAnywhere Wizard Choose Install Set window

10. In the Choose Install Set window, do one of the following:
 - To install both the server and the client, click **Typical**.
 - To install only the client, click **Client Only**.

11. Click **Next** to display the Choose Java Virtual Machine window.

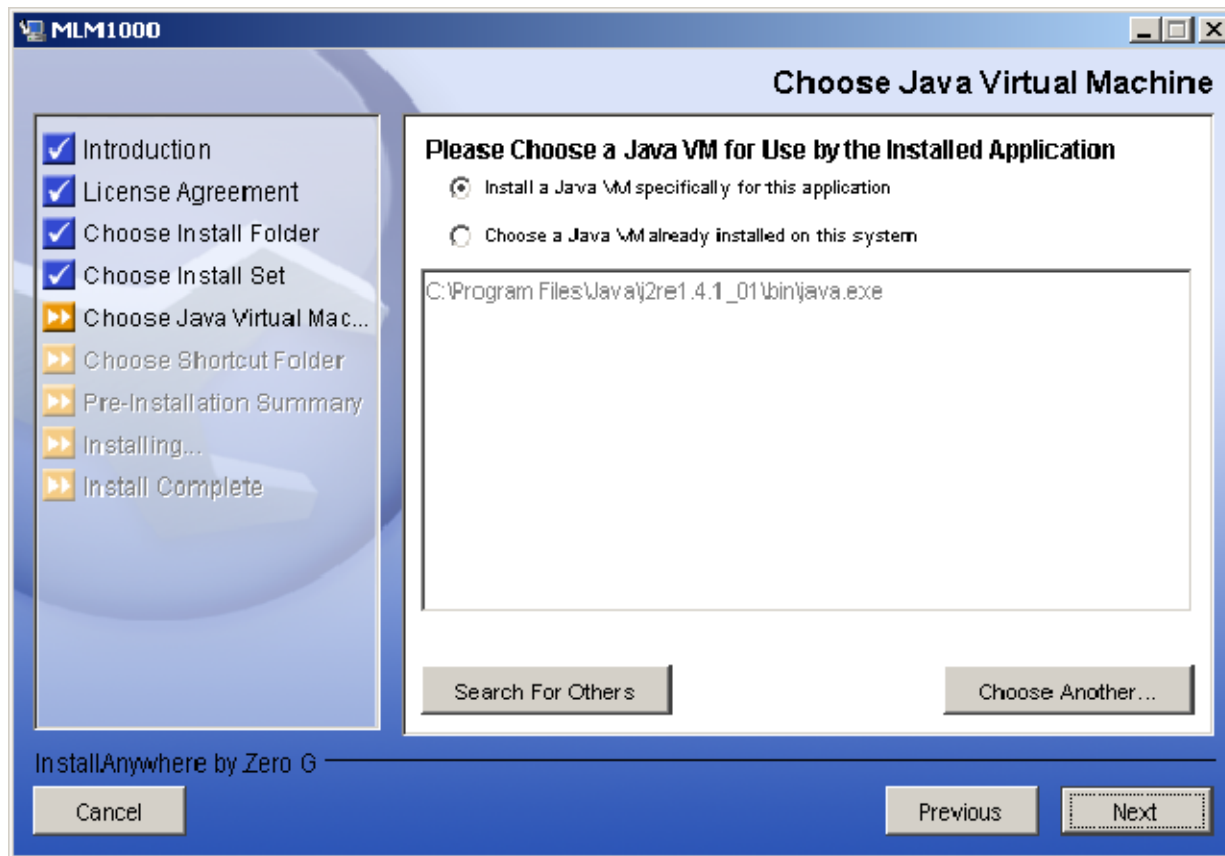


Figure 1-6: InstallAnywhere Wizard Choose Java Virtual Machine window

12. The Choose Java Virtual Machine window allows you to install the Java Virtual Machine or choose the location where the Java Virtual Machine is installed. In the Java Virtual Machine window, do the following:

- Select **Install a Java VM specifically for this application** option to install the Java Virtual Machine.

or

- Select **Choose a Java VM already installed on this system** option to select the Java Virtual Machine already installed on your system. Do one of the following:
 - To find other Java Virtual Machine installations, click **Search for Others**. The InstallAnywhere wizard searches the hard disk of your computer for other Java Virtual Machine installations and lists the

locations. You can select the preferred Java Virtual Machine file and click **Next**.

- To manually find a Java Virtual Machine, click **Choose Another** and browse for the location where the Java Virtual Machine is installed.
- Then, click **Next**.

13. Click **Next** to display the Choose Shortcut Folder window.

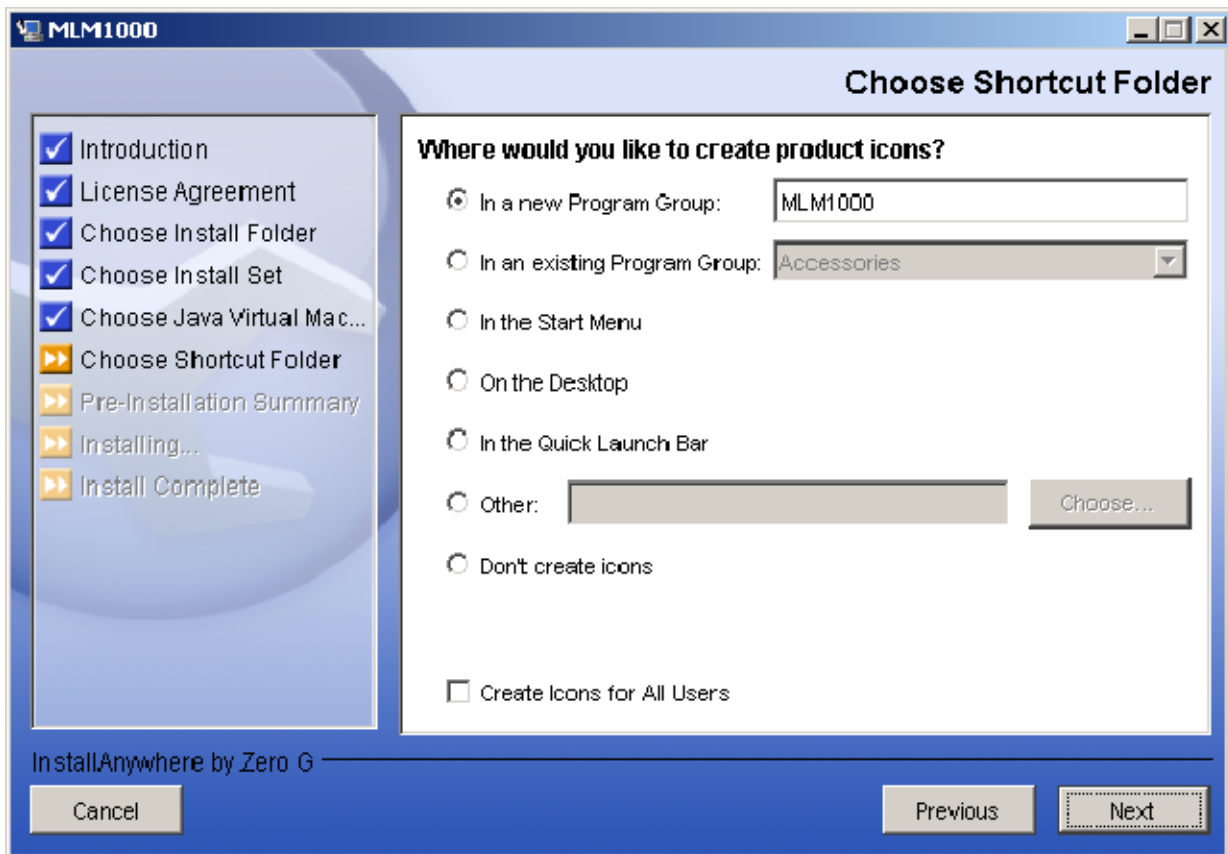


Figure 1-7: InstallAnywhere Wizard Choose Shortcut Folder window

14. To select shortcut folder where you would like to create the product icons, do one of the following:
- Select the **In a new Program group** option. You can either change or retain the program group name in the adjacent field.
 - Select the **In an existing Program group** option and select the program group name in the adjacent drop-down list.

- Select the **In the Start menu** option to create the product icons in the Start menu.
 - Select the **On the Desktop** option to create the product icons on the Desktop.
 - Select the **Other** option and click **Choose** to browse for the location where you want to create the icons.
 - Select the **Don't Create icons** option to not create the icons.
15. Select the **Create Icons for all users** check box to create the icons for the all the users of the computer.
16. Click **Next** to display the Pre-installation Summary window.

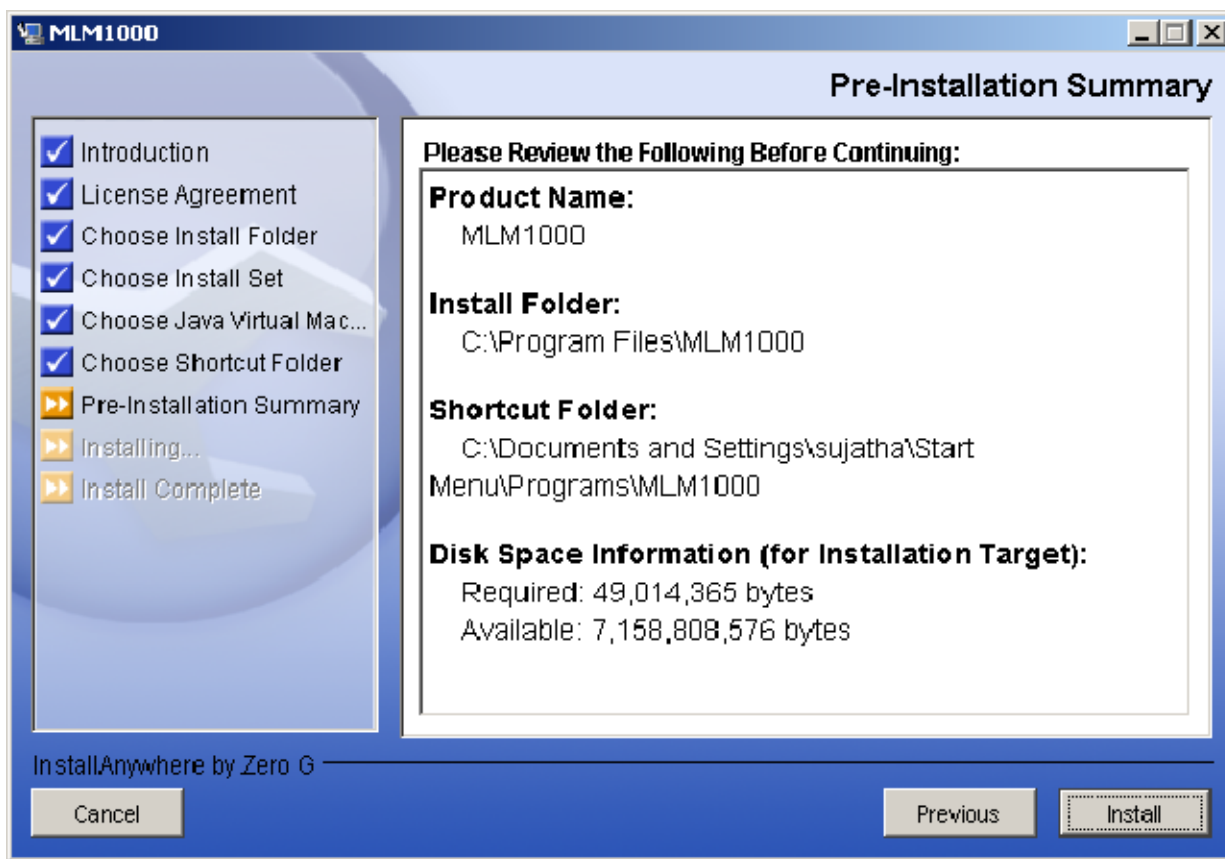


Figure 1-8: InstallAnywhere Wizard Pre-installation Summary window

17. Before continuing the installation, review the Product Name, Install Folder, Shortcut Folder, and Disk Space Information (for Installation Target) listed in Pre-installation Summary window.

- If the information is not correct, click **Previous** and change the settings.
 - If the information is correct, continue installation.
- 18.** Click **Install** to continue installation. The InstallAnywhere wizard will display a progress bar while installing the software. When the software installation is completed, the wizard will display the Install Complete window.
 - 19.** Click **Done** to quit the InstallAnywhere wizard.

Starting the Application

This section describes how to setup the Server, launch the application, and login to the MLM1000 monitoring system.

Launching the Server

Ensure that you launch the MLM1000 Server on a system that is not on a DHCP network.

To launch the Server, click **Start > Programs > MLM1000 > MLM1000 Server**.

NOTE. *The MLM1000 Server does not display a graphic user interface. You can run the MLM1000 Local Client in the system where the server is running to make any changes to the Server settings.*

Launching the Client Locally

To launch the Client locally, click **Start > Programs > MLM1000 > MLM1000 Client**.

Launching the Client Remotely

Launching the Client for the First Time

To launch the Client for the first time:

1. Open any Internet Browser.
2. Enter the MLM1000 Server URL (For example: `http://<MLM1000 Server>:< HTTP port number>`) in the browser address line, where
 - MLM1000 Server is the name or IP address of the system in which the MLM1000 Server is running
 - port number is 9999, and is the default port number

The Internet browser displays the MLM1000 web page, where you can select the launch modes.



Figure 1-9: MLM1000 web page

- Select the Applet mode, if you want to run MLM1000 in Applet mode.
or
- Select the Webstart Mode, if you want to install the Client in the system and run the MLM1000 software. In Webstart mode, every time you log in, the MLM1000 checks the Server for the updated version and installs if any.

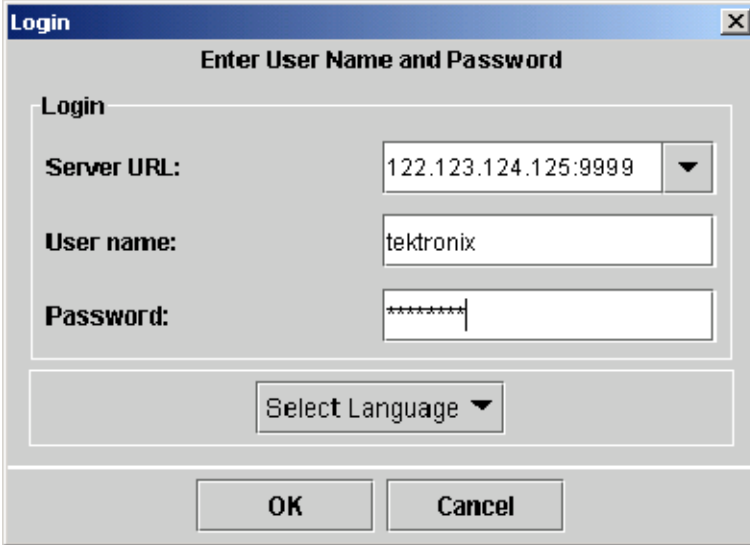
Launching the Client the Next Time

The next time you want to launch the Client:

1. In the Applet mode, enter the MLM1000 Server URL (Ex. `http://<MLM1000 Server>:<HTTP port number>`) in the Internet browser and press **Enter**.
2. In the Webstart mode, click on the icon that was added to your desktop the last time you logged into the Client in the Webstart mode.

Logging In

The Login dialog box varies depending on the mode in which you launch the application. In the Webstart mode, the Login dialog box displays a **Server URL** field in addition to Username field, Password field, and a Select Language drop-down list.



The screenshot shows a standard Windows-style dialog box with a title bar that says "Login" and a close button (X). The main area is titled "Enter User Name and Password". It contains three labeled input fields: "Server URL:" with the text "122.123.124.125:9999" and a small downward arrow; "User name:" with the text "tektronix"; and "Password:" with masked characters "*****". Below these fields is a "Select Language" drop-down menu. At the bottom of the dialog are two buttons: "OK" and "Cancel".

Figure 1-10: Login dialog box

1. In the **Server URL** field, enter the MLM1000 Server URL (For example: <MLM1000Server>:<port number>)
2. In the **Username** field, enter your user name.
3. In the **Password** field, enter your password.
4. In the **Select Language** drop-down list, select the language in which you want to launch the application.
If you do not select the language in the drop-down list, the MLM1000 software is launched in the language that you previously launched the MLM1000 software.
5. Select **OK** to login.

Setting Up the License

To use the MLM1000 software, you need to set up the license.

If you have not set up the license while the Initialization Wizard walks you through the preliminary setup and configuration of the MLM1000 software, then set up the license now.

NOTE. *The Initialization Wizard appears only if you are logging in for the first time.*

Tektronix provides you with a unique license number to entitle you with the number of devices you can control using the MLM1000 software.

To set up the license:

1. Select **Tools > License Management**. The License Management window appears.
2. In the Option Key field, enter the license number provided by Tektronix. The license information is available in a white envelope containing the important documents that are shipped along with the product.

Option key is 32 characters and is an alphanumeric string with permitted intermediate hyphen characters.

3. Click **Verify** and the MLM1000 software checks the validity of the license number and displays information on how many devices are supported.
4. Click **OK**.

Walking through the Initialization Wizard

The Initialization Wizard walks you through the preliminary setup and configuration of the MLM1000 software. The Initialization Wizard appears only if you are logging in for the first time.

The Initialization Wizard is a five-step procedure: Welcome, User Management, License Management, Discovery Settings, and Finish.

To navigate through the Initialization Wizard, do the following:

- Click **Next** to continue Initialization Wizard.
- Click **Back** to the previous window.

The Initialization Wizard will appear with the Welcome pane displayed.

1. In the Welcome pane of the Initialization Wizard, read the description of the Initialization Wizard and click **Next**. The Initialization wizard displays the User Management pane and User Management window.

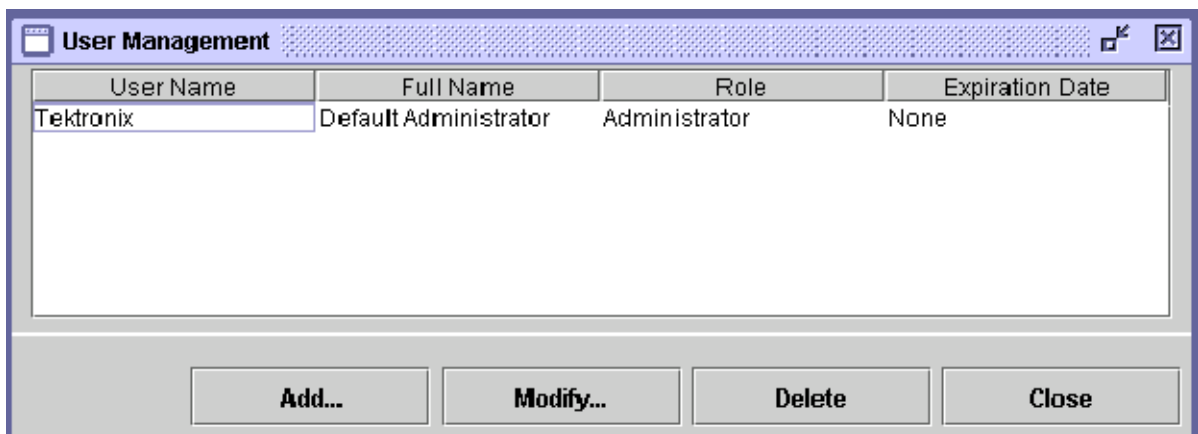


Figure 1-11: Initialization Wizard User Management window

2. In the User Management window, click **Add** to add your profile. The User Profile dialog box appears.
3. In the User Profile dialog box, enter the user name, password, role, full name, email ID, contact number, and expiration date. Then click **OK**.

4. In the User Management pane of the Initialization Wizard, click **Next** to display the License Management pane and License Management window.

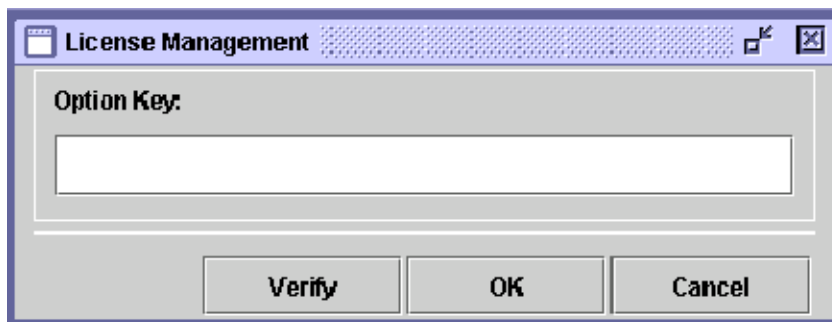


Figure 1-12: Initialization Wizard License Management window

5. In the License Management window, enter the Option Key to control the number and types of devices that can be accessed and controlled in the MLM1000 software.

NOTE. *If you do not enter the Option Key in the License Management window, the Initialization Wizard appears the next time you login. You cannot add or modify hotspots without entering the Option Key.*

6. In the License Management pane of the Initialization Wizard, click **Next** to display the Discovery Settings pane and the Discovery Settings window.

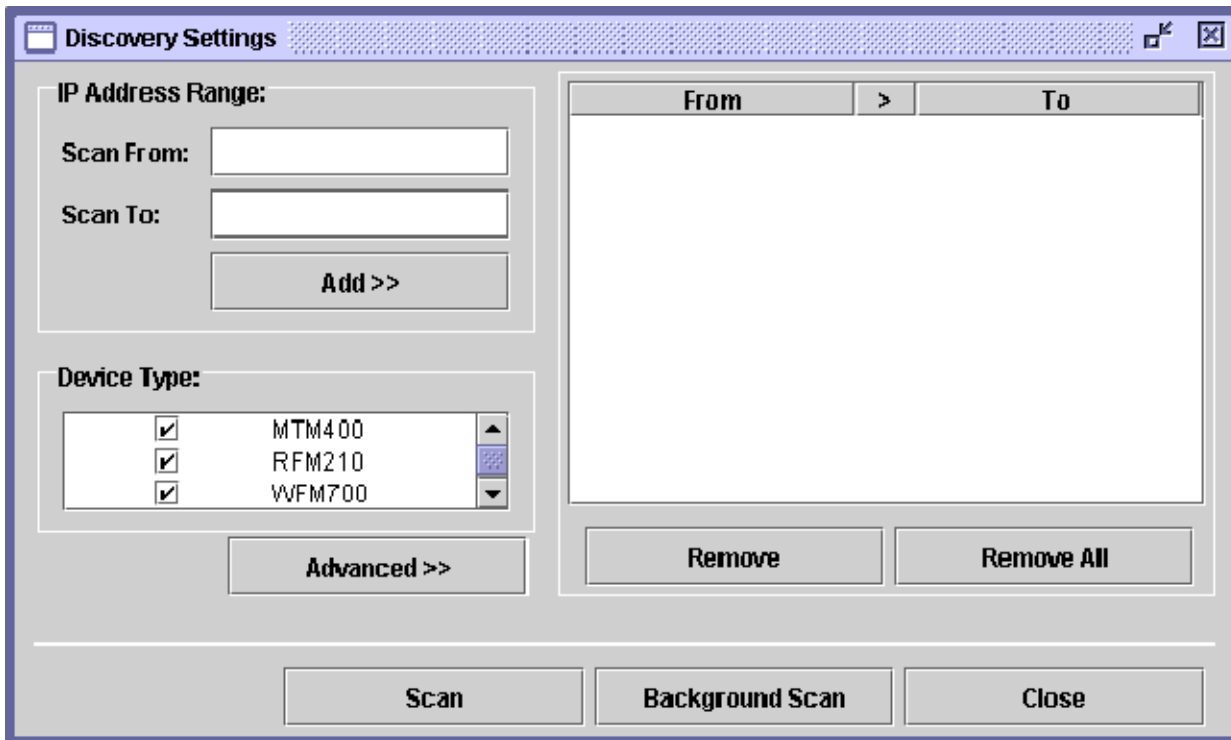


Figure 1-13: Initialization Wizard Discovery Settings window

7. In the Discovery Settings window, enter the specific ranges within which you want search for a selected device type.
After you login, the MLM1000 software automatically searches for devices within the specified range.
If you do not enter the IP address ranges, then the MLM1000 software does not automatically search for devices.
8. In the Discovery Settings pane of the Initialization Wizard, click **Next** to display the Finish pane of the Initialization Wizard.
9. The preliminary setup of the MLM1000 software is now complete. Click **Finish** to start the application.



Operating Basics

Operating Basics

This section provides an overview of the monitoring software and features of the MLM1000.

The application window contains the MLM1000 Desktop, Hotspot Tree, Hotspot Preview, Menu bar, Tool bar, Hotspot Panel, and Dialog Boxes.

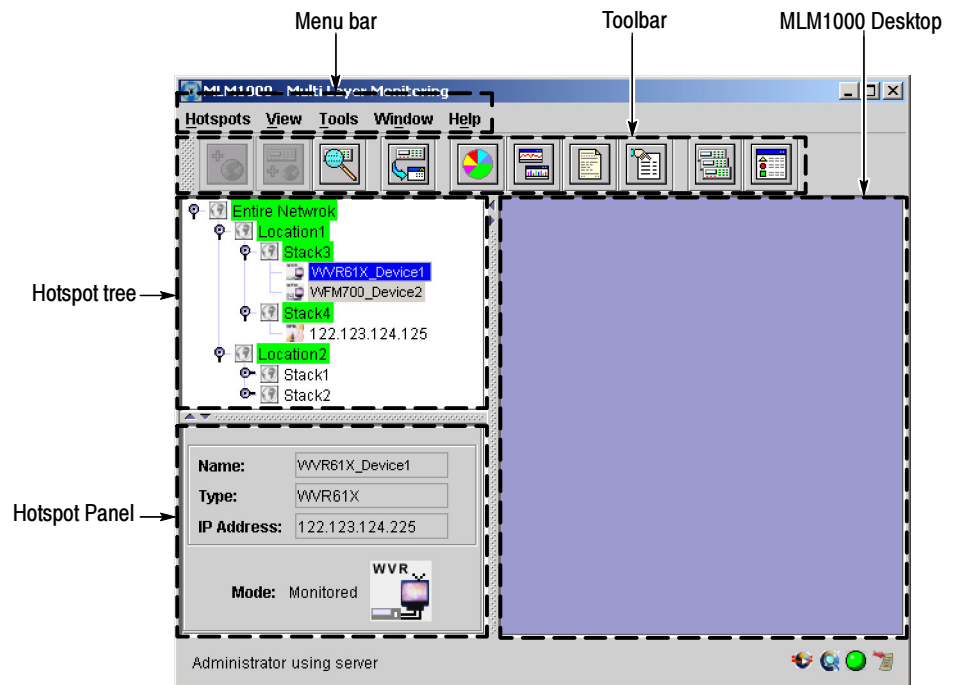


Figure 2- 1: Application window

MLM1000 Desktop

The right panel of the application that displays the dialog boxes, windows, and hotspot panels is MLM1000 Desktop. When you start the application, the MLM1000 Desktop is empty. Figure 2-2 shows the MLM1000 Desktop with windows open.

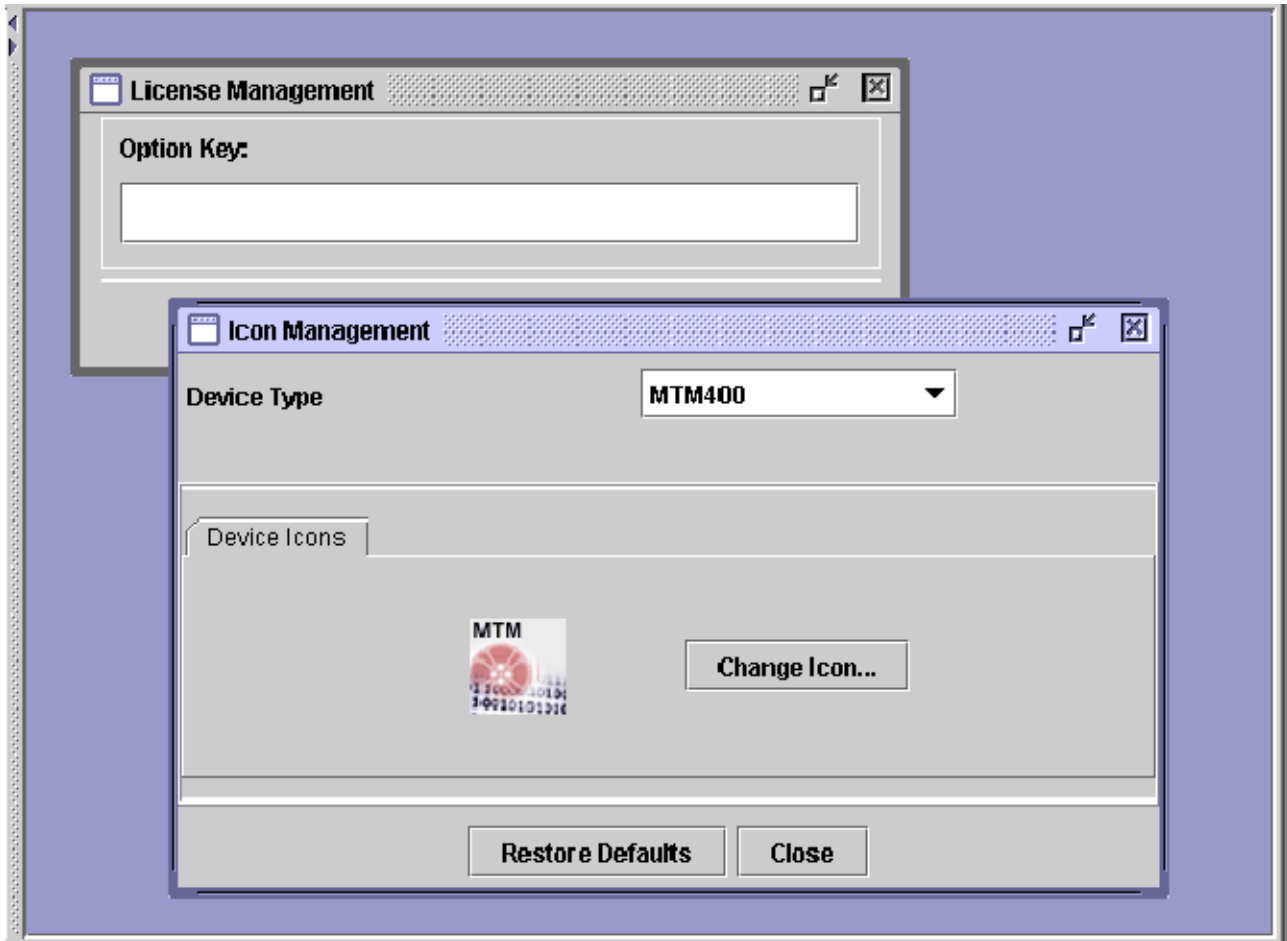


Figure 2-2: MLM1000 desktop

Hotspot Tree

The top-left panel that gives a tree-structured representation of the hotspots is the Hotspot tree. The hotspots can be either Maps or Devices. You can set the icon to maps and devices with the Properties dialog box. Figure 2-3 shows the Hotspot Tree.

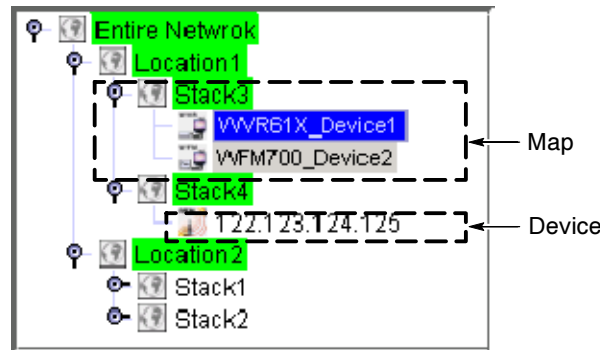


Figure 2-3: Hotspot tree

Hotspot Preview

The bottom-left panel that provides quick details of a selected hotspot is the Hotspot Preview.

If you select a map in the Hotspot Tree or Hotspot Panel, the Hotspot Preview displays information such as Name, Placements, Mode, and map icon.

When a map is selected in Hotspot Tree, the Hotspot Preview appears as shown in Figure 2-4.

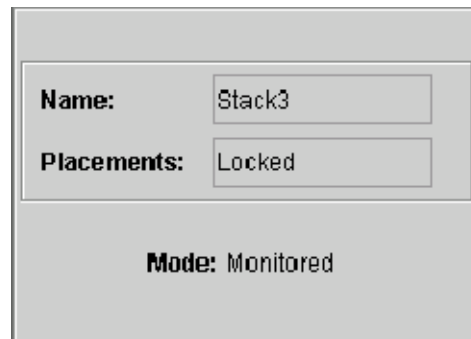


Figure 2-4: Map preview

If you select a device in the Hotspot Tree or Hotspot Panel, the Hotspot Preview displays information such as Name, Type, IP Address, Mode, and device icon.

When a device is selected in Hotspot Tree, the Hotspot Preview appears as shown in Figure 2-5.



Figure 2- 5: Device preview

Table 2-1 lists the description of Hotspot Preview interface elements.

Table 2- 1: Hotspot Preview interface elements

Interface element	Description
Name	Displays the name of the selected device or map.
Placements	Displays whether the placement of the map is locked or unlocked.
Type	Displays the type of the device.
IP Address	Displays the IP address of the device.
Mode	Displays whether the device or map is in monitored or unmonitored mode.

Menu Bar

The application menu bar has the following menus:

- Hotspots menu
- View menu
- Tools menu
- Window menu
- Help menu

The application menu bar has dynamic menus that appear only if the related dialog box or window is open. Table 2-2 lists the dynamic menus and the related dialog boxes or windows.

Table 2-2: Dynamic menus

Menu	Dialog box or window
Event Viewer menu	Event Viewer window
Device Graph menu	Alarm Occurrence window or Alarm Distribution window
New Devices menu	New Devices window

Hotspots Menu

Depending on whether map is selected or a device, the Hotspots menu items are enabled. Table 2-3 lists the description of Hotspots menu items.

Table 2-3: Hotspots menu

Menu item	Description
Add > Map	Adds a new map to the selected map.
Add > Device	Adds a device to the selected map.
Remove	Removes the selected map or device.
Search	Searches for a map or a device.
Configure	Allows you to configure the selected device.
Launch RUI	Launches the RUI of the selected device.
Alarm Distribution	Displays a pie chart distribution of all the alarms for a particular device.
Alarm Occurrence	Displays an alarm occurrence graph that updates the time of occurrences of each of the alarms for a particular device.
Generate Report	Generates the report for the selected device.
Acknowledge Alarms	Allows you to acknowledge the alarms that have occurred in the past.
Properties	Displays and allows you to change the properties of maps and devices.
Exit	Closes the application.

View Menu

Table 2-4 lists the description of View menu items.

Table 2-4: View menu

Menu item	Description
New Devices	Shows/Hides the New Devices window.
Hotspot Tree	Shows/Hides the Hotspot Tree.

Table 2-4: View menu (Cont.)

Menu item	Description
Hotspot Preview	Shows/Hides the Hotspot Preview.
Event Viewer	Shows/Hides the Event Viewer window.

Tools Menu

Table 2-5 lists the description of Tools menu items.

Table 2-5: Tools menu

Menu item	Description
Discovery Settings	Displays the Discovery Settings window that allows you to discover the devices in the specified IP address ranges.
User Management	Displays the User Management window that allows you to add, delete, or modify users.
Change Password	Displays the Change Password dialog box that allows you to change the password for the current user.
License Management	Displays the License Management window that allows you to enter the option key.
Icon Management	Displays the Icon Management window that allows you to change the default icons.
Options	Displays the Options dialog box that allows you to set the server settings, alarm settings and the display settings.

New Devices Menu

The New Devices menu appears only if the New Devices window is selected. Table 2-6 lists the description of New Devices menu items.

Table 2-6: New Devices menu

Menu item	Description
Remove All	Removes or hides all the devices in the container depending on the type of user.
Remove	Removes or hides the selected device in the container depending on the type of user.
Configure	Launches the RUI of the selected device and brings up the device configuration window.
Launch RUI	Launches the RUI of the selected device.

Event Viewer Menu The Event Viewer menu appears only if the Event Viewer window is selected. Table 2-7 lists the description of Event Viewer menu items.

Table 2-7: Event Viewer menu

Menu item	Description
Remove All	Removes all the event logs in the Event Viewer.
Export	Exports the event log to a CSV format file.

Device Graph Menu The Device Graph menu appears only if the Alarm Occurrence Graph window or Alarm Distribution Graph window is selected. Selecting the **Clear Device Graph** menu item from Device Graph menu clears the data in alarm occurrence or distribution graph and closes the window.

Window Menu Table 2-8 lists the description of Window menu items.

Table 2-8: Window menu

Menu item	Description
Cascade Windows	Arranges the open windows in the Hotspot Panel from upper-left to lower-right so that they overlap one another.
Tile Windows	Arranges the open windows in the Hotspot Panel without overlapping.
List of open windows	Allows you to jump to other open windows.

Help Menu Table 2-9 lists the description of Help menu items.

Table 2-9: Help menu

Menu item	Description
User Manual	Displays a PDF file of the User Manual.
Online Help	Displays the Help contents.
About MLM1000	Displays version and copyright information.

Toolbar

Figure 2-6 displays the MLM1000 toolbar.

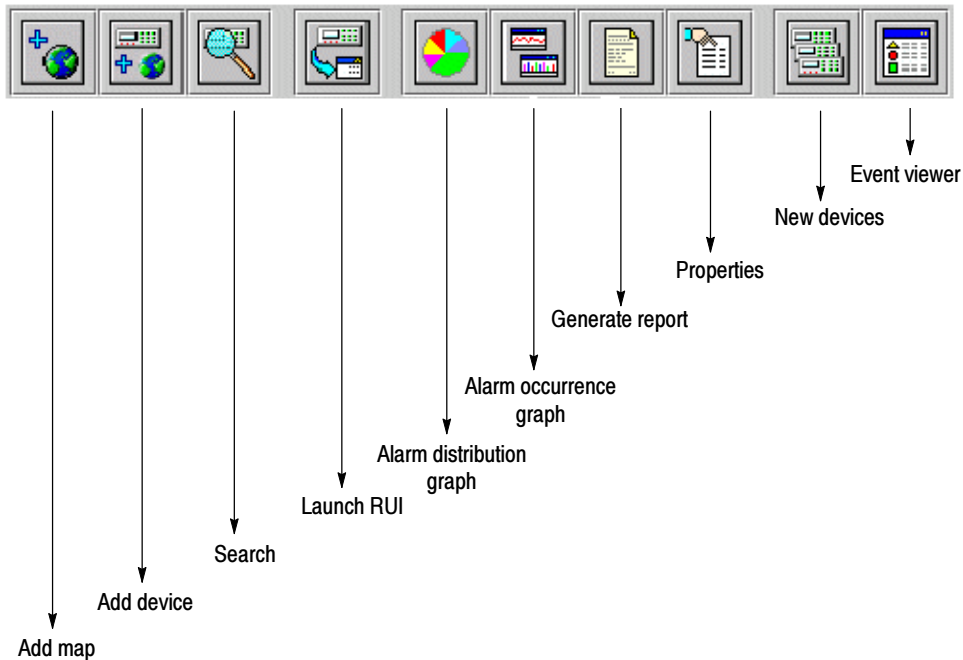


Figure 2-6: Toolbar

Depending on whether map is selected or a device, the Toolbar buttons are enabled. The next table lists the description of the Toolbar buttons.

Table 2-10: Toolbar buttons

Menu item	Description
Add Map	Adds a new map to the selected map.
Add Device	Adds a device to the selected map.
Search	Searches for a map or a device.
Launch RUI	Launches the RUI of the selected device.
Alarm Distribution Graph	Displays a pie chart distribution of all the alarms for a particular device.
Alarm Occurrence Graph	Displays an alarm occurrence graph that updates the time of occurrences of each of the alarms for a particular device.
Generate Report	Generates the report for the selected device.
Properties	Displays and allows you to change the properties of maps and devices.

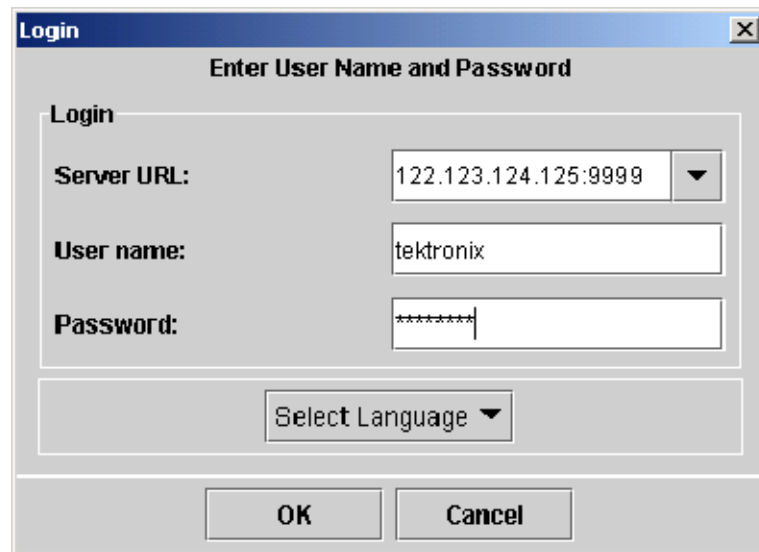
Table 2-10: Toolbar buttons (Cont.)

Menu item	Description
New Devices	Displays and allows you to remove the discovered devices.
Event Viewer	Allows you to remove or export the event logs.

Dialog Boxes or Windows

Login Dialog Box

This dialog box allows you to login and launch the application. You need to specify server URL, username, password, and language to log in. Figure 2-7 shows the Login dialog box.

**Figure 2-7: Login dialog box**

If you are logging in for the first time, use the default username and password. The default username and password are with administrative rights.

The default username is **Tektronix** and default password is **welcome**. It is recommended that you change the password after your first login.

The MLM1000 software lists the previous 10 server locations to which you have connected. You can launch the MLM1000 software in any language available in the Select Language language. English is the default language.

**Add Map
Dialog Box**

This dialog box allows you to create a new map, added as a child map to the selected hotspot map. Figure 2-8 shows the Add Map dialog box.

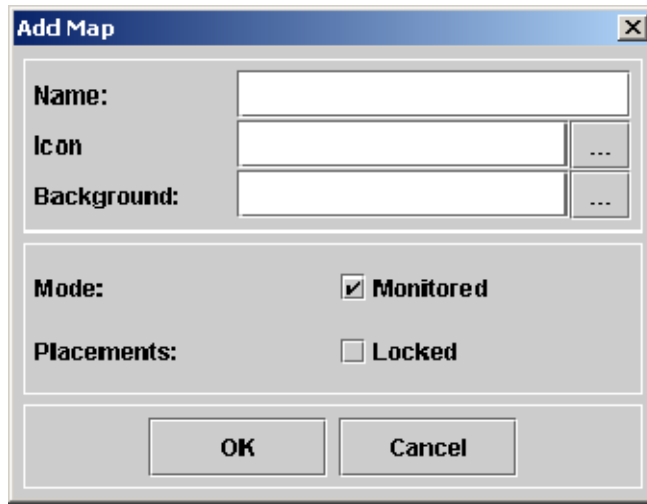


Figure 2- 8: Add Map dialog box

Ensure that the cursor in the Hotspot Tree is on a map to which you want to add the child map, and then select **Hotspots > Add > Map**.

With this dialog box, you can specify the name, the icon, and the background for the map. You can also select the map to be either monitored or unmonitored. You can also lock or unlock the map placement.

If you do not specify the icon, a default icon is used for the map. If you do not specify the background, the background for the map is blank.

You cannot add a map to a device or to a locked map. For information on locking or unlocking a map, see *Locking or Unlocking Map* on page 3-3.

Table 2-11 lists how the background and icon are set for a map.

Table 2-11: Mapbackground and icon

Background / Icon	Available	Not Available
Available	If you specify both, each is used for its intended purpose.	If you specify an icon but no background image, that map has no background image and will have the selected icon.
Not Available	If you specify a background image, but no icon then the application uses the background image as an icon.	If you specify none, the map background is empty and the application uses a default image as an icon.

Add Device Dialog Box

This dialog box allows you to add a new device to the selected hotspot map. Figure 2-9 shows the Add Device dialog box.

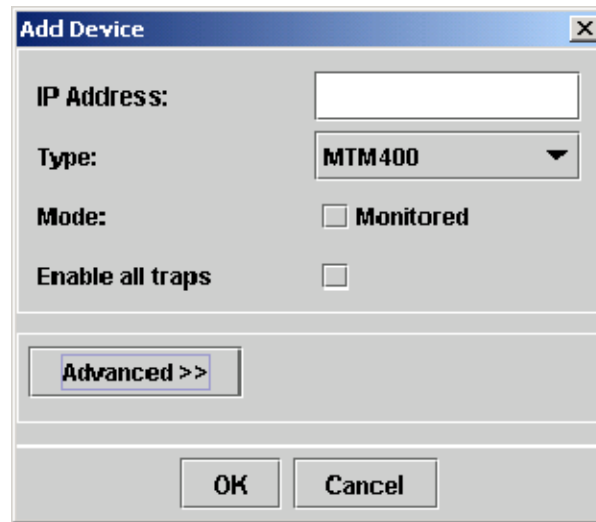


Figure 2-9: Add Device dialog box

You cannot add a device to a device or to a locked map. Ensure that the cursor in the Hotspot Tree is on a map to which you want to add the device and then select **Hotspots > Add > Device**.

With this dialog box, you can specify either the IP address or the name of the device in the IP Address field. You can also select the type of device and select the device to be in monitored or unmonitored mode.

The type of devices that you can select are MTM400, RFM210, WFM700, or WVR61X. If you select a wrong device type, the application corrects the type, once the device is up and running.

You can enable all the traps and set SNMP settings such as SNMP Version, SNMP Get Community, SNMP Set Community, Trap Community, and Retries.

Search Dialog Box

This dialog box allows you to search for maps and devices with the ID. Figure 2-10 shows the Search dialog box.

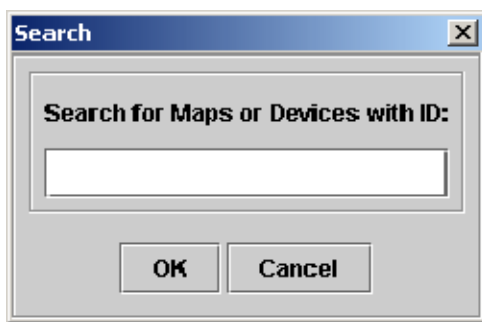


Figure 2- 10: Search dialog box

You need to specify the complete ID for the application to search for the device or a map.

Alarm Distribution Window

This window displays a pie chart distribution of all the alarms for the selected device. Figure 2-11 shows the Alarm Distribution window.

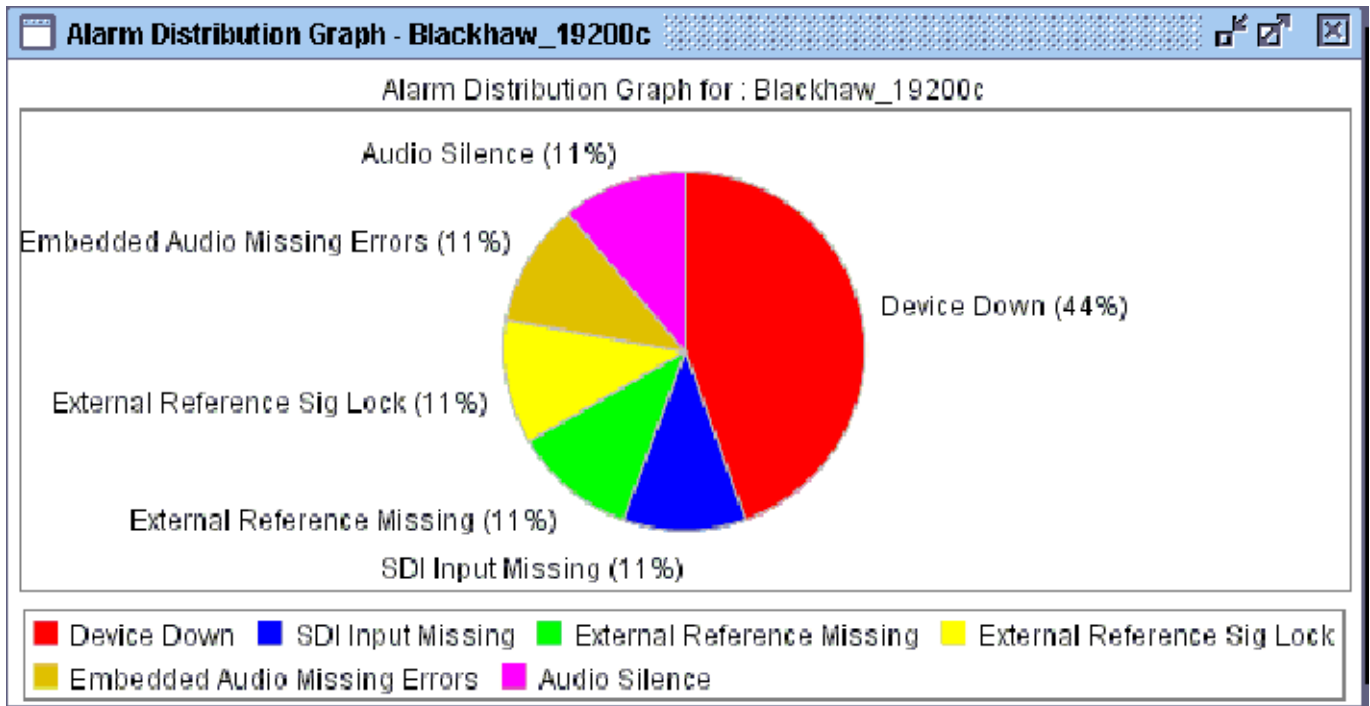


Figure 2-11: Alarm Distribution Graph window

The graph is updated real time. If a device is set unmonitored mode, the application does not update the Alarm Distribution graph. The updates resume once the device is reset to monitored mode.

Right-click on the Alarm Distribution Graph to display a context menu.

Using the Context menu, you can:

1. View or modify the chart properties, such as:
 - the Legend's Outline, Outline paint, Background, Series Label Font, Series Label Paint,
 - the Pie Plot's Insets, Outline stroke, Outline paint, Background paint, and
 - the Background paint of the Alarm Distribution window, Series Paint, Series Stroke, Series Outline Paint and Series Outline Stroke.
2. Save the alarm distribution graph as PNG image file.

3. Print the alarm distribution graph.

If you remove a device from a map, the application closes any open Alarm Distribution window.

Alarm Occurrence Window

This window displays the time of alarm occurrences for the selected device.

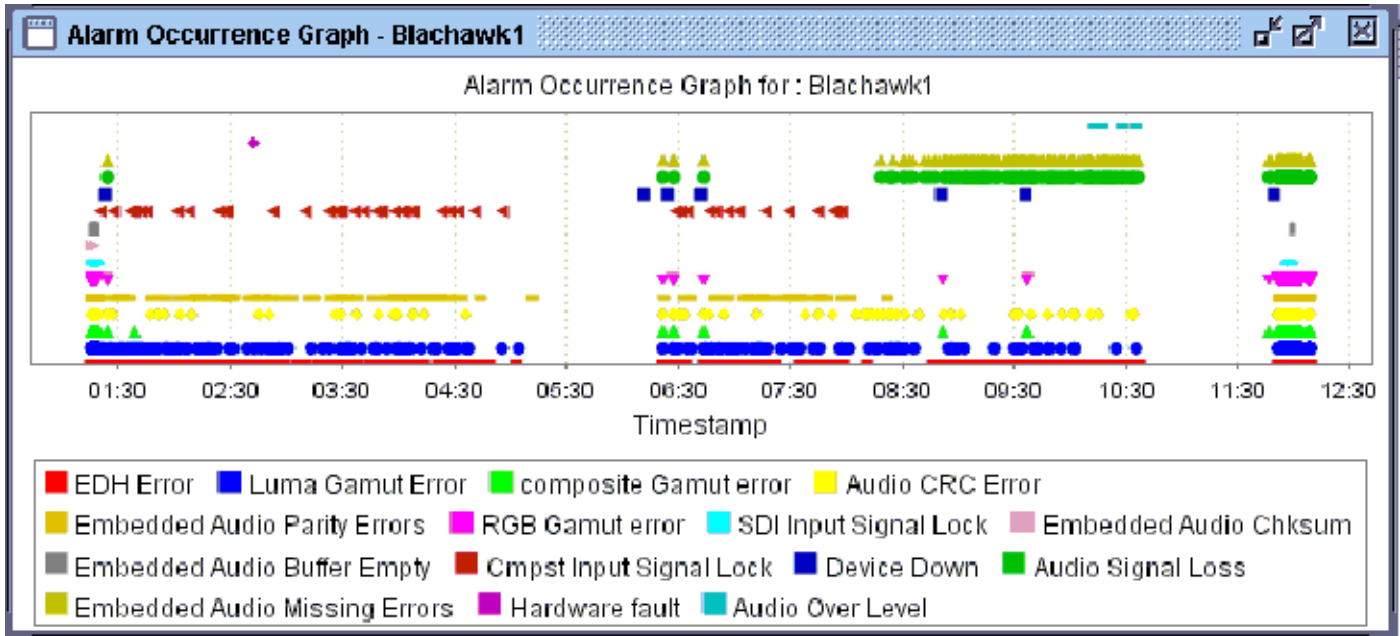


Figure 2- 12: Alarm Occurrence Graph window

The graph is updated real time. If a device is set unmonitored mode, the application does not update the Alarm Occurrence graph. The updates resume once the device is reset to monitored mode.

Right-click on the Alarm Occurrence Graph to display a context menu.

Using the Context menu, you can:

1. View or modify the chart properties, such as:
 - the Legend's Outline, Outline paint, Background, Series Label Font, Series Label Paint,
 - the XY Plot's Domain Axis, Range Axis, Appearance, and
 - the Background paint of the Alarm Occurrence window, Series Paint, Series Stroke, Series Outline Paint and Series Outline Stroke.

2. Save the alarm occurrence graph as PNG image file.
3. Print the alarm occurrence graph.
4. Zoom in or Zoom out the horizontal, vertical, or both the axes.
5. Auto Range the horizontal, vertical, or both the axes.

If you remove a device from a map, the application closes any open Alarm Occurrence window.

Map Properties Dialog Box

Placing the cursor on a map hotspot and selecting **Hotspots > Properties** displays the Map Properties dialog box. Figure 2-13 shows the Map Properties dialog box.

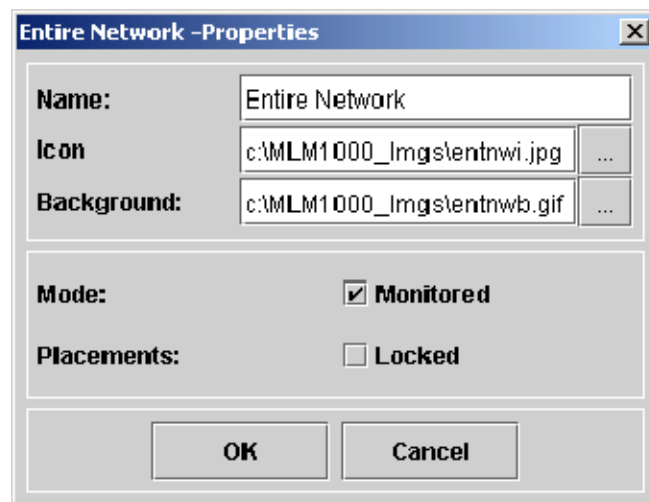


Figure 2-13: Map Properties dialog box

In this dialog box, you can modify the name of the map, the icon, and the background.

You can enable all traps of the device to be logged into the Event Viewer.

You can specify the mode as monitored or unmonitored and choose to lock or unlock the placement.

If you do not specify the icon, the default icon is used for the map.

Refer to *Table 2-11* that lists how the background and icon are set for a map.

Device Properties Dialog Box

Placing the cursor on a device hotspot and selecting **Hotspots > Properties** displays the Device Properties dialog box. Figure 2-14 shows the Device Properties dialog box.

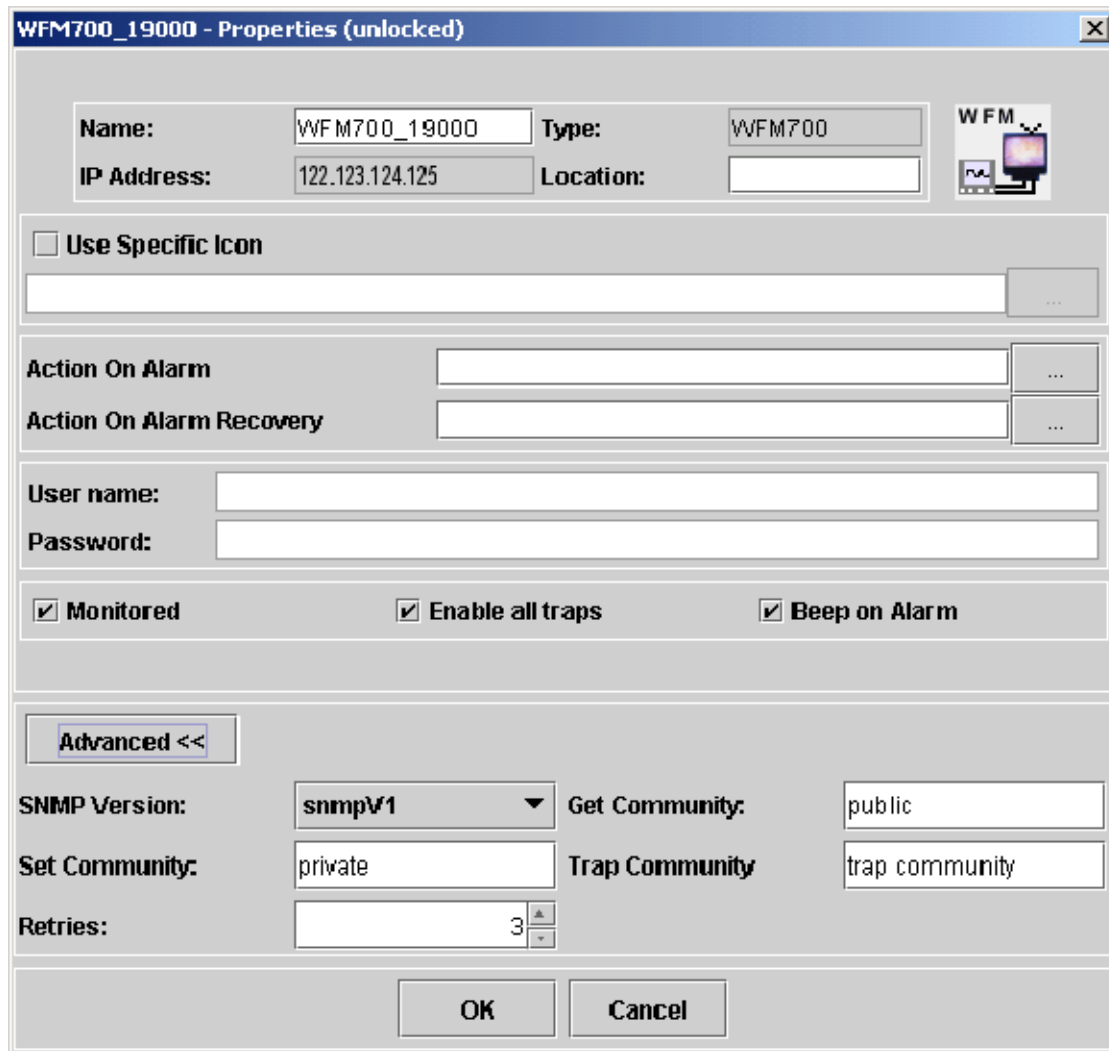


Figure 2- 14: Device Properties dialog box

In this dialog box, you can view the type, and IP address of the selected device. You can also select a specific icon for the device, and set the mode as monitored or unmonitored. You can set the name, choose to indicate on alarm using the default sound file or one of your choice, and enable all traps. You can enter the user name and password details, only if the device supports authentication. You can set an action on alarm and alarm recovery.

You can set SNMP settings such as SNMP Version, SNMP Get Community, SNMP Set Community, Trap Community, and Retries.

NOTE. You can select the executable for action on alarm and alarm recovery only if both the client and the server are running in the same machine.

Event Viewer Window

This window allows you to view all the logged events. The events are of the type: Information, Warning, Error, and Critical. Figure 2-15 shows the Event Viewer window.

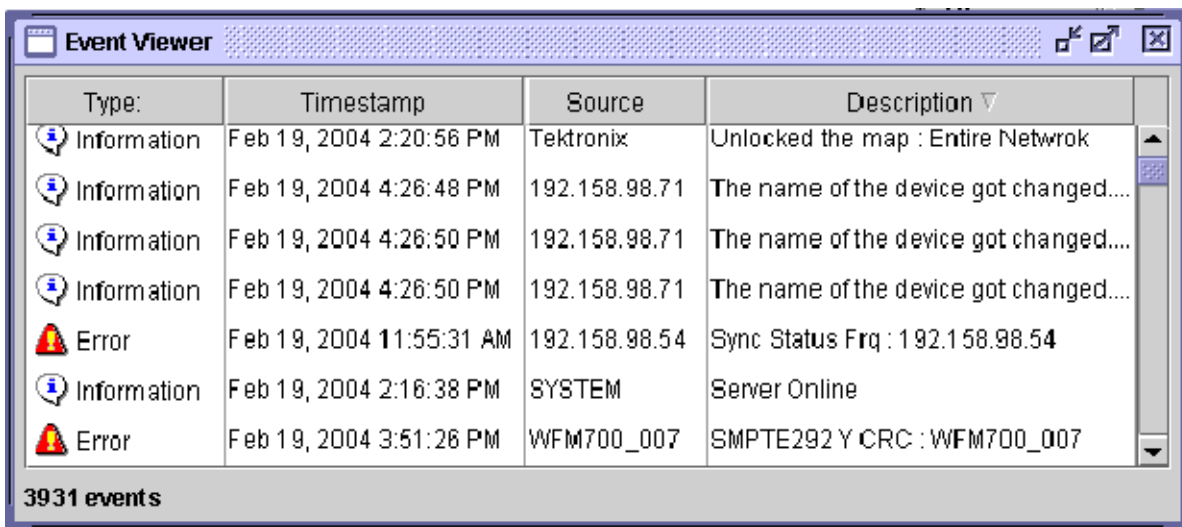


Figure 2-15: Event Viewer window

In this window, each event has information such as Type, Timestamp, Source, and Description.

The list is sorted in a descending order of the Timestamp by default. You can sort the event log information by all other columns such as Type, Source, and Description by clicking on the header.

The Event Viewer does not display duplicate events.

The default log file size is 1 MB. To change the maximum size of the log file, select **Tools > Options**.

NOTE. Only a user with Administrator privilege can change the maximum size of the log file.

If the Event Viewer is selected, an Event Viewer menu appears. The Event Viewer menu has two menu items - Remove All, and Export.

Selecting **Remove All** displays a confirmation message and removes all the logs from the server.

Selecting **Export** saves the event log in a .csv format file.

Discovery Settings Window

This window allows you to search for a device within specific ranges. Figure 2-16 shows the Discovery Settings window.

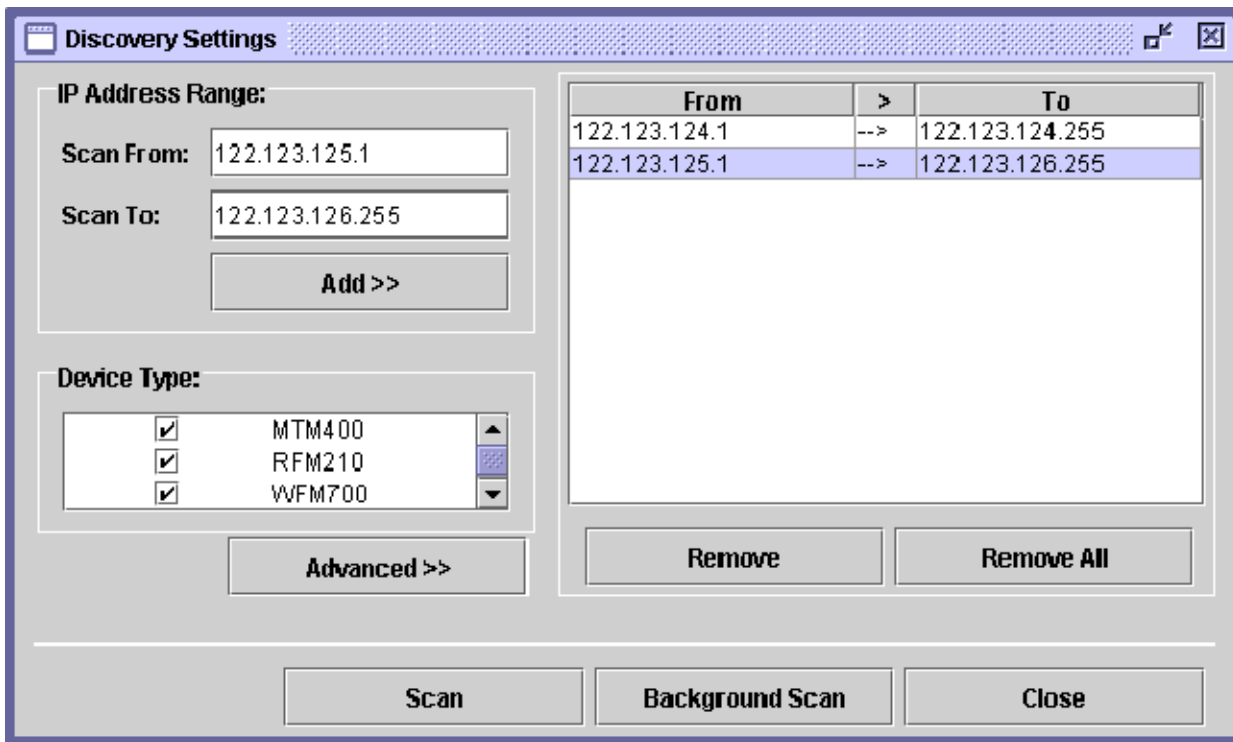


Figure 2- 16: Discovery Settings window

In this window, you can specify the IP address ranges, and select the type of device.

You can set the advanced options such as the SNMP version (snmpV1 or snmpV2), the SNMP community strings and the number of required retries.

Each retry shall be 500 milliseconds apart. Also the number of retries shall be an integer value ($0 < \text{Retries} \leq 10$).

For get community strings, separate the multiple community strings with commas. You cannot enter multiple set community strings. The specified community strings are commonly applied to all the selected device types.

You can choose either a background scan or a foreground scan. You can have any number of background scans at a time where as foreground scan can be only one.

The application discovers only those devices that are not in the map.

New Devices Window

This window displays the discovered devices. Figure 2-17 shows the New Devices window.

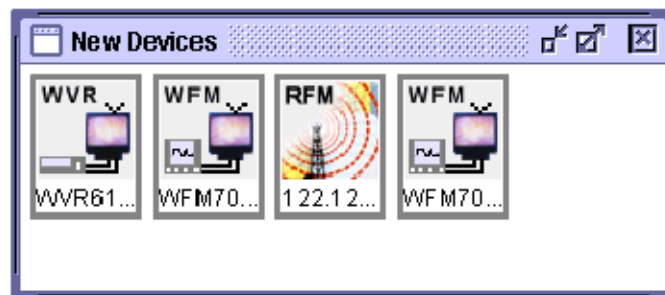


Figure 2-17: New Devices window

In this window, you can remove the discovered devices. If you are an administrator and remove the device from the New Devices, the device will not be shown in the New Devices for all users.

If you are a user and remove the device from the New Devices, the device will only be removed from your view. The next time you scan for the same device, the device will not be shown in the New Devices until you login the next time.

The New Devices menu appears if the New Devices window is selected. Using the New Devices menu, you can remove the devices in the New Devices window, launch the RUI of the selected device and configure the selected device.

Change Password Dialog Box

Use this dialog box to change the password for the active user. Figure 2-18 shows the Change Password dialog box.



Figure 2- 18: Change Password dialog box

In this dialog box, specify the old password, the new password and confirm the new password.

User Management Window

Use this window to add, modify and delete user profiles. Only an administrator can manage other users and user profiles. Figure 2-19 shows the User Management window.

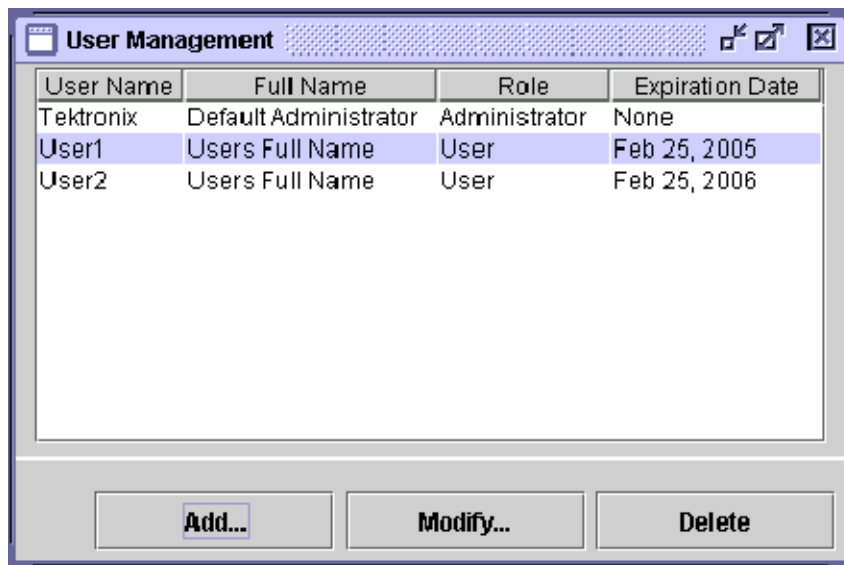


Figure 2- 19: User Management window

The User Profile contains information about the user such as user name, password, role, full name, email ID, contact number, and expiration date.

- **User name.** The username for the user to login to the Server. The user name should be an alphanumeric string with 4 to 16 characters. The first character should be a letter. Intermediate underscore characters are supported.
- **Password.** The password for the user to login to the Server. The password can be an arbitrary string with at least 4 and at most 16 characters.
- **Role.** The role of the user such as Administrator or User.
- **Full Name.** The name of the user. The full name can be an arbitrary string with at most 64 characters.
- **Email ID.** The email ID of the user should in the form **s1@s2.com**; where s1 and s2 are alphanumeric strings with optional intermediate underscores. Ensure that email IDs are valid.
- **Contact Number.** The contact number. The contact number should be a numeric string with optional characters like braces (), spaces, - and +.
- **Expiration Date.** The expiration date of the account.

License Management Window

Use this window to specify the Option Key to control the number and types of devices that can be accessed and controlled. Figure 2-20 shows the License Management window.

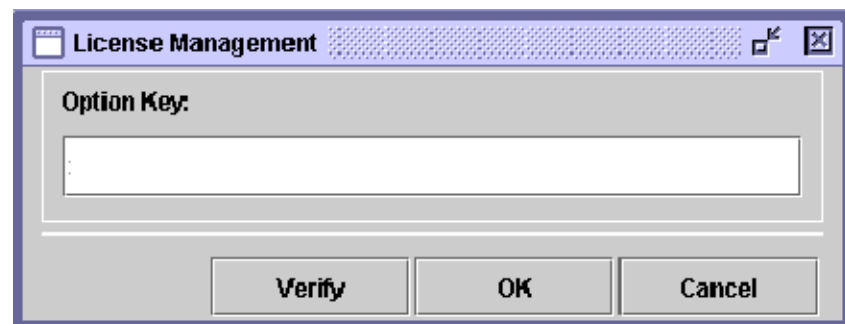


Figure 2-20: License Management window

The option key should be an alphanumeric string with permitted intermediate hyphen characters. The maximum allowed size is 32 characters.

Icon Management Window

This window allows you to represent icons for each type of device. Figure 2-21 shows the Icon Management window.

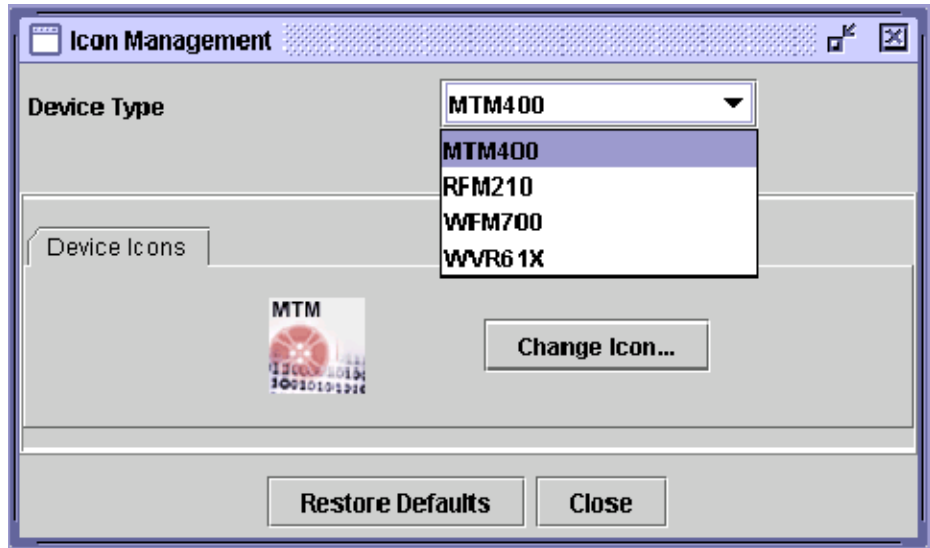


Figure 2- 21: Icon Management window

The type of devices that you can select are MTM400, RFM210, WFM700, or WVR6XX.

You can change the icon or restore the default.

Whenever the you change the icon for a particular device, all the clients reflect the change in their respective hotspots and New Devices window.



Using the MLM1000

Managing the Maps

This section explains how to add, remove, configure, and move maps. You can only move the maps if the Administrator has not locked the placement.

Adding a Map

You cannot add a map to a device or to a locked map.

To add a map:

1. Ensure that the cursor in the Hotspot Panel or Hotspot Tree is on a map that you want to add another map to.
2. Select **Hotspots > Add > Map**. The Add Map dialog box appears.

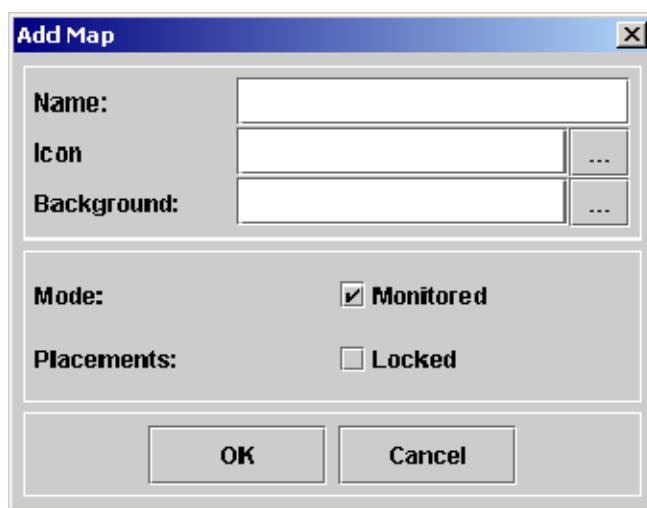


Figure 3-1: Add Map dialog box

3. Enter a name for the map in the **Name** field.
4. Click ... adjacent to the Icon field, and browse for an icon for the map.
5. Click ... adjacent to the Background field, and browse for a background for the map.
6. Set the **Mode** check box as monitored or unmonitored.
7. Select the **Placements** check box as Locked or Unlocked.

8. Select **OK**. The map is added and reflected in the Hotspot Tree and MLM1000 Desktop.

Modifying Map Properties

You can modify map properties such as Name, Icon, Background, Mode, and Placement.

To modify map properties:

1. Ensure that the cursor in the Hotspot Panel is on a map that you want to modify.
2. Select **Hotspots > Properties** or right-click on a map to display a context menu and select **Properties**.

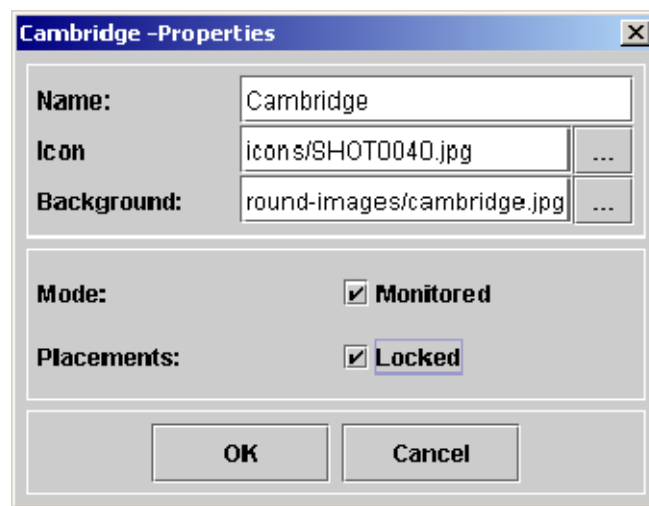


Figure 3- 2: Map Properties dialog box

3. In the **Name** field, change the name for the map.
4. Adjacent to the **Icon** field, click ... to browse for an icon for the map.
5. Adjacent to the **Background** field, click ... to browse for a map background.
6. Set the **Mode** check box as monitored or unmonitored.
7. Select or clear **Placements** check box to lock or unlock the map.
8. Select **OK**. The map properties are reflected in the Hotspot Tree and MLM1000 Desktop.

Removing a Map

You cannot remove a locked map. If you want to remove a locked map, you must first unlock the map. For more information on unlocking a map see section *Locking or Unlocking a Map* on page 3-3.

To remove an unlocked map:

1. Ensure that the cursor in the Hotspot tree is on a map that you want to delete.
2. Select **Hotspots > Remove** or right-click on a map to display the context menu and select **Remove**.
3. A message box appears with a message “*Contained maps will also be removed if any. Are you sure you want to remove*”.
4. Select **Yes**.

Renaming a Map

To rename a map:

1. Ensure that the cursor in the Hotspot tree is on a map that you want to rename.
2. Select **Hotspots > Properties** or right-click on a map to display the context menu and select **Properties**. The Map Properties dialog box appears.
3. Change the name of the map in the **Name** field.
4. Select **OK**. The new map name is reflected in the hotspot tree and the MLM1000 desktop.

Locking or Unlocking a Map

You can lock or unlock a map. You cannot add maps or devices to a locked map. You cannot move a map or a device from the locked map. You cannot remove or change the properties of a locked map.

NOTE. *Only an Administrator can lock or unlock a map.*

To lock or unlock a map:

1. Ensure that the cursor in the Hotspot tree is on a map that you want to lock.
2. Select **Hotspots > Properties** or right-click on the map and from the context menu, select **Properties**. The Map Properties dialog box appears.

3. Select or clear the **Placement** check box to lock or unlock the placement.
4. Select **OK**.

Monitoring or Stopping a Map from Being Monitored

You can specify to monitor or not to monitor a map.

To select whether a map is monitored:

1. Ensure that the cursor in the Hotspot tree is on a map that you want to monitor.
2. Select **Hotspots > Properties** or right-click on the map and from the context menu, select **Properties**. The Map Properties dialog box appears.
3. Set the **Mode** check box as monitored or unmonitored.
4. Select **OK**.

Setting the Map Background

You can specify the background for a map. To set a background for the map:

1. Ensure that the cursor in the Hotspot tree is on a map that you want to change the background for.
2. Select **Hotspots > Properties** or right-click on the map and from the context menu select **Properties**. The Map Properties dialog box appears.
3. Adjacent to the Background field, click on ... to display the Open dialog box.
4. Browse for the background image file and select **OK**. The file formats supported are JPEG and GIF. The new map background is reflected in the Map window on the MLM1000 desktop.

If you have not specified an icon and have set the map background, the application resizes and displays the background image as an icon in the Hotspot Tree and MLM1000 Desktop.

Setting the Map Icon

You can specify an icon for the map. To set an icon for the map:

1. Ensure that the cursor in the Hotspot tree is on a map that you want to change the icon of.
2. Select **Hotspots > Properties** or right-click on the map and from the context menu select **Properties**. The Map Properties dialog box appears.
3. Adjacent to the Icon field, click on ... to display the Open dialog box.
4. Browse for the icon image file and Select **OK**. The file formats supported are JPEG and GIF. The new map icon is reflected in the Hotspot Tree and the Map window on the MLM1000 desktop.

If you have specified an icon and not set the background, the application leaves the background blank.

If you do not specify the icon, the application uses a default icon.

Moving a Map to Another Map

In the Hotspot Tree, you can drag and drop any map to the other map.

You can move a locked map to an unlocked map.

You cannot a move a map to a locked map.

First unlock the map and then move the map. For information on unlocking a map see section *Locking and Unlocking a Map* on page 3-3.

Moving a Map Within the Map Window

Double-click the parent map in the Hotspot Tree to display the parent map window.

Drag and drop the child maps within the parent map window.

You cannot move a locked child map within the parent map window.

Managing the Devices

This section explains how to add, remove, and configure devices. You can move the devices from one location to the other in the Map window or move the devices from one map to the other. You can move the devices if the Administrator has not locked the placement.

Adding a Device Manually

You cannot add devices to a locked map. First unlock the maps, and then add devices.

To add a device manually:

1. Ensure that the cursor in the Hotspot Panel is on a map to which you want to add the device.
2. Select **Hotspots > Add > Device**. Figure 3-3 shows the Add Device dialog box that appears.

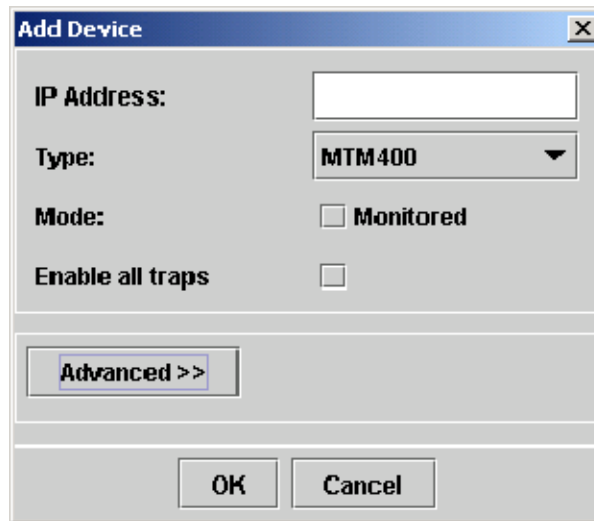


Figure 3-3: Add Device dialog box

3. Enter the IP Address of the device in the **IP Address** field.
4. Select the type of device in **Type** drop-down list. If a mismatch between the device type you select and the actual device occurs, the application corrects this while discovering the device.

5. Select the **Mode** check box as monitored or unmonitored.
6. Select the **Enable all traps** check box to enable all the traps.
7. Click **Advanced** and set SNMP settings such as - SNMP Version, SNMP Get Community, SNMP Set Community, Trap Community, and Retries.
8. Select **OK**. The device is added and reflected in the Hotspot Tree and MLM1000 Desktop.

Adding a Discovered Device to a Map

Once you scan for devices, the discovered devices are placed in the New Devices window. You need to add the discovered devices to the map for monitoring.

To add a discovered device:

1. In the Hotspot Tree, click on the map to which you want to add the device. The Map window opens.
2. Click **View > New Devices** to open the New Devices window.
3. Drag and drop the devices from the New Devices window to the Map Window.
4. If the device you want to add to the map is not present in the New Devices window, then scan for new devices. For information on scanning for new devices, see *Discovering the Devices* on page 3-13.

Moving Devices to Another Map

You can move devices from one map to another in the Hotspot Tree or MLM1000 Desktop. To move a device from one map to the other map:

1. In the Hotspot Tree, select the device that you want to move.
2. Drag and drop the device to another map.
or
1. To open the map window from which the device will be moved, click on that map in the Hotspot Tree.
2. To open the map window to which the device will be moved, click on that map in the Hotspot Tree.
3. Drag and drop the device from one map window to the other map window.

You cannot move devices from a unlocked map to a locked map or from a locked map to an unlocked map.

Moving Devices Within the Map Window

You can move devices within the map window by dragging and dropping.

Monitoring or Stopping a Device From Being Monitored

To monitor or stop a device from being monitored:

1. In the Hotspot tree, place the cursor on a device that you want to monitor or stop monitoring.
2. Select **Hotspots > Properties** or right-click on the device and from the context menu select **Properties**. The Properties dialog box appears.
3. Select or clear the **Mode** check box to monitor or stop a device from being monitored.
4. Select **OK**.

Changing the Device Icon

You can change the way the device icon appears in the Hotspot Tree and MLM1000 Desktop. Do the following to change the device icon.

1. Ensure that the cursor in the Hotspot tree is on a device that you want to monitor.
2. Select **Hotspots > Properties** or right-click on the device and from the context menu select **Properties**. The Properties dialog box appears.
3. Select the **Use specific icon** check box and click ... to display the Open dialog box.
4. Browse and select an icon in JPEG or GIF file format and click **Open**.
5. Select **OK**. The device icon is added and reflected in the Hotspot Tree and MLM1000 Desktop.

Managing Default Icons for All Devices

You can set the icons for each type of device. You can reset the icons to system default.

To set icons for the devices:

1. Select **Tools > Icon Management** to display the Icon Management window as shown in the next figure.

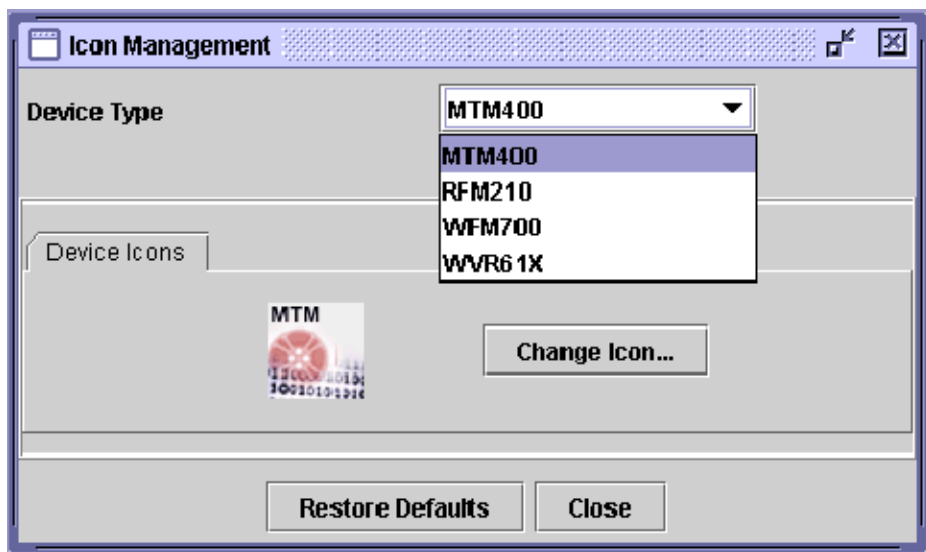


Figure 3- 4: Icon Management window

2. In the **Device Type** drop-down list, select the type of device.
3. Click **Change Icon** to change the icon for that device.
4. After you have set the icons, select **Close**. The device icons are added and reflected in the Hotspot Tree and MLM1000 Desktop.
5. If you want to reset the system default icons for the selected device type, click **Restore Defaults**.

Removing a Device from the Map

To remove a device from the map.

1. Ensure that the cursor in the Hotspot tree is on a device that you want to remove.
2. Select **Hotspots > Remove** or right-click on the device and from the context menu select **Remove**. The application displays a message “*Are you sure you want to remove?*”
3. Select **Yes** to remove the device.

Removing Devices from the New Devices Window

Once you scan for devices, the discovered devices are placed in the New Devices. You can remove the devices from the New Devices.

If a you are an administrator and remove the device from the New Devices:

The device will not be shown in the New Devices for all users.

If a you are an user and remove the device from the New Devices:

The device will only be removed from your view. The next time you scan for the same device, the device will not be shown in the New Devices until you login next time.

To remove all discovered devices from the New Devices window.

1. Click **View > New Devices** to open the New Devices window and display a dynamic menu - New Devices.
2. Select **New Devices > Remove All** to remove all the devices in the New Devices. The application displays a message *“Are you sure you want to delete the device selected from the container?”*.
3. Select **Yes**.

To remove a specific device from the New Devices window.

1. Ensure that the cursor in the New Devices is on a device that you want to remove.
2. Select **New Devices > Remove** to remove the selected devices from the New Devices. The application displays a message *“Are you sure you want to delete the device selected from the container?”*.
3. Select **Yes**.

Launching Device RUI

To launch the RUI of the device:

1. Ensure that the cursor in the Hotspot tree is on a device for which you want to launch the RUI.
2. Select **Hotspots > Launch RUI** or right-click on the device and from the context menu select **Launch RUI**.
or
Ensure that the cursor in the Map window is on a device that you want to launch RUI.

3. Right-click on the device and from the context menu select **Launch RUI**.

The application launches the RUI of the selected device.

If you have specified the username and password for the device in the Device Properties dialog box, then the RUI is automatically authenticated.

If you have not specified the username and password for the device in the Device Properties dialog box, then the RUI will prompt you to enter the user name and password to authenticate.

Discovering the Devices

This section explains how to discover devices in the network, configure and save discovery settings. You can discover devices within a specific range or multiple ranges of IP addresses. This section also explains how you can search for devices using the community strings.

There are two types of scans: Foreground scan and Background scan.

Foreground scan - Attempts to discover devices on the network and keeps the process running in the foreground. The application shows a progress bar while scanning for devices. You can perform only one foreground scan at a time.

Background scan - Attempts to discover devices on the network and keeps the process running in the background. The application does not show a progress bar while scanning for devices. You can perform multiple background scans simultaneously, using different ranges and different community strings.

You can cancel a foreground scan but not a background scan. The application discovers only those devices that are not in the map.

Foreground Scanning

To perform a foreground scan:

1. Select **Tools > Discovery Settings**. The Discovery Settings dialog box appears.
2. In the **Scan From** field, enter the starting IP Address of the range in which you want to discover devices.
3. In the **Scan To** field, enter the last IP Address of the range in which you want to discover devices.
4. Click **Add**. The IP address range is listed in the Range Table. You can add multiple IP address ranges to the Range Table.
5. In the **Device Type** list, select the relevant check boxes adjacent to the devices which you want to discover.
6. Click **Advanced** to set the advanced options. The Discovery Settings dialog box expands to display fields such as SNMP Version, Retries, SNMP Get Community, and SNMP Set Community. You can do the following:
 - a. In the **SNMP Version** drop-down list, select **snmpV1** or **snmpV2c** depending on the SNMP Version of the device you want to scan.

- b. In the **Retries** field, click on the arrow buttons to increase or decrease the number of retries. The acceptable range of retries is between 1 and 10.
- c. In the **SNMP Get Community** and **SNMP Set Community** fields, enter the SNMP community strings of the devices you want to scan for. You can enter multiple SNMP get community strings separated with commas.

NOTE. *The SNMP Community strings are alphanumeric and the maximum allowed size is 32 characters.*

7. Select **Scan** to perform a foreground scan.

Background Scanning

To discover devices in the background:

1. Select **Tools > Discovery Settings**. The Discovery Settings dialog box appears.
2. In the **Scan From** field, enter the starting IP Address of the range in which you want to discover devices.
3. In the **Scan To** field, enter the last IP Address of the range in which you want to discover devices.
4. In the **Device Type** list, select the relevant check boxes adjacent to the devices which you want to discover.
5. Click **Add**. The IP address range is listed in the Range Table. You can add multiple IP address ranges to the Range Table.
6. Click **Advanced** to set the advanced options. The Discovery Settings dialog box expands to display fields such as SNMP Version, Retries, SNMP Get Community, and SNMP Set Community. You can do the following:
 - a. In the **SNMP Version** drop-down list, select **snmpV1** or **snmpV2c** depending on the SNMP Version of the device you want to scan.
 - b. In the **Retries** field, click on the arrow buttons to increase or decrease the number of retries. The MLM1000 software will scan for the device as many number of time you have entered in the Retries field.
 - c. In the **SNMP Get Community** and **SNMP Set Community**, enter the SNMP community strings of the devices you want to scan for. You can enter multiple SNMP get community strings separated with commas.

NOTE. The SNMP Community strings are alphanumeric and the maximum allowed size is 32 characters.

7. Select **Background Scan** to scan for devices in the background. You can perform multiple background scans.

Adding an IP Address Range to the Device Discovery Settings

To add an IP address range to discover devices:

1. Select **Tools > Discovery Settings**. The Discovery Settings dialog box appears.
2. In the **Scan From** field, enter the starting IP Address of the range in which you want to discover devices.
3. In the **Scan To** field, enter the last IP Address of the range in which you want to discover devices.
4. Click **Add**. The IP address range is listed in the Range Table. You can add multiple IP address ranges to the Range Table.

Removing an IP Address Range from the Device Discovery Settings

To remove an IP address range to discover devices.

1. Select **Tools > Discovery Settings**. The Discovery Settings dialog box appears. The range table displays all the IP address ranges added for device discovery.
2. To remove an IP address range, select the range in the Range Table and click **Remove**.
3. To remove all the IP ranges, select **Remove All**.

Scanning for a Device in an IP Address Range

To discover a device in an IP address range.

1. Select **Tools > Discovery Settings**. The Discovery Settings dialog box appears.
2. In the **Scan From** field, enter the starting IP Address of the range in which you want to discover devices.

3. In the **Scan To** field, enter the last IP Address of the range in which you want to discover devices.
4. Click **Add**. The IP address range is listed in the Range Table. You can add multiple IP address ranges to the Range Table.
5. Select **Scan** to scan for devices in the foreground.
6. Select **Background Scan** to scan for devices in the background. You can perform multiple background scans.

Scanning for a Specific Device Type

To discover a specific device type:

1. Select **Tools > Discovery Settings**. The Discovery Settings dialog box appears.
2. In the **Scan From** field, enter the starting IP Address of the range in which you want to discover devices.
3. In the **Scan To** field, enter the last IP Address of the range in which you want to discover devices.
4. In the **Device Type** list, select the relevant check boxes adjacent to the devices for which you want to discover.
5. Click **Add**. The IP address range is listed in the Range Table. You can add multiple IP address ranges to the Range Table.
6. Select **Scan** to scan for devices in the foreground.
7. Select **Background Scan** to scan for devices in the background. You can perform multiple background scans.

Scanning for Devices with Community Strings

To discover a device with community strings:

1. Select **Tools > Discovery Settings**. The Discovery Settings dialog box appears.
2. In the **Scan From** field, enter the starting IP Address of the range in which you want to discover devices.
3. In the **Scan To** field, enter the last IP Address of the range in which you want to discover devices.

4. Click **Add**. The IP address range is listed in the Range Table. You can add multiple IP address ranges to the Range Table.
5. Click **Advanced** to set the advanced options. The Discovery Settings dialog box expands to display fields such as SNMP Version, Retries, SNMP Get Community, and SNMP Set Community. You can do the following:
 - a. In the **SNMP Version** drop-down list, select **snmpV1** or **snmpV2c** depending on the SNMP Version of the device you want to scan.
 - b. In the **Retries** field, click on the arrow buttons to increase or decrease the number of retries.
 - c. In the **SNMP Get Community** and **SNMP Set Community**, enter the SNMP community strings of the devices you want to scan for. You can enter multiple SNMP community strings separated with commas.

NOTE. *The SNMP Community strings are alphanumeric and the maximum allowed size is 32 characters.*

6. Select **Scan** to scan for devices in the foreground.
7. Select **Background Scan** to scan for devices in the background. You can perform multiple background scans.

Setting Up Auto Discovery

To set up automatic discovery of devices:

1. Select **Tools > Options** to display the Options dialog box as shown in Figure 3-5.

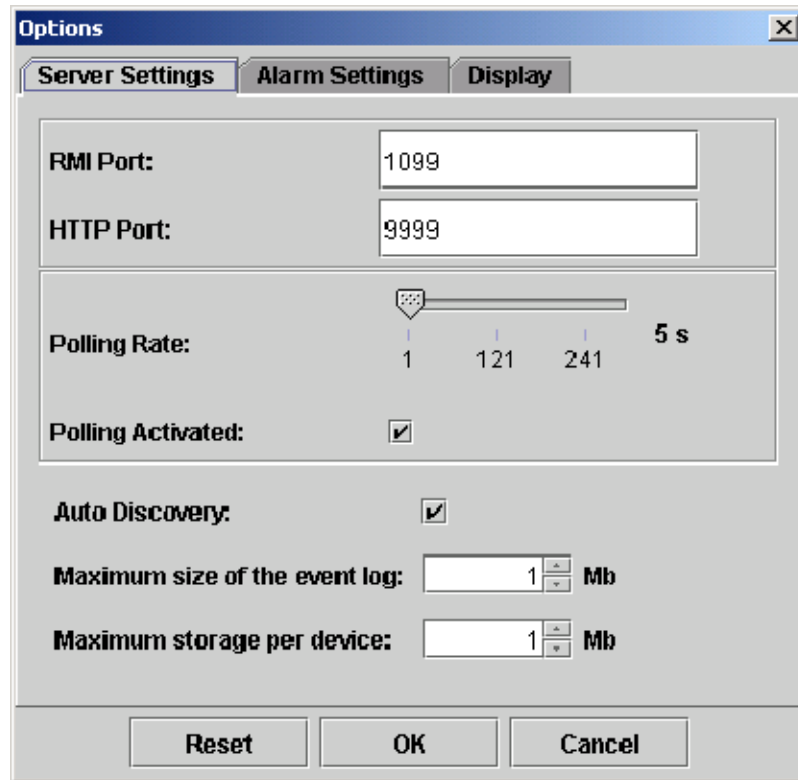


Figure 3- 5: Server Settings tab of Options dialog box

2. Select the **Server Settings** tab.
3. Select the **Auto Discovery** check box and then click **OK**.

Saving Device Discovery Settings

Only an user with administrator privilege can save the discovery settings.

To save the device discovery settings:

1. Select **Tools > Discovery Settings**. The Discovery Settings dialog box appears.
2. In the **Scan From** field, enter the starting IP Address of the range in which you want to discover devices.
3. In the **Scan To** field, enter the last IP Address of the range in which you want to discover devices.
4. In the **Device Type** list, select the relevant check boxes adjacent to the devices for which you want to discover.
5. Click **Add**. The IP address range is listed in the Range Table. You can add multiple IP address ranges to the Range Table.
6. Click **Advanced** to set the advanced options. The Discovery Settings dialog box expands to display fields such as SNMP Version, Retries, SNMP Get Community, and SNMP Set Community. You can do the following:
 - a. In the **SNMP Version** drop-down list, select **snmpV1** or **snmpV2c** depending on the SNMP Version of the device you want to scan.
 - b. In the **Retries** field, click on the arrow buttons to increase or decrease the number of retries.
 - c. In the **SNMP Get Community** and **SNMP Set Community**, enter the SNMP community strings of the devices you want to scan for. You can enter multiple SNMP get community strings separated with commas.

NOTE. *The SNMP Community strings are alphanumeric and the maximum allowed size is 32 characters.*

7. Click **Close** and the application displays a message “*Do you want to save the discovery settings?*”. This message box is displayed only for those users who have Administrator privileges.
8. Select **Yes** to save the discovery settings.

The next time you open the Discovery Settings dialog box, the last saved settings are loaded.

Managing the User Accounts

The two types of user roles are - Administrator, and User. Only an administrator can manage other users and user profiles. This section describes how an administrator can add or modify a user account, and delete a user account. You can change your password even if you do not have administrator privilege.

Adding a User Account

Only a user with administrator privileges can add a user.

To add a user:

1. Select **Tools > User Management** to display the User Management window.

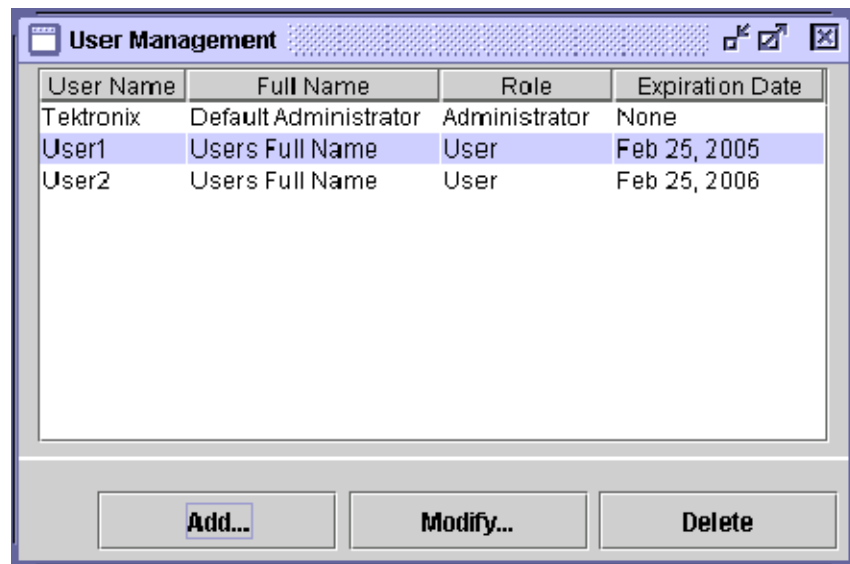
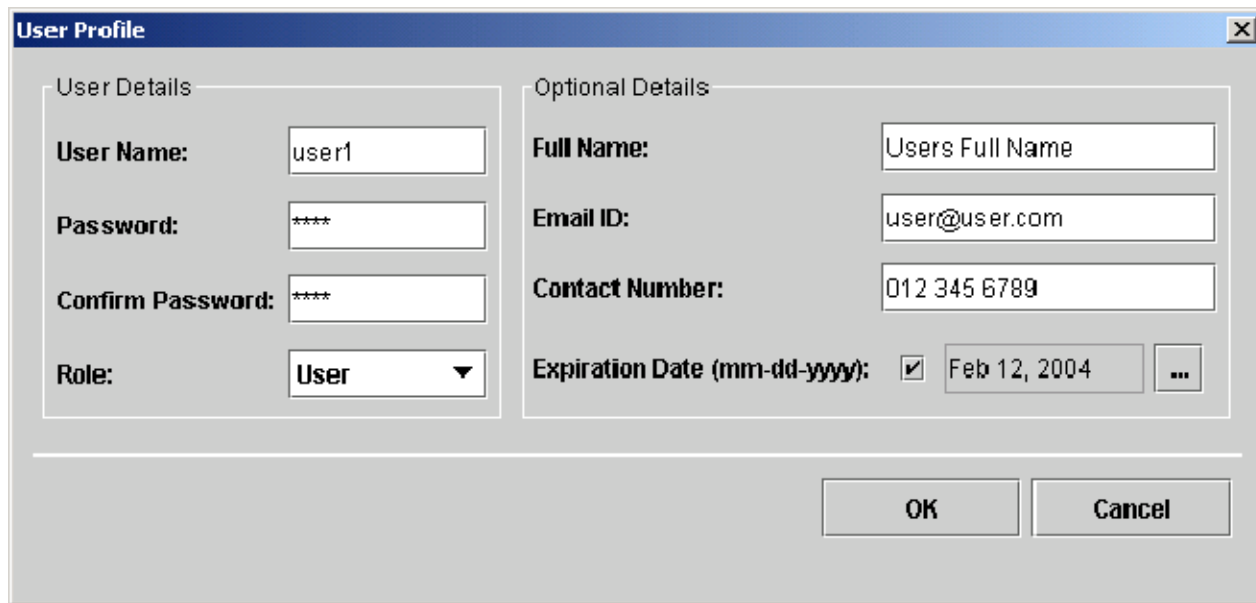


Figure 3-6: User Management window

2. Click **Add** to display the User Profile dialog box as shown in Figure 3-7.



The image shows a 'User Profile' dialog box with two main sections: 'User Details' and 'Optional Details'. The 'User Details' section includes fields for 'User Name' (containing 'user1'), 'Password' (containing '****'), 'Confirm Password' (containing '****'), and a 'Role' dropdown menu (set to 'User'). The 'Optional Details' section includes fields for 'Full Name' (containing 'Users Full Name'), 'Email ID' (containing 'user@user.com'), 'Contact Number' (containing '012 345 6789'), and 'Expiration Date (mm-dd-yyyy)' (checked, containing 'Feb 12, 2004' with a calendar icon). At the bottom right are 'OK' and 'Cancel' buttons.

Figure 3-7: User Profile dialog box

3. In the User Profile dialog box, do the following:
 - a. Enter the user name in the **User Name** field.
 - b. Enter the password and confirm the password in the **Password** and **Confirm Password** fields.
 - c. Select either User or Administrator in the **Role** drop-down list.
 - d. Enter the user's name in the **Full Name** field.
 - e. Enter the email ID in the **Email ID** field.
 - f. Enter the phone number in the **Contact Number** field.

- g. Select the **Expiration Date (mm-dd-yyyy)** check box and click on ... to select the Expiration date. The *Choose a date* dialog box appears as shown in Figure 3-8.

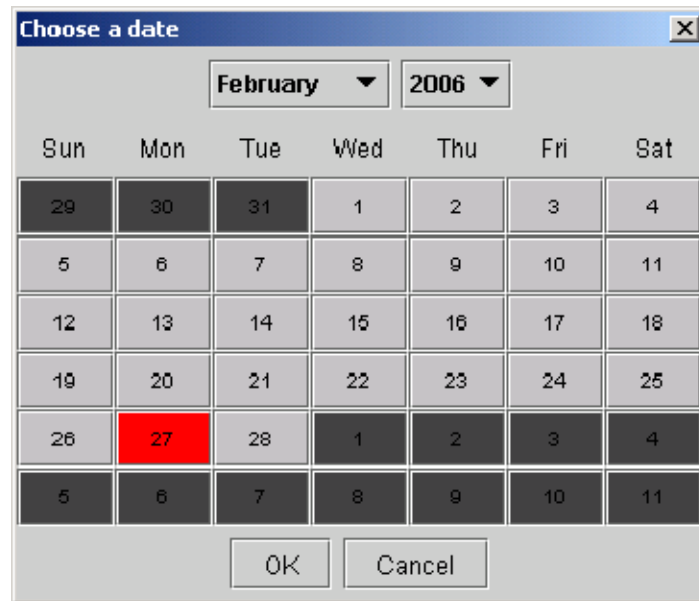


Figure 3-8: Choose a date dialog box

- h. Use the drop-down lists to change the month and the year.
- i. Select a day and click **OK**.
4. Click **OK** to add the user.

Modifying a User Profile

Only a user with administrator privileges can modify the profile of another user.

To modify a user profile:

1. Select **Tools > User Management** to display the User Management window.
2. Select the user profile that you want to modify.
3. Click **Modify** to display User Profile dialog box as shown in the Figure 3-7.
4. In the User Profile dialog box, modify the settings in the profile as needed.
5. Click **OK** to modify the user profile.

Changing Your Password

To change your password:

1. Select **Tools > Change Password** to display the Change Password dialog box as shown in Figure 3-9.



Figure 3-9: Change Password dialog box

2. In the **Old Password** field, enter the current password.
3. In the **New Password** and **Confirm Password** fields, enter the new password.
4. Click **OK**.

Changing the Password of Another User

Only a user with administrator privileges can change the password of another user. To change the password of another user:

1. Select **Tools > User Management** to display the User Management window.
2. Select the user profile whose password you want to change.
3. Click **Modify** and the application displays the User Profile dialog box as shown in the Figure 3-7.
4. Modify the password and confirm the password in the **Password** and **Confirm Password** fields.
5. Click **OK**.

Setting the Expiration Date

Only a user with administrator privilege can set or change the Expiration date for another user. You cannot set the Expiration date for the last administrator in the list.

To set the expiration date for another user:

1. Select **Tools > User Management** to display the User Management window.
2. Select the user profile whose expiration date you want to modify.
3. Click **Modify** and the application displays the User Profile dialog box as shown in the Figure 3-7.
 - a. Click on ... to select the expiration date. The *Choose a date* dialog box appears as shown in the Figure 3-8.
 - b. Use the drop-down lists to change the month and the year.
 - c. Click **OK**.
4. Click **OK**.

Changing the Role of a User

Only a user with administrator privileges can change the role of another user.

To change the role of another user:

1. Select **Tools > User Management** to display the User Management window.
2. Select the user profile that you want to modify the role.
3. Click **Modify** and the application displays the User Profile dialog box as shown in the Figure 3-7.
4. Select either User or Administrator in the **Role** drop-down list.
5. Click **OK**.

Removing a User

Only a user with administrator privileges can remove another user.

To remove a user:

1. Select **Tools > User Management** to display the User Management window.
2. Select the user profile that you want to delete.

3. Click **Delete** and the application displays a message confirming your deletion.
4. Click **OK**.

Removing an Administrator

Only a user with administrator privileges can remove another administrator. You cannot remove the only remaining administrator in the list.

To remove an administrator:

1. Select **Tools > User Management** to display the User Management window.
2. Select the administrator's user profile that you want to delete.
3. Click **Delete** and the application displays a message confirming your deletion.
4. Click **OK**.

Managing the Event Logs

This section explains how to export, remove, or set up an event log. The Event Log is actually a collection of several files. You can set the maximum size for the event log files to ensure that the total file size does not exceed the defined limit. If the total file size exceeds the defined limit, the application deletes the older files as required to ensure the total file size does not exceed the defined limit.

Exporting an Event Log

You can export an Event log to a CSV (Comma delimited) format file. The CSV (Comma delimited) file format saves only the text and values separated by commas, and each row of data ends in a carriage return. To export an event log:

1. Select **View > Event Viewer**. The Event Viewer window opens in the MLM1000 Desktop and the Event Viewer dynamic menu appears in the menu bar. Figure 3-10 shows the Event Viewer window.

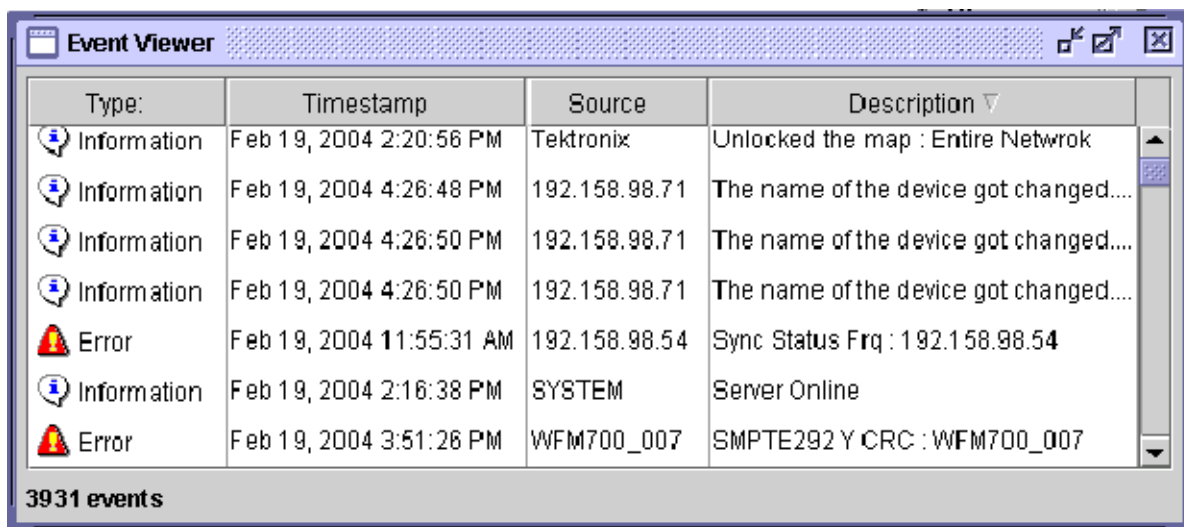


Figure 3-10: Event Viewer window

2. Select **Event Viewer > Export**. The Save As dialog box appears.
3. Select the path and enter a unique name for the event log.
4. Click **Save**. The event log is saved in CSV format. You can open CSV format files in Microsoft Excel, Wordpad, or any other editor.

Removing Event Logs

To remove an event log:

1. Select **View > Event Viewer**. The Event Viewer window opens in the MLM1000 Desktop and the Event Viewer dynamic menu appears.
2. To remove all the event logs, select **Event Viewer > Remove All**. A message *“Do you want to remove the logs?”* appears to confirm the deletion.
3. Select **OK**. The application removes all the logs in the Event Viewer.

Setting the Maximum Event Log Size

You can set up the event log size within the range of 1 MB to 1024 MB. You can also set up the event log size for each device within the acceptable range of 1 MB to 1024 MB. The default log size is 1 MB.

To set up an event log size:

1. Select **Tools > Options** to display the Options dialog box as shown in Figure 3-11.

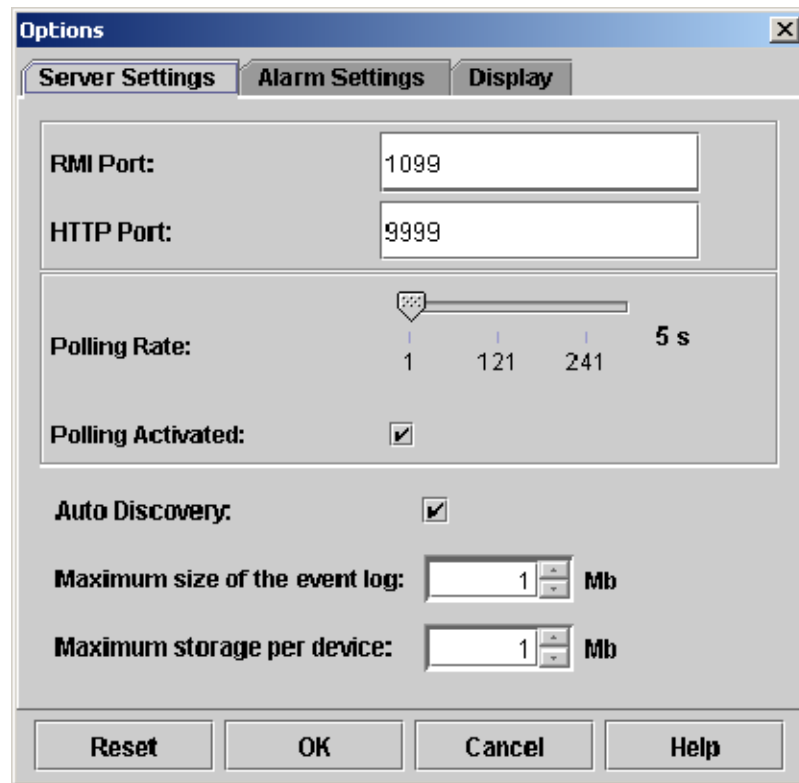


Figure 3-11: Server Settings tab of Options dialog box

2. Select the **Server Settings** tab.
3. In the **Maximum Size of the event log** field, type a value or select a value from the spin box. This value sets the maximum limit of the log file in Megabytes.
4. In the **Maximum Storage per device** field, type a value or select a value from the spin box. This value sets the maximum limit of the log file for each device in Megabytes.
5. Select **OK**. The application sets the specified event log size.

To set the values to their defaults, click **Reset**.

Managing the Application User Interface

This section explains how to show or hide the different views on the desktop and how to arrange windows.

- Select **View > New Devices** to show or hide the New Devices window.
- Select **View > Hotspot Tree** to show or hide the Hotspot Tree.
- Select **View > Hotspot Preview** to show or hide the Hotspot Preview.
- Select **View > Event Viewer** to show or hide the Event Viewer window.
- To arrange all open windows in the MLM1000 Desktop, click **Window > Cascade Windows**, or **Window > Tile Windows**.
- To jump to another window, click **Window** and select that window in the list.

Managing the Alarms

This section explains what each hotspot color means, how to acknowledge alarms, and set alarm properties.

The following table describes what each hotspot color means.

Table 3-1: Color representation

Hotspot	Color	Description
Map	Red	Alarms are occurring now on one or more devices.
Map	Yellow	Alarms have occurred in the past on one or more devices.
Map	Green	No device is currently indicating an alarm.
Map	White	No devices are being monitored.
Device	Red	An alarm is occurring now on the device.
Device	Yellow	Alarms have occurred in the past on the device.
Device	Green	No alarms have occurred on the device or the alarms have been acknowledged.
Device	Grey	The device is down.
Device	White	The device is not being monitored.

Acknowledging Alarms

You can acknowledge the alarms to indicate that you have viewed the event log of the device. You can acknowledge alarms for a particular device or a map, only if the hotspot is displayed in Yellow.

To acknowledge alarms:

1. Ensure that the cursor in the Hotspot tree is on a device or a map that you want to acknowledge alarms.
2. Select **Hotspots > Acknowledge Alarms** or right-click on the hotspot and from the context menu select **Acknowledge Alarms**.

The hotspot state is represented with green indicating that the alarms have been acknowledged.

Setting the Map Window to Pop Up on an Alarm

You can set the map window to pop up when one or more devices indicates an alarm in that map. To set a map window to pop up on alarm:

1. Select **Tools > Options** to display the Options dialog box.
2. Select the **Alarm Settings** tab and the Options dialog box appears as shown in Figure 3-12.

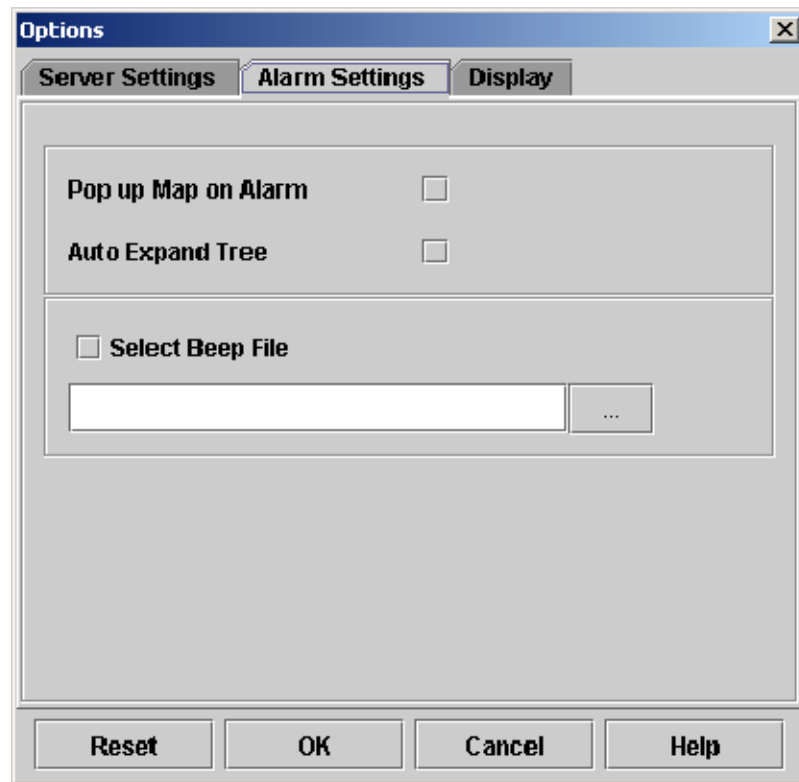


Figure 3- 12: Alarm Settings of Options dialog box

3. Select the **Pop up on alarm** check box and then click **OK**.

Setting Hotspot Tree to Expand on Alarm

To set the Hotspot Tree to expand when a device indicates an alarm:

1. Select **Tools > Options** to display the Options dialog box.
2. Select the **Alarm Settings** tab.
3. Select the **Auto Expand Tree** check box and then click **OK**.

Setting a Beep on Alarm for a Specific Device

To set the application to beep when a specific device indicates an alarm:

1. Ensure that the cursor in the Hotspot tree is on the device for which you want to set an alarm beep.
2. Select **Hotspots > Properties** or right-click on the device and select Properties from the context menu. The Properties dialog box appears as shown in Figure 3-13.

WFM700_19000 - Properties (unlocked)

Name: WFM700_19000 Type: WFM700
 IP Address: 122.123.124.125 Location:

Use Specific Icon

Action On Alarm
 Action On Alarm Recovery

User name:
 Password:

Monitored Enable all traps Beep on Alarm

Advanced <<

SNMP Version: snmpV1 Get Community: public
 Set Community: private Trap Community: trap community
 Retries: 3

OK Cancel

Figure 3-13: Device Properties dialog box

3. Select the **Beep on Alarm** check box and then click **OK**.

Setting an Action on Alarm for a Specific Device

To set the application to perform an action when a specific device indicates an alarm:

1. Ensure that the cursor in the Hotspot tree is on the device for which you want to set an alarm beep.
2. Select **Hotspots > Properties** or right-click on the device and select Properties from the context menu. The Properties dialog box appears as shown in Figure 3-13.
3. Click ... adjacent to the **Action on Alarm** field to browse for the application you want to run when a specific device indicates an alarm.
4. Click **OK**.

Setting an Action on Alarm Recovery for a Specific Device

To set the application to perform an action when a specific device indicates an alarm recovery:

1. Ensure that the cursor in the Hotspot tree is on the device for which you want to set an alarm beep.
2. Select **Hotspots > Properties** or right-click on the device and select Properties from the context menu. The Properties dialog box appears as shown in Figure 3-13.
3. Click ... adjacent to the **Action on Alarm Recovery** field to browse for the application you want to run when a specific device indicates an alarm recovery.
4. Click **OK**.

Changing the Alarm Indicator Sound

To set the sound to indicate an alarm:

1. Select **Tools > Options** to display the Options dialog box.
2. Select the **Alarm Settings** tab.
3. Select the **Select Beep File** check box and then click ... to display the Open dialog box.
4. Select an audio file in .wav file format and then click **Open**.
5. Click **OK**.

Viewing an Alarm Occurrence Graph

An Alarm Occurrence Graph displays the time of occurrence for each of the alarms for the selected device. To view the Alarm Occurrence Graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose occurrence graph you want to view.
2. Select **Hotspots > Alarm Occurrence** or right-click on the device and select Alarm Occurrence from the context menu. Figure 3-14 shows the Alarm Occurrence Graph window.

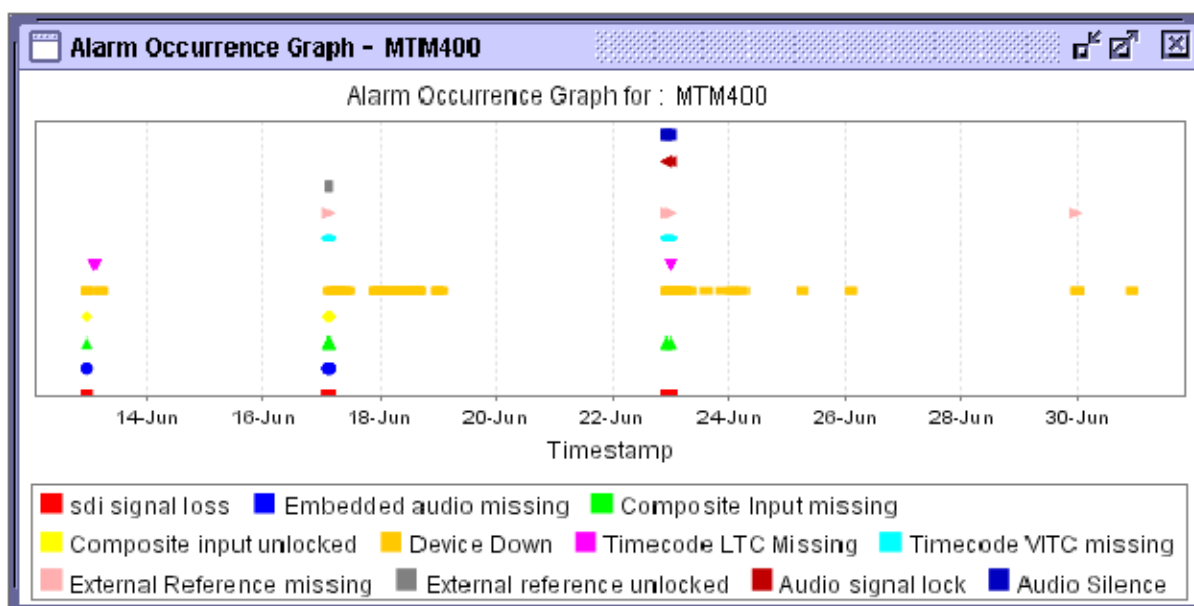


Figure 3-14: Alarm Occurrence Graph window

Setting the Legend Properties for the Alarm Occurrence Graph

To set the legend properties of the Alarm Occurrence Graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose occurrence graph you want to view.
2. Select **Hotspots > Alarm Occurrence** or right-click on the device and select Alarm Occurrence from the context menu. The Alarm Occurrence Graph window appears.

3. To modify the chart properties, right-click on Alarm Occurrence Graph and select **Properties** from the context menu. The Chart Properties dialog box appears.
4. Select the **Legend** tab to display the Chart Properties dialog box as shown in Figure 3-15.

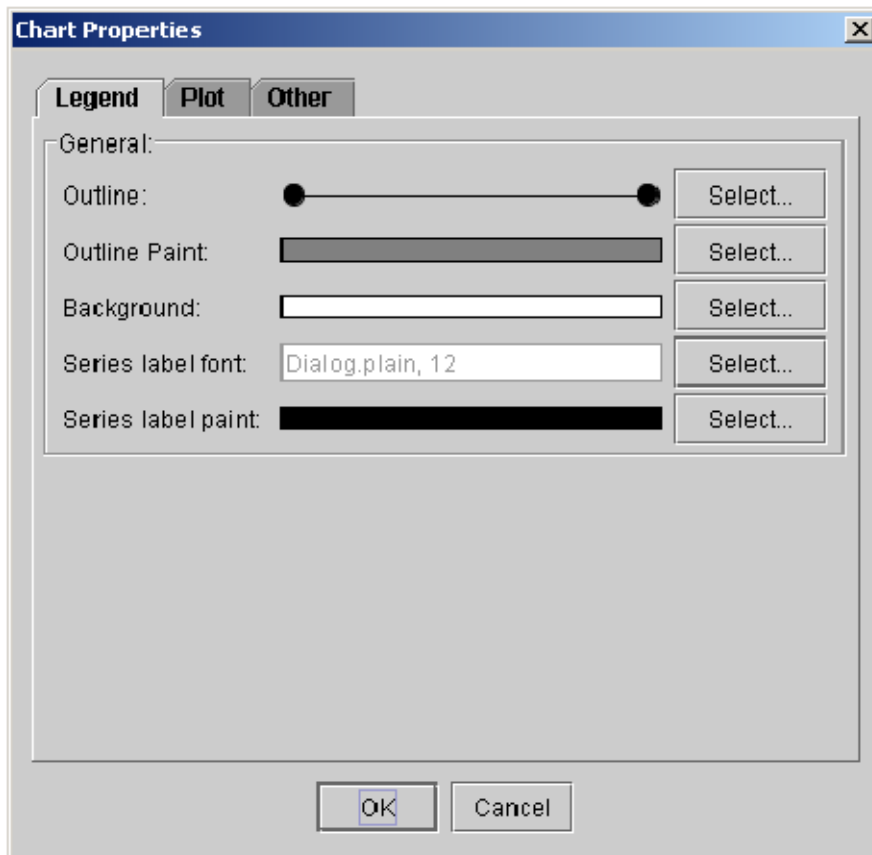


Figure 3- 15: Legend tab of Alarm Occurrence graph

5. Click **Select** adjacent to the **Outline** field to display the Pen/Stroke Selection dialog box as shown in Figure 3-16.

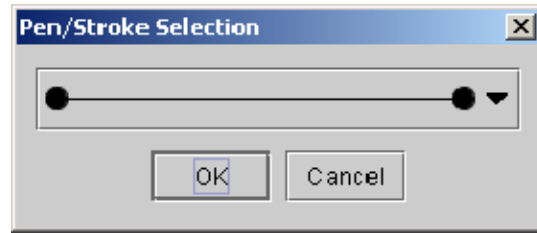


Figure 3-16: Pen/Stroke Selection dialog box

- Select the pattern of the line in the drop-down list and click **OK**.
6. Click **Select** adjacent to the **Outline Paint** field to display the **Outline Color** dialog box as shown in Figure 3-17.

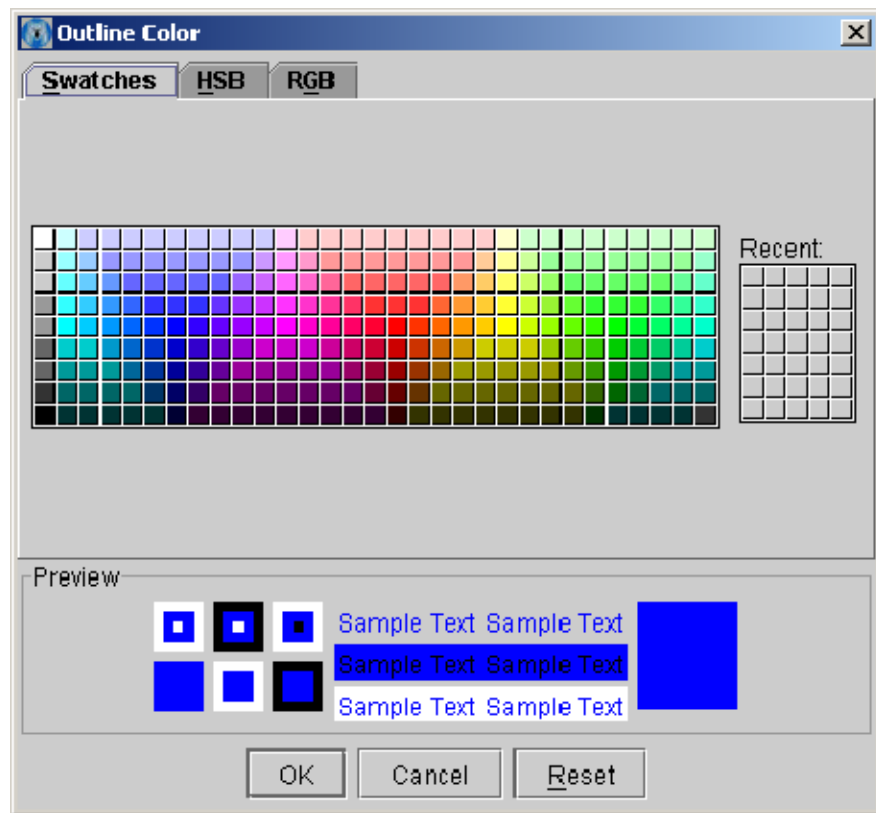


Figure 3-17: Outline Color dialog box

- Select a color in the **Swatches** tab, or
 - In the **HSB** tab, enter the H, S, and B values for the color, or
 - In the **RGB** tab, select the R, G, and B values for the color in the relevant spin box.
7. Click **OK** to set the legend properties.

You can select **Reset** to set the default legend properties.

Setting Up Plot Properties for Alarm Occurrence Graph

To set the plot properties of the Alarm Occurrence Graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose occurrence graph you want to view.
2. Select **Hotspots > Alarm Occurrence** or right-click on the device and select **Alarm Occurrence** from the context menu. The Alarm Occurrence Graph window appears.
3. To modify the plot properties, right-click on the Alarm Occurrence Graph and select **Properties** from the context menu.
4. Select the **Plot** tab to display the Chart Properties dialog box as shown in Figure 3-18.

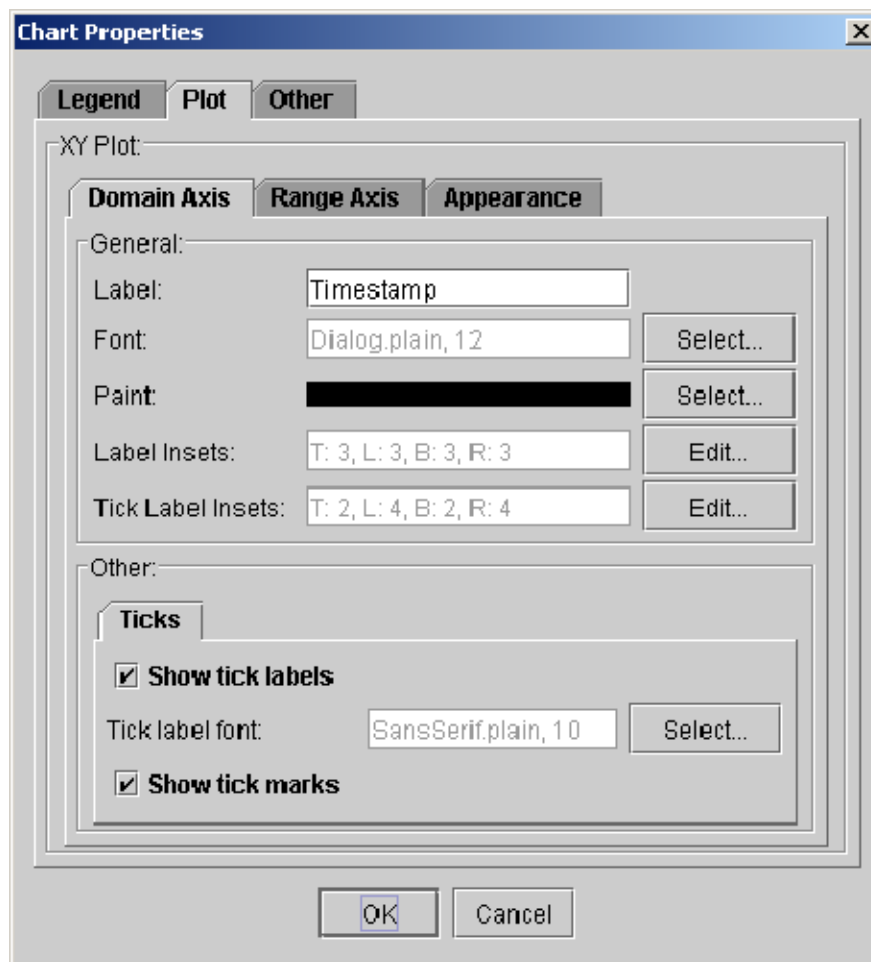


Figure 3-18: Plot properties tab of Alarm Occurrence graph

5. In the Domain Axis tab, do the following:
 - a. Enter the label name in the **Label** field.
 - b. Click **Select** adjacent to the **Font** field to select a font and font size for the domain axis label.
 - c. Click **Select** adjacent to the **Paint** field to select a color for the domain axis label. The Label Color dialog box is similar to the Outline Color dialog box. For information see *Setting the Legend Properties for Alarm Occurrence Graph* on page 3-37.
 - d. Select **Edit** adjacent to the **Label Insets** field to set the domain axis label insets at the top, left, bottom, and right. The Edit Insets dialog box appears as shown in Figure 3-19.

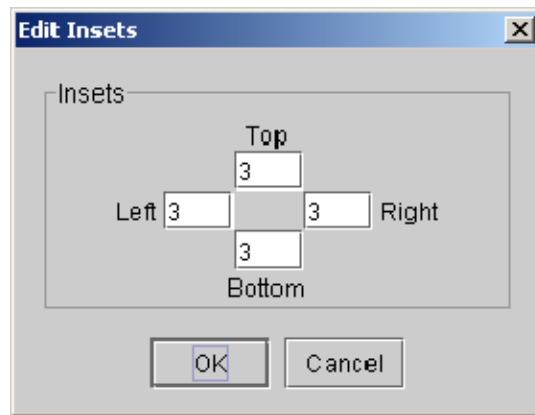


Figure 3- 19: Edit Insets dialog box

- e. Enter the inset value in the Top, Left, Bottom, and Right fields.
 - f. Click **OK**.
 - g. Select **Edit** adjacent to the **Tick Label Insets** field to set the tick label insets at the top, left, bottom, and right. The Edit Insets dialog box appears.
 - h. Enter the tick label inset value in the Top, Left, Bottom, and Right fields.
 - i. Click **OK**.
 - j. Select the **Show tick labels** check box and click **Select** adjacent to the **Tick label font** field to select the font and font size for the tick labels.
 - k. Select the **Show tick marks** check box to show the tick marks on the domain axis.
6. In the Range Axis tab of XY Plot, do the following:
 - a. Enter the label name in the **Label** field.
 - b. Click **Select** adjacent to the **Font** field to select a font and font size for the range axis label.
 - c. Click **Select** adjacent to the **Paint** field to select a color for the range axis label. The Label Color dialog box is similar to the Outline Color dialog box. For information on using this dialog box, see *Setting the Legend Properties for Alarm Occurrence Graph* on page 3-37.
 - d. Select **Edit** adjacent to the **Label Insets** field to set the label insets at the top, left, bottom, and right. The Edit Insets dialog box appears.

- e. Enter the inset value in the Top, Left, Bottom, and Right fields.
- f. Click **OK**.
- g. Select **Edit** adjacent to the **Tick Label Insets** field to set the tick label insets at the top, left, bottom, and right. The Edit Insets dialog box appears.
- h. Enter the tick label inset value in the Top, Left, Bottom, and Right fields.
- i. Click **OK**.
- j. Select the **Show tick labels** check box and click **Select** adjacent to the **Tick label font** field to select the font and font size for the tick labels.
- k. Select **Show tick marks** check box to show the tick marks on the range axis.
- l. Click the **Ranges** tab and do one of the following:
 - Select the **Auto-adjust range** check box to automatically adjust the range.
 - Enter the minimum and maximum range values in the **Minimum range value** field and the **Maximum range value** field.

NOTE. *Selecting the **Auto-adjust range** check box disables the **Minimum range value** and **Maximum range value** fields.*

7. In the Appearance tab of XY Plot, do the following:
 - Select **Edit** adjacent to the **Insets** field to set the insets at the top, left, bottom, and right. The Edit Insets dialog box appears.
 - Click **Select** adjacent to the **Outline stroke** field to display the Pen/Stroke Selection dialog box.
 - Select the outlines in the drop-down list and click **OK**.
 - Click **Select** adjacent to the **Outline Paint** field to select a color for the outline. The Outline Color dialog box appears. For information on using this dialog box, see *Setting the Legend Properties for Alarm Occurrence Graph* on page 3-37.
8. Click **OK** to set the plot properties.
9. Select **Reset** to set the default plot properties.

Setting Up Other Properties for Alarm Occurrence Graph

To set the other properties of the Alarm Occurrence Graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Occurrence** or right-click on the device and select **Alarm Occurrence** from the context menu. The Alarm Occurrence Graph window appears.
3. To modify other properties, right-click on the Alarm Occurrence Graph and select **Properties** from the context menu.
4. Select the **Other** tab to display the Chart Properties dialog box as shown in Figure 3-20.

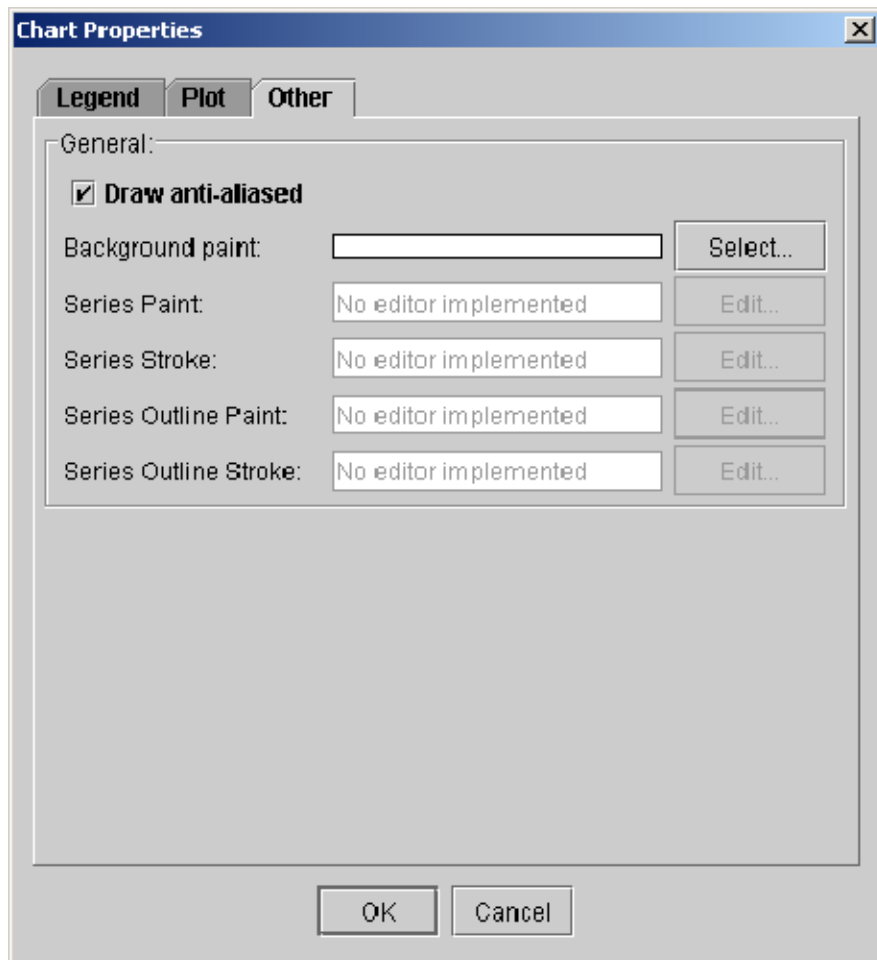


Figure 3-20: Other tab of Alarm Occurrence graph

5. Select the **Draw anti-aliased** check box.
6. Click **Select** adjacent to the **Background Paint** field to select the background color for the Alarm Occurrence Graph. The Background color dialog box appears similar to the Outline Color dialog box. For more information on using this dialog box, *Setting Up Legend Properties for Alarm Occurrence Graph* on page 3-37.
7. Click **OK**.

Saving an Alarm Occurrence Graph

To save an Alarm Occurrence Graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Occurrence** or right-click on the device and select Alarm Occurrence from the context menu. The Alarm Occurrence Graph window appears.
3. Right-click on Alarm Occurrence Graph and select **Save As** from the context menu. The Save As dialog box appears.
4. Enter the file name and select the path where you want to save the graph.
5. Click **Save**. You can save the Alarm Occurrence Graph only in PNG file format.

Printing an Alarm Occurrence Graph

To print an Alarm Occurrence Graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Occurrence** or right-click on the device and select Alarm Occurrence from the context menu. The Alarm Occurrence Graph window appears.
3. Right-click on Alarm Occurrence Graph and select **Print** from the context menu. The Page Setup dialog box appears.
4. Specify the paper size, paper source, orientation and the margins.
5. Click **OK** to print to the default printer.
6. Select **Printer** to change the printer and then click **OK** to print.

Zooming In and Out

To zoom in and out on the Alarm Occurrence Graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Occurrence** or right-click on the device and select Alarm Occurrence from the context menu. The Alarm Occurrence Graph window appears.
3. Right-click on Alarm Occurrence Graph and select **Zoom in** or **Zoom out** from the context menu. You can zoom in or zoom out along the vertical and horizontal axes.

Viewing an Alarm Distribution Graph

An alarm distribution graph displays a pie chart distribution of all the alarms for the selected device. To view the alarm distribution graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Distribution** or right-click on the device and select Alarm Distribution from the context menu. The Alarm Distribution Graph window appears as shown in Figure 3-21.

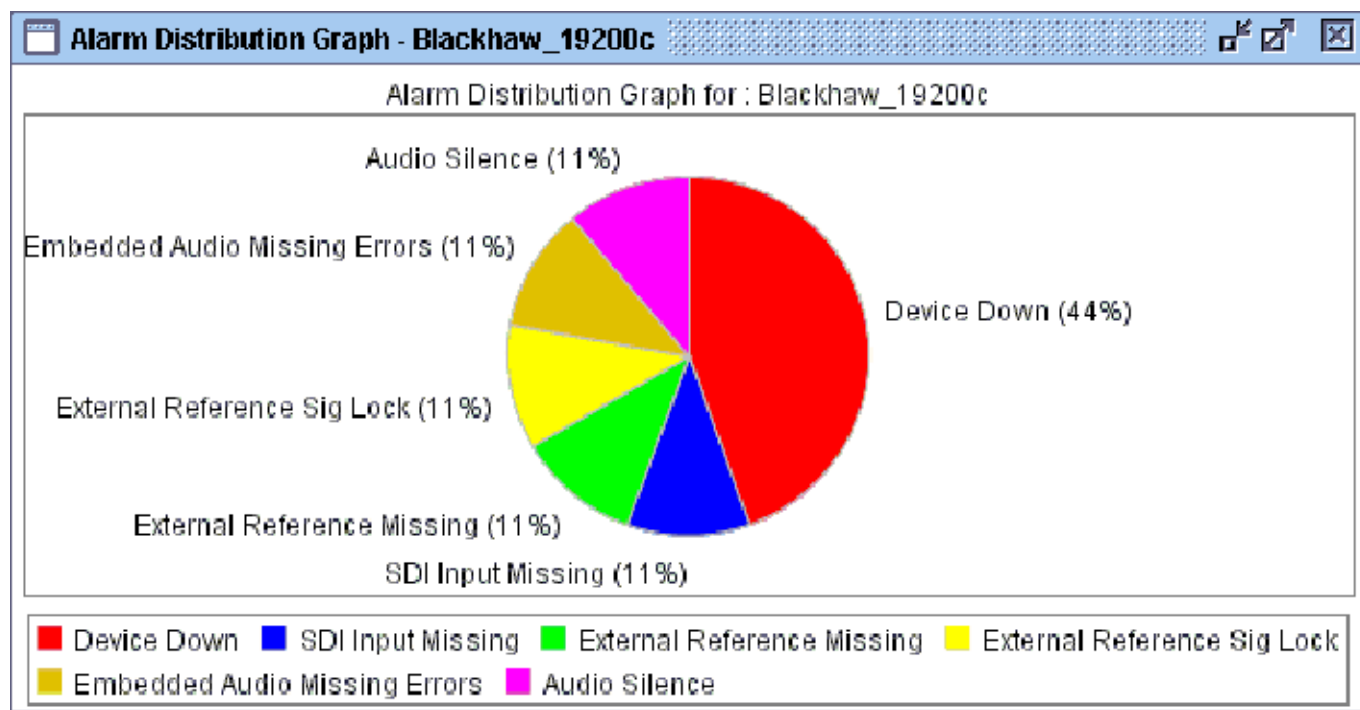


Figure 3-21: Alarm Distribution Graph window

Setting the Legend Properties for the Alarm Distribution Graph

To set the legend properties of the alarm distribution graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Distribution** or right-click on the device and select Alarm Distribution from the context menu. The Alarm Distribution Graph window appears.
3. To modify the chart properties, right-click on Alarm Distribution Graph and select **Properties** from the context menu.
4. Select the **Legend** tab to display the Chart Properties dialog box as shown in Figure 3-22.

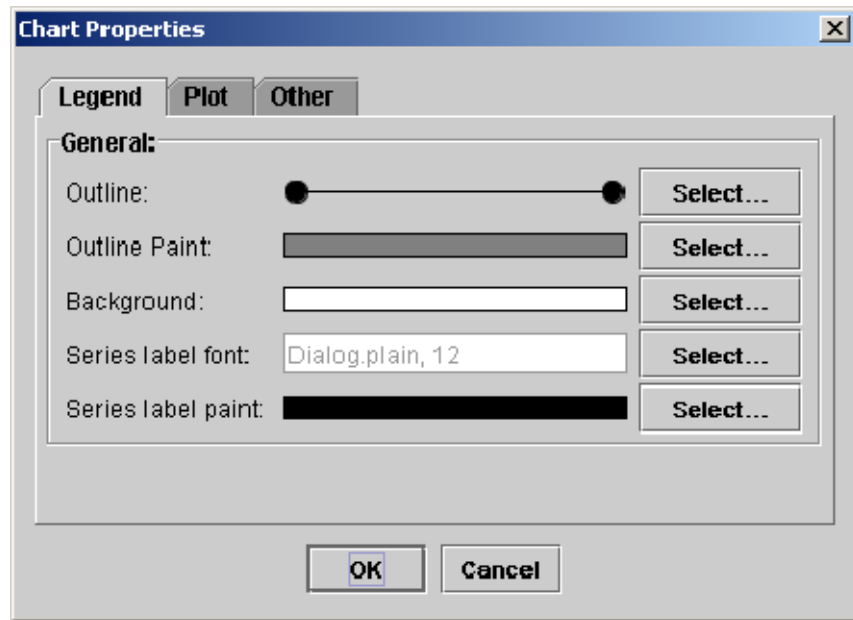


Figure 3-22: Legend tab of Chart Properties dialog box

5. Click **Select** adjacent to the **Outline** field to display Pen/Stroke Selection dialog box. Select the outlines in the drop-down list and click **OK**.
6. Click **Select** adjacent to the **Outline Paint** field to display the **Outline Color** dialog box.
7. Select a color in the **Swatches** tab and do one of the following:
 - In the **HSB** tab, enter the H, S, and B values for the color.
 - In the **RGB** tab, select the R, G, and B values for the color in the relevant spin box.
8. Click **OK** to set the legend properties.
9. Select **Reset** to set the default legend properties.

Setting the Plot Properties for the Alarm Distribution Graph

To set the plot properties of the alarm distribution graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.

2. Select **Hotspots > Alarm Distribution** or right-click on the device and select Alarm Distribution from the context menu. The Alarm Distribution Graph window appears.
3. To modify the plot properties, right-click on Alarm Distribution Graph and select **Properties** from the context menu.
4. Select the **Plot** tab to display the Chart Properties dialog box as shown in Figure 3-23.

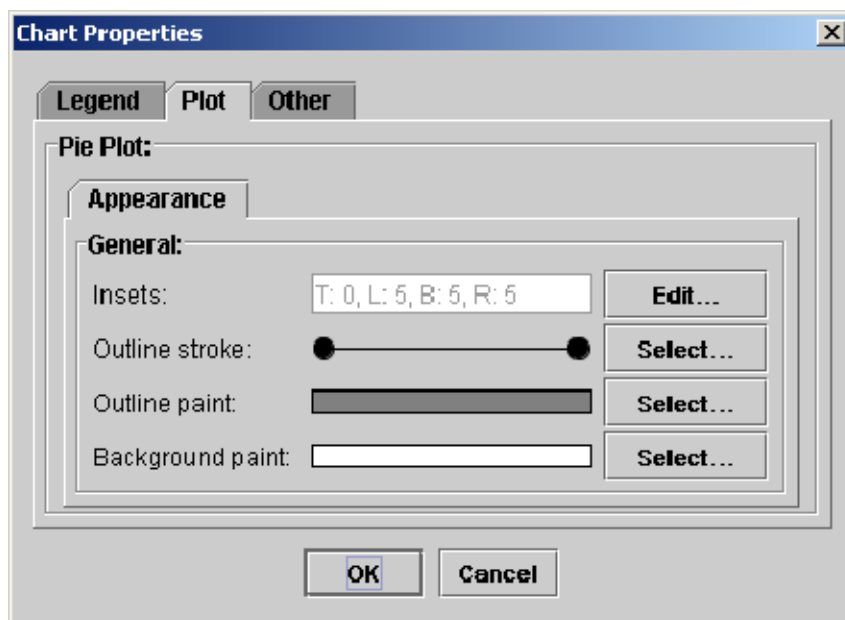


Figure 3-23: Plot properties tab of Chart Properties dialog box

5. In the Appearance tab, do the following:
 - a. Select **Edit** adjacent to the **Insets** field to set the insets at the top, left, bottom, and right. The Edit Insets dialog box appears.
 - b. Click **Select** adjacent to the **Outline stroke** field to display the Pen/Stroke Selection dialog box.
 - c. Select the outlines in the drop-down list and click **OK**.
 - d. Click **Select** adjacent to the **Outline Paint** field to select a color for the outline. The Outline Color dialog box appears. For information on using this dialog box, see *Setting Up Legend Properties for Alarm Occurrence Graph* on page 3-37.

- e. Click **Select** adjacent to the **Background Paint** field to select the background color for the alarm distribution graph. The Background color dialog box appears similar to the Outline Color dialog box. For more information on using this dialog box, see *Setting Up Legend Properties for Alarm Occurrence Graph* on page 3-37.
6. Click **OK** to set the plot properties.
7. Select **Reset** to set the default plot properties.

Setting Other Properties for the Alarm Distribution Graph

To set other properties of the Alarm Occurrence Graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Distribution** or right-click on the device and select Alarm Distribution from the context menu. The Alarm Distribution Graph window appears.
3. To modify the chart properties, right-click on Alarm Distribution Graph and select **Properties** from the context menu.
4. Select the **Other** tab to display the Chart Properties dialog box as shown in the next figure.

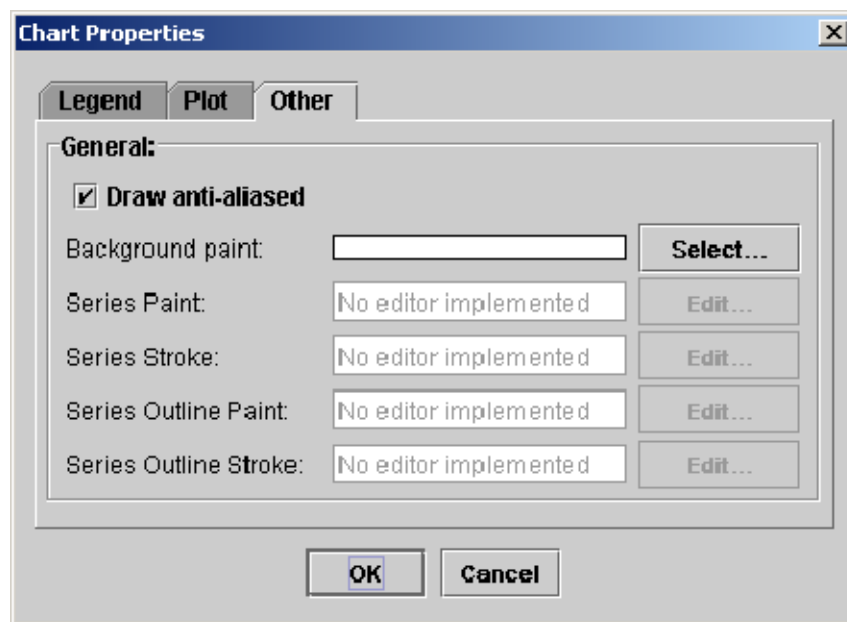


Figure 3-24: Other tab of Chart Properties dialog box

5. Select the **Draw anti-aliased** check box.
6. Click **Select** adjacent to the **Background Paint** field to select the background color for the alarm distribution graph. The Background color dialog box appears similar to the Outline Color dialog box. For more information on using this dialog box, see step 6 in *Setting Up Legend Properties for Alarm Occurrence Graph*.
7. Click **OK**.

Saving an Alarm Distribution Graph

To save an alarm distribution graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Distribution** or right-click on the device and select Alarm Distribution from the context menu. The Alarm Distribution Graph window appears.
3. To modify the chart properties, right-click on Alarm Distribution Graph and select **Properties** from the context menu.
4. Enter the file name and select the path where you want to save the graph.

5. Click **Save As**. You can save the alarm distribution graph only in PNG file format.

Printing an Alarm Distribution Graph

To print an alarm distribution graph:

1. Ensure that the cursor in the Hotspot tree is on the device whose alarm occurrence graph you want to view.
2. Select **Hotspots > Alarm Distribution** or right-click on the device and select Alarm Distribution from the context menu. The Alarm Distribution Graph window appears.
3. Right-click on Alarm Distribution Graph and select **Print** from the context menu. The Page Setup dialog box appears.
4. Specify the paper size, paper source, orientation and the margins.
5. Click **OK** to print to the default printer.
6. Select **Printer** to change the printer and then click **OK** to print.

Setting the Options

This section explains how to configure the server, alarm, and display settings. User options can be set only by an administrator.

Configuring Server Options

You can configure the server settings such as RMI Port, HTTP Port, Polling Rate, Auto Discovery, and so on. To configure the server options:

1. Select **Tools > Options** to display the Options Dialog Box.
2. Select the **Server Settings** tab and the Options Dialog Box appears as shown in Figure 3-25.

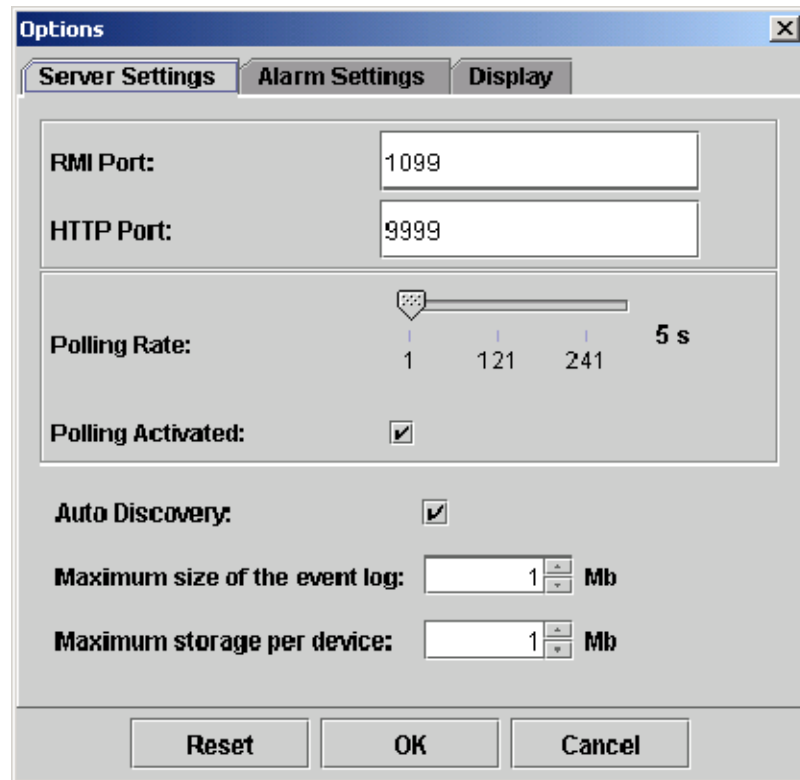


Figure 3-25: Server Settings tab of Options dialog box

3. In the RMI Port field, enter the RMI port number.

4. In the HTTP Port field, enter the HTTP port number.
5. For the Polling Rate slider, move the slider to the right to increase the polling rate in seconds. The range is 1 to 300 seconds. Depending on the network condition, the minimum polling rate changes.
6. Select or clear the **Polling Activated** check box to activate or deactivate the polling.
7. Select or clear the **Auto Discovery** check box to automatically or manually discover devices.
8. In the **Maximum size of the event log** spin box, select the event log size in megabytes. The range is 1 MB to 1024 MB. The default event log size is 1 MB.
9. In the **Maximum storage per device** spin box, select the storage size in megabytes. The range is 1 MB to 1024 MB. The default storage size is 1 MB.
10. Select **OK** to apply the settings.

Configuring Alarm Options

You can configure the alarm settings to sound the beep, and display the window in which the alarm occurred.

To configure the alarm options:

1. Select **Tools > Options** to display the Options Dialog Box.
2. Select the **Alarm Settings** tab and the Options Dialog Box dialog box appears as shown in Figure 3-26.

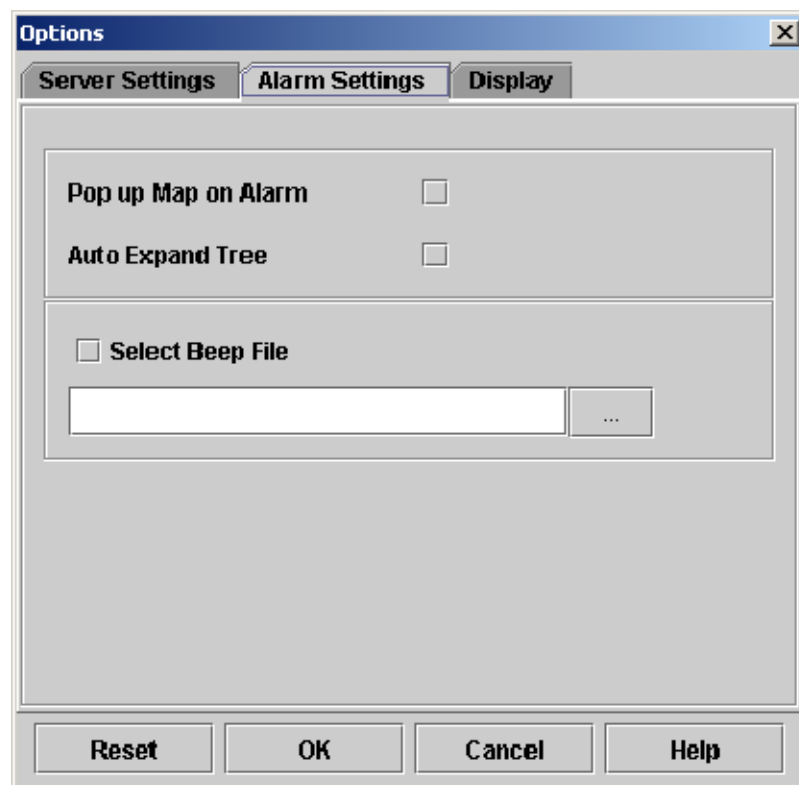


Figure 3-26: Alarm Settings tab of Options dialog box

3. Select the **Pop up Map on Alarm** check box to display the map window when an alarm occurs.
4. Select the **Auto Expand Tree** check box to automatically expand the Hotspot tree and locate the map with the alarm.

NOTE. Only an administrator can set a sound to indicate the alarm.

5. Select the **Select Beep File** check box to set a beep to indicate an alarm.
6. Select ... to browse for a beep file (.wav).

Configuring Display Options

To configure the display settings and language used for the application:

1. Select **Tools > Options** to display the Options Dialog Box.
2. Select the **Display** tab. The Options Dialog Box appears as shown in Figure 3-27.

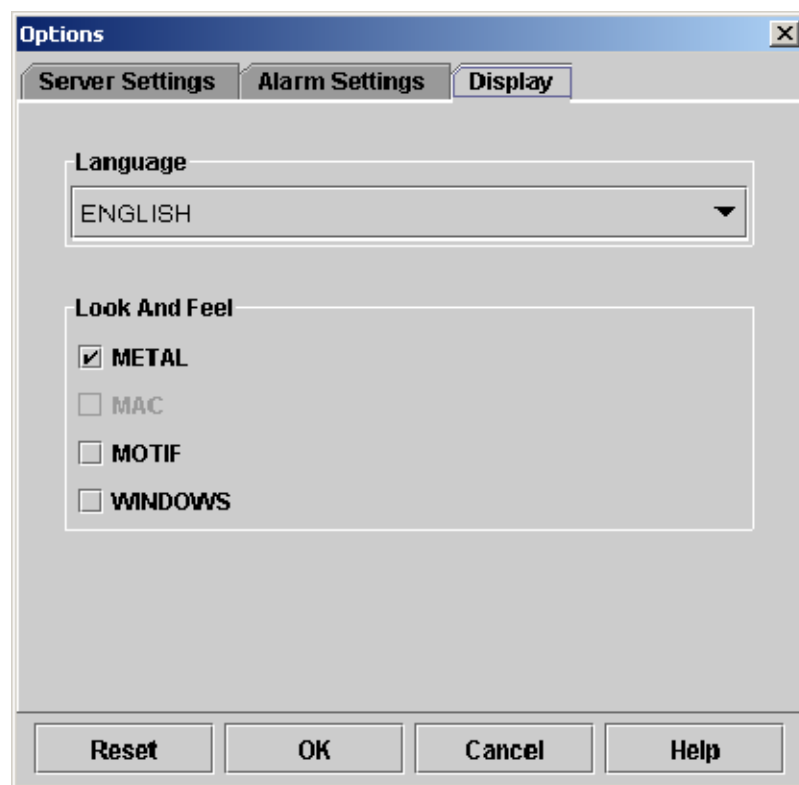


Figure 3-27: Display tab of Options dialog box

3. Select the user interface language in the **Language** drop-down list. The default is English.

4. Select the Look and Feel of the user interface - METAL, MAC, MOTIF, or WINDOWS.
5. Click **OK** to apply the display settings.

Resetting the Default Options

To reset the default options:

1. Select **Tools > Options** to display the Options Dialog Box.
2. Select **Reset** and then **OK**.

Generating the Reports

This section explains how to generate a report for the selected device, save a report in PDF format, export a report, and print a report.

To generate a report:

1. Place the cursor on the device that you want to generate a report for.
2. Select **Hotspots > Generate Report** or right-click and select **Generate Report** from the context menu. The Print Preview of the report appears as shown in Figure 3-28.

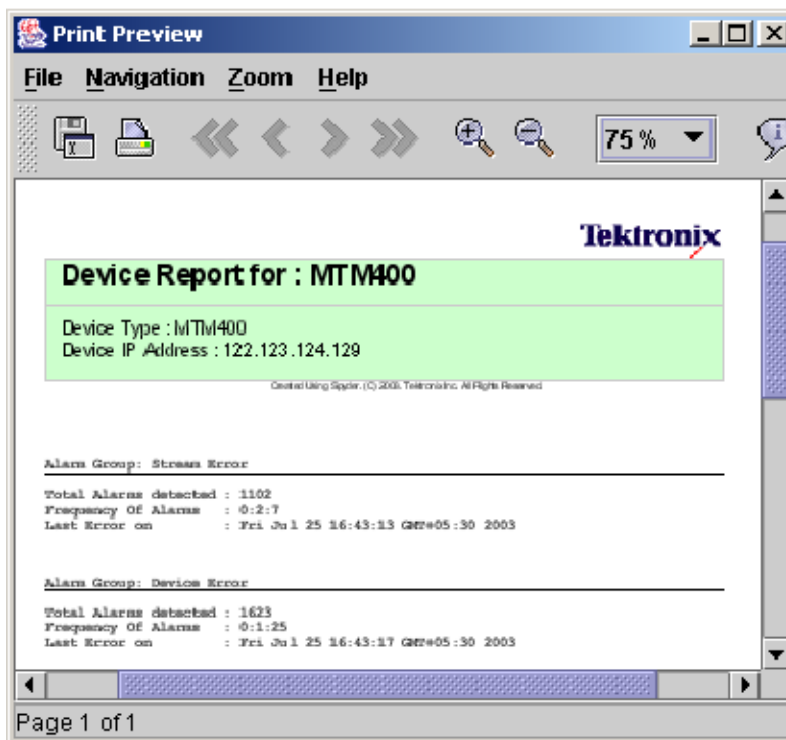


Figure 3-28: Report Preview

The report includes the following information:

- Device name, type, and IP Address
- Alarm groups based on the alarm type
- Each alarm group with total alarms detected, frequency of alarms, and the time when the last error occurred.

Saving Reports

You can save a report in either PDF format or text format. To save a report, you must first generate a report. The Print Preview window must be displayed to save a report.

To save a report in PDF format:

1. Select **File> Save as PDF** in the Print Preview window. The **Saving Report into a PDF file** dialog box appears as shown in Figure 3-29.

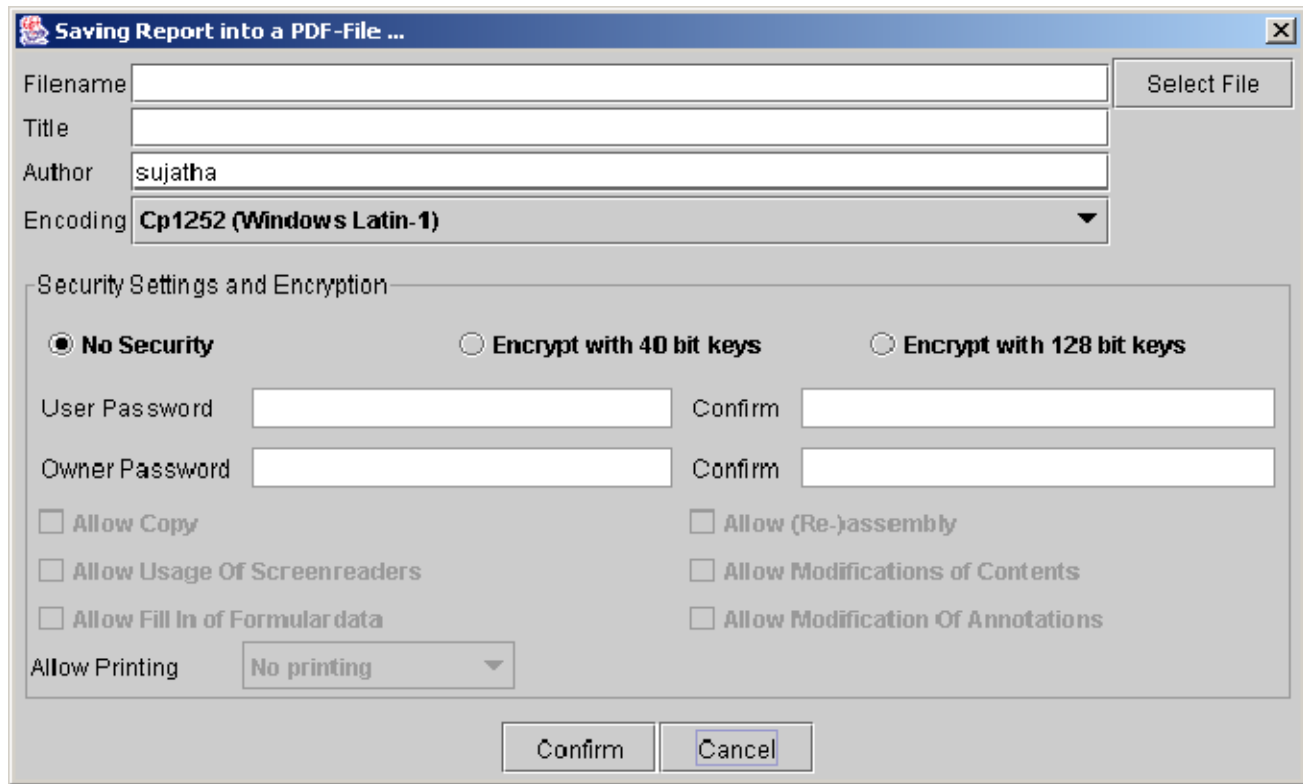


Figure 3-29: Saving Report into PDF file dialog box

2. Enter the filename in the **Filename** field and the title in the **Title** field.
3. Specify the author's name in the **Author** field. By default this field displays the user login name.
4. In the **Encoding** drop-down list, choose the type of encoding. The default type of encoding is **Cp1252 (Windows Latin-1)**.
5. In the Security Settings and Encryption group, select **No Security, Encrypt with 40 bit keys**, or **Encrypt with 180 bit keys** check box.
6. Enter the user and owner password and confirm it in the adjacent fields.
7. Select or deselect the **Allow Copy** check box to allow or not allow the user to copy the content from the PDF file.
8. If you have enabled encryption, follow these steps:
 - Select or deselect the **Allow Usage of Screenreaders** check box to allow or not allow the user to use the screen readers.
 - Select or deselect the **Allow Fill in of Formular data** check box to allow or not allow the user to fill the formulary data in the PDF file.
 - Select or deselect the **Allow (Re-)assembly** check box to allow or not allow the user to reassemble the contents of the report.
 - Select or deselect the **Allow Modifications of Contents** check box to allow or not allow the user to modify the content in the PDF file.
9. Select or deselect the **Allow Modification of Annotations** check box to allow or not allow the user to modify the annotations in the PDF file.
10. Select an option in the **Allow Printing** drop-down list to allow or not allow the user to print the PDF.
11. Click **Confirm** to save the report in PDF format.

To save a report in text format do the following:

1. Select **File> Save as PDF** in the Print Preview window. The **Saving report to a PDF file** dialog box appears as shown in Figure 3-30.

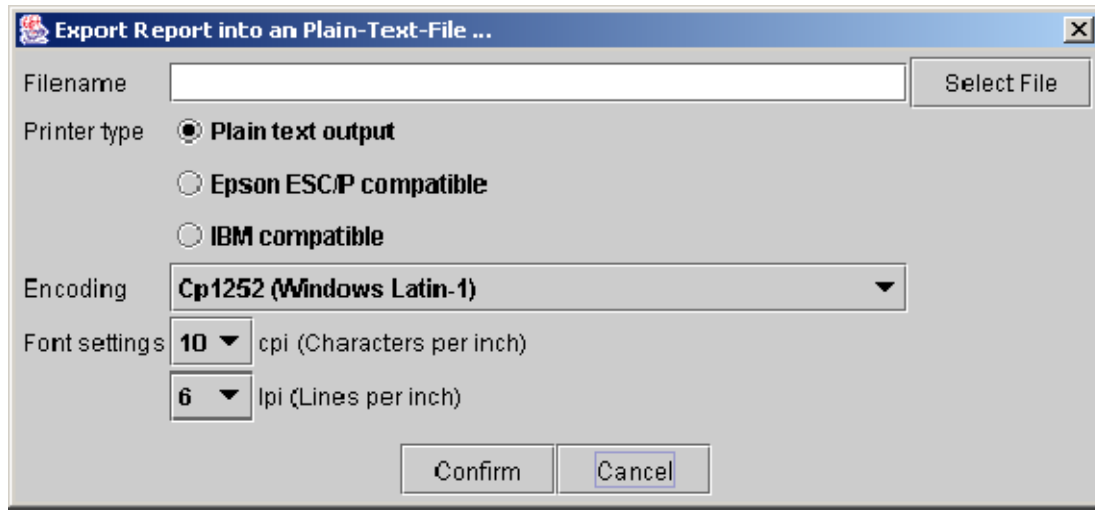


Figure 3-30: Export Report into a Plain Text File dialog box

2. Enter the filename in the **Filename** field.
3. Select the Printer type option as:
 - **Plain text output** to save the report in plain text format.
 - **Epson ESC/P compatible** to save the report in Epson compatible format.or
 - **IBM compatible** to save the report in IBM compatible format.
4. In the **Encoding** drop-down list, choose the type of encoding. The default type of encoding is **Cp1252 (Windows Latin-1)**.
5. In the **Font settings** drop-down lists, select the characters per inch and lines per inch values.
6. Click **Confirm** to save the report in the text format.

Exporting Reports

You can export the report in Microsoft Excel, HTML, and CSV format.

To export the report in Microsoft Excel format:

1. Select **File> Export as excel** in the Print Preview window. The **Export Report into an Excel File** dialog box appears as shown in Figure 3-31.

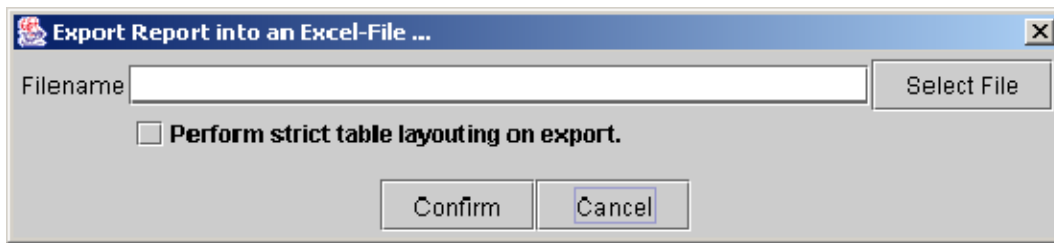


Figure 3-31: Export Report into an Excel File dialog box

2. Enter the filename in the **Filename** field.
3. Select or deselect the **Perform strict table layouting on export** check box to apply strict table layout to the report exported in Microsoft Excel format.
4. Click **Confirm** to export the report into Microsoft Excel format.

To export the report in HTML format, do the following:

1. Select **File > Export as html** in the Print Preview window. The **Export Report into an Html File** dialog box appears as shown in Figure 3-32.

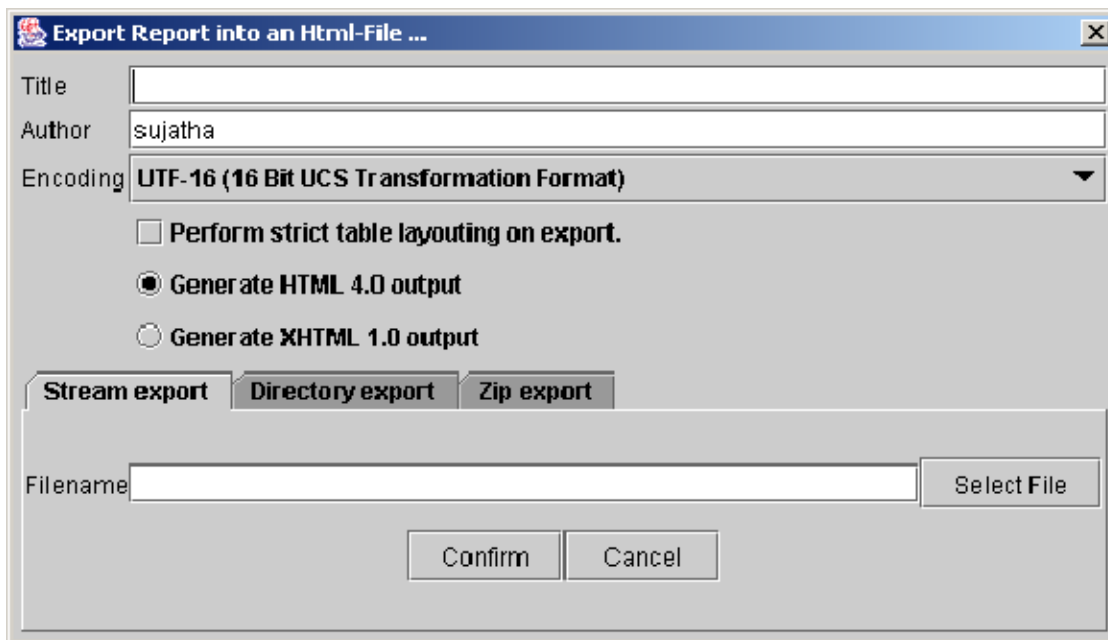


Figure 3-32: Export Report into an HTML File dialog box

2. Enter the filename in the **Filename** field.

3. Specify the author's name in the **Author** field. By default this field displays the login user name.
4. In the **Encoding** drop-down list, choose the type of encoding. The default type of encoding is **UTF-16 (16 Bit UCS Transformation Format)**.
5. Select or deselect the **Perform strict table layouting on export** check box to apply strict table layout to the report exported in HTML format.
6. Select either Generate HTML 4.0 output or Generate XHTML 1.0 output depending on the type of output you want to generate.
7. Select either the Stream export, Directory export, or Zip export tab and enter the Filename and Data Directory, if necessary.
8. Click **Confirm** to export the report into HTML format.

To export the report in CSV format, do the following:

1. Select **File> Export as CSV** in the Print Preview window. The **Export report into a CSV file** dialog box appears as shown in Figure 3-33.

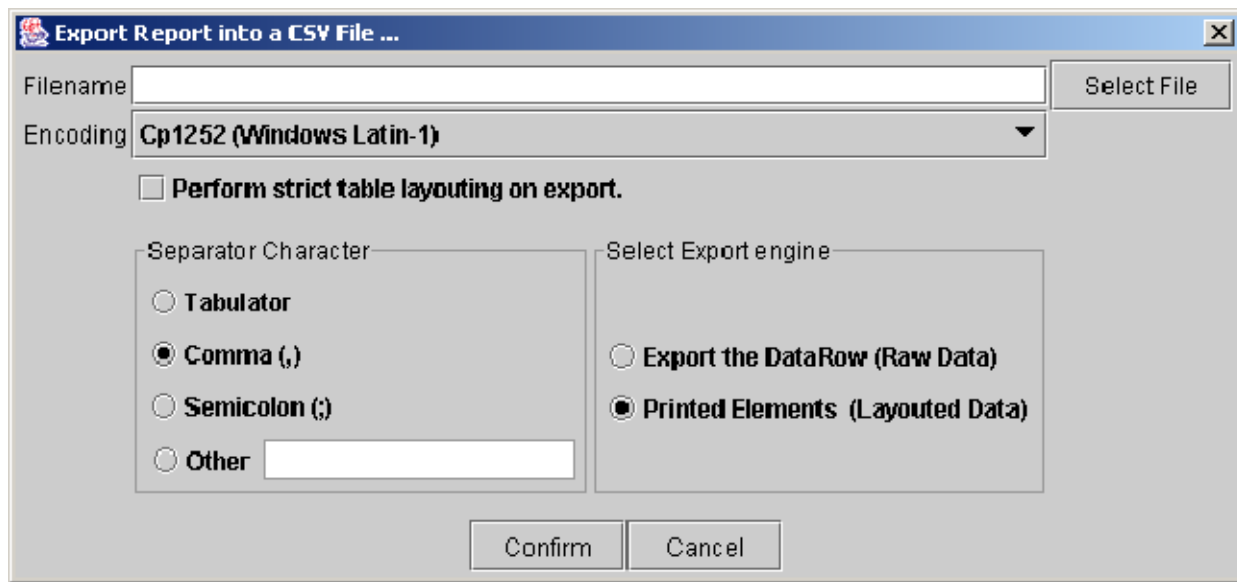


Figure 3-33: Export Report into a CSV File dialog box

2. Enter the filename in the **Filename** field.
3. In the **Encoding** drop-down list, choose the type of encoding. The default type of encoding is **Cp1252 (Windows Latin-1)**.

4. Select or deselect the **Perform strict table layouting on export** check box to apply strict table layout to the report exported in HTML format.
5. Select the **Separator Character** option as either Tabulator, Comma (,), Semicolon (;) or Other. If you select Other, enter the separator character in the adjacent field.
6. Select the **Select Export engine** option as either Export the DataRow (Raw Data) or Printed Elements (Laid out Data).
7. Click **Confirm** to export the report into CSV format.

Changing the Page Setup

You need to set the page size, orientation, and margins before printing the report. To change the page setup:

1. Select **File > Page Setup** in the Print Preview window. The **Page Setup** dialog box appears as shown in Figure 3-34.

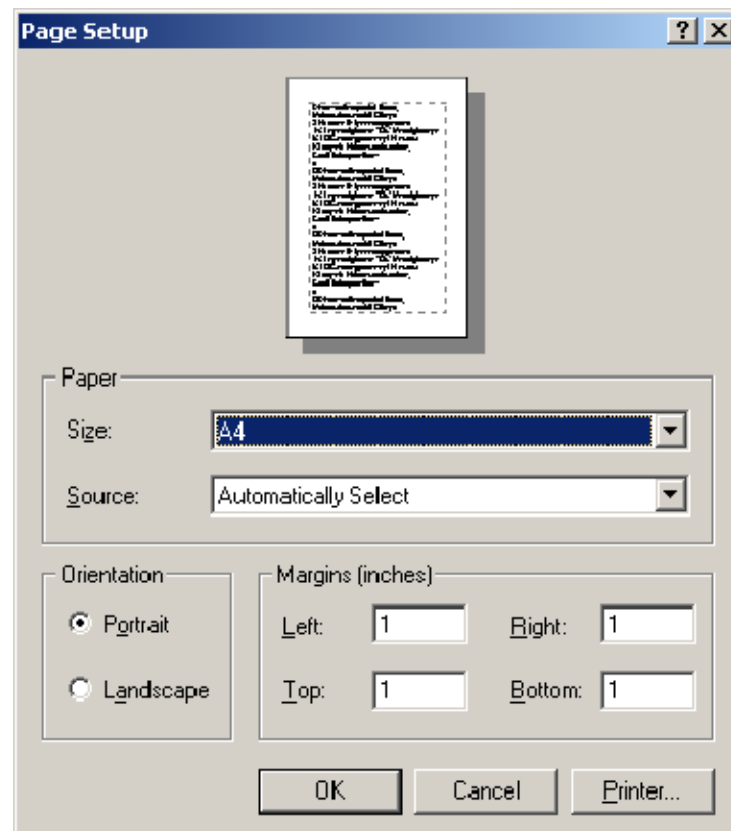


Figure 3-34: Page Setup dialog box

2. In the **Paper** group, select size and source from the Size and Source drop-down list.
3. In the **Orientation** group, select either Portrait or Landscape option.
4. In the **Margins** group, enter the left, right, top, and bottom margins in inches.
5. Select **OK** to apply the page setup.

Printing Reports

To print the report:

1. Select **File > Print** in the Print Preview window. The **Print** dialog box appears.
2. Select the printer on which you want to print the report.
3. Select the pages that you want to print and then select **OK**.

Navigating the Report

You can navigate the first page, last page, or any page in-between.

To navigate the report:

1. Select **Navigation > Go to page** and enter the page number to view a particular page directly.
2. Select **Navigation > Home** to view the first page.
3. Select **Navigation > End** to view the last page.
4. Select **Navigation > Back** to view the previous page.
5. Select **Navigation > Forward** to view the next page.

You can also use the toolbar buttons to navigate the report.

Zooming In or Out

You can zoom in or zoom out the report display by percentage, or by increasing or decreasing the zoom factor. You can select the zoom in, zoom out, and zoom % drop-down list in the toolbar to zoom.

You can also use the **Zoom** menu and select one of the percentages to zoom the display.



Appendices

Appendix A: Error Messages

This section lists error messages, their descriptions and possible solutions.

Table A- 1: Error messages

Error message	Description	Possible solution
Login error messages		
The URL entered is not in the correct format.	This error message appears if the specified MLM1000 Server URL format is incorrect.	Specify the correct MLM1000 Server URL in http://<MLM1000 Server>:<port number> format.
Unable to connect to Server. Check if the Server is online.	This error message appears if the MLM1000 Server is not online or not on the network.	Ensure that the MLM1000 Server is online and on the network.
Invalid username or password! Please try again.	This error message appears if the username or password is invalid.	Enter the correct username and password.
Server and Client versions do not match.	This error message appears if the Java Runtime Application installed on MLM1000 Server and Client are not the same version.	Ensure that the Java Runtime Application installed on MLM1000 Server and Client are the same version.
Login Failed.	This error message appears if both the user name and password are incorrect.	Specify the correct user name and password. Note that both the user name and password are case-insensitive.
<language> fonts not available.	This error message appears if the fonts for the designated language are not available.	Install the fonts for the supported characters.
Could not determine the Server version.	This error message appears if the application is unable to determine the MLM1000 Server version.	Ensure that the MLM1000 Server and Client versions are the same.
Could not determine the current user privileges.	This error message appears when the MLM1000 Server application installation is corrupted.	Restart the MLM1000 Server or reinstall the MLM1000 software.
Could not download supported device type list from Server.	This error message appears when the MLM1000 Server application installation is corrupted.	Restart the MLM1000 Server or reinstall the MLM1000 software.
Unable to get the beep file from Server.	This error message appears if the sound file is corrupted or not available.	Upload a new sound file.
Unable to get the sound file from Server.	This error message appears if the sound file is corrupted or not available.	Upload a new sound file.
Unable to get the default map icon name from Server.	This error message appears if the default map corrupted.	Reinstall the application.
Unable to get hotspot configuration from Server.	This error message appears if the map structure is not available.	Recreate the map structure.
Unable to get user settings from Server.	This error message appears if the MLM1000 Server is unable to retrieve the user settings.	Reinstall the application.
The user account is expired.	This error message appears if you login with an user account that has expired.	Contact your administrator to set the expiration date.

Table A-1: Error messages (Cont.)

Error message	Description	Possible solution
Discovery error messages		
Invalid IP Address.	This error message appears if the IP Address format is incorrect.	Ensure that the IP Address is in XXX.XXX.XXX.XXX format.
Can not scan backwards (“To” should be larger than “From” address).	This error message appears if the From IP Address is larger than To IP Address. You cannot scan backwards. For example, you cannot scan from 122.123.124.125 to 122.123.124.120.	Ensure that the From IP Address is not larger than the To IP Address.
Specify “From” value for the Scan Range.	This error message appears if you do not specify the From IP Address.	Ensure that you specify the From IP Address. If you do not specify the To IP Address, the application scans for only that IP Address that is entered in the From IP Address field.
The entered range already exists.	This error message appears if the From IP Address and the To IP Address matches the range that already exists.	Enter an IP Address range that is different than from the existing range.
Retries should be an integer between 1 and 10.	This error message appears if the value entered in the Retries field is not numeric and is not within 1 and 10.	Enter a numeric value within 1 and 10 in the Retries field.
No range specified for the scan. Can not start scan.	This error message appears if you do not enter an IP Address range and scan for devices.	Enter an IP Address range and then scan for devices.
No device type selected for scan. Can not start scan.	This error message appears if you do not select the device type to scan.	Select the device type and then scan for devices.
Unable to store discovery settings.	This error message appears when you click Close and save discovery settings.	Check the file permissions or restart the MLM1000 Server.
Unable to retrieve current discovery settings.	This error message appears if you do not have file permissions or if the file is corrupted.	Check the file permissions or restart the MLM1000 Server.
Could not start discovery.	This error message appears if the MLM1000 Server is unable to start the discovery.	Restart the MLM1000 Server.
Could not cancel discovery.	This error message appears if the MLM1000 Server is unable to cancel the discovery.	Restart the MLM1000 Server.
Server busy. Could not start scan, please try after some time.	This error message appears if the MLM1000 Server is busy.	Try after some time.
Could not determine scan status.	This error message appears if the application is unable to get scan status from the MLM1000 Server.	Restart the MLM1000 Server.

Table A- 1: Error messages (Cont.)

Error message	Description	Possible solution
Remote user interface launch error messages		
Unable to launch the device RUI.	This error message appears if the application is unable to launch the device RUI.	Check for network problems. Ensure that the Java bin directory is part of the user environment PATH variable.
Remote user interface related error messages		
Could not cancel the download.	This error message appears if you try to cancel the download and the application fails to cancel .	-
Could not determine the download status.	This error message appears if the application fails to determine the download status.	Restart the download to ensure the validity of the resulting file.
User manual related error messages		
Could not open the user manual.	This error message appears if the application is unable to open the PDF file of the user manual.	Ensure that the Acrobat directory is part of your PATH environment variable.
Event log related error messages		
Unable to remove logs.	This error message appears if the application is unable to remove the event log entries.	Retry removing the logs.
Hotspot management error messages		
The device type is not supported by MLM1000.	This error message appears if you add a device that is not supported by the MLM1000 software.	Ensure that the device you are trying to manage is a valid device type: Tektronix WFM700, WVR6XX, RFM210, and MTM400.
A device with the same IP address already exists.	This error message appears if you try to add a device with the same IP address as one that exists within the Hotspot Tree.	Resolve the conflict with the IP addresses.
A map with the same name already exists.	This error message appears if you try to add a map with the as one that exists in the Hotspot Tree.	Resolve the name conflict between maps. Change the name of the map you are trying to add.
Insufficient licenses to add the new device.	This error message appears if you try to add more devices than your license supports.	Purchase a license from Tektronix that allows you to add more devices. Go to www.tektronix.com , or call your local Tektronix representative.
No licenses are set up to manage devices.	This error message appears if you have not set up the license.	Set up the license using the procedure on page 1-18.
Could not add the device.	This error message appears when an unknown error is detected while attempting to add a device.	Contact your administrator or restart the MLM1000 Server.
Could not add the map.	This error message appears when an unknown error is detected while attempting to add a map.	Contact your administrator or restart the MLM1000 Server.
Could not load the new image.	This error message appears if the application is unable to load the image selected for the Background of the map.	Ensure that the location of the file is part of the PATH environment variable and that the image file is not corrupt.

Table A-1: Error messages (Cont.)

Error message	Description	Possible solution
Invalid hotspot movement.	This error message appears if you try to move a map or a device to an invalid location.	Do not move a map to a device. Do not move a device to another device.
Placements locked on the destination map.	This error message appears if you try to move a hotspot to or within a locked hotspot.	Unlock the hotspot placement and then try to move the hotspot.
Can not move maps into New Devices window.	This error message appears if you try to move maps into the New Devices window.	You cannot move maps to the New Devices window.
The name field cannot be empty.	This error message appears if you leave the name field empty.	Enter your name in the Name field.
Cannot add a device in monitored mode to an unmonitored map. Device unmonitored.	This error message appears if you try to add a monitored device to unmonitored map.	Ensure that the device being moved and the destination map are in the same mode.
Selected icon file is invalid.	This error message appears if the application is unable to load the image selected as an Icon.	Ensure that the location of the file is part of the PATH environment variable and that the image file is not corrupt.
One of the child maps is locked. Cannot remove map.	This error message appears if you try to delete a map that has a locked child map.	Unlock the child map, and then remove the map.
User management error messages		
Could not delete user.	This error message appears when an unknown error is detected while attempting to delete a user.	Contact your administrator or restart the MLM1000 Server.
Could not add user.	This error message appears when an unknown error is detected while attempting to add a user.	Contact your administrator or restart the MLM1000 Server.
Could not modify user information.	This error message appears when an unknown error is detected while attempting to modify the user information.	Contact your administrator or restart the MLM1000 Server.
New passwords do not match. Please retry.	This error message appears when trying to change passwords and different passwords are detected in the New Password and Re-enter Password fields..	Ensure that the passwords entered in New Password and Re-enter Password fields match.
Password size is not within 4 to 16 characters.	This error message appears when the password is either less than 4 characters or greater than 16 characters.	Use a password that is between 4 and 16 characters.
Could not change the password.	This error message appears if the MLM1000 Server is unable to change the password.	Log off and back on again, and then try changing the password.
Username size is not within 4 to 16 characters.	This error message appears if the user name is less than 4 characters and greater than 16 characters.	Use a user name that is between 4 and 16 characters.
The user name should start with an alphabet and should be alphanumeric.	This error message appears when the user name is not an alphanumeric and does not start with an alphabet.	Use a user name that starts with an alphabet and is alpha numeric.

Table A- 1: Error messages (Cont.)

Error message	Description	Possible solution
Full name should contain only alphabets, space or special characters such as "." or ",".	This error message appears when the full name does not contains letters, spaces or special characters such as "." or ",".	Ensure that the Full name contains only letters, spaces or special characters such as "." or ",".
Full name size is not less than 64 characters.	This error message appears when the full name exceeds 64 characters.	Use a full name within 64 characters.
User name already exists.	This error message appears when entering a user name that already exists.	Enter a different user name.
There must be at least one administrator account in the system.	This error message appears the last administrator account in the User Management dialog box is deleted.	Ensure that at least one administrator account is available.
No user with this name exists.	This error message appears if an administrator deletes the user that you are currently editing.	Recreate the user profile.
Current password invalid.	This error message appears when an incorrect password is detected in the Current Password field while trying to change the password.	Retype the current password into the Current Password field. The password field is case-sensitive.
Invalid expiry date. The expiry date occurs on or before today.	This error message appears if you are setting the expiration date in the User Profile dialog box to a date on or before today.	Ensure that you select a date in the future for expiration.
Contact number should contain only digits or special characters like () - +	This error message appears if you are entering the contact number in the User Profile dialog box with special characters other than () - +.	Ensure that you enter a contact number that contains only digits or special characters such as () - +.
Incorrect email address.	This error message appears if you are entering the a wrong email address in the User Profile dialog box.	Ensure that you enter a correct email address.
Icon management error messages		
No devices are supported. Hence Icon Management is not needed.	This error message appears if you have an application version mismatch.	Reinstall the application.
Could not get the image file name from the Server.	This error message appears if the application is unable to retrieve the image file name from the MLM1000 Server.	Ensure that the location of the file is part of the PATH environment variable and that the image file is not corrupt.
Could not open the image file.	This error message appears if the application is unable to open the image file.	Ensure that the location of the file is part of the PATH environment variable and that the image file is not corrupt.
Could not read the image file.	This error message appears if the application is unable to read the image file.	Ensure that the location of the file is part of the PATH environment variable and that the image file is not corrupt.
Changing the image call failed.	This error message appears if the application is unable to change the image file.	Log off and back again, and then try changing the image file.

Table A-1: Error messages (Cont.)

Error message	Description	Possible solution
Could not reset icons to default images.	This error message appears if the application is unable to reset icons to default images.	Log off and back again, and then try setting the icons to default.
Option dialog box related error messages		
HTTP Port should be an integer between 1 and 65535.	This error message appears if the value you have entered for the HTTP Port is not between 1 and 65535.	Enter a value for the HTTP Port between 1 and 65535.
RMI Port should be an integer between 1 and 65535.	This error message appears if the value you have entered for the RMI Port is not between 1 and 65535.	Enter a value for the RMI Port between 1 and 65535.
Both RMI and HTTP ports cannot have same value.	This error message appears if the value you have entered for the RMI Port and the HTTP port is the same.	Ensure that you enter a different value for RMI and HTTP port.
Maximum log size should be between 1 and 1024 MB.	This error message appears if the value you have entered for Maximum log size is not between 1 and 1024 MB.	Enter a value for Maximum log size between 1 and 1024 MB.
Device log size should be between 1 and 1024MB.	This error message appears if the value you have entered for Device log size is not between 1 and 1024 MB.	Enter a value for Device log size between 1 and 1024 MB.
Error getting HTTP port.	This error message appears if the MLM1000 Server is unable to get the HTTP port.	Restart the MLM1000 Server.
Error setting HTTP port.	This error message appears if the MLM1000 Server is unable to set the HTTP port.	Restart the MLM1000 Server.
Error getting RMI port.	This error message appears if the MLM1000 Server is unable to get the RMI port.	Restart the MLM1000 Server.
Error setting RMI port.	This error message appears if the MLM1000 Server is unable to set the RMI port.	Restart the MLM1000 Server.
Error setting polling cycle duration.	This error message appears if the MLM1000 Server is unable to set the polling cycle duration.	Restart the MLM1000 Server.
Error getting polling cycle duration.	This error message appears if the MLM1000 Server is unable to get the polling cycle duration.	Restart the MLM1000 Server.
Error setting poll activation state.	This error message appears if the MLM1000 Server is unable to set the poll activation state.	Restart the MLM1000 Server.
Error getting poll activation state.	This error message appears if the MLM1000 Server is unable to get the poll activation state.	Restart the MLM1000 Server.
Error setting auto discovery mode.	This error message appears if the MLM1000 Server is unable to set the auto discovery mode.	Restart the MLM1000 Server.

Table A- 1: Error messages (Cont.)

Error message	Description	Possible solution
Error getting auto discovery mode.	This error message appears if the MLM1000 Server is unable to get the auto discovery mode.	Restart the MLM1000 Server.
Error getting Log Size.	This error message appears if the MLM1000 Server is unable to get the Log Size.	Restart the MLM1000 Server.
Error setting Log Size.	This error message appears if the MLM1000 Server is unable to set the Log Size.	Restart the MLM1000 Server.
Error getting Device Log Size.	This error message appears if the MLM1000 Server is unable to get the Device Log Size.	Restart the MLM1000 Server.
Error setting Device Log Size.	This error message appears if the MLM1000 Server is unable to set the Device Log Size.	Restart the MLM1000 Server.
Error getting Beep File.	This error message appears if the MLM1000 Server is unable to get the sound file.	Restart the MLM1000 Server.
Error setting Beep File.	This error message appears if the MLM1000 Server is unable to set the sound file.	Restart the MLM1000 Server.
Unable to set the new beep file. Beep file is invalid.	This error message appears when the selected sound file is invalid.	Select a new sound file.
MLM1000 server connection related error messages		
Server not responding... Disconnecting client.	This error message appears if the MLM1000 Server is shutdown or the network is not working.	Restart the MLM1000 Server.
Search specific error messages		
Could not find a matching device or map.	This error message appears when the application cannot find a device or a map that you are searching for.	Ensure that the spelling is correct, or ensure that the item being searched for exists in the domain being searched.
Not a valid string for search.	This error message appears if you have not entered a string to search.	Enter a valid string to search.
License Specific Error Messages		
The number of devices in the maps exceeds your license limit. Some devices have been removed from Maps.	This error message appears if the current license supports fewer devices than the previous license.	Enter the license number for the license supporting the greater number of devices. All the devices that have been removed from Maps will be available in New Devices window.
The license you have entered is invalid.	This error message appears when an invalid license number is detected.	Enter the correct license number.

Appendix B: Device Types

About the MTM400

The MTM400 is a single-stream, extended-confidence, MPEG-2 protocol, rackmounted monitoring device. It is used to monitor a single transport stream in MPEG-2, DVB and ATSC environments.

The basic MTM400 provides confidence monitoring by making key measurements and comparing them with pre-set parameters; inconsistencies can be reported as varying levels of error. Integrated flexibility allows the software to be upgraded with diagnostic capabilities and to supply detailed information to enable fault identification and analysis.

The RUI and the MLM1000 communicate with the MTM400 through the open standard Simple Network Management Protocol (SNMP) and Hypertext Transfer Protocol (HTTP).

ASI (Asynchronous Serial Interface) and SMPTE 310M (Society of Motion Picture and Television Engineers) interfaces are provided as standard; optional QAM (Quadrature Amplitude Modulation) and QPSK (Quaternary Phase Shift Keying) (L-Band) interfaces are available as options for the MTM400.

About the RFM210

The RFM210 DVB-T Measurement Receiver operates in accordance with the ETSI EN 300 744 standard. The RFM210 provides both 2K and 8K carrier mode options, and supports all DVB modulation options, guard intervals and FEC rates. Different versions support VHF, UHF, and for 6/7/8 MHz bandwidths.

The RFM210 accepts a standard RF or baseband input and demodulates the COFDM signal to give both SPI and ASI MPEG transport streams. BNC connectors on the rear of the unit allow you to display of constellation and channel state diagrams on a standard oscilloscope. A range of status and alarm outputs are also available. A built-in Digital Signal Processor enables real-time monitoring and measurement of the baseband modulating signals (I, Q) in accordance with TR 101 290, including Modulation Error Ratio (MER) measurement.

The RFM210 can be controlled from the front panel or from a PC using the rear panel RS232 port.

About the WFM700

The WFM700 waveform monitor is designed to meet the multi-format monitoring and measurement needs of digital video for program production, post-production, and transmission.

The WFM700 waveform monitor combines the features of traditional waveform monitors with the advantages of digital technology. Digital processing provides accuracy and repeatability of measurements.

The waveform monitor can be configured for different applications within a TV facility. Feature enhancements can be achieved by installing additional modules or by downloading software.

The waveform monitor has three base models:

- WFM700HD. Monitors high-definition (SMPTE 292M) video.
- WFM700A. Monitors standard-definition (ITU--R BT.601) and high-definition (SMPTE 292M) video.
- WFM700M. Measurement instrument for standard-definition (ITU--R BT.601), high-definition (SMPTE 292M), and hybrid serial digital operations.

Each waveform monitor includes:

- External Reference module
- One video module (with two inputs)

At the time of purchase or at a later date, you can add an additional video module and/or the optional AES audio module (Option DG) to any of the three base-model waveform monitors.

About the WVR6XX

The WVR610A & WVR611A uses fully digital processing that ensures accurate, stable, and repeatable measurements. The WVR610A & WVR611A provide a powerful monitoring solution for broadcasting, production, and post-production environments. The combination of Tektronix exclusive gamut displays, session screens, alarms, and error logging help you speed and simplify the process of solving problems with your content.

The WVR610A supports only standard definition (SDI) inputs, while the WVR611A supports both standard definition and analog composite inputs. They are ideally suited to facilities transitioning from analog to digital environments. Both models offer audio options to allow multiple-channel audio monitoring.

The digital architecture of the WVR610A & WVR611A delivers important benefits to users. Digital instruments offer accuracy and stability that is unattainable in traditional analog designs. Analog components age and drift with fluctuations in ambient temperature, and systems based on these components require periodic calibration. The fully digital architecture of the WVR610A & WVR611A provides accuracy, repeatability, and stability that surpasses traditional analog designs.

The high-quality display of the WVR610A & WVR611A is well suited to meet the needs of production and post-production applications including camera shading and alignment, color balancing, film-to-tape and format conversion, and special effects work.

Sometimes you simply need to know that your signal is valid. You need to ensure that a signal will be compatible with compliant operational equipment such as when you combine content from many sources including live in-studio, tape, contribution feeds, and perhaps mobile feeds. Any of these sources might deliver content with errors that could affect the quality of your transmission. The tiled-display of the WVR610A & WVR611A enables you to quickly check the integrity of the signal by displaying up to four views of the signal simultaneously.

Appendix C: Troubleshooting

Table C-1 describes possible problems you may encounter while using the MLM1000 software and solutions for those problems.

Table C- 1: Troubleshooting

Description	Possible Solution
Server	
Unable to launch the MLM1000 Server.	<p>The default HTTP port is 9999.</p> <p>The default RMI port is 1099.</p> <p>Check for port conflicts between other applications. If another application uses one of the MLM1000 default ports, close the other application and change the HTTP and/or RMO ports in the MLM1000 to avoid conflicts.</p>
Could not connect to the MLM1000 Software.	<p>Version of MLM1000 Server and Local Client are different.</p> <p>Reinstall the MLM1000 software.</p>
Local Client	
Cannot find the required language in the Select Language drop-down list of the Login dialog box.	Install the required language fonts.
An empty line appears in the Select Language drop-down list of the Login dialog box.	Ensure that the fonts are properly installed.
Unable to login to the MLM1000 Software.	Try the default username (tektronix) and password (welcome). If these do not work, contact your administrator for further information.
Cannot drag and drop devices into a map window.	Ensure that the current license is correct and the map is unlocked.
The Device added remains in the unmonitored mode.	Ensure that the device you are trying to manage is a valid device type: Tektronix WFM700, WVR6XX, RFM210, and MTM400.
Cannot remove a map.	Unlock the map and then try to remove.

Table C-1: Troubleshooting (Cont.)

Description	Possible Solution
Unable to launch RUI of the device.	Ensure that the device is ON. or Install Java on the local system and launch it. or Ensure that the Java bin directory is part of the environment PATH variable.
Cannot access the user manual.	Ensure that the Adobe Acrobat directory is part of the PATH variable.
Alarm Occurrence Graph is empty.	Ensure you that you have set the device in monitored mode.
Cannot acknowledge the alarms.	Acknowledge alarms in the yellow state.
New alarms are not seen in the Event Viewer window.	Ensure that you have sorted the event log by date.
Cannot get traps from a monitored device.	Ensure that you have entered only one correct value in the Set community strings field.
The system removed a lot of devices from the map that you had set to monitored.	Ensure that you have an adequate license for the number of devices you are trying to monitor. If necessary revert to the precious license, or contact your Tektronix representative.
The icon selected for a device is not displayed.	Try assigning the icon file again. or Ensure that the icon file is .jpg or .gif. or Reinstall the MLM1000 software.
Forgot the password.	Contact your administrator.
The application takes too long to detect alarms.	Set the Polling Rate to a lower value.
The application does not automatically recognize a new device.	In the Options dialog box, select the Auto Discover Device check box.
Every alarm is popped up on the screen.	In the Options dialog box, clear the pop-up alarm check box.

Table C- 1: Troubleshooting (Cont.)

Description	Possible Solution
Unable to discover a particular device.	Check whether the device is already in a map. or If a device was recently deleted, the New Devices window will not display that device. To discover the device again, restart the MLM1000.
Problem in aligning or locating the devices in Map window.	Use the scroll bar to locate the devices in the map window. Remember that devices are aligned to top-left corner.
Received only a limited number of traps even when the device generates more.	In the Options dialog box, select Enable all traps check box to receive all the traps.
A device for particular device type displays an icon different from the default icon.	Set the default icon option in the Properties dialog box for devices you want to display the default icon.

Appendix D: Shortcut Keys and Default Values

The following table lists the shortcut keys.

Table D- 1: Shortcut Keys

Task	Shortcut Key
Add a Map	ALT+H+A+M
Add a Device	ALT+H+A+D
Remove a Hotspot	ALT+H+R
Search for Hotspots	ALT+H+S
Configure the Hotspot	ALT+H+F
Launch the RUI of the device	ALT+H+L
View the Hotspot Alarm Distribution	ALT+H+D
View the Hotspot Alarm Occurrence	ALT+H+O
Generate a Report	ALT+H+T
Acknowledge Alarms	ALT+H+E
View Properties	ALT+H+P
Exit the Application	ALT+H+X
View the New Device window	ALT+V+C
View the Hotspot Tree	ALT+V+T
View the Hotspot Preview	ALT+V+P
View the Event Viewer window	ALT+V+E
Open the Discovery Settings dialog box	ALT+T+D
Open the User Management dialog box	ALT+T+U
Open the Change Password dialog box	ALT+T+P
Open the License Management dialog box	ALT+T+L
Open the Icon Management dialog box	ALT+T+I
Open the Options dialog box	ALT+T+O
Cascade Windows	ALT+N+C
Tile Windows	ALT+N+T
View the User Manual	ALT+E+U
View the Online Help	ALT+E+O
View about MLM1000 software	ALT+E+A
Cancel	ESC

The following table lists the default values.

Table D-2: Default Values

Parameter	Default Value
User name	tektronix
Password	welcome
Language	English
HTTP port	9999
RMI port	1099
Polling rate	3 seconds
Polling	Activated
Autodiscovery	Activated
Maximum size of Event log	1 MB
Maximum storage per device	1MB
Look and feel	Metal
Popup map on alarm	OFF
Auto expand tree on alarm	OFF
Get community string	public
Set community string	private
SNMP version	snmpV1
Number of retries	3
Device types selected for discovery	All



Index

Index

A

- Acknowledging Alarms, 3-33
- Add Device dialog box, 2-11
- Add Map dialog box, 2-10
- Adding
 - Device Manually, 3-7
 - Discovered Device to a Map, 3-8
 - IP Address Range to the Device Discovery Settings, 3-15
 - Map, 3-1
 - User Account, 3-21
- Adding a Device Manually, 3-7
- Adding a Discovered Device to a Map, 3-8
- Adding a map, 3-1
- Adding a User Account, 3-21
- Adding an IP Address Range to the Device Discovery Settings, 3-15
- Alarm Distribution Graph Window, 2-13
- Alarm Occurrence Graph Window, 2-14
- Application Window, 2-1

B

- Background Scanning, 3-14

C

- Change Password dialog box, 2-20
- Changing
 - Beep File, 3-36
 - Device Icon, 3-9
 - Page Setup, 3-65
 - Role of a User, 3-25
 - the Password of Another User, 3-24
 - Your Password, 3-24
- Changing Page Setup, 3-65
- Changing the Beep File, 3-36
- Changing the Device Icon, 3-9
- Changing the Password of Another User, 3-24
- Changing the Role of a User, 3-25
- Changing Your Password, 3-24
- Configuring
 - Alarm Options, 3-55
 - Display Options, 3-56
 - Server Options, 3-53

- Configuring Alarm Options, 3-55
- Configuring Display Options, 3-56
- Configuring Server Options, 3-53

D

- Device
 - Types, 1-2
 - types, 1-2
- Device Graph Menu, 2-7
- Device Properties dialog box, 2-16
- Device Types, B-1
 - MTM400, B-1
 - RFM210, B-2
 - WFM700, B-3
 - WVR6XX, B-4
- Dialog Boxes/Windows, 2-9
 - Add Device dialog box, 2-11
 - Add Map dialog box, 2-10
 - Alarm Distribution Graph Window, 2-13
 - Alarm Occurrence Graph Window, 2-14
 - Change Password dialog box, 2-20
 - Device Properties dialog box, 2-16
 - Discovery Settings dialog box, 2-18
 - Event Viewer window, 2-17
 - Icon Management window, 2-22
 - License Management window, 2-21
 - Login dialog box, 2-9
 - Map Properties dialog box, 2-15
 - New Devices window, 2-19
 - Search dialog box, 2-12
 - User Management window, 2-20
- Discovering, Devices, 3-13
- Discovering Devices, 3-13
 - Adding an IP Address Range to the Device Discovery Settings, 3-15
 - Background Scanning, 3-14
 - Foreground Scanning, 3-13
 - Removing an IP Address Range from the Device Discovery Settings, 3-15
 - Saving Device Discovery Settings, 3-19
 - Scanning for a Device in an IP Address Range, 3-15
 - Scanning for a Specific Device Type, 3-16
 - Scanning for Devices with Community Strings, 3-16
 - Setting Up Auto Discovery, 3-18
- Discovery Settings dialog box, 2-18

E

- Error Messages, A-1
- Event Viewer Menu, 2-7
- Event Viewer window, 2-17
- Exporting, Event Log, 3-27
- Exporting, Report, 3-62
- Exporting an Event Log, 3-27
- Exporting Report, 3-62

F

- Foreground Scanning, 3-13

G

- Generating, Reports, 3-59
- Generating Reports, 3-59
 - Changing Page Setup, 3-65
 - Exporting Report, 3-62
 - Navigating the Report, 3-66
 - Printing Report, 3-66
 - Saving Report, 3-60
 - Zooming In or Out, 3-66

H

- Help Menu, 2-7
- Hotspot Tree, 2-3
- Hotspot Preview, 2-3
- Hotspots Menu, 2-5

I

- Icon Management window, 2-22
- Initialization Wizard
 - Walking Through, 1-19
 - Welcome, 1-19
- Installing the Application, 1-5

L

- Launch Modes, 1-3
 - Applet, 1-3
 - Webstart, 1-3
- Launching Device RUI, 3-11
- License Management window, 2-21
- Licensing, 1-2
- Locking or Unlocking, Map, 3-3
- Login dialog box, 2-9

M

- Managing, Maps, 3-1
- Managing
 - Alarms, 3-33
 - Application User Interface, 3-31
 - Devices, 3-7
 - Event Log, 3-27
 - User Accounts, 3-21
- Managing Alarms, 3-33
 - Acknowledging Alarms, 3-33
 - Alarm Occurrence Graph
 - Setting the Legend Properties, 3-37
 - Setting the Other Properties, 3-44
 - Setting the Plot Properties, 3-40
 - Zooming In or Out, 3-46
 - Changing the Beep File, 3-36
 - Printing an Alarm Distribution Graph, 3-52
 - Printing an Alarm Occurrence Graph, 3-45
 - Saving an Alarm Distribution Graph, 3-51
 - Saving an Alarm Occurrence Graph, 3-45
 - Setting a Beep on Alarm for a Specific Device, 3-35
 - Setting an Action on Alarm for a Specific Device, 3-36
 - Setting an Action on Alarm Recovery for a Specific Device, 3-36
 - Setting Hotspot Tree to Expand on Alarm, 3-34
 - Setting Legend Properties for the Alarm Distribution Graph, 3-47
 - Setting Other Properties for the Alarm Distribution Graph, 3-50
 - Setting Plot Properties for the Alarm Distribution Graph, 3-48
 - Setting the Map Window to Pop Up on an Alarm, 3-34
 - Viewing an Alarm Distribution Graph, 3-46
 - Viewing an Alarm Occurrence Graph, 3-37
- Managing Default Icons for All Devices, 3-9
- Managing Devices, 3-7
 - Adding a Device Manually, 3-7
 - Adding a Discovered Device to a Map, 3-8
 - Changing the Device Icon, 3-9
 - Launching Device RUI, 3-11
 - Managing Default Icons for All Devices, 3-9
 - Monitoring or Unmonitoring a Device, 3-9
 - Moving Devices to Another Map, 3-8
 - Moving Devices Within the Map Window, 3-9
 - Removing a Device from the Map, 3-10
 - Removing Devices from the New Devices Window, 3-11

- Managing Maps, 3-1
 - Adding a Map, 3-1
 - Locking or Unlocking a Map, 3-3
 - Modifying Map Properties, 3-2
 - Monitoring or Unmonitoring a Map, 3-4
 - Moving a Map Within the Map Window, 3-5
 - Removing a Map, 3-3, 3-5
 - Renaming a Map, 3-3
 - Setting the Map Background, 3-4
 - Setting the Map Icon, 3-5
 - Managing the Application User Interface, 3-31
 - Managing the Event Log, 3-27
 - Exporting an Event Log, 3-27
 - Removing Event Logs, 3-28
 - Setting the Maximum Event Log Size, 3-28
 - Managing User Accounts, 3-21
 - Adding a User Account, 3-21
 - Changing the Password of Another User, 3-24
 - Changing the Role of a User, 3-25
 - Changing Your Password, 3-24
 - Modifying a User Profile, 3-23
 - Removing a User, 3-25
 - Removing an Administrator, 3-26
 - Setting the Expiry Date, 3-25
 - Map Properties dialog box, 2-15
 - Menu
 - Device Graph, 2-7
 - Event Viewer, 2-7
 - Help, 2-7
 - Hotspots, 2-5
 - New Devices, 2-6
 - Tools, 2-6
 - View, 2-5
 - Window, 2-7
 - Menu bar, 2-4
 - Minimum System Requirements, 1-1
 - MLM1000 Desktop, 2-2
 - Modifying
 - Map Properties, 3-2
 - User Profile, 3-23
 - Modifying a User Profile, 3-23
 - Modifying Map Properties, 3-2
 - Monitoring or Unmonitoring
 - Device, 3-9
 - Map, 3-4
 - Monitoring or Unmonitoring a Device, 3-9
 - Monitoring or Unmonitoring a Map, 3-4
 - Moving
 - Devices to Another Map, 3-8
 - Devices Within the Map Window, 3-9
 - Moving a Map Within the Map Window, 3-5
 - Moving Devices to Another Map, 3-8
 - Moving Devices Within the Map Window, 3-9
 - MTM400, B-1
 - Multi-lingual Support, 1-3
- ## N
- Navigating, Report, 3-66
 - Navigating the Report, 3-66
 - New Devices Menu, 2-6
 - New Devices window, 2-19
- ## O
- Operating Basics, 2-1
 - Application Window, 2-1
 - Dialog Boxes/Windows, 2-9
 - Add Device dialog box, 2-11
 - Add Map dialog box, 2-10
 - Alarm Distribution Graph Window, 2-13
 - Alarm Occurrence Graph Window, 2-14
 - Change Password dialog box, 2-20
 - Device Properties dialog box, 2-16
 - Discovery Settings dialog box, 2-18
 - Event Viewer window, 2-17
 - Icon Management window, 2-22
 - License Management window, 2-21
 - Login dialog box, 2-9
 - Map Properties dialog box, 2-15
 - New Devices window, 2-19
 - Search dialog box, 2-12
 - User Management window, 2-20
 - Hostspot Tree, 2-3
 - Hotspot Preview, 2-3
 - Menu bar, 2-4
 - Device Graph Menu, 2-7
 - Event Viewer Menu, 2-7
 - Help Menu, 2-7
 - Hotspots Menu, 2-5
 - New Devices Menu, 2-6
 - Tools Menu, 2-6
 - View Menu, 2-5
 - Window Menu, 2-7
 - MLM1000 Desktop, 2-2
 - Toolbar, 2-8

P

Printing

- Alarm Distribution Graph, Other Properties, 3-52
 - Alarm Occurrence Graph, Other Properties, 3-45
 - Report, 3-66
- Printing an Alarm Distribution Graph, 3-52
- Printing an Alarm Occurrence Graph, 3-45
- Printing Report, 3-66

R

Remote User Interface, 1-2

Removing

- Administrator, 3-26
 - Device from the Map, 3-10
 - Devices from the New Devices Window, 3-11
 - Event Logs, 3-28
 - IP Address Range from the Device Discovery Settings, 3-15
 - Map, 3-3
 - User, 3-25
- Removing a Device from the Map, 3-10
- Removing a Map, 3-3, 3-5
- Removing a User, 3-25
- Removing an Administrator, 3-26
- Removing an IP Address Range from the Device Discovery Settings, 3-15
- Removing Devices from the New Devices Window, 3-11
- Removing Event Logs, 3-28
- Renaming a Map, 3-3
- Resetting the Default Options, 3-57
- RFM210, B-2

S

Saving

- Alarm Distribution Graph, Other Properties, 3-51
 - Alarm Occurrence Graph, Other Properties, 3-45
 - Report, 3-60
- Saving an Alarm Distribution Graph, 3-51
- Saving an Alarm Occurrence Graph, 3-45
- Saving Device Discovery Settings, 3-19
- Saving Report, 3-60

Scanning

- Background, 3-14
 - for a Device in an IP Address Range, 3-15
 - for a Specific Device Type, 3-16
 - for Devices with Community Strings, 3-16
 - Foreground, 3-13
- Scanning for a Device in an IP Address Range, 3-15

Scanning for a Specific Device Type, 3-16

Scanning for Devices with Community Strings, 3-16

Search dialog box, 2-12

Setting

- Action on Alarm for a Specific Device, 3-36
 - Action on Alarm Recovery for a Specific Device, 3-36
 - Alarm Distribution Graph
 - Legend Properties, 3-47
 - Other Properties, 3-50
 - Plot Properties, 3-48
 - Alarm Occurrence Graph
 - Legend Properties, 3-37
 - Other Properties, 3-44
 - Plot Properties, 3-40
 - Beep on Alarm for a Specific Device, 3-35
 - Hotspot Tree to Expand on Alarm, 3-34
 - Map Window to Pop Up on an Alarm, 3-34
- Setting
- Auto Discovery, 3-18
 - Device Discovery Settings, 3-19
 - Expiry Date, 3-25
 - Map Background, 3-4
 - Map Icon, 3-5
 - Maximum Event Log Size, 3-28
 - Options, 3-53
- Setting a Beep on Alarm for a Specific Device, 3-35
- Setting an Action on Alarm for a Specific Device, 3-36
- Setting an Action on Alarm Recovery for a Specific Device, 3-36
- Setting Hotspot Tree to Expand on Alarm, 3-34
- Setting Legend Properties for the Alarm Distribution Graph, 3-47
- Setting Options, 3-53
- Configuring Alarm Options, 3-55
 - Configuring Display Options, 3-56
 - Configuring Server Options, 3-53
 - Resetting the Default Options, 3-57
- Setting Other Properties for the Alarm Distribution Graph, 3-50
- Setting Plot Properties for the Alarm Distribution Graph, 3-48
- Setting the Expiry Date, 3-25
- Setting the Legend Properties for the Alarm Occurrence Graph, 3-37
- Setting the Map Background, 3-4
- Setting the Map Icon, 3-5
- Setting the Map Window to Pop Up on an Alarm, 3-34
- Setting the Maximum Event Log Size, 3-28
- Setting the Other Properties for the Alarm Occurrence Graph, 3-44

- Setting the Plot Properties for the Alarm Occurrence Graph, 3-40
- Setting Up Auto Discovery, 3-18
- Shortcut Keys and Default Values, D-1
- Starting the Application, 1-15
 - Launching the Client Locally, 1-15
 - Launching the Client Remotely, 1-15
 - Launching the Client for the first time, 1-15
 - Launching the Client the next time, 1-16
 - Launching the Server, 1-15
 - Logging In, 1-17

T

- Terms and Definitions, 1-4
 - Device, 1-4
 - Hotspot Panel, 1-4
 - Hotspot, 1-4
 - Hotspot Tree, 1-4
 - Locked Placement, 1-4
 - Map, 1-4
 - Monitored Mode, 1-4
 - Unlocked Placement, 1-4
 - Unmonitored Mode, 1-4
- Toolbar, 2-8
- Tools Menu, 2-6
- Trouleshooting, C-1
 - Local Client, C-1
 - Server, C-1

U

- User Management window, 2-20
- Users and Passwords, 1-2
 - Administrator, 1-2
 - User, 1-2

V

- View Menu, 2-5
- Viewing
 - Alarm Distribution Graph, Other Properties, 3-46
 - Alarm Occurrence Graph, 3-37
- Viewing an Alarm Distribution Graph, 3-46
- Viewing an Alarm Occurrence Graph, 3-37

W

- Walking through the Initialization Wizard, 1-19
- WFM700, B-3
- Window Menu, 2-7
- WVR6XX, B-4

Z

- Zooming In or Out, 3-66
 - Alarm Occurrence Graph, Other Properties, 3-46

