MonitorWare Console 2.0

Table of Contents

Index 0

1   Introduction

1.1   Overview of MonitorWare Console

1.1.1   MonitorWare Console

Adiscon MonitorWare Console works together with the other members of Adiscon's MonitorWare line of products to provide a centralized view of the system-generated events data.

MonitorWare Console is the newest member of Adiscon's MonitorWare line of products. It's a user-friendly, graphical interface for log viewing and analysis.

With MonitorWare Console, network administrators can quickly watch what is going on in the network. It also enables security administrators to find weak spots and aids in detecting intrusions as well as forensic analysis.

If you would like to contact Adiscon, please email us at <u>support@adiscon.com</u> for technical questions and <u>info@adiscon.com</u> for all others.

1.1.2   Features

Customizeable Views

Users can define their own views of the data in a system. MonitorWare Agent logs the data to a central database and MonitorWare Console allows users to view that data in various combinations.

Flexible Reporting

MonitorWare Console ships with several pre built great reporting options and users can create and add their own custom reports by applying various filters. Reporting sub-system is based on HTML reports that have been built using great templates.

Reports are now available in two flavors i.e. Pix Reporting Module and Windows Reporting Module.

Report Generation using Files

MonitorWare Console can now generate intelligent reports using log files. Previously MonitorWare Console was only able to generate reports using the under lying database i.e. MonitorWare Central Database. Now MonitorWare Console is able to generate reports on PIX Log files as well as Log files for Windows.

Changing Database for Report Generation on the fly

Now, you can generate reports by mentioning the database on the fly. It doesnt matter which database MonitorWare Console is connected to. You can simply generate the same report on various database without restarting MonitorWare Console.

Knowledge Base

Keep and track important notes and technical details or articles regarding your system in one centralized Knowledge Base. Search articles against specific system events and specific devices in your network.

Track System Devices

Keep track of all the machines and devices in your network by creating a profile for each. MonitorWare Console also helps discovering new reporting devices in the system automatically.

Tools

MonitorWare Console comes with various tools that will help the network administrator. As a user, you have the option of using the following tools:

1).   ICMP Lookup Tool
2).   Database Maintenance Tools
       a.   Delete Records Tool
       b.   Backup Records Tool
       c.   Retrieve Records Tool
3).   Network Tools
       a.   Ping Tool
       b.   TraceRoute Tool
       c.   PortScan Tool
4).   Export / Import Database Settings Tool

Job Manager

MonitorWare Console comes with a Window Service that is called Job Manager. Job Manager is a very powerful feature that has the capability of generating reports according to your defined schedule. You can also ask the Job Manger to generate the reports at the specified time and then send them to your specified recipients via email.

Time Zone Handling

MonitorWare Console provides transparent handling and conversion of time zone related issues in a geographically spread system. All system-generated events are logged after converting to UTC time and are retrieved and displayed to the users in their configured time zones. Thus, users always get to view and analyze the data in their own time zones.

Database Support

Now MySQL has been added in the list of supported databases. Previously MonitorWare Console supported both Microsoft Access, Microsoft SQL Server databases. Support for SQL Server also implies that MonitorWare Console and MonitorWare Agent can be used with the free version of this product, i.e. MSDE.

User management

You can create different user profiles and can select various time zones for them. The data will be converted to the local time based on the specified UTC Offset.

Localization Support

MonitorWare Console can be localized to any of the world languages, including right-to-left scripts like Hebrew and Arabic. End users can request Adiscon to provide support for a particular language or even translate and localize the product themselves – using step by step instructions provided by Adiscon on request.

1.2   Components

1.2.1   MonitorWare Console

MonitorWare Console is an analysis tool that builds on top of the MonitorWare Database that has been gathered either by MonitorWare Agent or by WinSyslog. It ships with several pre-built reports, pre-defined views and a sample database for immediate testing after setup.

Depending upon the size of the network and the auditing policy, MonitorWare Agent or WinSyslog gather huge amount of data in the central MonitorWare Database. All of this data will be meaningless to the network administrator if he/she is not able to analyze it properly. In fact, such huge amount of data cannot be analyzed manually. You need to have some great tool that could extract important information from that huge data repository. MonitorWare Console is the tool that would help you out in this analysis. With MonitorWare Console, you can view many reports which have been made after extensive research in data analysis field. These reports provide you with great information that would help you out in identifying the problematic areas in your network. We, at Adiscon, are totally "Customer Oriented". Addressing the needs of the customers is our top most priority. We keep this philosophy in mind at all times. We have even developed MonitorWare Console keeping this philosophy in mind. It means that if you require any specific report that is not currently present, you can simply contact support@adiscon.com and tell us your requirements. We will create exact report in which you are interested, and will ship that report to you. You will simply place it in the specified folder and it will become part of MonitorWare Console without re-installation or any other configuration changes.

Apart from the reporting module, you can take advantage of the Views module in Console. In this module, you can define your *own* views. The data is displayed in the form of hierarchies which help in a great understanding of the otherwise meaningless data. Once again, keeping our "Customer Oriented" philosophy in mind, we have developed this module, again, in such a way that if you are feeling problems in creating a view, you can contact us and we can make that view for you absolutely for free and will ship the required view to you. You will simply place it in the specified folder and it will become part of MonitorWare Console without any hassle.

There are many other modules in MonitorWare Console which you will see in detail as you read this manual. Since there are many modules in MonitorWare Console and each one of them is not necessarily required by all customers, so we have designed MonitorWare Console in such a way that only those modules could be purchased in which you are interested. With this approach, we have ensured that our valuable customers only pay for the specific functionality in which they are interested in, and hence reducing the cost.

MonitorWare Console has been divided into following 7 sub modules for efficient and

cost effective working:

1. Base Product (This has to be purchased in order to use other modules)
2. Network Scanning Tools
3. Windows Reporting Module
4. PIX Reporting Module
5. Knowledge Base Module
6. Devices' Module
7. Views Module

Important Note: Although MonitorWare Agent and WinSyslog are not components of MonitorWare Console directly, but MonitorWare Console will be useless without these. The reason is that the MonitorWare Console performs all of its analysis on the data that has been gathered by either MonitorWare Agent or WinSyslog and logged into MonitorWare Central Database.

1.3   System Requirements

- The client machine must be Microsoft .NET ready in order to run the MonitorWare Console application. Thus, the machine must at least meet the minimum hardware requirements for hosting .NET framework. The setup program will install the .NET runtime files and other dependencies.

- For a list of hardware and software requirements for .NET visit http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpguide/html/cpconnetframeworksystemrequirements.asp

- MonitorWare Console requires around 20 MB of hard disk space when installed. This includes provision for sample Access database that consists of around 45,000 records of sample event data.

- Some modules of MonitorWare Console are quite memory and processor intensive, like Reporting and the Views modules. A Pentium III-class processor and at least 128 MB of RAM are suggested for good performance; however, MonitorWare Console will work with much less.

2   Getting Started

2.1   Setup

Installing the MonitorWare Console is simple and easy. A standard setup program installs the application.

There are a number of different download versions of the product available. The main difference is whether or not a current version of the Microsoft Windows Installer program is included. If you use recent software (e.g. Windows XP or Windows 2003 Server), you can typically use the small install set. Install sets have different names. Those ending in "max" are typically the version for older operating systems without a current installer. If in doubt, use an install set whoms name ends in "max". All files are direct install sets, so there is no need to unzip them to find a setup.exe or such.

Depending on the download directory, the setup program may also be supplied in a ZIP file.

2.2   Running Console the First Time

Once MonitorWare Console is started, a dialog box similar to the one shown in figure 1 would be displayed.
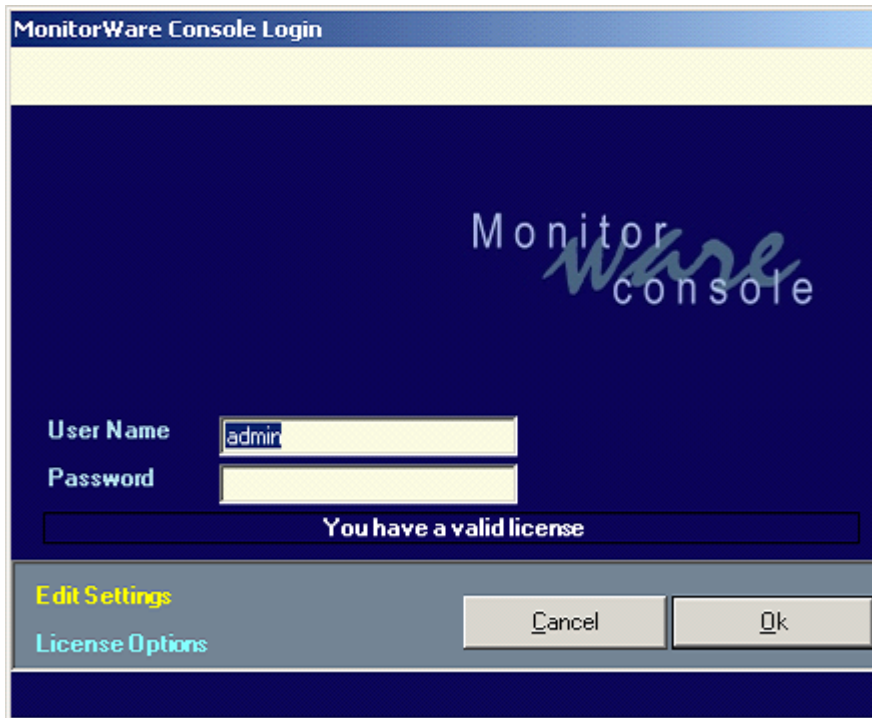

Figure 1: MonitorWare Console: Startup Dialog Box

The default user name is "admin" and password is nothing (as shown above). Please note that the password is not the word "nothing" but actually it is empty. Once a user enters into the application, this password can be changed.

At the bottom left corner of this dialog box, there are two links "Edit Settings" and "License Options" The latter one is self-explanatory. If you click on it, a license dialog appears where you can view or change your license key and license name. There is also a link to order the product directly via our online ordering system. Please note that MonitorWare Console has Modular Licensing now. For getting more details on License, please see License Options
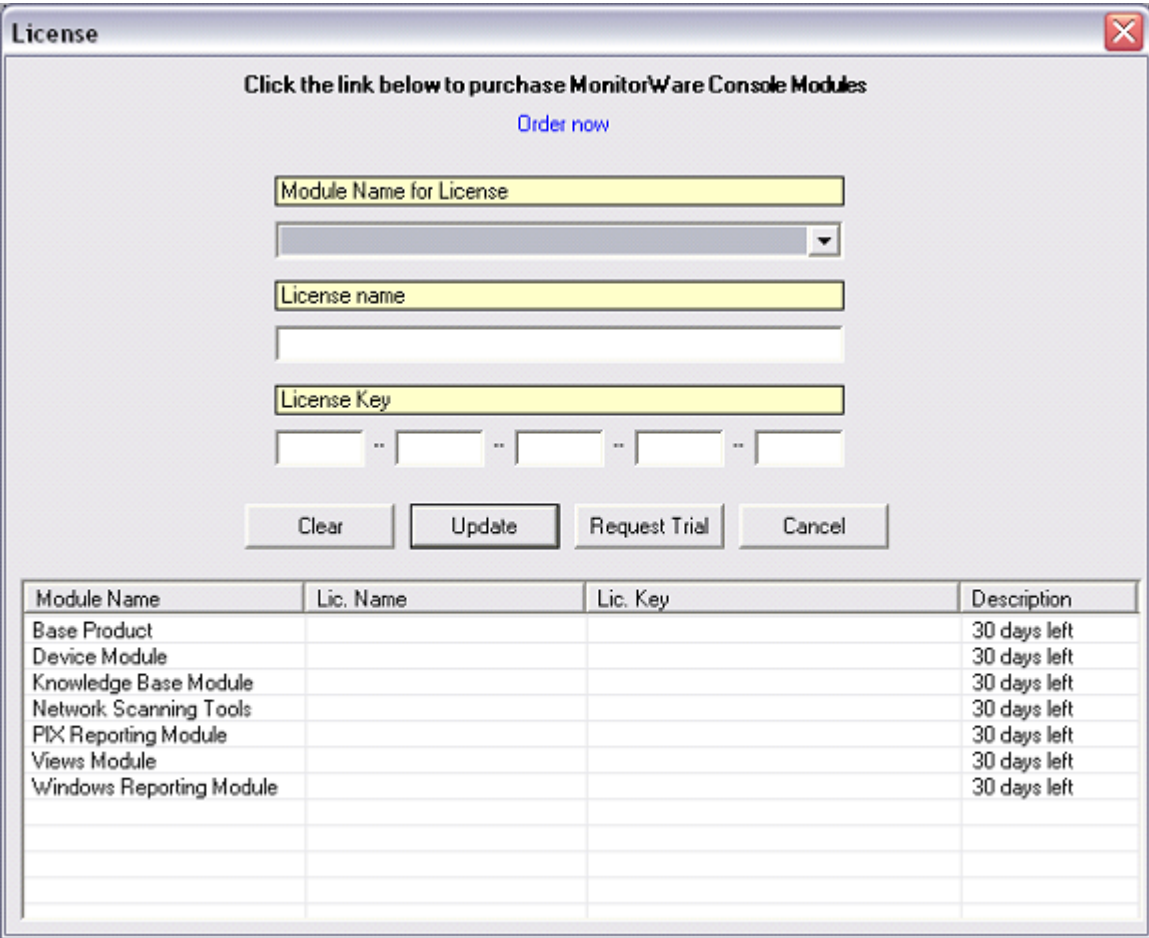
Figure 2: Licence options Dialogue Box

The other link in the login dialog, "Edit Settings" is used if the user wants to change the database connection or other settings. Currently MonitorWare Console supports Microsoft Access, SQL Server and MySQL. Once the above mentioned link is clicked, a dialog box, as shown in figure 3, will pop up. Using this dialog box, the user can change the underlying database or other settings.

Figure 3: Dialog Box to change the underlying database

For details about this dialog box, please see General Settings

After saving the settings, click on OK. This will take you back to Figure 1.

After you click OK, there could be following cases.

Six Cases that can happen when starting MonitorWare Console

Case 1: Your login and password is validated and is correct and there is no update required for the underlying database that you set in Figure 3. If this is the case, you will enter MonitorWare Console successfully and you will see a form similar to the one shown below:
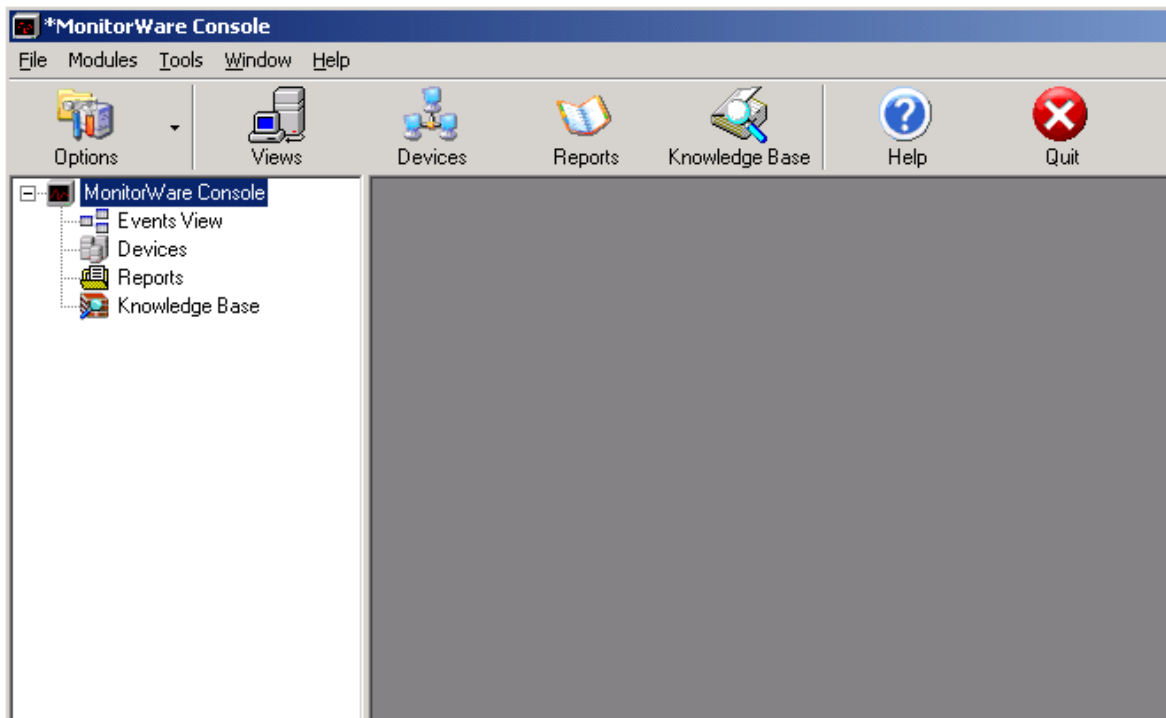
Figure 4: Main Form of MonitorWare Console

Case 2: Your login and password fails because you have either entered wrong login and wrong password. If this is the case, you will stay on this dialog box and it will ask you for the correct login and password again. Following message box will be displayed to you:

Figure 5: Login Fail Dialog

Case 3: Your database to which the DSN in figure 3 is pointing to is not a valid DSN. By valid DSN, we mean that the DSN is not pointing to the database that contains SystemEvents table. In this case, you will get the following message box:
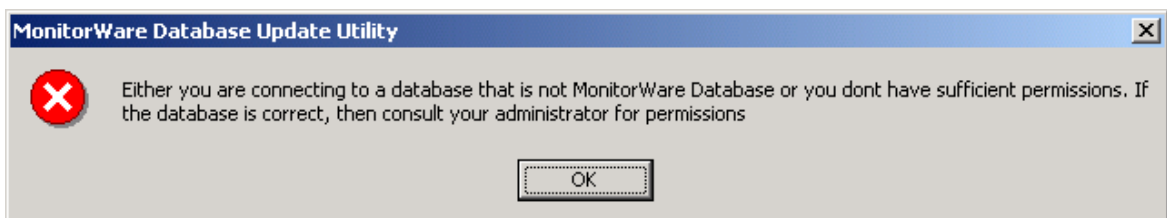

Figure 6: Invalid Database

Case 4: Your database to which the DSN in figure 3 is pointing to is valid but you

dont have sufficient permissions to query it. In this case, once again a dialog box similar to the one shown in figure 6 will be displayed

Case 5: You dont have sufficient permissions to write something to the registry. In this case, again a dialog box complaining that you dont have sufficient permissions will be displayed to you.

Case 6: Your login and password is valid and your DSN is pointing to the correct MonitorWare database but the database is old. MonitorWare Console will display you the following message:
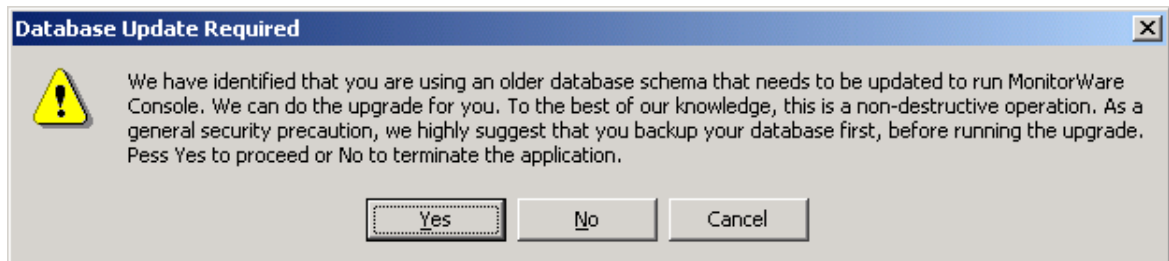

Figure 7: Database Update Required Database

If you click on Yes, the database will be updated (because console needs some additional tables for house keeping). If you click on No or Cancel, the dialog box will disappear taking you to the main dialog in figure 1.

2.3   Obtaining a Printable Manual

A printable version of the manual can be obtained at
http://www.monitorware.com/en/Manual/

The manuals offered on this web page are in PDF format for easy browsing and printing. The version on the web might also include some new additions, as we post manual changes – including new samples – frequently and as soon as they become available.

3   Using MonitorWare Console

MonitorWare Console now comes with Multiple license options. This means that you dont have to purchase complete product. Obviously the needs of different customers are different. We, at Adiscon, always keep our customers in mind. With this Multiple License approach, you dont have to pay for those things in which you are not interested. You can simply order for those modules that best suit you according to your needs and hence this reduces the cost tremendously.

MonitorWare Console comes with the following modules:

1). Base Product (This has to be purchased in order to use other modules)
2). Network Scanning Tools
3). Windows Reporting Module
4). PIX Reporting Module
5). Knowledge Base Module
6). Devices' Module

7). Views Module

3.1 General Things

3.1.1 Main Form

Once inside the main application, user will see a form similar to the one shown in Figure 1

1). Menu Bar
2). Tool Bar
3). Tree View
4). Main area where all child forms would be displayed
5). Tree Nodes
6). Status Bar

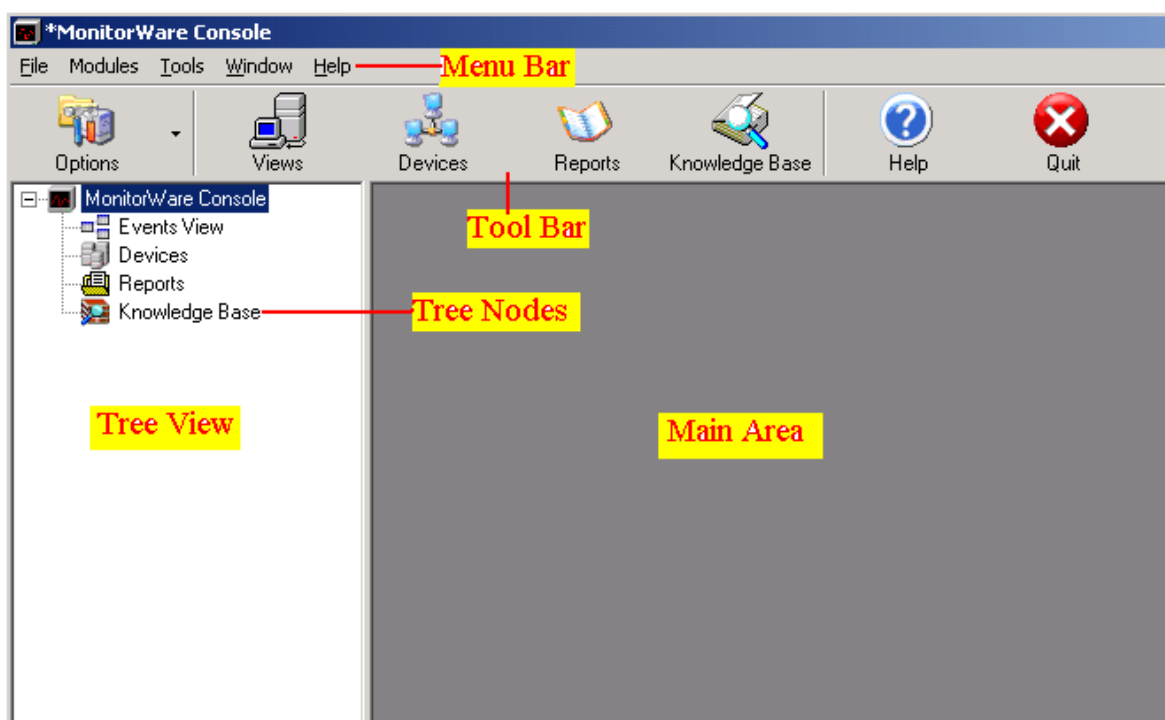*Figure 1: MonitorWare Console: Main Form*

Introduction to the components of Main Form

Menu Bar: It contains sub menus, which will take the user to different modules present in this application.

Tool Bar: Tool bar has a number of different buttons on it and it also does more or less the same thing as done by sub menu items in the menu bar. Clicking on these buttons would take the user to another module of this application.

Tree View: The left region of the application is the Tree View, which displays

different Tree Nodes in it.

Tree Nodes: When the application starts, it displays 4 main tree nodes. Clicking on any of them would take the user to the respective module.

Main Area: The gray region in the center is currently not showing any thing. When any of the nodes from the tree view is clicked, or a button from the tool bar is clicked, or user selects some sub menu item from the menu bar, it displays the main form, corresponding to the selected module.

Status Bar: It informs the users about important messages through out the application usage.

3.1.2 MonitorWare Console License Options

There are two ways of accessing this Licesne form.

1). Starting Console and clicking on "License Options" Link on bottom left.
2). Clicking on Options -> MonitorWare Console License Options in the main form of MonitorWare Console.

In any case, it will open up a dialog box similar to the one shown below:

Figure 1: Licence options Dialog Box

In this dialog, you can view/enter information related to the module name, license name and license key. There is also a link (i.e. Order Now Button) to order the product directly via our online ordering system.

MonitorWare Console now comes with a different licensing structure. MonitorWare Console license structure has been splitted into two essential parts that is:

1. Base Product Key and,
2. Your Required Module Key

The modules which are shipped with MonitorWare Console are:

1). Device Module
2). Knowledge Base Module
3). Windows Reporting Module
4). Pix Reporting Module
5). Views Module
6). Network Scanning Tools

The base product and every module calls for an individual license. This approach has been adopted keeping in mind the customer's ease. Another reason for adopting this

approach is for reducing the total cost of the product for the end user.

For example a customer might be interested in the Windows Reporting Module only and the other modules of the MonitorWare Console are of no use for him. So why should he pay a high cost for the modules in which he isn't interested? With the convention that we have adopted the customer wouldn't pay for the modules that he is not interested in. In the quoted example the customer would need the Base Product plus the Windows Reporting Module only.

Note 1: You have to buy the Base Product Key (that is a must), as without it you will not be able to use the MonitorWare Console application.

Note 2: All modules are shipped with MonitorWare Console but these are available only when the license for a specific module is entered.

MonitorWare Console either runs in:

    1). Licensed mode or,
    2). Trial mode

Download MonitorWare Console from the following URL:
http://www.mwconsole.com/en/Download/

Once you have downloaded and installed MonitorWare Console, the base product and all the supported modules will run in a trial mode (i.e. for 30 days).

Once the trial period is over you can't use the application any more. You have to buy the license key for the base product plus the license key for the modules in which you are interested.

Note: Please bear in mind that if for some reason the Base Product has expired (trial period is over, or the license has expired), you will not be able to use the other modules or features of MonitorWare Console (even if the modules are licensed). MonitorWare Console Base Product should be running in licensed or trial mode for accessing these modules and features.

Note: Trial keys follow the same set of rules as defined for the license .i.e the base product and all modules calls in for an individual trial key.

In the main Form there is a "Request Trail" Button. The following example will help you to better understand how the request trail button works.

We assume that you have downloaded and installed MonitorWare Console on 1st/Jan (to be more specific). Since the application is running in a trial mode it will expire after 30th/Jan. Once your copy of MonitorWare Console is expired, you can't access the application as the Base Product has expired. A dialog as shown below will be displayed:
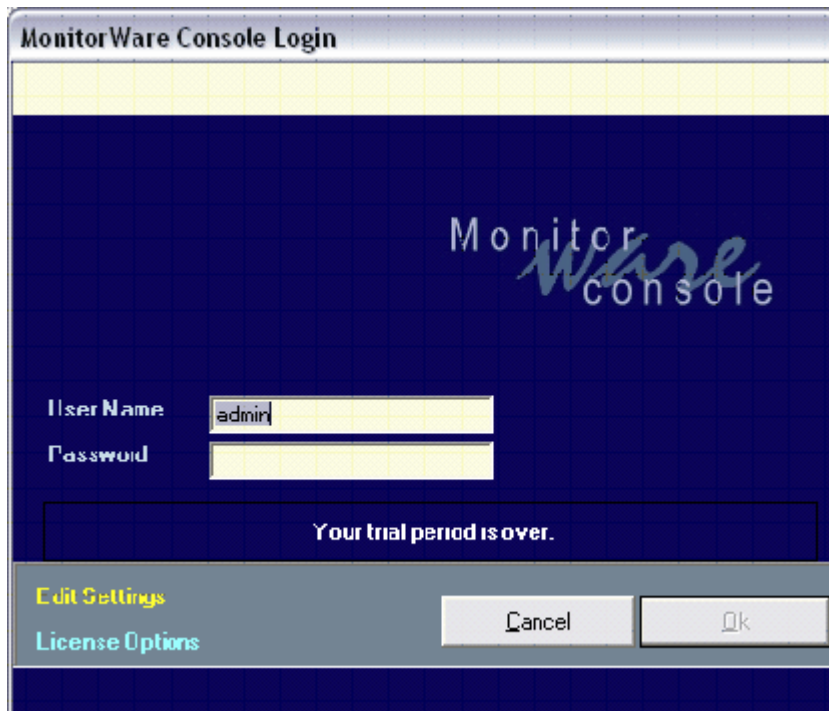
Figure 2: MonitorWare Console main dialog – showing trial period is over

As you can see that the "OK" button is disabled i.e. you can't enter the MonitorWare Console application. If you press the License Option a dialog similar to the one shown in figure 2 will open up.

Now if you selecet any module from the list (displayed in the bottom of the form), and press "Request Trial" a dialog is displayed that says: "You can only request trials for other modules if your base product is in trial or is licensed."

So, This will call for a license key for the Base Product. Assume that you had bought the product key and entered the key. If you now press the request trial button after entering the license key for the base product, it will not switch the desired module to trial version. A dialog similar is displayed that says: "You cannot request trial for this module for another 30 days".

This is because the user will get at most a 30 day trial period followed by a 30 day disabled period. In the above quoted example your MonitorWare Console application worked through the month of January. In February the application expired. Now if you press the request trial button during March for a specified module, it will switch to the trial version.

Note: The user can press the "Request Trial" Button, maximum 4 times i.e. 30 day trial period followed by a 30 day disabled period and so on. After 4 times the MonitorWare Console will not go into the trial version anymore.

If the "Request Trial" is pressed for the Fifth time, a dialog appears that says: "You cannot request trial for this module any more".

Note: Please bear in mind that you can't "Request Trial" for the base product.

The fields used in this form are described below:

Module Name for License
This option allows you to choose the module which you are interested in. A drop down list displays the following options:

  1). Base Product
  2). Device Module
  3). Knowledge Base Module
  4). Windows Reporting Module
  5). Pix Reporting Module
  6). Views Module
  7). Network Scanning Tools

License Name

The option allows you to enter the license name for each individual module.

License Key

This option allows you to enter the license key for each individual module.

Clear

This option will clear all the enteries made in license name and key.

Update

Allows you to make updation to old entries.

Note: Please select the name of the module that you are updating from the list displayed as in figure 1 and not from the drop down list of Module Name for License.

Request Trial

This option will allow you to request for a trial version for the desired module.

Note: Please select the name of the module that you are requesting trial for from the drop down list of Module Name for License and displayed as a list in figure 1.

Cancel

Closes the form.

3.1.3   EventID.NET License Options

You can access this by clicking on Options -> EventID.net License Options. Once clicked, the following dialog box will be displayed:
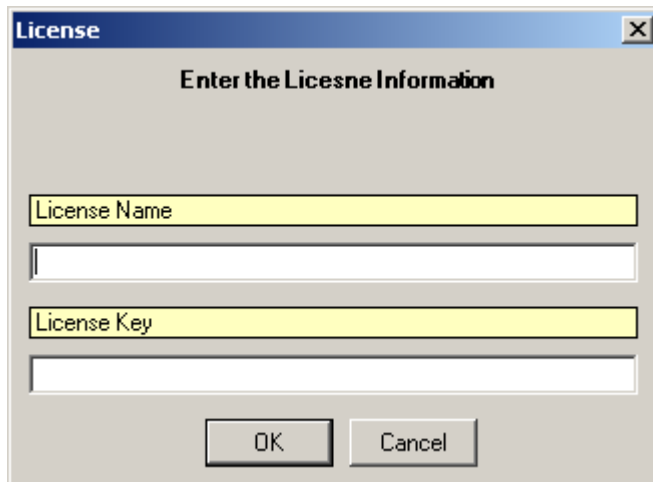

Figure 1: License Form for EventId.net

In this form, you can enter the License Name and the key given by EventId.net. Even if you don't enter the License Name and Key, still you will be able to search for event ids (on eventId.net site) that are displayed in the reports. However, with the license, you get some additional benefits.

The fields used in this form are described below:

License Name

License Name given by EventID.net

License Key

License Key given by EventID.net

OK

Saves the settings and closes the form

Cancel

Closes the form without saving the information

3.1.4 Web Search URLs

If you click on Options -> Web Search URLs, you will see a dialog box similar to the one shown below:
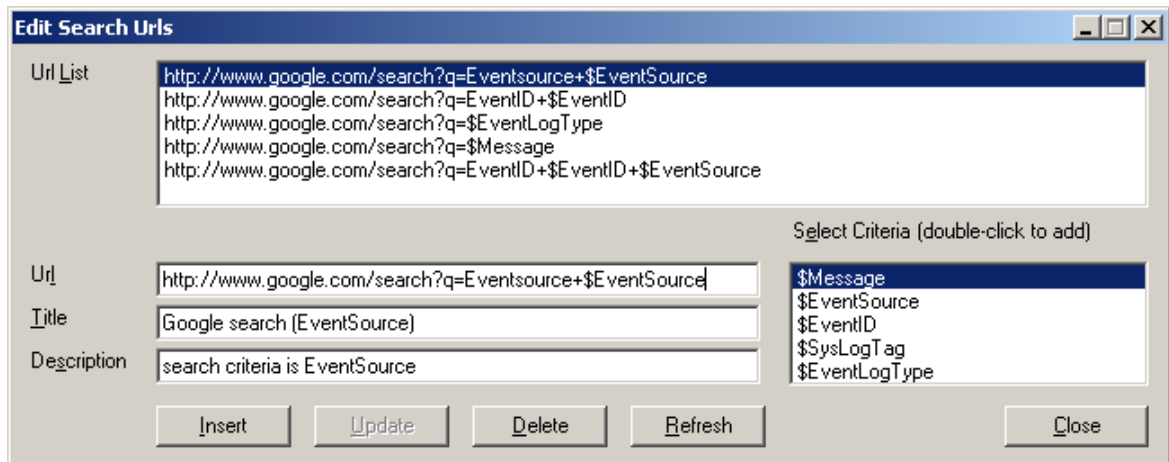

Figure 1: Web Search URLs

Using this form, you can define your query strings (URLs) that will be used for searching of a particular thing from the views form or from the devices form by clicking on the "Web Search" button.

Select Criteria List

This list can be used to add a tag to the URL. For example, if "$EventSource" is double clicked, it will move in the URL text field. Now when you use the above mentioned URL to search, it will replace "$EventSource" with the "EventSource" value for that particular event in the views form. Similarly, you can define the combination of different criteria as well as shown above in the URL List. This list will be displayed when you press the Down Arrow on the Web Search button as shown below:
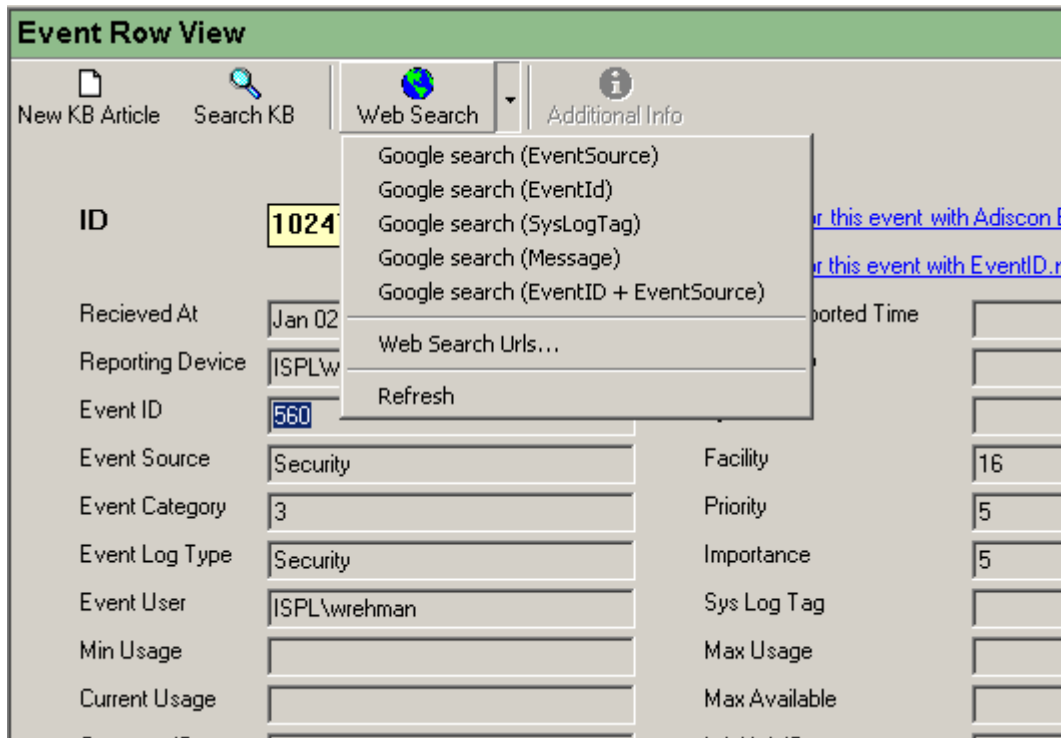
Figure 2: Web Search Button

The list that you can see above, is actually the list that you have defined in Figure 1. So it is recommended, that you use meaningful names for each query string so that you know that when I click on a particular query string, it will look for what.

The fields used in this form are described below:

Insert

Insert is used to insert a new entry of URL to the URL list.

Delete

Delete is used to delete some existing entry of the URL in the URL list.

Update

Update is used to update some existing entry of the URL in the URL list.

URL List

It displays all existing entries of the URLs.

Refresh

It simply refreshes the URL list from the database.

Close

Closes the form.

3.1.5 General Options

Once you click on the File Menu, the following options are displayed as shown in the dialog. Options available are:
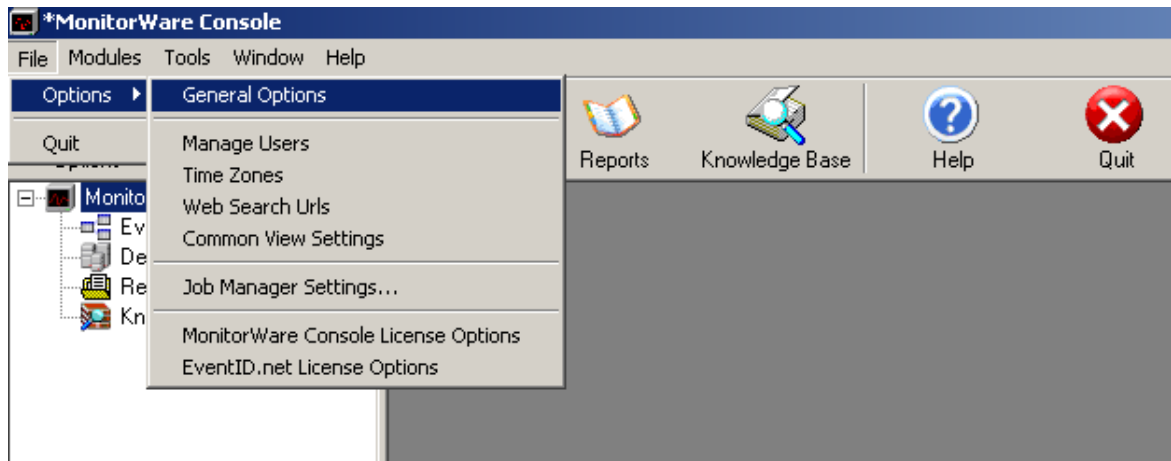
1). Options
2). Quit

Figure 1: File Menu

Click on Options and then click on General Options

Note: Options can be accessed by clicking on the Options button in the MonitorWare Console main window.

3.1.5.1 Lookup

Once you click on the General Options the following Screen shot is displayed:
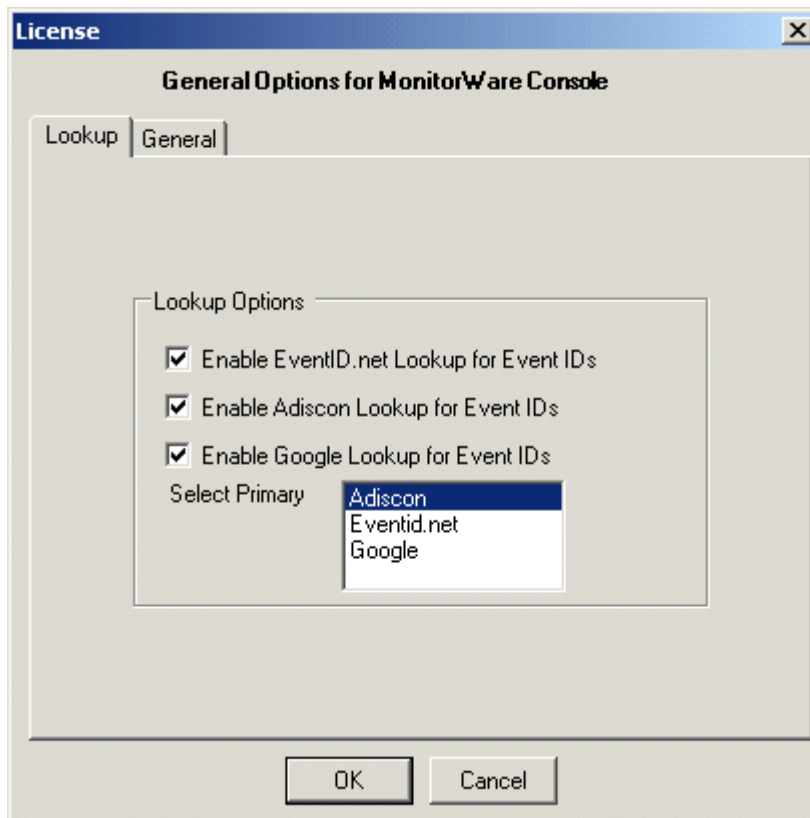

Figure 1: Lookup Tab

The Lookup tab allows you to specify the links that you would like to see in the reports in which Event IDs are present. Currently, these links will be displayed in "Needle in the HayStack Report" and "System Status Report".

Lookup Options

In the Lookup Options you would see three check boxes:

    1). Enable EventID.net Lookup for Event IDs
    2). Enable Adiscon Lookup for Event IDs
    3). Enable Google Lookup for Event IDs

For all those checkboxes that are checked, a lookup link will be shown in the generated reports wherever any EventID is displayed. That link will take you to the respective site. For example, if you have selected "Enable Adiscon Lookup for Event IDs", then in the report, you will see a link for all Event IDs. Clicking on these links will take you to the Adiscon Events' Repository and you will find a description of that event.

Select Primary

If more than one check boxes are selected, then you can use this option to select the

primary link. The one that is selected as the primary link, will be displayed on top of others. For example, Lets say that you have selected all three checkboxes above. Then you selected Adiscon as the primary Lookup link. In this case, when the report is generated, it will show you all three links for the Event IDs but the Adiscon Links will be displayed before other links.
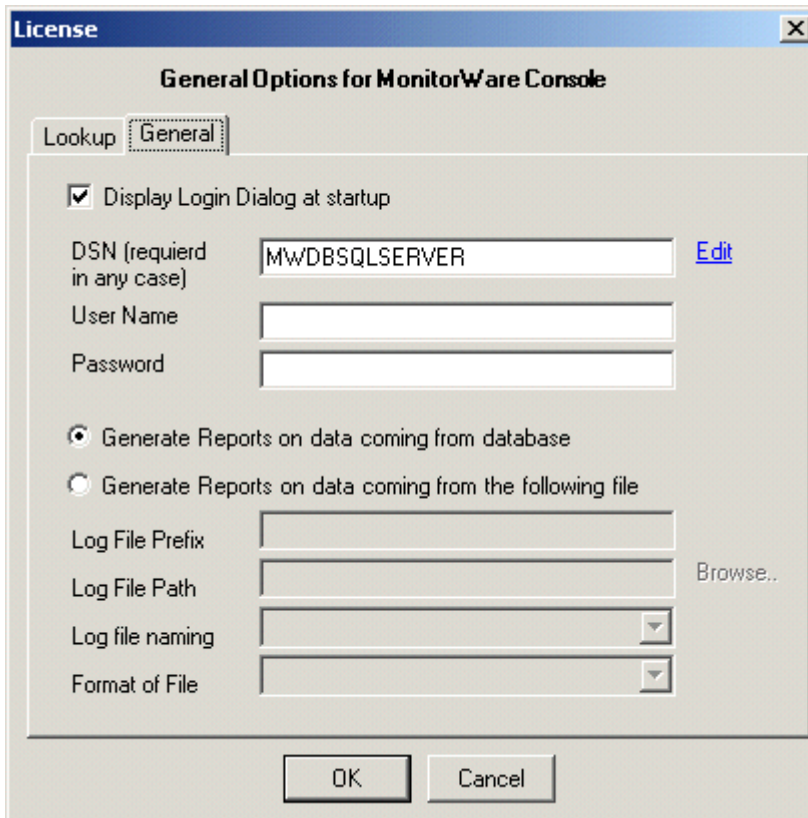
3.1.5.2 General

Figure 1: General Tab

Display Login Dialog at Startup

If checked the dialog box in figure 2 appears every time at the startup of the MonitorWare Console application. If unchecked it will directly take you into the Monitorware Console main application without displaying Figure 2.
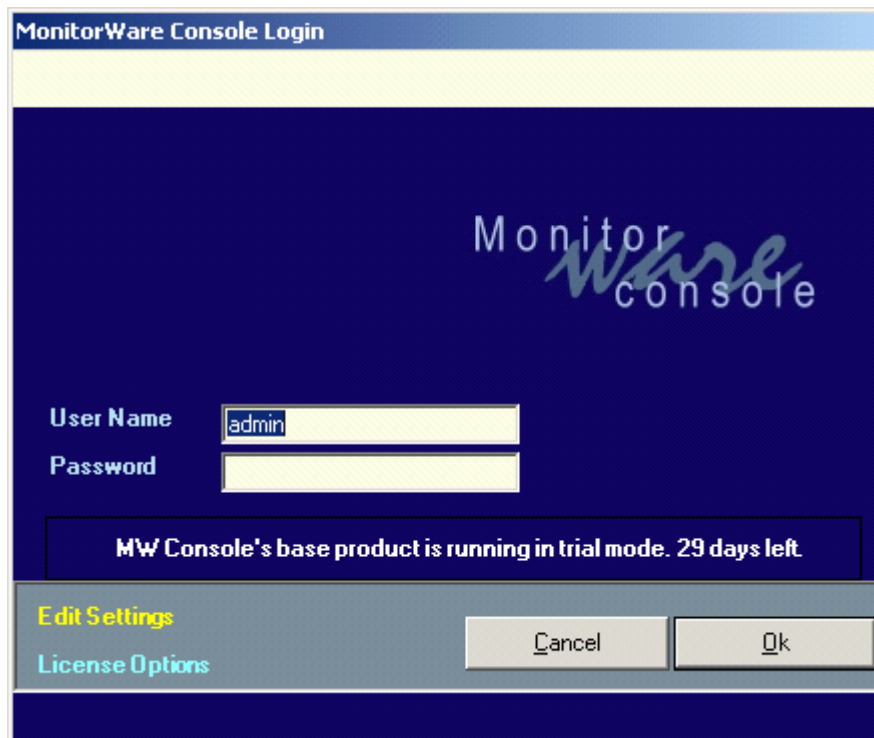
Figure 2: Main dialog

Note: The dialog in Figure 2 would appear irrespective of the setting of the above checkbox if:

1). The underlying database used by MonitorWare Console needs to be updated.
2). MonitorWare Console can't connect to the underlying database.
3). Login and Password aren't correct.
4). If the Base Product has expired.

DSN
This field is mandatory. This will point to the DSN of the database which will store all the settings related to the MontitorWare Console . And later on this will work as the underlying database to which MonitorWare Console is connected.

Edit
This options opens up a dialog box for creating the DSN. A dialog similar to the one displayed opens where you can configure the settings according to your environment.
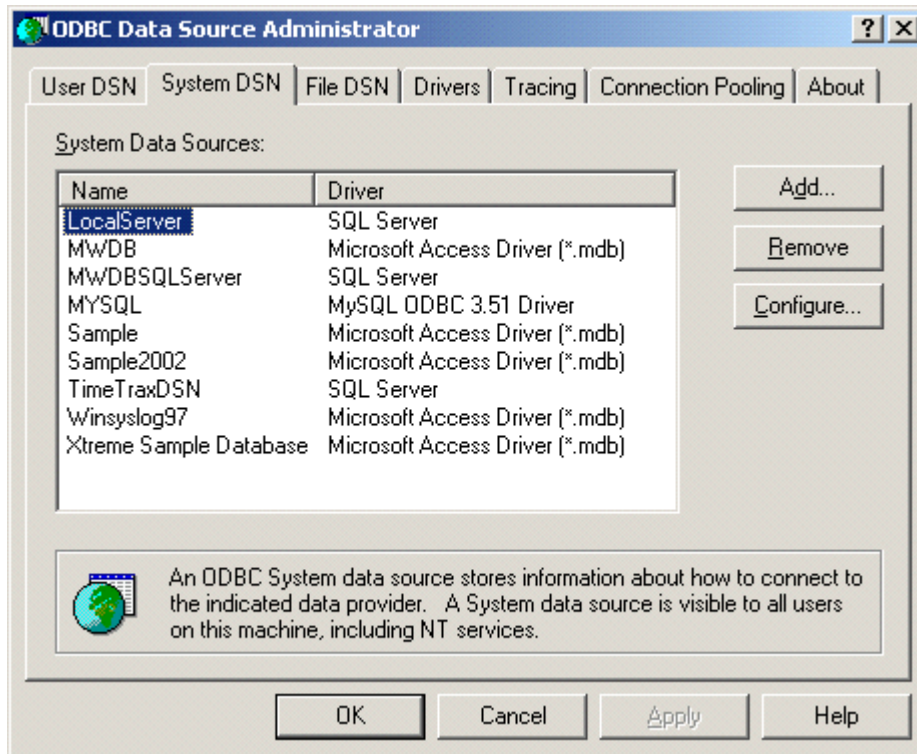
Figure 3: Dialog Box to create a DSN

Once the provider and the connection has been selected, Test Connection button can test whether the connection with the specified database has been established or not.

If the dialog box, as shown in figure 4, is displayed, it means that the connection with the specified database has been set up properly and the user can proceed further by pressing the OK button
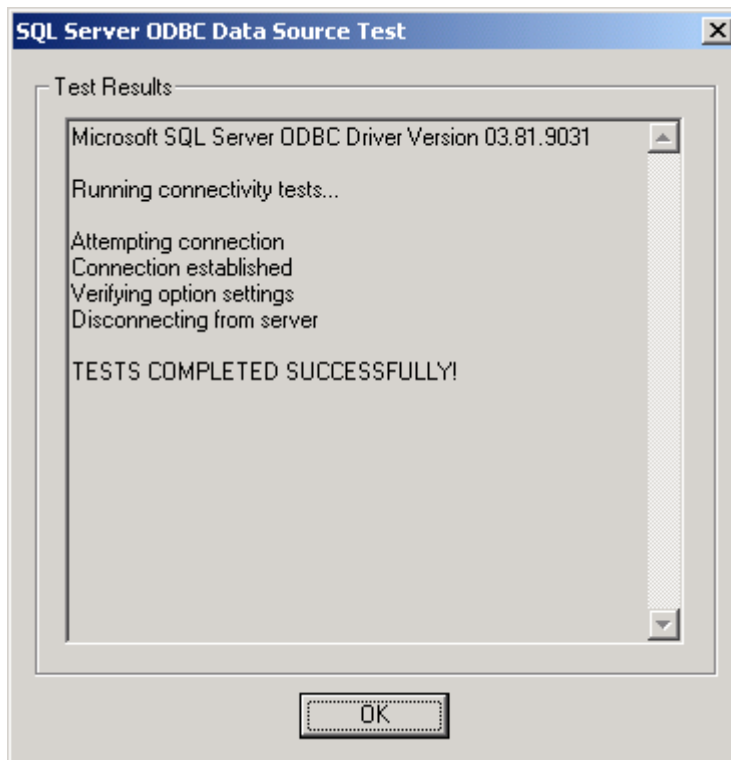
Figure 4: Success dialog

On the other hand, if a dialog box, as shown in figure 5 is displayed, it means that there is something wrong and the connection with the mentioned database has not been established.
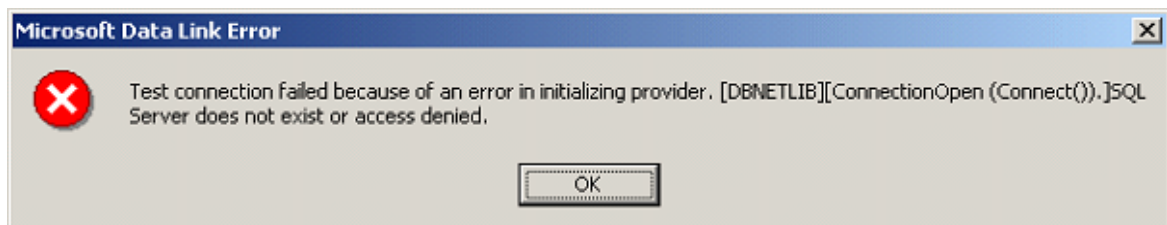

Figure 5: Connection Failure Dialog Box

User Name

This option allows you to configure the User Name for connecting to the database.

Password

This option allows you to configure the Password for connecting to the database.

Note: If you had created the DSN with the "Windows Integerated Security", then you don't need to give any user name or password.

Generate Reports on data coming from database

If this option is checked then in Windows Reporting Module and Pix Reporting Module

the reports would be generated on the basis of the underlying database. We have provided this option so that if your main data on which you want to generate reports is present in some other database, then you can give its DSN over here.

Generate Reports on data coming from the following file

If this option is checked then in Windows Reporting Module and Pix Reporting Module the reports would be generated on the basis of the configured log files and not on any database

Log File Prefix

This option allows you to enter the prefix of the log files that have been generated by our other products. MonitorWare Console will go in the specified path and will look for files starting with this prefix.

Log File Path

This option allows you to enter the path of the folder which contain the log files.

Browse

This option will open a dialog box from where you can select the path of the log files. A dialog similar to the one below opens up.
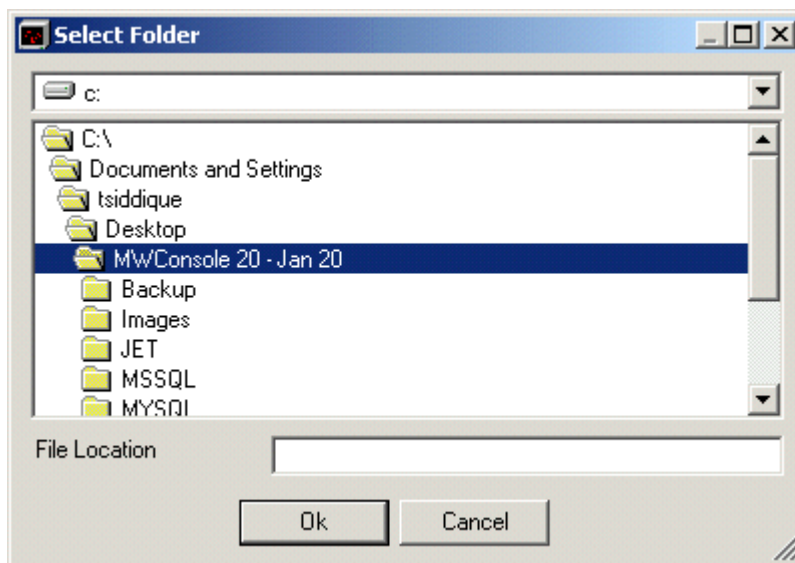

Figure 6: Browse - Select Folder Form

Log File Naming

This option allows you to select the naming convention for your log files. Options available are:

    1). Adiscon(LogPrefix-yyyy-mm-dd.log)
    2). Single

Note: Console expects a certain format of the log files. If the log files are not in the correct format, then in that case no report will be generated. You can take a look at the format in Windows Reporting module for windows log files and PIX Reporting Module for PIX log files.

Type of Parser

This option allows you to select the type of the parser used for parsing the log files. Options available are:

    1). Adiscon Parser for PIX
    2). Adiscon Parser for XML

Note: If you are interested in PIX Reports then choose Adiscon Parser for PIX. If you are interested in Windows Report then choose Adiscon Parser for XML.

OK

Saves the settings and quits the form.

Cancel

Quits the form without saving the settings.

Note: Please note that the settings for this dialog box are global settings. It means that whenever you open up any report, it will be opened up with these settings. You can overwrite these settings for each report on individual basis.

3.2   Modules

3.2.1   Base Product

Base Product is the core of MonitorWare Console. You cannot use MonitorWare Console without the Base Product. So lets say that you are interested only in "Windows Reporting Module", then you would have to purchase 2 licenses. One for the "Base Product" and the other one will be for "Windows Reporting Module". Base Product gives you following functionality:

1). ICMP Lookup Tool
2). Database Maintences Tools
3). Exporting and Importing Database Settings Tool
4). Managing Users Tool
5). Time Zone handling tool

3.2.1.1   ICMP Lookup Tools

ICMP Lookup is a feature that helps to get information on the basis of ICMP type and ICMP sub type.

To access this tool, go to the tools menu in the main menu bar, select ICMP Lookup sub menu. It will show you a dialog box similar to the one shown below:
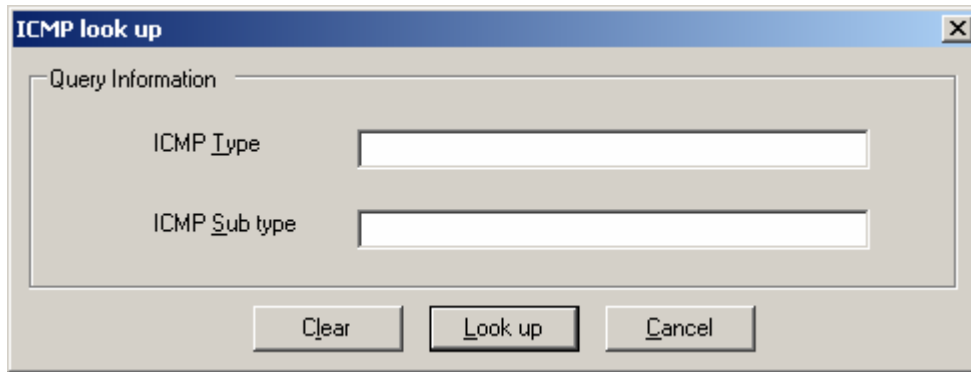
Figure 1: ICMP Look up form

The fields used in this form are described below:

ICMP Type

This option allows you to enter ICMP Type number e.g. 3

ICMP Sub Type

This option allows you to enter ICMP Sub Type number e.g. 2

Look up

After pressing the Look Up button, it will take you to Adiscon's Repository (a web page will be opened), where a description of the desired ICMP code would be displayed.

Clear

It will clear the form.

Cancel

It will take you out of the ICMP Look up form.

3.2.1.2   Export / Import Database Settings Tool

MonitorWare Console settings are saved in the database to which it is connected, instead of saving it to the registry files. With this tool you have the flexibility to import or export the database settings to which MonitorWare Console is connected. This is specifically helpful during support routine as this enables us to create the exact scenario in our test lab.

To access this tool, go to the tools menu in the main menu bar, and select Export / Import Database Settings Tool. Once this has been done, the following dialog box will appear:

Figure 1: Export / Import Databse settings Tool

The fields used in this form are described below:

As you can see from the dialog box, this dialog has been divided into three parts. Here is a brush-up detail.

The first part of the form allows you to choose the operation that you are interested in precisely. Each one is defined separatley below:

Export Database Settings

This option allows you to export settings of the selected tables to an xml file.

Import Database Settings

This option allows you to import settings of the selected tables from the selected xml file.

The second part of the form provides a list of tables that can be exported. Each of the options are defined below:

Reports Related

This option enables you to export reports related tables only.

Job Manager Related

This option enables you to export job manager related tables only.

User Preferences Related

This option enables you to export user preferences related tables only.

User Info Related

This option enables you to export user info related tables only.

Note: When you press Export button for this table then the user information i.e the user's defined login and password is also exported. A dialog box will appear as shown below:
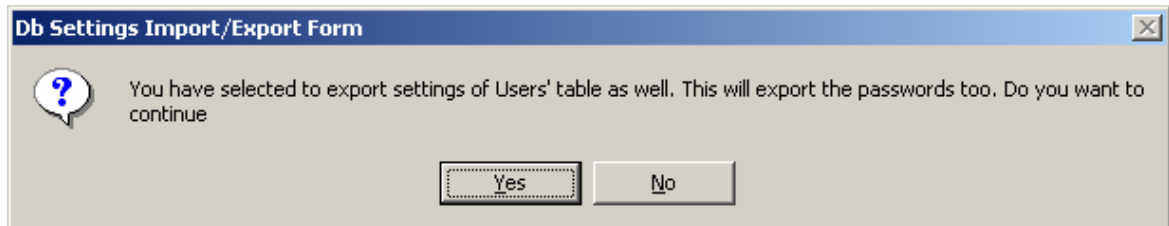

Figure 2: Database Settings Import/Export Form

Web Search Related

This option enables you to export web search related tables only.

The third part of the form allows you to manipulate file options. Each is defined as below:

FileName

This option allows you to specify the name of the file that is to be exported.

Note: This field would only be available if the user wants to export the tables, he is interested in.

File Path

This option allows you to specify the name of the file that is to be exported.

Note: If the user is exporting then this field will point to the path of that file. If the user is importing then this field will contain the file name and its path.

Browse

When this button is pressed, a dialog appears which allows the user to select the desired path on which the xml file is residing.

The Fourth part of the form allows you to manipulate the form as a whole. Each is defined as below:

Export / Import

When this button is pressed then either it exports or imports the settings, depending upon the selection that the user have made.

Note: If the Export Database Settings is checked then this button will appear as Export. If the Import Database Settings is checked then this button will appear as Import.

Cancel

When this button is pressed, it takes you out of the export / import database settings form.

3.2.1.3   Managing Users

To create, update or delete a user for MonitorWare Console application, Manage Users form is used. This form can be opened in one of the following ways.

1). Click on Options button the main tool bar and then select "Manager Users".
2). Go to File menu and select options. In options, you will find "Manage Users" Menu.

After the user has selected one of the above-mentioned methods, the following form will open up.
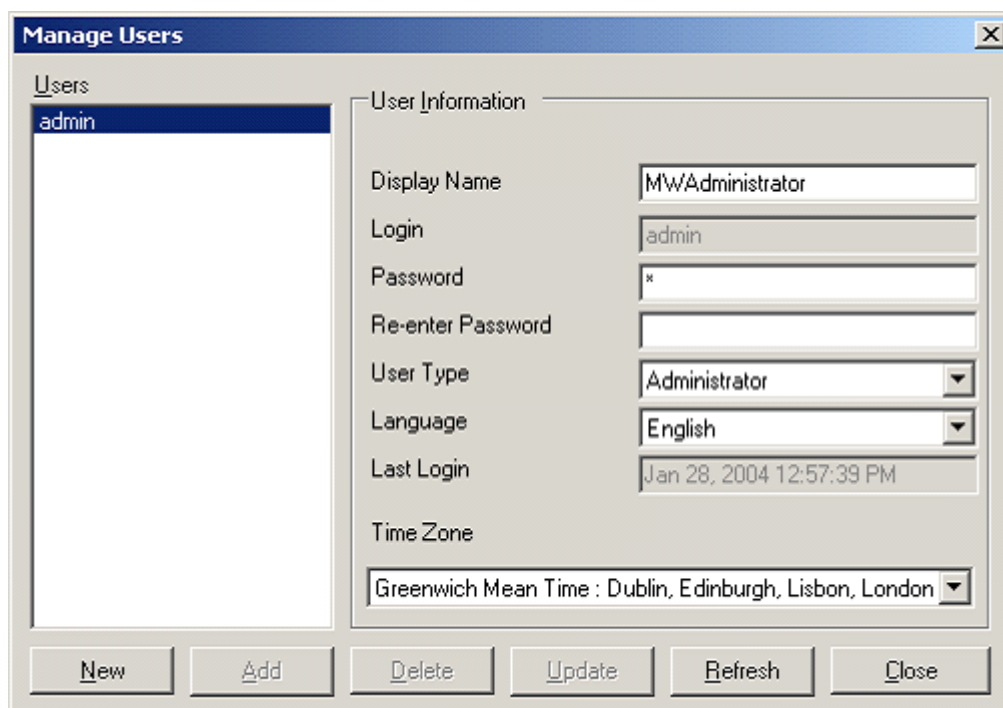

Figure 1: Manage Users Form

Notice that Login text field, User Type combo box, New, Add, Delete and Refresh buttons are disabled. The reason is that this snap shot has been taken when a regular user (not administrator) was logged on to this application. In other words, if a normal user enters into MonitorWare Console application he can only update his status (except for login and user type). On the other hand, if the user enters into this application as an administrator, then he has the full control on all the users. He can

create a new user, delete an existing user or update an existing user.

Following is a brief summary of each component on this form:

- **Display Name:** The text written in it will be used as the display name for the user .

- **Login:** The text written in it will be the actual login of the user that will be used in the User Verification form when the application is started (available for administrator only).

- **Password:** Contains the password of the user.

- **Re-enter Password:** When creating a new user, make sure that Password and Re-enter Password text fields have the same contents.

- **User Type:** Can either be an administrator or a simple user (available for administrator only).

- **Language:** In the current version, only English can be selected.

- **Last Login:** Displays the last login date and time for the selected user.

- **Time Zone:** Displays the time zone of the selected user.

- **Users:** The list box "Users" displays all the users that can use this application.

- **New:** This button is used to create a new user (Available for administrator only).

- **Add:** This button adds a new user (available for administrator only).

- **Delete:** This button deletes selected user (available for administrator only).

- **Update:** This button updates an existing user.

- **Refresh:** Refreshes the list of users from the database.

- **Close:** Closes the "Manage User" form.

3.2.1.4 Time Zones

Time zones can be modified by one of the following ways:

1). Click on the Options button and then on Time Zones menu in the main tool bar.
2). In File menu, you will find Time Zones menu. Click on it to open up the Time Zones form.

After the user has selected one of the above-mentioned ways, a dialog box, similar to the one shown in the figure 1 would be displayed:

In the current version, only the "Name" and "Offset UTC" field are in a working condition. The other fields are related to Day Light Saving concept but are to be implemented.

A brief summary of all of the components on this form is given below:

- **Name:** It displays the name of the currently selected time zone.

- **Offset UTC:** It tells the difference of the current time zone from GMT in minutes.

- **New:** This button is used for creating a new time zone.

- **Add:** This button is used for adding the newly created time zone to the database.

- **Delete:** It deletes the selected time zone permanently from the database.

- **Update:** It updates an existing time zone.

The changes made from this form will be visible in the Manage Users form's Time Zone combo box as well.

Figure 1: Time Zones

3.2.1.5 Database Maintenance Tools

3.2.1.5.1 Backup Records Tool

With this tool you have the flexibility to take the backup of the records from the database to which MonitorWare Console is connected.

To access this tool, go to the tools menu in the main menu bar, and select Database Maintenance Tools, then select Backup Records from sub menu. Once this has been done, the following dialog box will appear:
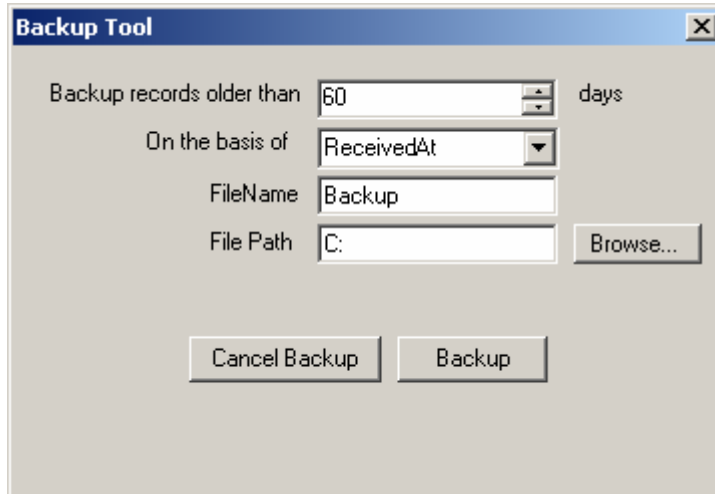

Figure 1: Backup Tool Form

The fields used in this form are described below:

Backup records older than 'x' days

This option allows you to take the backup of the records older than 'x' number of days where x is user defined.

On the basis of

This option allows you to take backup on the basis of DeviceReportedTime and ReceivedAt Time (these fields are defined in the SystemEvents Table).

Note: DeviceReportedTime and ReceivedAt Time are different from each other.

The DeviceReportedTime is actually the time that is there in the Windows Event Log i.e. the time at which the (e.g. syslog) message was written into the Windows Event Log.

ReceivedAt time on the other hand is the time when the (e.g. syslog) message is received at the configuration program e.g. MonitorWare Agent.

File Name

This option allows you to define the name of the file in which to backup the data.

File Path

This option allows you to define the path of the file where the backup will be taken.

Browse

When this button is pressed, a dialog appears which allows the user to select the desired path on which the backup file would be saved.

Cancel Backup

When this button is pressed, the backup procedure is cancelled.

Backup

When this button is pressed, the backup procedure is initiated.

After Filling the required information and pressing the Backup button, a dialog similar to the one displayed below appears:
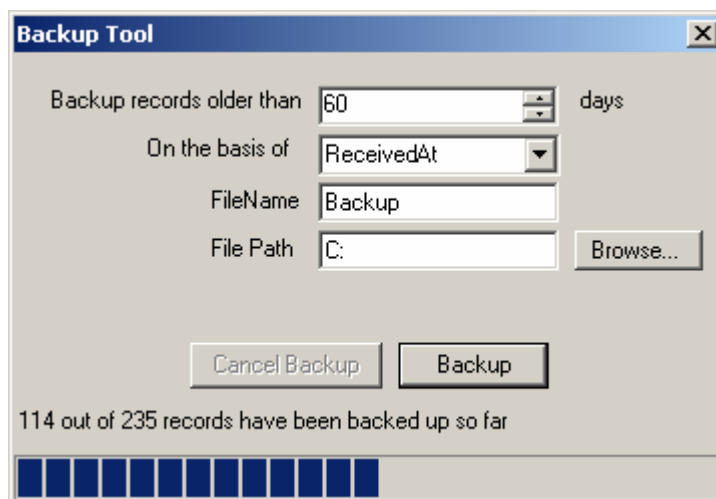

Figure 2: Backup Procedure under process

Note: The backup file saved on the desired location is saved in an xml format. The Backup file Name has the format similar to the one in the example e.g. Backup2004-2-16.xml (i.e. File Name + Date appended). If you keep on taking backup frequently, this file format will help you to distinguish between the files generated during the backup procedure.

3.2.1.5.2 Delete Records Tool

The underlying database to which the MonitorWare Console is connected can grow very rapidly depending on the incoming traffic. If you want to delete the old records for more disk space then this tool will provide you the flexibility to delete the records or to take the backup and then delete the records from the database to which MonitorWare Console is connected.

To access this tool, go to the tools menu in the main menu bar, and select Database

Maintenance Tools, then select Delete Records from sub menu. Once this has been done, the following dialog box will appear:
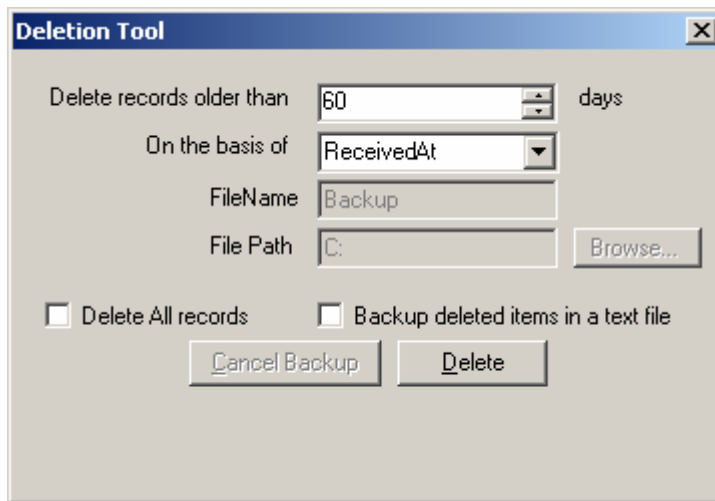

Figure 1: Delete Tool Form

The fields used in this form are described below:

Delete records older than 'x' days

This option allows you to delete the records older than 'x' number of days where x is user defined.

On the basis of

This option allows you to take backup on the basis of DeviceReportedTime and ReceivedAt Time (these fields are defined in the SystemEvents Table).
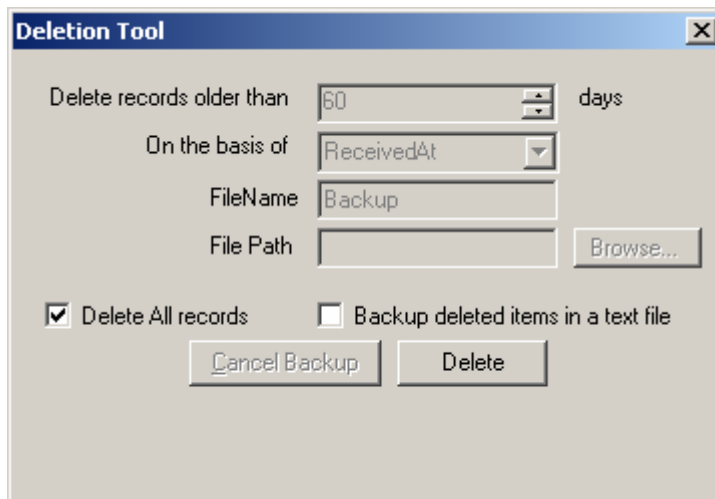
Note: DeviceReportedTime and ReceivedAt Time are different from each other.

The DeviceReportedTime is actually the time that is there in the Windows Event Log i.e. the time at which the (e.g. syslog) message was written into the Windows Event Log.

ReceivedAt time on the other hand is the time when the (e.g. syslog) message is received at the configuration program e.g. MonitorWare Agent.

Delete All Records

If you check this option than all the records are deleted from the database to which the MonitorWare Console is connected.

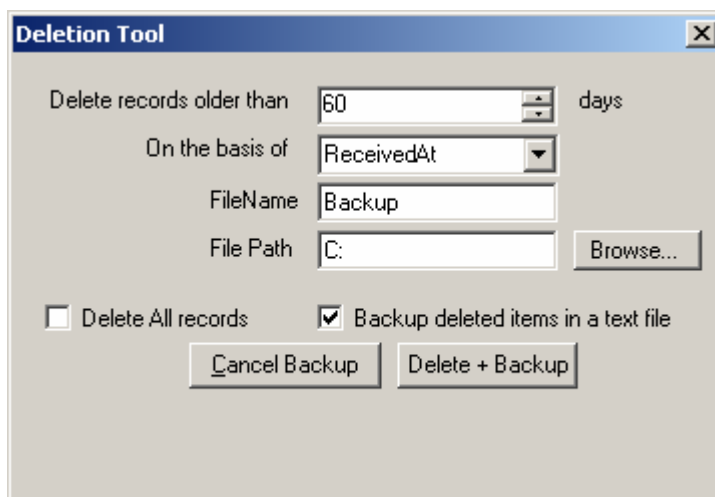*Figure 2: Delete Tool Form - Delete all records*

Note: If you press the "Backup deleted items in a text file" over here then it will take the backup of all the records and then these records are deleted from the underlying database to which MonitorWare Console is connected.

Delete

When you press this button a message box will appear that will give you a warning that this will delete all the records permanently. If you press yes to it, the records would be deleted permanently.

Backup deleted items in a text file

As you can see from the "Deletion Tool Form" in figure 2, the File Name, File Path and Browse Button are grey-scaled. This scenario occurs if you have not checked "Backup deleted items in a text file" option. Once you have checked the "Backup deleted items in a text file" option these options become valid as shown below:

Figure 3: Delete Tool Form - Backup Deleted item in a text file

If this option is checked then it also takes the backup of deleted (which are to be deleted) records in the specified path.

File Name

This option allows you to define the name of the file in which the backup of the deleted records wouldl be taken.

File Path

This option allows you to define the path of the file where the backup of the deleted records would be taken.

Browse

When this button is pressed, a dialog appears as shown in the figure 4. This allows the user to select the desired path on which the backup file will be saved.
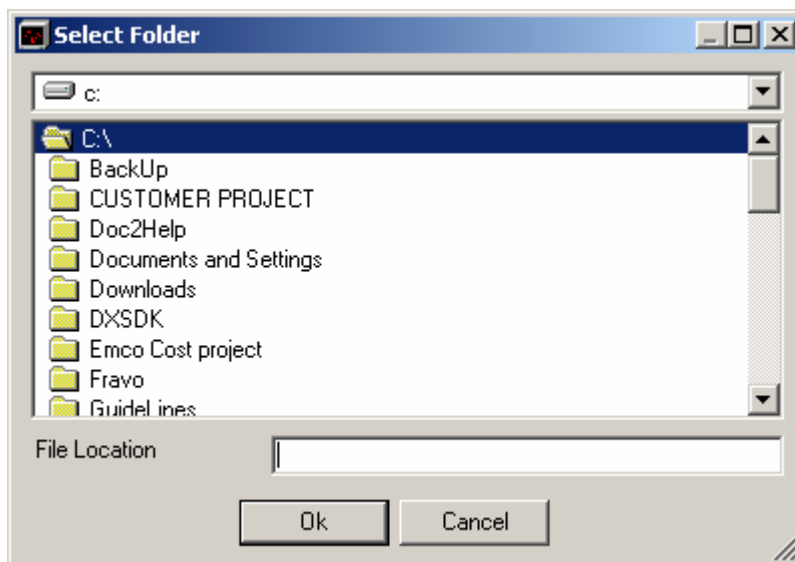

Figure 4: Browse - Select Folder Form

Delete + Backup

When this button is pressed then the records that are defined in the specifed range are deleted from the database to which MonitorWare Console is connected but the backup is taken before hand.

Cancel Backup

By pressing this button, the "Deletion Tool" form is closed.

3.2.1.5.3 Retrieve Records Tool

With this tool you have the flexibility to retrieve the records into the database to which MonitorWare Console is connected.

To access this tool, go to the tools menu in the main menu bar, and select Database Maintenance Tools, then select Retrieve Records from sub menu. Once this has been done, the following dialog box will appear:
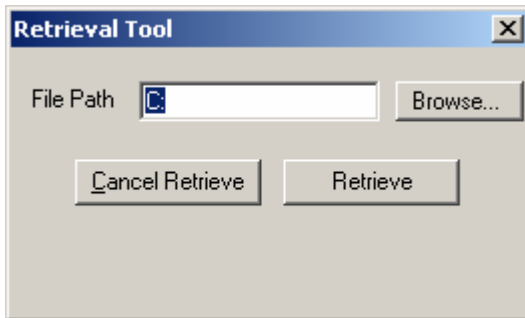

Figure 1: Retrieval Tool Form

The fields used in this form are described below:

File Path

This option allows you to enter the path of the file that will be used for retrieving the records.

Browse

When this button is pressed, a dialog appears which is user configurable. This dialog allows the user to select the desired path on which the backup file resides i.e. to be used for record retrieval purpose.

Cancel Retrieve

When this button is pressed, the records retrieval process is cancelled.

Retrieve

When this button is pressed, the records retrieval process is initiated.

Note: If you haven't deleted the records after taking the backup and you retrieve the backup file; then records are retrieved into the database to which MonitorWare Console is connected. In this case there would be a duplication of records. But if the records have been deleted and then retrieved then there would be no duplication of records.

3.2.2 The Reporting Module

Adiscon MonitorWare Console offers flexible and extendible reporting features. In addition to several useful reporting templates provided with the application, users can order new reports exactly according to their own requirements and these new reports will be incorporated in MonitorWare Console application seamlessly.

The Reporting Engine of MonitorWare Console has been designed in such a way that the reports can act as Plug and Play components. If you feel that you need a report that is not present in MonitorWare Console, you can ask us at support@adiscon.com and we will look into what it takes to generate the report. We will then let you know if there is any cost associated for creating this report. Even better, during the introductory phase of MonitorWare Console, reports are free of charge!

Once you give us a go, we create the new report exactly according to your requirements and will send you the plug in component. All that you have to do is to put the component in the proper place (which we will let you know when we ship the component to you) and it will become fully integrated with MonitorWare Console. Even you do not have to install MonitorWare Console again.

Any reports generated by Adiscon will become part of the standard product. As such, you can be sure that your report will always be adjusted to new product versions - without any cost at all!

Reporting Module is subdivided into two main modules for which you would have to purchase the license separately.

1. PIX Reporting Module
2. Windows Reporting Module

In the next chapter, we will discuss the things which are general and common to both PIX and Windows Reporting Module. Then we will proceed to the specifics of PIX and Windows Reporting Module and also will explain the Job Manager which is used for scheduling of reports.

3.2.2.1 General Things

3.2.2.1.1 Defining Global Settings

You can define some global settings for the reports. These settings will be shown for each report when you click on any report. Ofcourse, you have the liberty to overwrite these settings. These settings help you out if you want to generate many reports with almost the same settings. You can access the form for setting the global settings for reports in one of the following ways:

1). By clicking on Options-> General Options-> General Tab
2). By clicking on File-> Options -> General Options-> General Tab
3). Starting Console-> Clicking on Edit Settings on the bottom left of the main dialog box.

For details about this form, please see Genaral Tab of General Options

3.2.2.1.2 Report Manager

You can open up Report Manager by:

1). Clicking on "Reports" button in the main tool bar.
2). Clicking on Modules -> Reports from the menu bar.
3). Clicking on "Reports" node in the tree view on the left.

After you have followed any of the above mentioned steps, you will see something similar to the following figure:
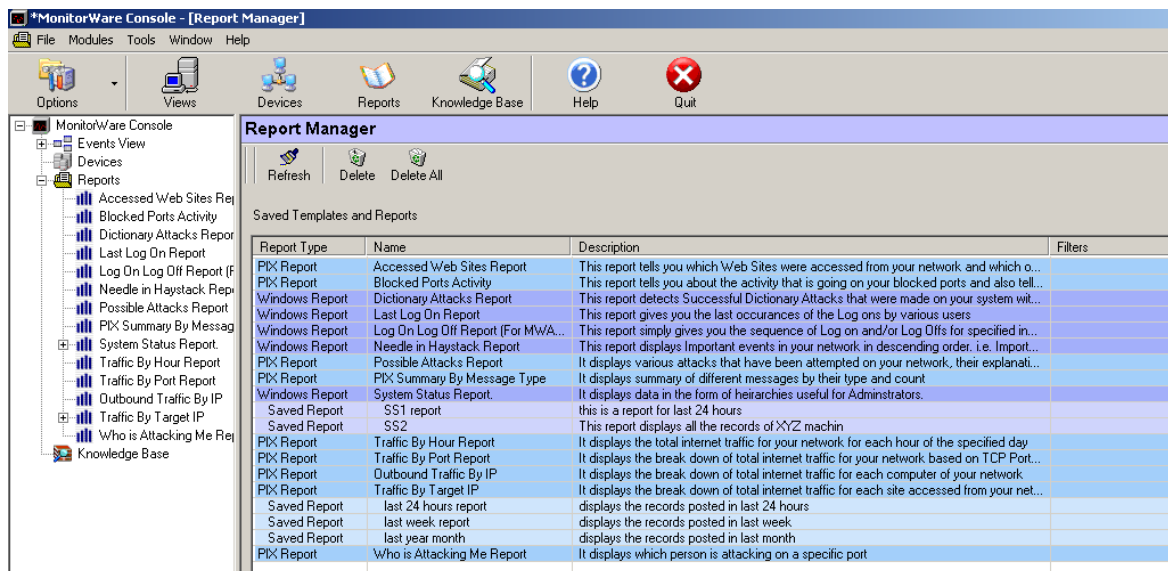

Figure 1: Report Manager

Before we proceed, its important to give 2 definitions here that will be frequently used throughout the Reporting Module.

Report Template

Report Tempate is the report that is shipped with MonitorWare Console. All of the reports with which "PIX Report" is written or "Windows Report" is written, are Report Templates. You can create as many "Saved Reports" as you like from these "Report Templates" by applying different filters for different Saved Reports

Saved Report

Saved Reports are the reports which you can save by opening up a specific template. For each report you can specifiy different settings that will apply to only that Saved Report. For example, in the above figure, there are 3 "Saved Reports", which the user has saved himself for the Report Template "Traffic By Target IP". Each Saved Report can have its own name, own description, own settings and own filters. In the above sample, the first saved report i.e. "last 24 hours report" has been saved by applying the filter so that the "Traffic by Target IP" is displayed for the last 24 hours only.

Report Manager (RM) provides a centralized control over all Reporting related

functions. In Figure 1 RM is the screen visible on the right hand side – visually it is identified with title in a lilac band on the top of the screen. Report Manager provides following functions:

1). RM displays the list of all templates and saved custom reports. In the Report Manager, you will see some reports in Blue color and some in Purple color. The reports in Blue color are PIX reports. The reports in the Purple color are the Windows Reports. The ones in the lighter shade are their corresponding Saved Reports that the user has saved after applying some filters on that report.

2). RM is synchronized with the Tree control present on the left hand side of the main window. The same templates and saved custom reports are shown hierarchically in the tree control as well. Saved custom reports are shown as sub nodes to the corresponding templates. In the above figure, a plus (+) sign with System Summary template in the tree control tells that there are saved custom reports available for this template.

Refresh

This button in the RM toolbar fetches the fresh list of reports.

Delete

Deletes the selected template and its corresponding saved reports as well. Note that, templates (being .dll files) are not physically deleted from the folder, they only get un-registered from the application. To register them again, simply click on "Refresh".

Delete All

Deletes all of the reports and their corresponding saved reports.

3.2.2.1.2.1 Opening a Report

If you double click on any report, it will open up the following form
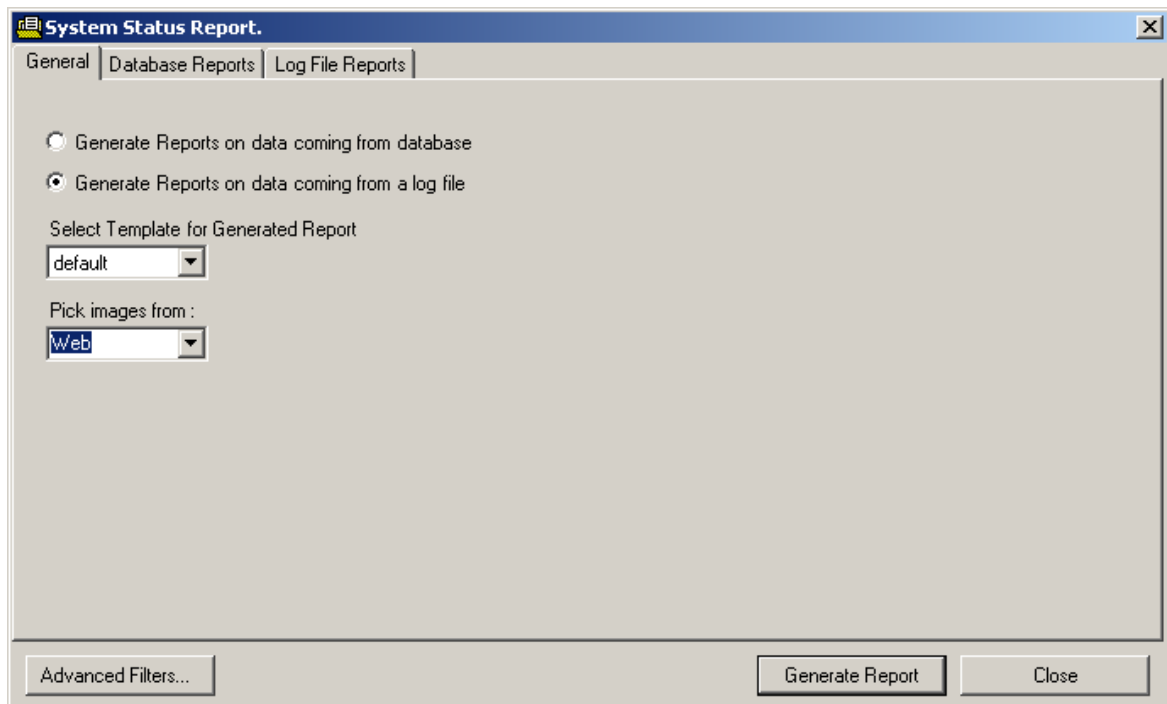

Figure 1: Report Options

This form displays the report options. If you double clicked on any "Template", then in that case, this form will open up with default options that you had set. (See Defining Global Settings). On the other hand, if you double clicked on any "Saved Report", then this form will open up and will display you the settings that you had saved.

Advanced Filters

In some of the reports, you will find this Advanced Filter Button on the Filter Form. These filters are those filters that are required specifically by the current report and don't have any thing to do with the underlying database. For example for the System Status Report, clicking on "Advanced Filters" button will open up a form similar to the one shown below:

Figure 2: Advanced Filter Form for System Status Report

Generate Report

This button will generate the report according to the settings that you have made in this form.

Close

Simply closes this form.

In the following chapters, the three tabs on this form will be explained.

Figure !: General Tab

Generate Reports on data coming from database

If you select this option, then the report will be generated on the configured database. If this option is selected, then all of the controls on "Log File Reports" tab will be disabled.

Generate Reports on data coming from a log file

If you select this option, then the report will be generated on the configured log file. If this option is selected, then all of the controls on "Database Reports" tab will be disabled.

Select Template for Generated Report

You can select various templates for the HTML reports that will be generated.

Pick images from

This option allows you to pick images from web or from the local disk

Figure 1: Database Reports Tab

You have the option of generating the reports on the fly. Even if MonitorWare Console is connected to some other database, still you can give any DSN, its user name and its password in the above fields and the report will be generated on that particular database to which the DSN is pointing to.

DSN

The Data Source Name that is pointing to the database on which you want to generate the reports.

User Name

The user name for that database. If you have generated the DSN using Windows Authentication, then you don't need to enter any thing in this field.

Password

The password for that database. If you have generated the DSN using Windows Authentication, then you don't need to enter any thing in this field.

Select Column

With this combo box, you can select the column on which you want to apply the filter.

Select Operator

Several operators are provided for applying meaningful filters. These operators generally correspond to the most common SQL operators that maybe mentioned in the WHERE clause. For additional information on the use of operators see Operators' Reference.

Select Lower Value

In the "Select Lower Value" combo box, values corresponding to the selected field (Select Column combo box) are picked from the database for user's convenience.

Note: Only top 100 values corresponding to each field are picked for this purpose. However, users can enter their own values if required.

Select Upper Value

In the "Select Upper Value" combo box, values corresponding to the selected field (Select Column combo box) are picked from the database for user's convenience.

Note: Only top 100 values corresponding to each field are picked for this purpose. However, users can enter their own values if required.

Add

This button will be enabled only when "is one of" or "is not one of" operator is selected from "Select Operator" Combo box. You can select different values from "Select Lower Value" combo box and click this button to add to the list on its right. Please note that the filter will not be added, until you click on "Add Filter" button.

Remove

This button will be enabled only when "is one of" or "is not one of" operator is selected from "Select Operator" Combo box. You can select different values from the list on its right and click this button to remove them from the list on its right. Please note that the filter will not be updated, until you click on "Add Filter" button.

Add Filter

Clicking the "Add Filter" button, after specifying the filter, adds that filter to be applied to the report. All added filters are displayed in the text box on the filter form. Any number of filters maybe added. However, only one operator maybe applied on one field at time. Trying to add another filter on the same field will simply result in over-writing the previous filter for that field.

All filters, applied to several different fields, are ANDed together to form one complete filter condition. This complete condition is always updated in the text box in the filter form for display.

Delete Filter

This button is used to delete a filter that has been applied earlier. Simply select the field / column on which you applied the filter from "Select Column" combo box. Once you have selected, it will display its details in the remaining controls. Simply click on delete. The filter will be removed from the text box below.

Save Report

Lets say you have appleid 5 or 10 different filters and you want to generate the same report with the same 5 or 10 filters daily. With this Save Report option, you can save this report so that you don't have to apply these filters daily. You will simply save the report and the next day you will double click on your saved report and all of the filters will be there. Saving a custom report displays the following form:
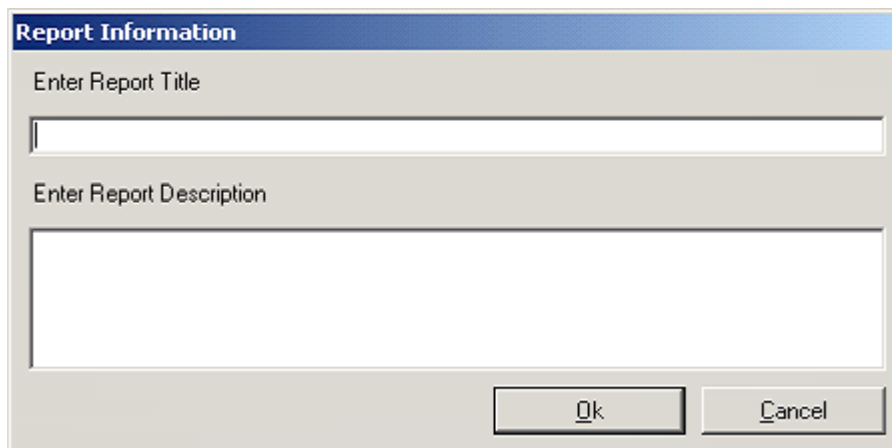
Figure 2: Saving Custom Reports

Users must enter "Report Title" and optionally, some short description for later reference. This information is later displayed in the Report Manager form for quickly finding the desired report.

Important point to note is that a custom report (that is with applied filters) can only be created against an existing template. However, any number of custom reports maybe saved for each registered template. If filters are not saved then users will need to define and apply the same filters again if they ever wish to see the same report again.

Note: Some of the controls on the filter form are only enabled under special conditions. For example, the date time picker controls are only enabled when the selected field is of DateTime type. Controls in the section "Select Upper Value" are only enabled if the selected operator requires a range of values rather than a single value. For example, "is between" operator requires a lower and an upper value to be defined for its proper working.
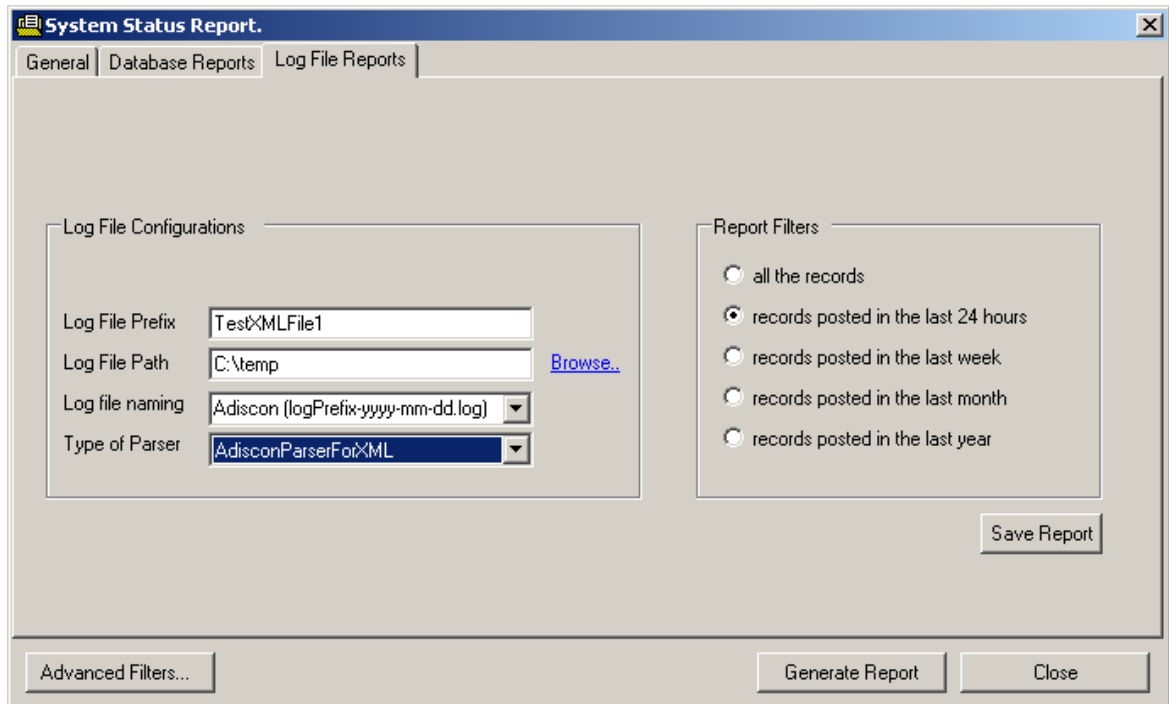

Figure 1: Log File Reports Tab

You have the option of generating the reports on the fly. Even if MonitorWare Console is connected to some other database, still you can give Log File Configurations in the above fields and the report will be generated on that particular log file.

Log File Prefix

This option allows you to enter the prefix of the log files that have been generated by our other products. MonitorWare Console will go in the specified path and will look for files starting with this prefix (depending upon the filter that you have applied).

Log File Path

This option allows you to enter the path of the folder which contain the log files.

Browse

This option will open a dialog box from where you can select the path of the log files. A dialog similar to the one below opens up.
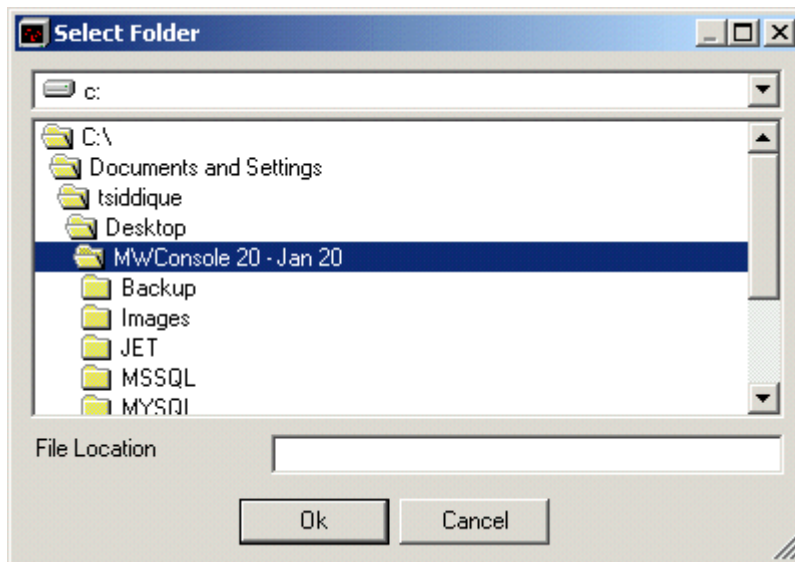
Figure 2: Browse - Select Folder Form

Log File Naming

This option allows you to select the naming convention for your log files. Options available are:

1. Adiscon(LogPrefix-yyyy-mm-dd.log)
2. Single

Note: MoniotrWare Console expects a certain format for the log files. If the log files are not in the correct format, then report will not be generated. You can take a look at the format in Windows Reporting module for Windows log files and PIX Reporting Module for PIX log files.

Type of Parser

This option allows you to select the type of the parser used for parsing the log files. Options available are:

1. Adiscon Parser for PIX
2. Adiscon Parser for XML

Note: If you are interested in PIX Reports then choose Adiscon Parser for PIX. If you are interested in Windows Report then choose Adiscon Parser for XML.

All the Records

If you have applied this filter, then the report will be generated on all the records that are present in the specified folder.

Records Posted in the last 24 hours

If you have applied this filter, then the report will be generated on only those records

that were logged in the last 24 hours.

Records Posted in the last week

If you have applied this filter, then the report will be generated on only those records that were logged in the last week.
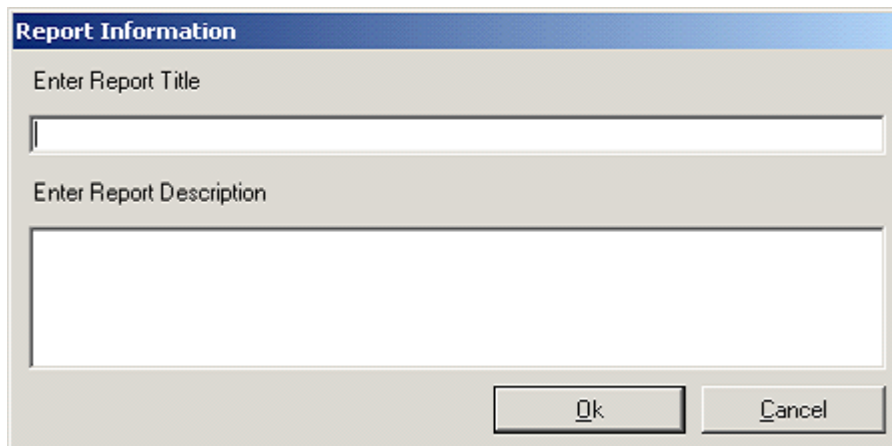
Records Posted in the last month

If you have applied this filter, then the report will be generated on only those records that were logged in the last month.

Records Posted in the last year

If you have applied this filter, then the report will be generated on only those records that were logged in the last year.

Save Report

Let us say you have given some settings for Log File Configurations and applied some filter too and you want to generate the same report with the same settings daily. With this Save Report option, you can save this report so that you don't have to apply these settings daily. You will simply save the report and the next day you will double click on your saved report and all of the settings will be there. Saving a custom report displays the following form:

Figure 3: Saving Custom Reports

Users must enter "Report Title" and optionally, some short description for later reference. This information is later displayed in the Report Manager form for quickly finding the desired report.

Important: Point to note is that a custom report (that is with applied filters) can only be created against an existing template. However, any number of custom reports maybe saved for each registered template. If settings are not saved then users will need to define and apply the same settings again if they ever wish to see the same report again.

Figure 1: Database Reports Tab - Report Filters

"Select Operator" combo box is used to apply an operator on the selected field.
"Select Operator" contains the following operators:

1. ***is any value:*** This filter can be applied when no filter is to be applied on a field.
2. ***is equal to:*** This will bring only those records that match the criteria against "is equal to" e.g. ID is equal to 4 will bring only those records where ID is equal to 4.
3. ***is not equal to:*** This will bring only those records that match the criteria against "is not equal to" e.g. ID is not equal to 4 will bring all those records where ID is not equal to 4.
4. ***is one of:*** When "is one of" is selected, user has to press the add button to add the values to the list. If any of the values matches, the record is brought. e.g. ID is one of 4, 5, 6 will bring all those records where ID is equal to 4 or ID is equal to 5 or ID is equal to 6.
5. ***is not one of:*** Same as above but the difference is that it will not bring those records that have been added in the list.
6. ***is less than:*** This will bring all the records that are less than the specified value. E.g., ID is less than 5 will bring all the records where ID value is less than 5 in the database. Note: that it will not bring a record with ID value equals to 5. In other words, the specified value is exclusive.
7. ***is less than equal to:*** Same as above but with the difference that it will bring the specified value as well. E.g. ID is less than or equal to 5 will bring all those records where ID is 5 or less. Note that in this case, the specified value is inclusive.
8. ***is greater than:*** This will bring all the records that are greater than the specified value. E.g., ID is greater than 5 will bring all the records where ID value is greater than 5 into the database. Note that it will not bring a record with ID value equals to 5. In other words, the specified value is exclusive.
9. ***is greater than equal to:*** Same as above but with the difference that it will bring the specified value as well. E.g., ID is greater than or equal to 5 will bring all

those records where ID is 5 or greater than 5. Note that in this case, the specified value is inclusive.

10. ***is between:*** This will bring the records between the specified limits. E.g., ID is between 5 and 7 will bring records where ID value is between 5 and 7. Note that in this operator, upper and lower values are inclusive. In other words it will bring records for ID equals to 5 and 7 as well if they exist in the database.

11. ***is not between:*** Same as above with the difference that it will bring all the values that are not there in the specified range. This operator is inclusive too.

12. ***is like*** & ***is not like:*** These operators are only visible in "Select Operator" combo box if the user selects a column from "Select Column" combo box whose data type in the database is *Text*. These operators work exactly like the SQL operators *Like* and *Not Like,* respectively – note that the SQL version and dialect of the underlying provider affects what syntax may be used for these operators. The operators allow users to use wild cards in filters. Refer to the following table for simple wild card characters that maybe used with Access and SQLServer databases.

Consult the SQL documentation for a more detailed list of possible wild card options and their usage:

Operation	*SQLServer*	*Access*
Match any string	%	*
Match any character	_ *(Underscore character)*	?

3.2.2.2   Windows Reporting Module

All of the reports that are shown in Purple colour are Windows Reports.

Windows Reports

Following are the Windows Reports that are present in this release.

Report Name	Report Description
System Status Report	It displays data in the form of heirarchies useful for Adminstrators.
Needle in Haystack Report	This report displays important events in your network in descending order. i.e. important ones are displayed before the less important ones.
Dictionary Attacks Report	This report detects Successful Dictionary Attacks that were made on your system within the specified period of time.
Last Log On Report	This report gives you the last occurances of the Log ons by various users.
Log On Log Off Report (For MWAgent 2.0)	This report can only run if the data has been entered in the database by MonitorWare Agent 2.x). This report gives you the sequence of Log on and/or Log Offs for specified inputs.

For detailed information on these reports, please visit
http://www.mwconsole.com/en/Product/reports.asp

Format of the Log File

If you want to generate the above Windows' Reports on log files, then its absolutely necessary that the log files are in a specific format. Only the following two check boxes in the "Write to File Action" of EventReporter, MonitorWare Agent or WinSyslog should be checked.
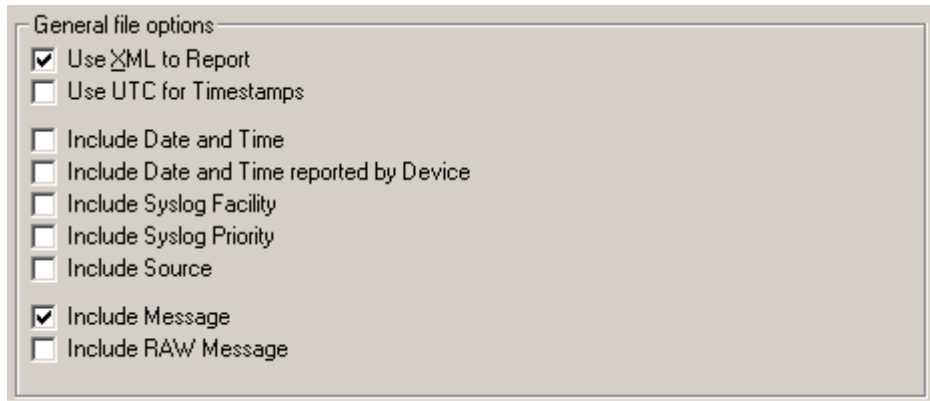
Figure 1: Write to File Action of EventReporter, WinSyslog and MonitorWare Agent.

If any of these check boxes is not checked or any other check box is checked apart from the above shown, then the report will not be generated. If the log file entries are not in the correct format, then MonitorWare Console will write error messages for first 50 lines in Windows Event Log and will ignore them for the generation of report

Note: Do NOT check "Use Legacy Format" in your event log monitor service. If you check this, the records can not properly be compressed and you will receive a very large report.

3.2.2.3   PIX Reporting Module

All of the reports that are shown in Blue colour are PIX Reports.

PIX Reports

Following are the PIX Reports that are present in this release.

Report Name	Report Description
Accessed Web Sites Report	This report tells you which Web Sites were accessed from your network and which ones were accessed the most..
Blocked Ports Activity Report	This report tells you about the activity that is going on your blocked ports and also tells the ip address from where this activity is initiating.
Possible Attacks Report	It displays various attacks that have been attempted on your network, their explanation and what should be done to avoid them.
PIX Summary By Message Type	It displays summary of different messages by their type and count.
Traffic By Hour Report	It displays the total internet traffic for your network for each hour of the specified day.
Traffic By Port Report	It displays the break down of total internet traffic for your network based on TCP Ports for each hour of the specified day.
Outbound Traffic By IP	It displays the break down of total internet traffic for each computer of your network.
Traffic By Target IP	It displays the break down of total internet traffic for each site accessed from your network.
Who is Attacking Me Report	It displays which person is attacking on a specific port.

For detailed information on these reports, please visit
http://www.mwconsole.com/en/Product/pix-reports.asp

Format of the Log File

If you want to generate the above PIX Reports on log files, then its absolutely necessary that the log files are in a specific format. Only the following check boxes in the "Write to File Action" of EventReporter, MonitorWare Agent or WinSyslog should be checked.
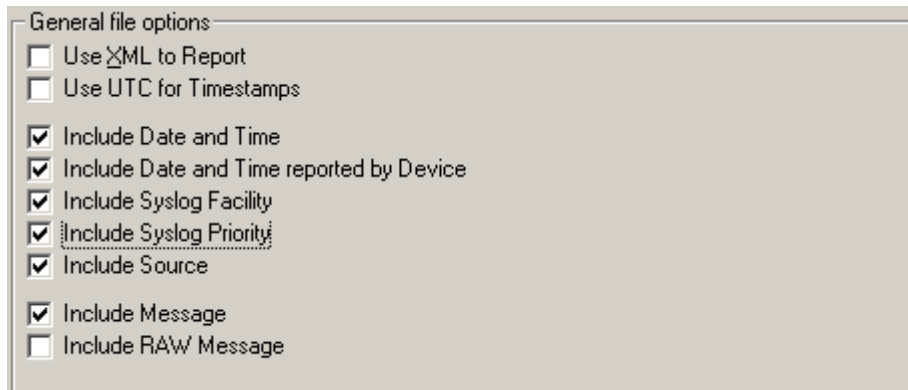

Figure 1: Write to File Action of EventReporter, WinSyslog and MonitorWare Agent

3.2.2.4 Job Manager (JM)

Job Manager is a Window Service that runs in the background and generates the reports according to user-defined schedule. It also has the capability of sending the generated reports to specified recipients via email. The settings of this service are done from the MonitorWare Console Client. This client will only be available to you if you have a valid license for "Windows Reporting Module" or "PIX Reporting Module" or both. Once you open up Job Manager Settings form as shown below, you will be able to schedule all of the reports (whether PIX or Windows) but only those reports will be generated whose license is valid. So, for example, you have PIX Reporting Module license with you, then you will be able to access the screen shown below and configure all of the reports but Job Manager will only generate those reports that are PIX and will not generate any of the configured Windows Report since you dont have the license for it.

We now have introduced Profiles for Job Manager. You can associate different reports to different profiles and they will be generated according to your specified time and date. You can create as many profiles as you like in Job Manager which means that now, you can generate the same report as many times as you would like in one day.

Job Manager can now also generate those reports that you have saved in the Reporting Module by applying various filters. The reports that are indented in Figure 1 are those reports that had been saved using Report Manager.

Job Manager helps you in generating reports on specified days and times. For example, you can tell Job Manager to generate the System Status report at 7:00 am on monday, tuesday and friday. Now, every time you come to office, you will see a complete report on your system on the above mentioned days and you can take necessary actions right away.

To access the client of Job Manager that makes settings for different reports, click on Options button on the main tool bar and then press "Job Manager Settings". You will see a dialog similar to the one shown below:

Figure 1: Job Manager Form (General Tab)

JM form will show all the available reports on the left side of the form in a list view. Select the list from this list box and use other tabs to specify different settings.

Cancel

Closes the form without saving the settings.

Back

Takes you to the previous tab, if any.

Next

Takes you to the next tab, if any.

Save

Saves the settings and restart the service only if it was already running. If it was not running, then it asks you to go to the administrative tools to manually start the service.

Selected Profile

All of the settings will be applied to the selected profile. You can create, update or delete the profiles by clicking on "Edit Profiles" button. You can create different profiles and associate the same report with that particular profile. In this way, you can schedule the generation of the same report at different times according to the settings that you have done in that profile.

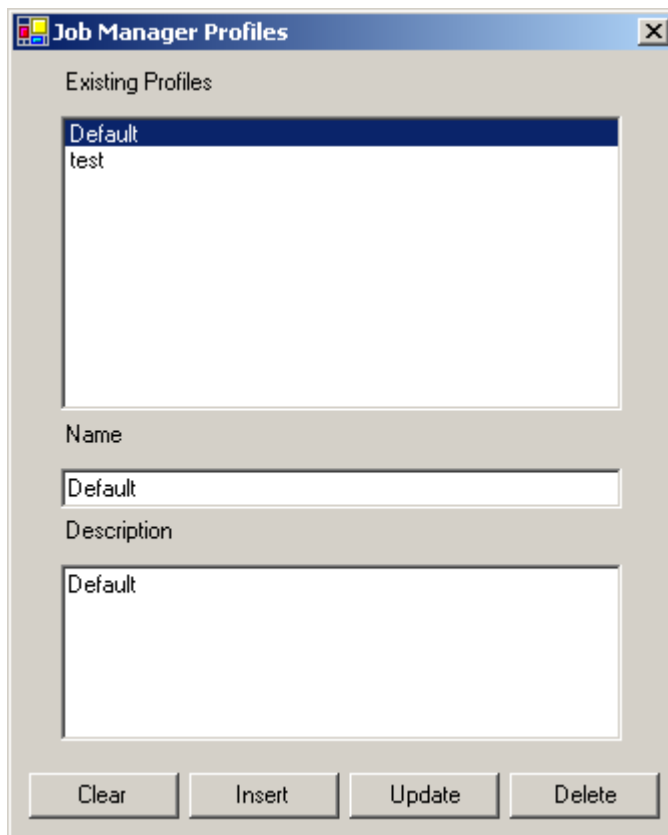**Edit Profiles**

This link opens up the following dialog box:

Figure 2: Job Manager Profiles

Existing Profiles: This list displays a list of existing profiles.

Name: Name of the profile.

Description: Description of the profile.

Insert: Inserts a new profile.

Update: Updates the selected profile.

Delete: Deletes the selected profile.

3.2.2.4.1 General Tab

Figure 1: Job Manager Form (General Tab)

Job Manager Interval

It is the interval after which the Job Manager will wake up and look for the reports that are to be generated. If it finds that its time to generate a particular report, it generates it and goes to sleep again. If it doesn't find any report scheduled for that time, then it goes into sleep again and wakes up again after this interval.

UTC Offset (minutes)

Using this you can specify the UTC offset of your locale in minutes. Please note that if you have logged the data in the file or in the database using Local Time and not as UTC time, then you should set this to zero (as shown above)

3.2.2.4.2 Action Tab

Figure 1: Job Manager Form (Action Tab)

"File Prefix" is the prefix that you want to append to the complete file name (Complete file name also includes the current date and time on which the report is generated. This is appended by the application)

You can specify in this tab that whether you want to save the report that will be generated on the specified time on the hard disk or you want to attach this report as an attachment and send it to someone.

If you want to send this report as email, select the upper radio button and press the SMTP settings button. It will ask for the server name. Write the server name over there. Then press the Message Settings button. It will open up another dialog box with information like To, CC, BCC, Subject, and Message etc. Fill in the required information and press ok.

Note: From field is mandatory in the "send as attachment in email", otherwise it will not work.

If you want to save this report on the hard disk locally, select the lower radio button and press the File Settings button. Select the path on which you want to save the file

and press ok.

3.2.2.4.3 Schedule Tab

Figure 1: Job Manager Form (Schedule Tab)

In this tab, you can specify that the selected report should run on which days and at what times. For example, in the above figure, Accessed Web Sites Report is scheduled to run only on friday at 12:00 PM

3.2.2.4.4 Filter Tab

Figure 1: Job Manager Form (Filter Tab)

In this tab, you can specify the filters that you want to apply on the generated reports. The filters shown above in the diagram are self-explanatory. Please note that if you have selected some "Saved Report" that you had saved using Reports Module, then these filters will be applied in addition to the other filters that you had applied while saving the report. When you click on any saved report, its filters are also displayed as shown below:

Figure 2: Saved Reports showing saved filters

Now this report will be generated for all those entries that have been posted in the last 24 hours AND whose Event ID is not equal to 114 AND whose Event Source is AdisconMonitorWareAgent

3.2.2.4.5 Source Tab

Figure 1: Job Manager Form (Source Tab)

Please see <u>General Tab of General Options</u> for details of these fields

If you now select some other report from the list shown on the left, these settings would be saved temporarily. They will be saved permanently only when the Save button is pressed. Once the save button is pressed and if the JM Service is already running at that time, it would give you a warning that saving these records will cause the service to restart. If you say yes to this message, your settings would be saved permanently and the service would be started again. If the service was not running at the time when save button is pressed, it will display you a message that you would have to manually start the service from the Control Panel and would save the settings permanently.

Note: For starting the AdisconMWCJobManager go to Start, click Control Panel, click Administrative Tools, Choose Services, a window will pop up. Select AdisconMWCJobManager and press start.

3.2.3 The Views Module

Views module (Raw Log Analysis) is one of the most powerful features of MonitorWare Console. Using this module, you can define your own views according to your needs. This module also supports the concept of "Drill Down". You can define various levels of field hierarchies in view definition. As you proceed towards the lower levels of hierarchies, the data is filtered using the above hierarchy levels. In addition to that, you can also apply some other filters on the data, which include: Time based filters, Device based filters and Info Unit Based filters. The details are given in the coming sections.

For views, you can define some global settings. The global settings are picked up by each view when you create it. Ofcourse, you can overwrite these values for each individual view but it definitely saves a lot of time if you want to create many new views with almost same settings. First of all, we will discuss these "Global Settings" and then we will move on to the "View Manager"

Note: For better results, it is highly recommended that "Legacy Format" is not selected in "Event Log Monitor" service in EventReporter or MonitorWare Agent.

3.2.3.1 Defining Global Settings

In this module, there is a concept of a Global Settings. Global Settings are the settings that will be applied to all the newly created views by default, although you have the flexibility to modify them for each view definition individually. To initialize Global Settings or Common View Settings, go to the Options Button in the Main Tool bar and click on "Common View Settings". A dialog box similar to the one shown in the following figure will open up:
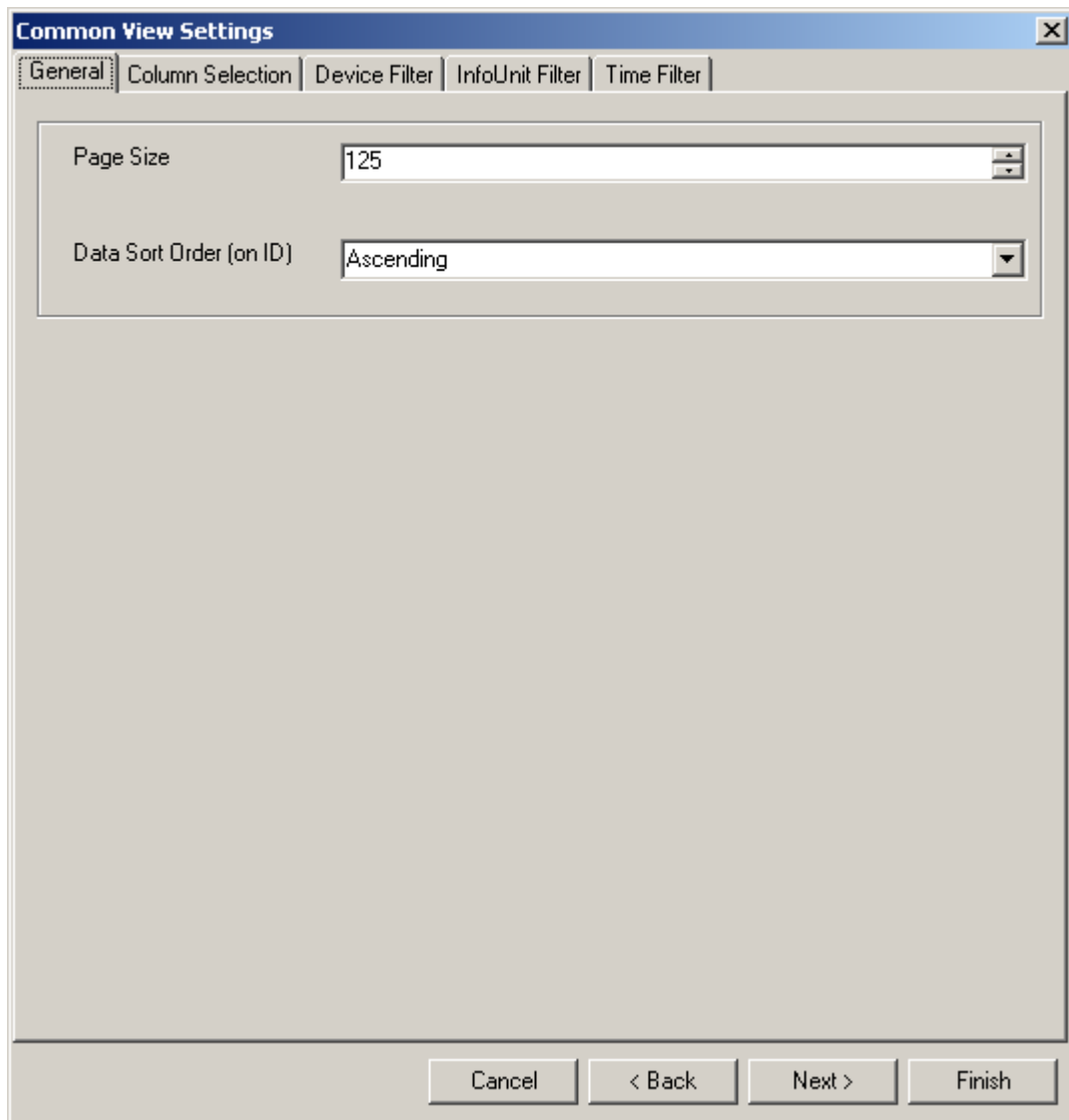
Figure 1: Common View Settings (General Tab)

This dialog box has five tabs. The following sections will describe each tab in detail.

Important Note: Please note that the filters defined in "Device Filter" tab, "InfoUnit Filter" tab and "Time Filter" tab will be ANDed together

3.2.3.1.1 General Settings

On this Tab, you can specify Page size and Data Sort Order.
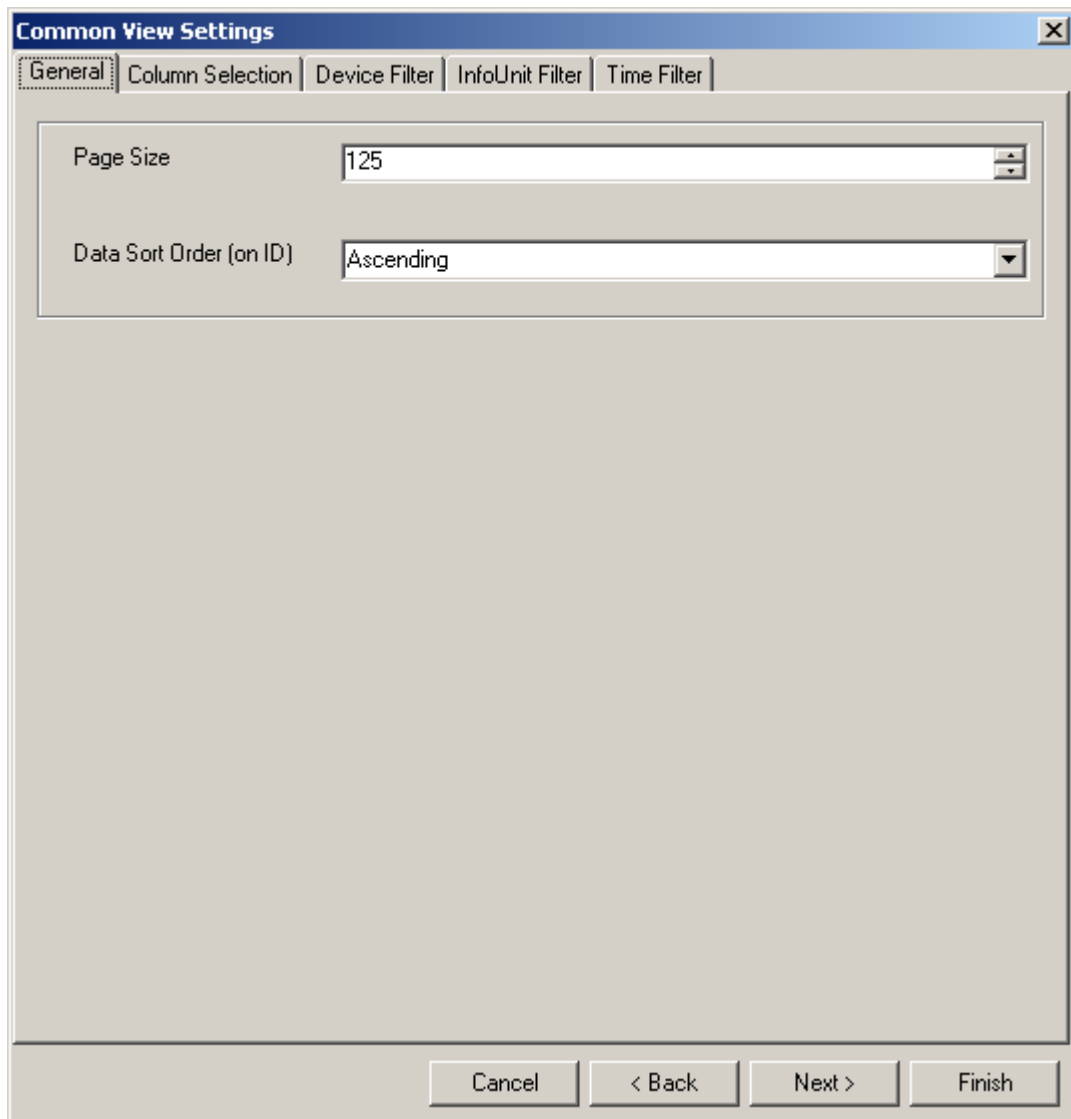
Figure 1: Common View Settings - General Tab

Page Size: Page size is the maximum number of records that user can see on one page in the data grid. If the number of records brought by the query is greater than the page size for that view, user has the option of pressing the "Next" button (will be explained in the coming sections) to go to the next page. In short, at one time user will not be able to see records greater than "Page Size" specified in this tab.

A paging algorithm has been implemented in MonitorWare Console to improve efficiency. Had there been no paging algorithm, then the data grid had to display ALL the records that are returned from the database (imagine 1 million records being returned) and the user had to wait for a very long interval of time to see the results. The paging algorithm only brings those many records at one time that are specified in the page size. So greater the page size, more will be the time for each page to be

displayed because of more number of records that are to be brought from the database but the total number of pages would be less. On the other hand, if the page size is kept small, then less time will be taken for each page to be displayed because of less number of records are to be brought from the database but this will increase the total number of pages. Depending upon your requirements, you should make some compromise between these two things and set the page size accordingly.

Data Sort Order: This is the sort order according to which the data will be brought in the data grid. Currently this sorting is applied on the ID column.

3.2.3.1.2 Column Selection

Pressing the "Next" button at the bottom of the dialog box, or pressing the "Column Selection" Tab from the top, will take you to the next page as shown below:

Figure 1: Common View Settings (Column Selection Tab)

This tab will allow you to select the columns that you want the application to show in the data grid when a view is executed. Simply check the columns that you want to see in a view. This tab also gives you the flexibility of changing the names of the columns. Double clicking on any item in the list view will open up another dialog box, in which you can specify the display name for that column. You also have an option of changing the order in which the columns should appear on the grid by pressing the up and down buttons present on the right side of the above form. The top most column displayed in the above form will be the first column that will be displayed in the data grid when the view is displayed and bottom most (Selected column) will be the last column (on extreme right side) on the gird.

3.2.3.1.3 Device Filter

Pressing the "Next" button at the bottom of the dialog box, or pressing the "Device Filter" Tab from the top, will take you to the next page as shown below:

Figure 1: Common View Settings (Device Filter Tab)

With this tab, you can specify a filter based on devices. If you do not want to apply this filter, simply check the check box. If you want to apply the filter, you would have to; first uncheck the checkbox because otherwise the list box would remain un-editable.

Select the device on which you want to apply the filters. All the devices that you will select from the list box will be ORed together. E.g. If you have selected WS01 and WS03 from the above list, then it will bring all the records where device name is either WS01 or WS03.

3.2.3.1.4 Info Unit Filter

Pressing the "Next" button at the bottom of the dialog box, or pressing the "Info Unit Filter" Tab from the top, will take you to the next page as shown below:
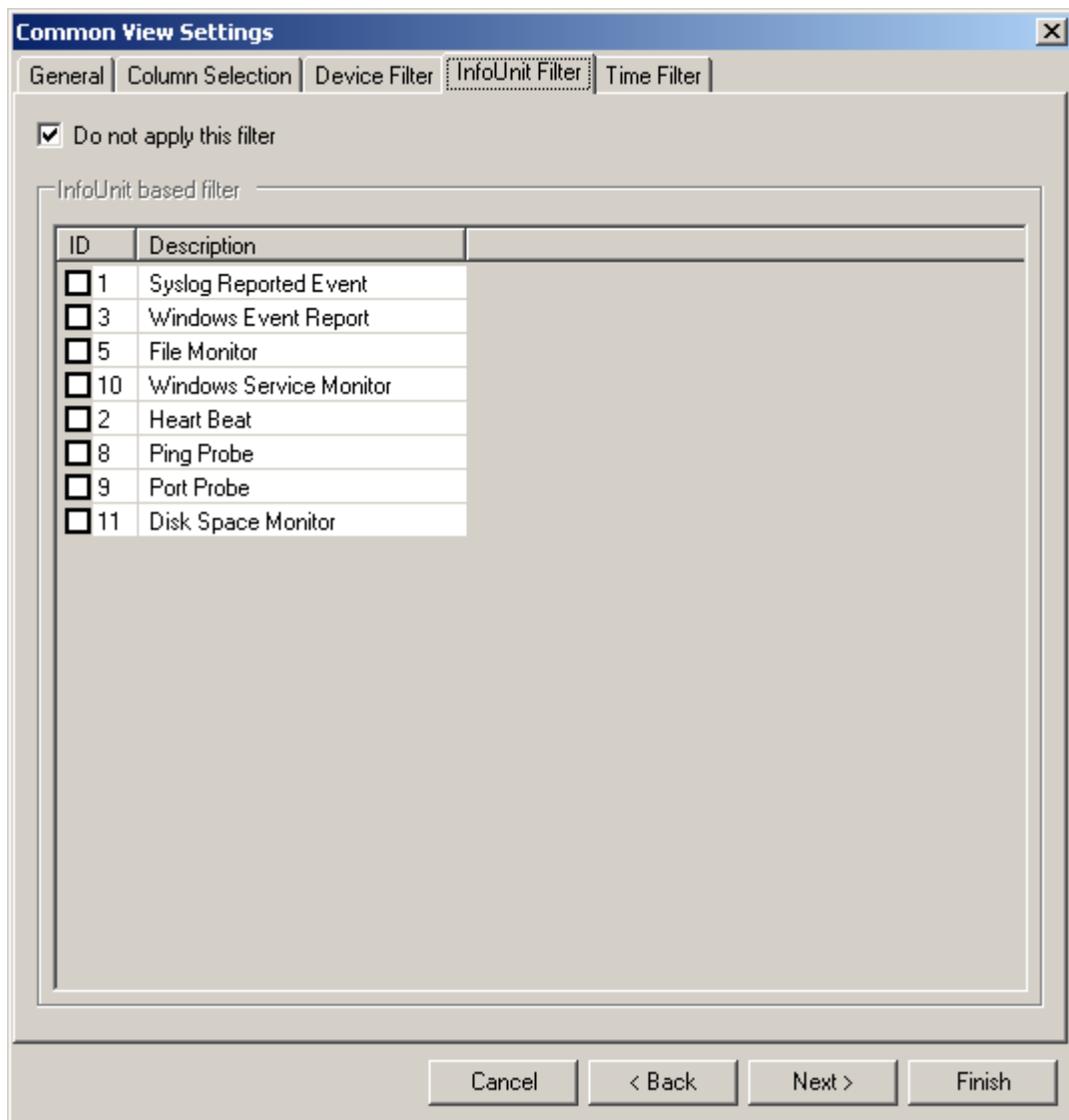
Figure 1: Common View Settings (Info Unit Filter Tab)

With this tab, you can specify filter based on Info Units. If you want to apply the filter, you would have to uncheck the checkbox so that the list box is enabled. As mentioned above in the Devices Tab, the Info Units that you have selected from the above list will be ORed together.

3.2.3.1.5 Time Filter

Pressing the "Next" button at the bottom of the dialog box, or pressing the "Time Filter" Tab from the top, will take you to the next page as shown below:

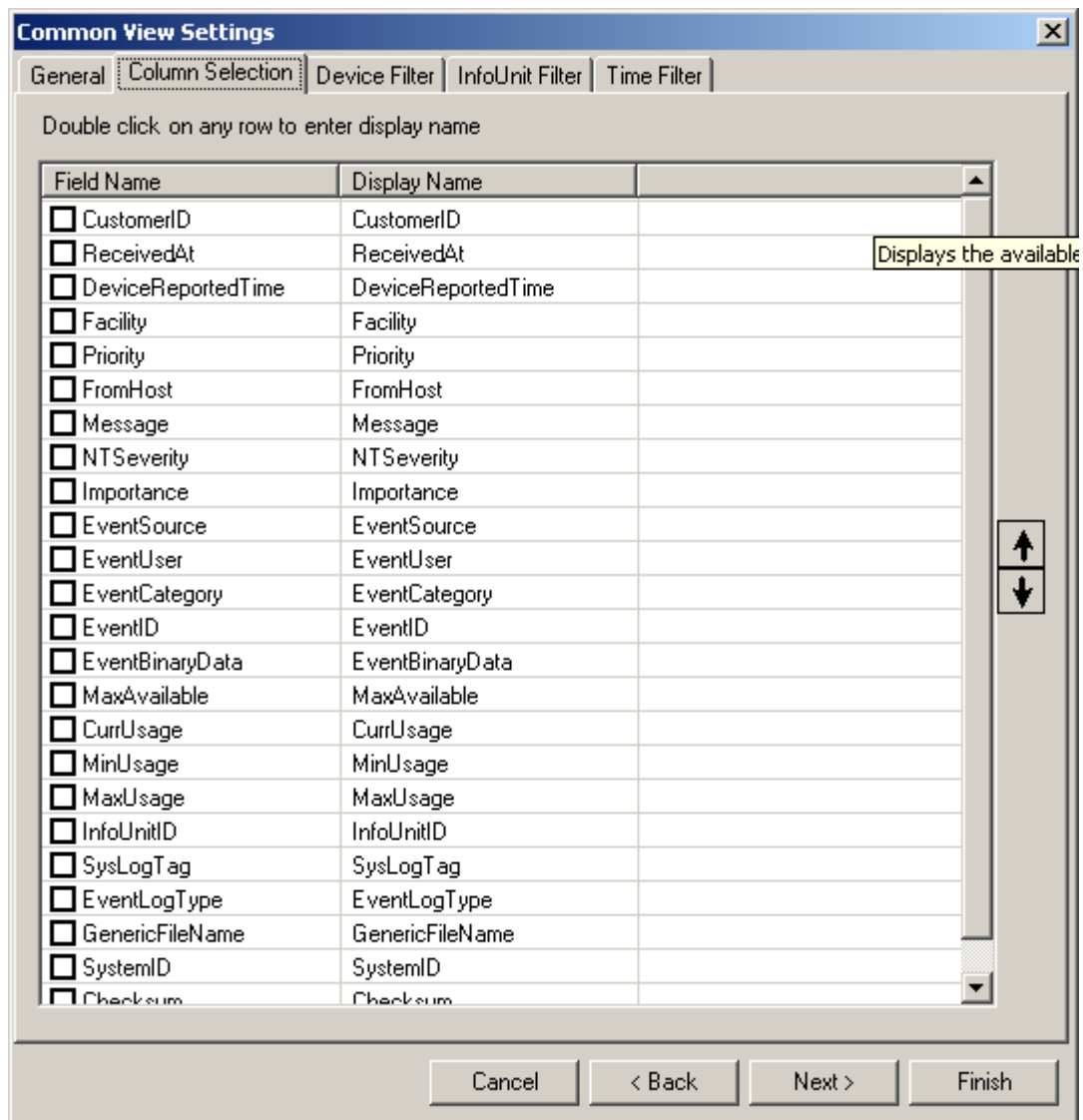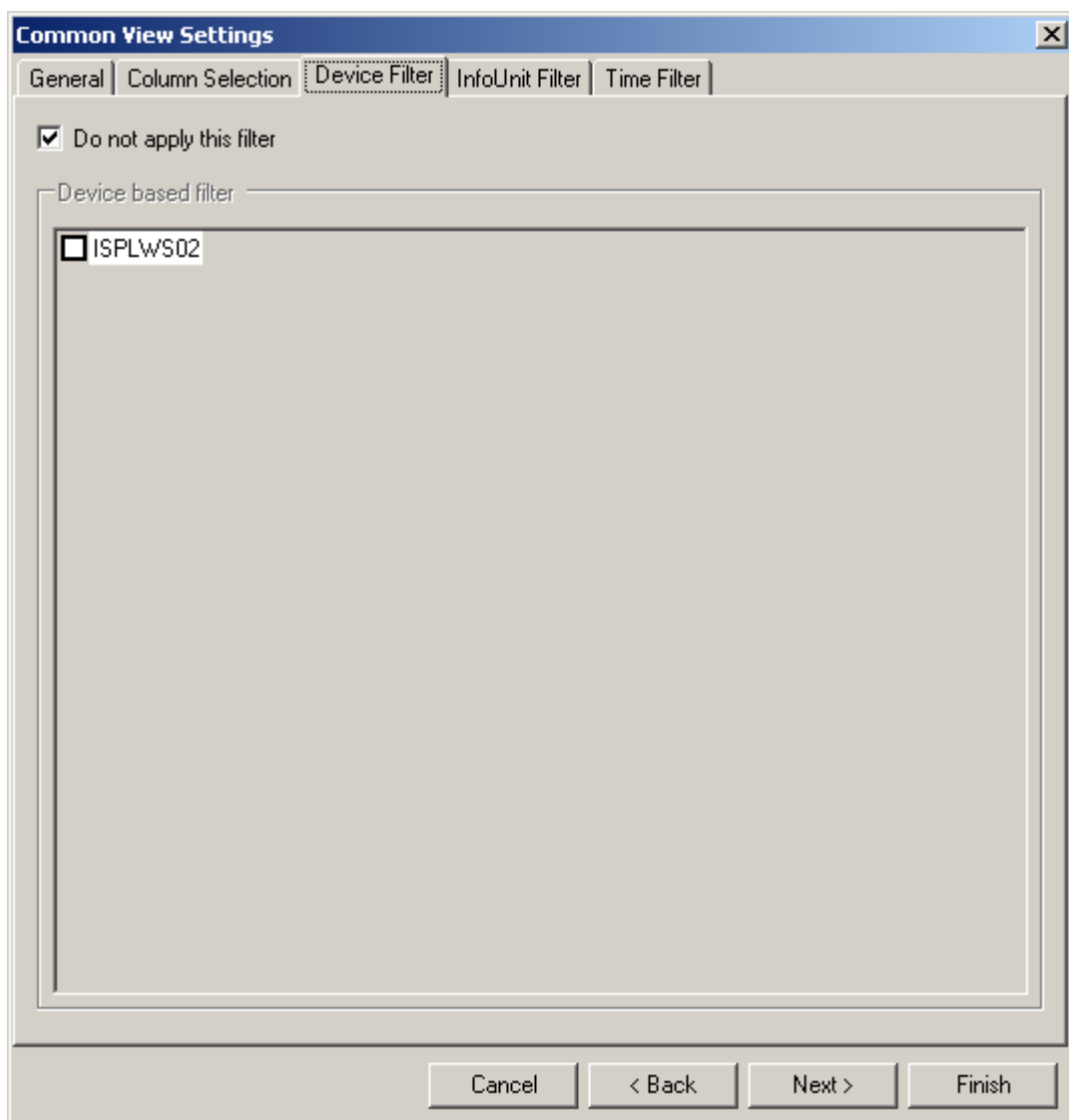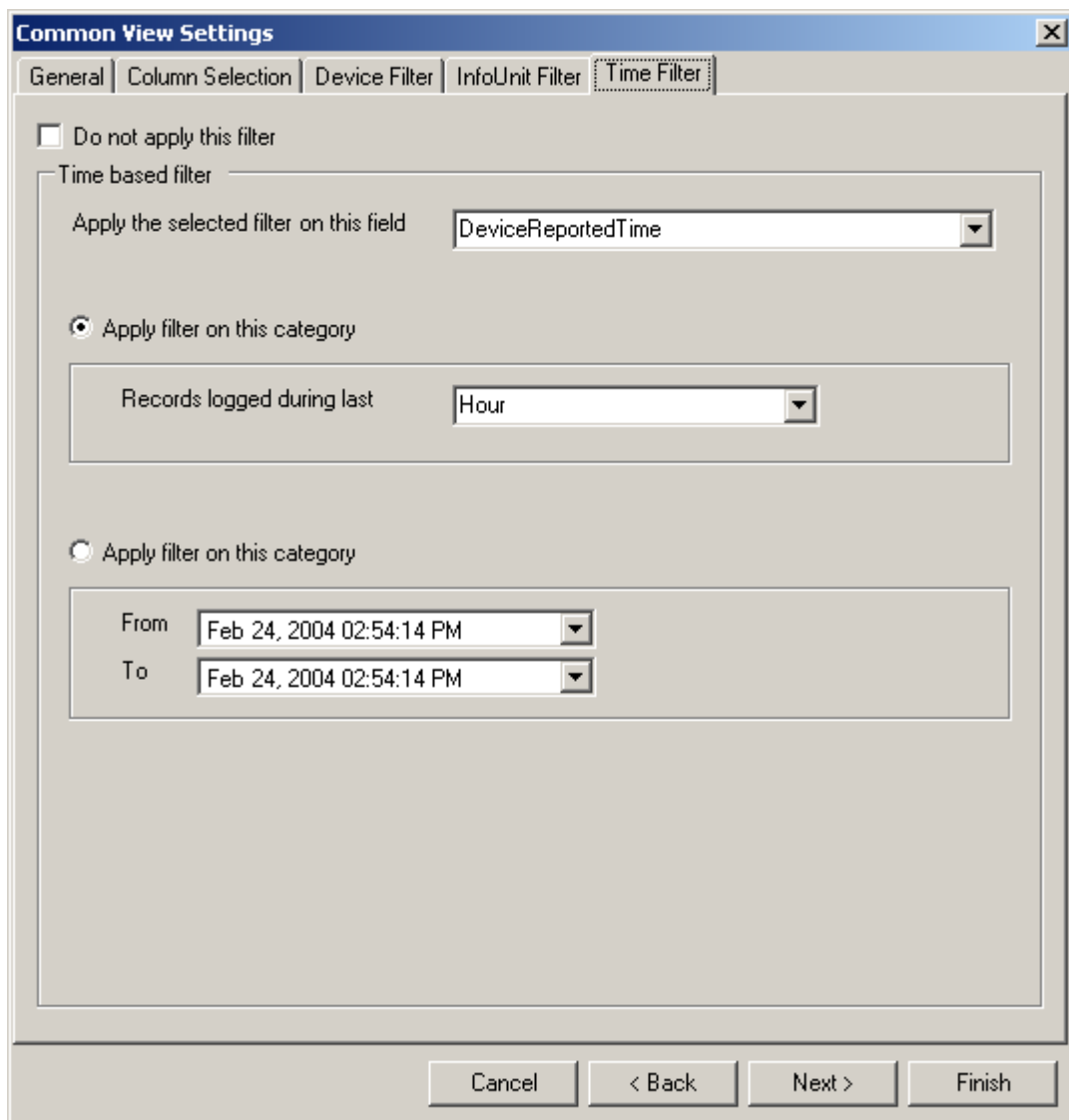*Figure 1: Common View Settings (Time Filter Tab)*

Using this tab, you can specify filters based on time. If you want to apply time-based filters, you would have to uncheck the check box at the top to enable the options below. You have two options to apply filters in this case.

Note: Both of these options are mutually exclusive. If you select the above

radio button, then the filter would be applied on the basis of "Records logged during last" option and if the lower radio button is selected then the filter would be applied on the range that you will specify in the from and to date time picker combo boxes. However, both of these filters cannot be applied simultaneously.

3.2.3.2 View Manager

View Manager can be opened in one of the following ways:

1). Click on the "Views" button in the main Tool Bar.
2). Click on "Modules" in the main Menu Bar and click on "Views".
3). Click the "Events View" Node in the tree view.

Once the View Manager is opened, you will see the following screen:
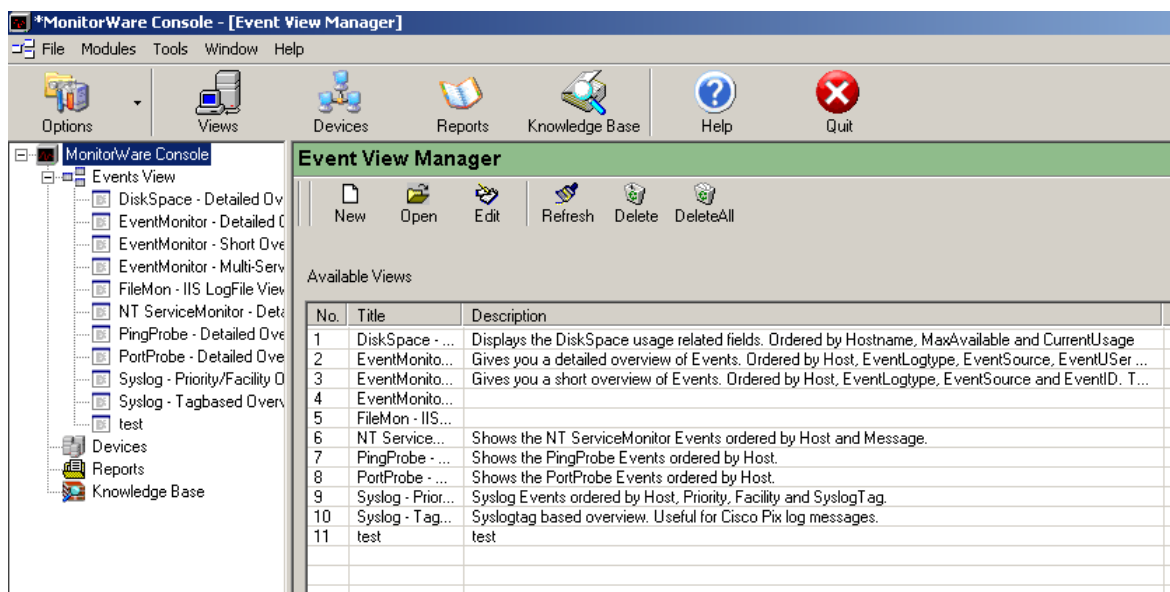
Figure 1: Event View Manager

If you already have made some views earlier, the list view on the right side will show you those views. They will also be present in the form of Nodes under the Events View Node.

3.2.3.2.1 Creating a New View

A new view can be created in one of the following ways:

1). Click the new button in the View Manager Tool Bar.
2). Right click on the list view on the right side of the screen in the above figure and click on new.
3). Right click on Events View node and click on New.

Once you have done this, the same screen as shown in figure 1 will open up but with an additional tab of Field Hierarchy as shown below:
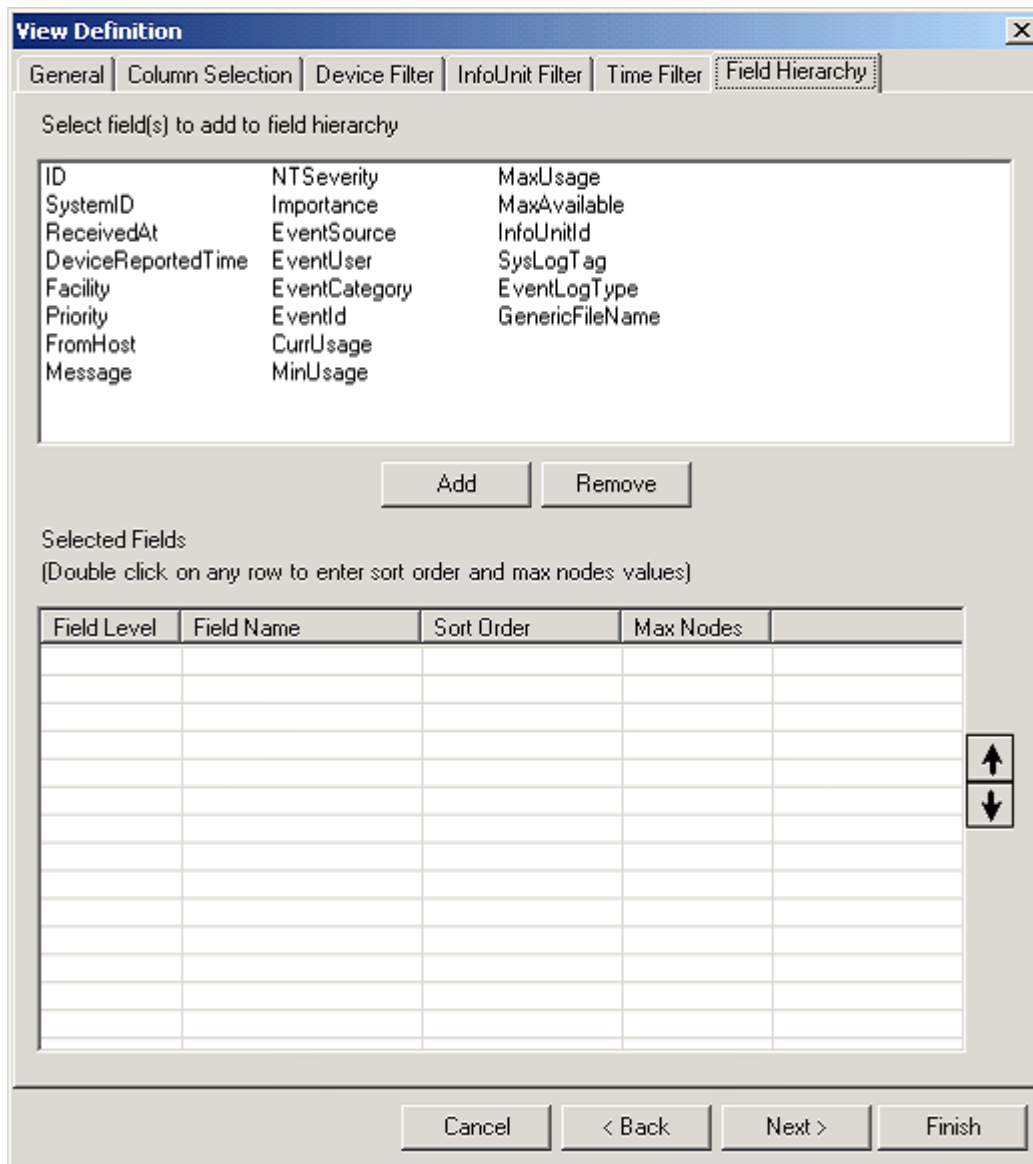
Figure 1: Field Hierarchy Tab

As you can see from the above figure that apart from the Field Hierarchy tab, all of the other tabs are the same as explained in the Common View Settings except for the General tab which now contains some additional information that you need to enter as shown below:

Figure 2: General tab containing additional fields

In this tab, the above group box is the same as that in the common view settings. There is a new group box at the bottom, which is specific for each view. In this group box, you can enter the title, description and file name of the view. Note that File Name is must in this case. If you don't specify a file name, view cannot be saved. Title and Description are optional but it is always a good idea to enter some descriptive sentence so that later on you can identify the functionality of this view.

When a new view is opened for creation, the first five tabs will show the settings that you saved in the Common View Settings (global Filters). You can override these settings by defining new settings for the view that you are currently creating.

The Field Hierarchy tab allows you to define Levels of Hierarchies that you want to see in the Tree view. Double clicking on any of the fields from the above list will bring that

field in the lower list as the level 1 field. You can also add a field to Selected Fields list by clicking on the "Add" button after selecting that field from the above list. If you add another field to the Selected Fields list box, it will be added as the level 2 field and so on. After adding a field to Selected Fields list box, if you want to change the level of a specific field, simply select that field and use the up or down arrow on the right side to increment or decrement its field level respectively.

In order to change the maximum nodes or the sort order associated with a specific field level, double click that field in the selected fields list view. A dialog box will open up where you can enter this information. You can sort based on four different things:

1). Ascending on field values
2). Descending on field values
3). Ascending on volume
4). Descending on volume

The ascending and descending on volume can be used when you are interested to see the events that have occurred very seldom or very frequent respectively.

3.2.3.2.2 Editting a View

To edit a view, you can use one of the following ways:

1). Select a view and press the edit button in the View Manager's Tool bar.
2). Right click on any view in the View Manager's List view and click on edit.
3). Right click on any view in the tree view and click on edit.
4). While the view is open, you can also edit it by pressing the edit button on that view form. Any changes that you will make while looking at the view will be reflected as soon as you close the edit dialog box.

Once you select any method mentioned above, the same screen as that shown in the new view is opened but this time all the fields will show the settings that were saved with this view when it was created. You can change any of the values and press finish. This will update the view.

3.2.3.2.3 Refreshing the list of views

To refresh the list of views, you can use any of the following methods:

1). Press the Refresh button in the View Manager's Tool bar.
2). Right click on the list view of View Manager and click on Refresh.
3). Right click on the Events View node and click on Refresh.

Once any of the above-mentioned ways has been selected, the list of views in the Tree view as well as in the list view would be updated from the views folder.

3.2.3.2.4 Deleting Selected Views / Deleting All Views

Deleting Selected Views

A view can be deleted in one of the following way:

1). Select view(s) and press Delete button in View Manager's Tool bar.
2). Right click on a view in the list view and press delete.
3). Right click on a view in the tree view and press delete.

After pressing delete the selected views will be permanently deleted and you will not be able to access them again.

Deleting All Views

In order to delete all the views permanently, use one of the following ways:

1). Press the Delete All button in the View Manager's Tool Bar.
2). Right click on the Events View node in the Tree View and click on Delete All.

After 1 or 2, all the views will be permanently deleted and you will not be able to access them again.

3.2.3.2.5 Opening a View

A view can be opened in one of the following ways:

1). Select a view and press the Open Button in the View Manager's Tool Bar.
2). Double click on any view in the List View of View Manager.
3). Click on any view node in the Tree View.

Once a view is opened, you will see the following screen
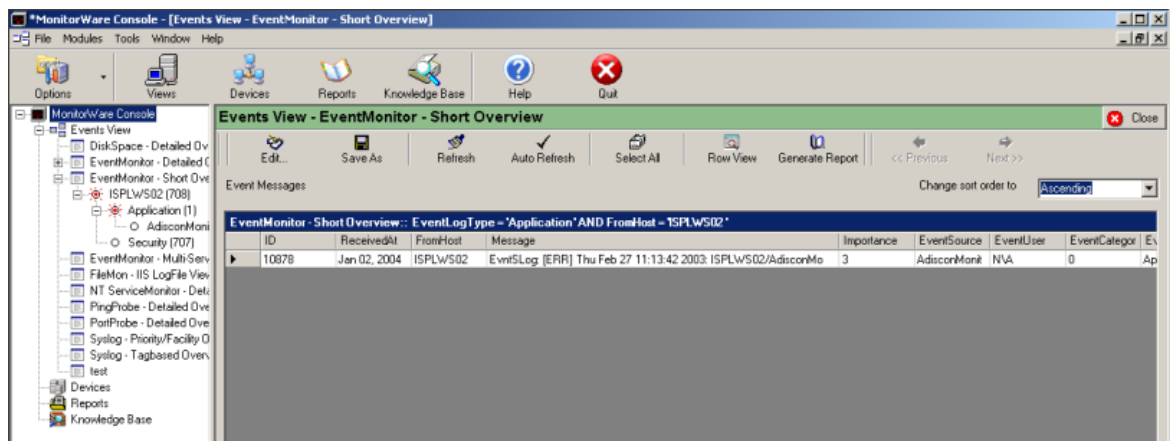
Figure 1: Opened View

The above figure shows you an opened view. The right side of the figure is a data grid, which will display you the records according to the query that was constructed according to the filters that you applied while creating this view. The columns displayed are those that you selected while creating a view. They are also displayed in

the order in which you have placed them while creating the view. The header text is that text that you assigned as the display name.

When you open up a view, it will display the columns with default width values. If you want to change the column width, simply drag the column and make the width according to your choice. This width would now be saved permanently for you so that even if you close the application and open it once again on the next day, you will see the new widths of the column so that you don't have to adjust them every time.

When a view is opened, there are two aspects that need to be explained: First is the Event View form and second is the Tree View itself. The following sections will explain both.

3.2.3.2.5.1 Event View Form

On the right hand side, you will see this Event View Form.
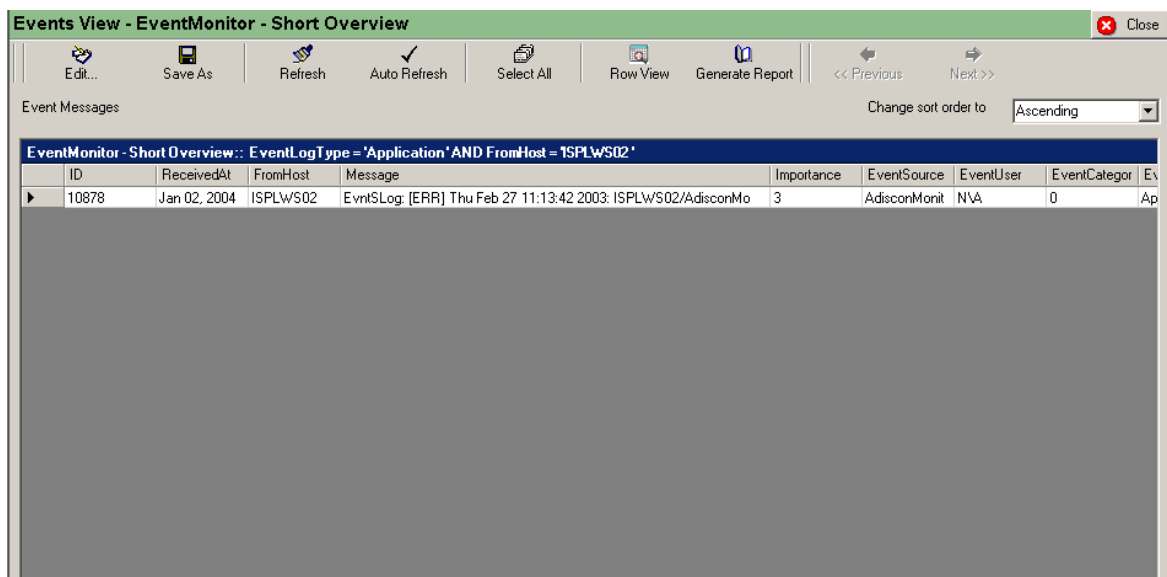
Figure 1: Event View Form

Editing a View

When the edit button is pressed, form shown in "Editting a View" would pop up. You can make any changes that you want and then pressing the finish button on that form will reflect all the new changes in this currently open view.

Saving the Records

Select the records that you want to save and click on the "Save As" button in the Event View Form's tool bar.

Refresh

Simply refreshes the records.

Auto Refresh

This feature will refresh the view automatically from the database after specified interval of time. When this button is pressed a dialog box similar to the one shown below will open up.
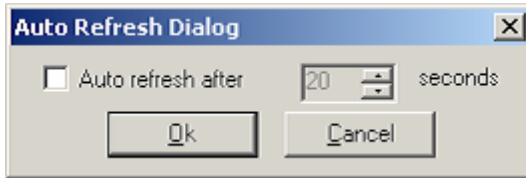
Figure 2: Auto Refresh Form

Check the check box in the above figure if you want to have the auto refresh feature. When the checkbox is checked, you can also specify the number of seconds after which your view would be refreshed.

One thing that must be kept in mind regarding the Auto Refresh feature is that if you have set a very large value of the page size and a very small time interval after which the page should refresh, then the performance of the Auto Refresh feature might not be good. The reason is that the previous records will not be brought yet from the database when the time for the next refresh comes and then it goes back to the database to fetch the fresh records once again.

We strongly recommend using small page values for the view for which you intend to use Auto Refresh feature so that the above mentioned problem is not encountered.

Select All

Selects all the rows that are present in the data grid.

Row View

If you want to see the details of any row, simply select that row and press the "Row View" button in the Event View's tool bar. The second option is that you double click on that row whose details are required. Another from will open up which will show you the details of that event. For details about this form, please read Row View Form.

Generate Report

Views Module is one of the most powerful modules of MonitorWare Console and you can use it to create very powerful views exactly according to your requirements. If you click on this button "Generate Report", it will generate an HTML based report for the current view. With this approach, you can generate the reports that suit your requirements. This feature gives you a great power in defining your customized reports.

Previous

Pressing the Previous Button will take you to the previous page of this view.

Next

If the number of records is more than the Page Size that you specified for this view, then pressing the Next button will take you to the next page.

Changing the Sort Order

You can also change the sort order of an open view. Simply use the "Change Sort Order to" combo box to change the sort order of the currently displayed view. As mentioned above, this sort order is based on the ID.

Clicking on the "Row View" button will open up a form similar to this one.

Figure 1: Row View Form

New KB Article

You can create a new KB (Knowledge Base) Article associated with this event view row by pressing the "New KB Article Button". Refer to Devices module for more details.

Search KB Article

You can search the Knowledge base for the articles associated with this Event Row View. Refer to Devices module for more details.

Web Search

You can search the net for some articles for this event view row. When you press the down arrow on this button, you would see that there are some searches already defined. Lets say you select "Google search on Event Id", then it will open up a browser and will search for Event ID = x, where x is the event id that is currently displayed on the Row View Form. If you would like to define your own query strings, you can click on Web Search Button down arrow and select "Web Search Urls" or

alternatively, you can open it up from the Options button of the main tool bar and then selecting "Web Search Urls". After selecting any of the above mentioned ways, you will see the following dialog box:
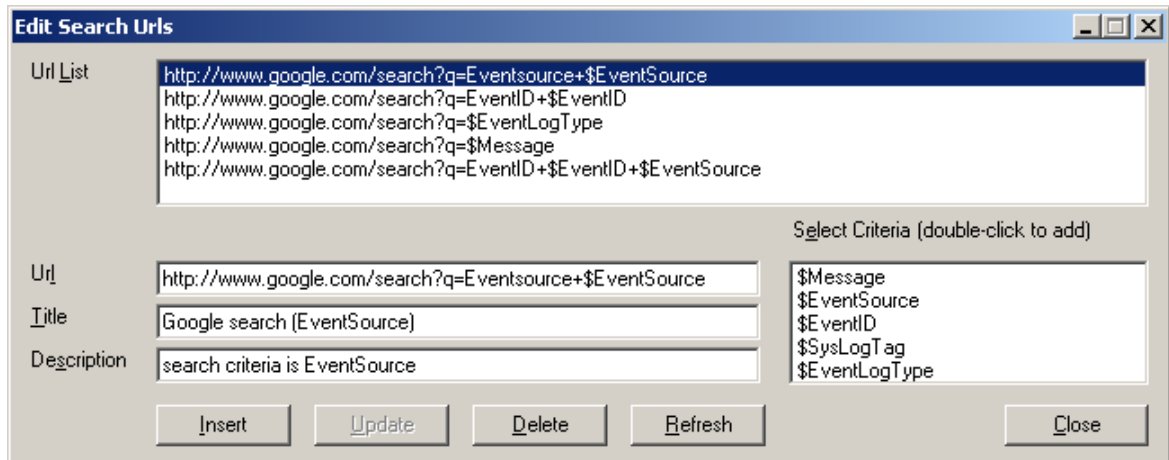
Figure 2: Web Search URLs

The Url is the actual url value that you want to send to the browser. Note that the $ signs will be replaced by the values from the event row view form (the form from where you will initiate this search).

If you want to insert a new url, make sure that the base string (http://www.google.com/search?q=) stays the same. You then have an option of selecting from the list that is displayed on the right side. Simply double click on any value and it will be added to your url string. Once done, press the "Insert" button and it will add a new search url string at the top most list. For details about Web Search URL form, please read Web Search URLs.

Additional Info

This button would normally be disabled, however if the message field contains some information regarding ICMP, then this button would be enabled. Clicking on this button would pop up another dialog box in which some additional details regarding the message can be seen.

3.2.3.2.5.2 Tree View
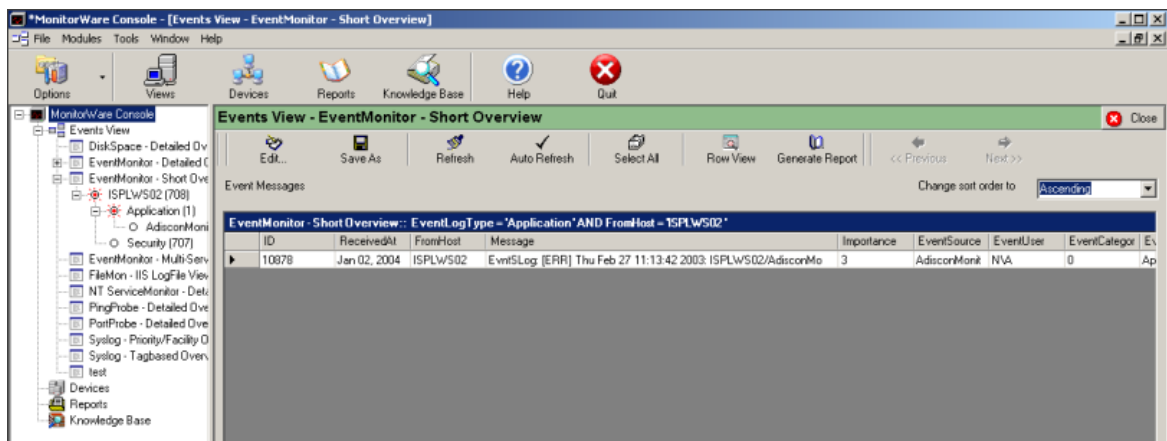
Figure 1: Tree View

When you click on any view, it will display you all the distinct level 1 fields values (along with their counts). If the number of nodes brought by the query for this first level is greater than the maximum nodes that you defined for this first level field while creating the view, then a new node "See More" will be created in blue color. Clicking on this node will bring the remaining nodes.

Note: that it will bring the nodes in chunks of Max Nodes that you defined for this field.

Once you click on any level 1 field, a red light as shown in figure 1 will be displayed along with that node meaning that user has expanded this node. Now if you had defined any level 2 field in the field hierarchy of this view, then all the distinct values of that field would be displayed under the clicked node. Secondly, the Data grid on the right side would also be updated according to new query. E.g., take a closer look at figure 1. When you click on ISPLWS02 from the tree view, the data grid will show you all those records where the Machine name is ISPLWS02. Now, as in the figure, if you click on "Application" node in the tree view (under the ISPLWS02 node), the grid will display you all those records where Machine name is ISPLWS02 and EventLogType is Application. Similarly this where clause keeps on increasing as you move deeper into the field hierarchies.

3.2.4   Network Scanning Tools

With the purchase of this module's license, you will have 3 Network Scanning Tools:

1). PortScan Tool
2). TraceRoute Tool
3). Ping Tool

3.2.4.1 PortScan Tool

The PortScan tool is a very powerful one to check open ports of a target. It can be access either using the Tools -> Network Tools menu or by right clicking a device in the left tree-view. The results of the PortScan are added into a Listview with the port number, a description (if available), a response (if there is any) and the time that a particular scan took. Additionally, there is a textbox at the bottom of the window, which displays more detailed information. The PortScan Dialog can be opened multiple times, so you can run multiple PortScans at the same time. For details PortScan, see the screenshot below:

Figure 1: PortScanner Form

IP / Hostname

The hostname or IP you want to scan for open ports

Connect TimeOut

This value in milliseconds is used for Send / Receive operations' on open ports. It is also used for a Timeout when trying to connect to ports.

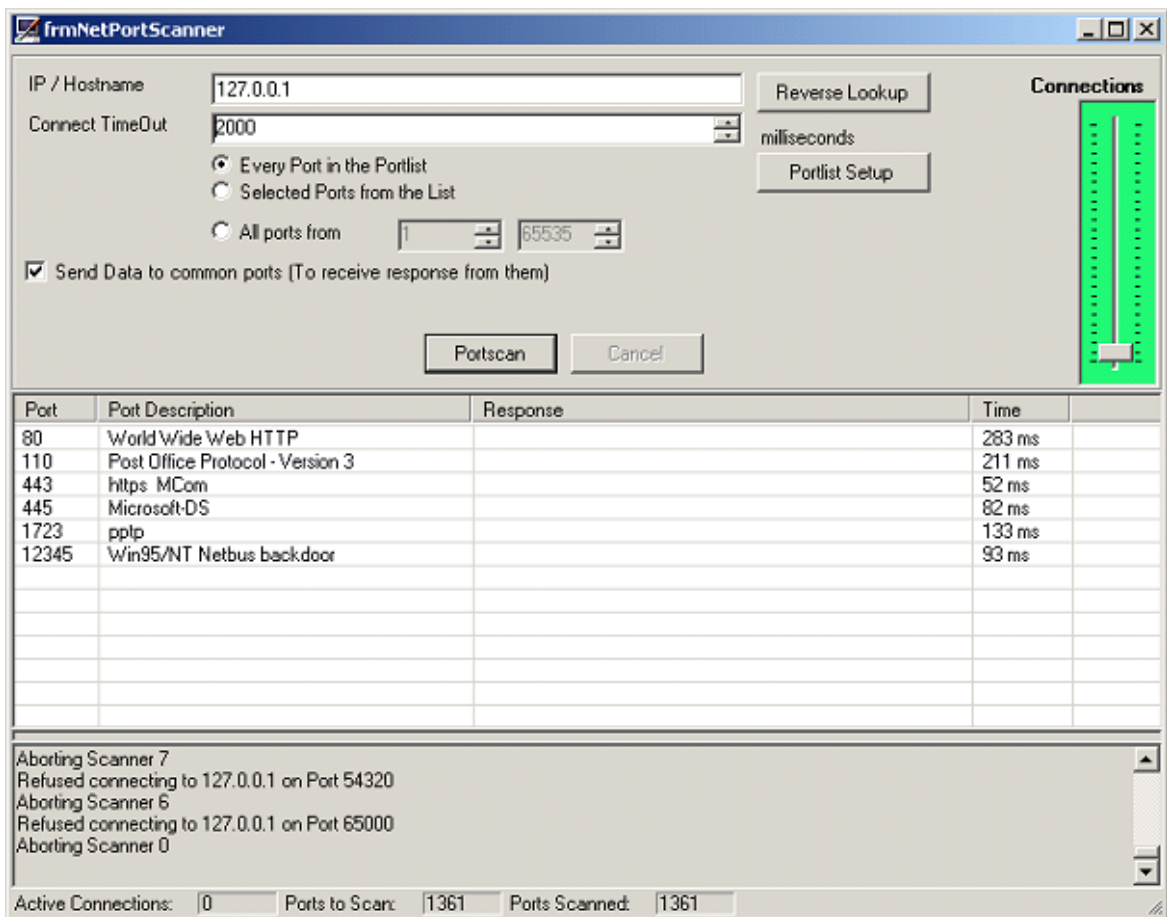**Every Port in the Portlist**

When this option is selected, all ports from a common list will be scanned. To view /

edit this List see the Portlist setup.

Selected Ports from the List

If this option is selected, only selected ports from the common Portlist will be scanned. To view edit this list, see the Portlist setup.

All Ports from

This option is used to give a Range of ports to scan. This means to scan all ports from a Start value and a End value. By default, this is 1 to 65535, which means every possible port will be scanned.

Send Data to common ports

If enabled, the PortScan tries to send messages to found open ports. For example on Port 80, it tries to send a standard GET request.

Reverse Lookup

Use this function to get the DNS name of an IP (if possible).

Connections Slider

This slider will set the number of parallel connections that will be used for the PortScan. By default, this value is set to 10, which is rather low. You can increase this number from 1 to 250. Be careful with the high connection-scans (like with 250). Some DSL Routers, or slow dialup links can be "killed" by such a high connection scan. This is includes the Scanning side as well as the side that is scanned!

However, more connections mean faster results, but also more data (traffic) per second.

PortScan

Hit this button to start the PortScan operation. Once started, you can abort it by clicking the Cancel button or closing the Window.

Cancel

Use this button to cancel a PortScan operation. Please be patient after you have clicked this button. Depending on how many connections you are using, it can take a while until all scans are stopped.

Portlist Setup

Use this button to view or edit the common Portlist. In this list, you will see well-known ports including a description, and a checkbox for each port. Use the checkboxes to define which ports should be scanned during a "Selected Ports from the List" PortScan. See the screenshot below for more details:
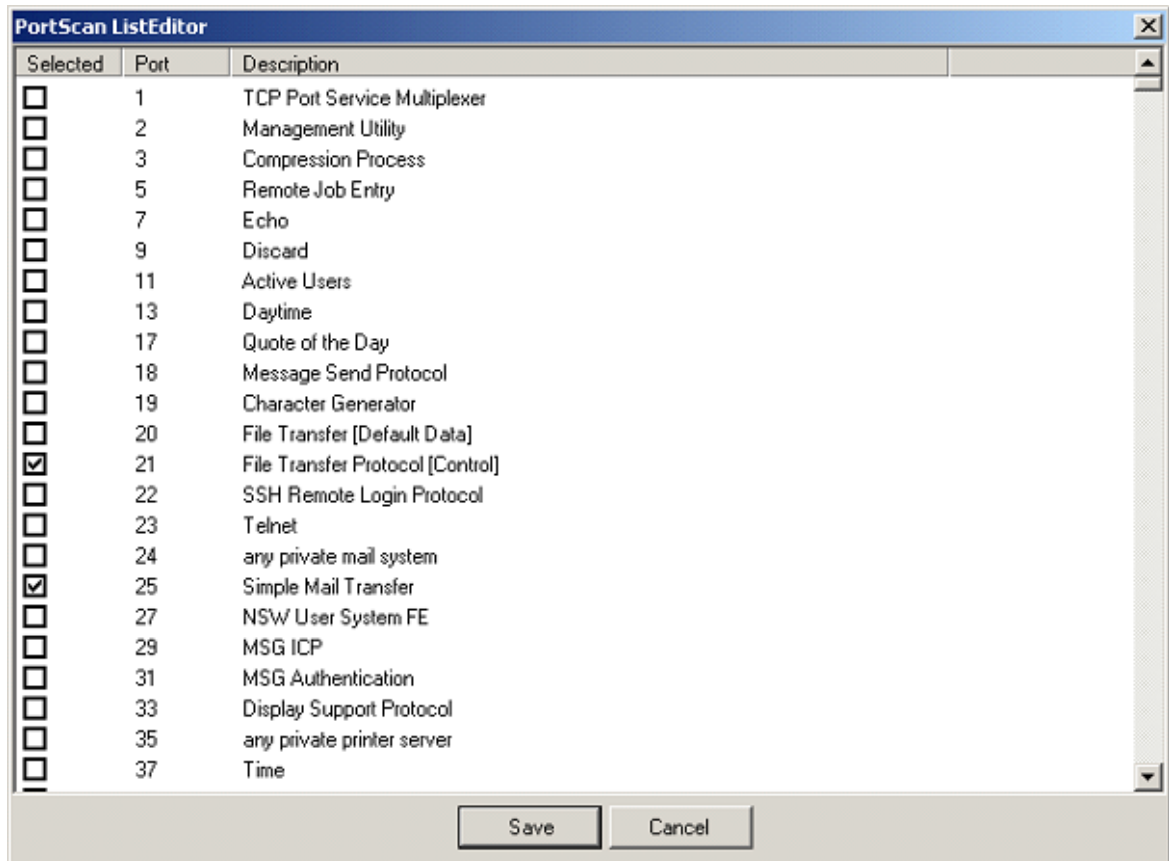
Figure 2: PortScan List Editor Form

Save

Hit the save button to save changes (If you selected or deselected any ports).

Cancel

This will just do the same as if you close the window. Changes that were made will be discarded and the window will be closed.

3.2.4.2   TraceRoute Tool

The TraceRoute is similar to the "tracert system command" of Windows. It can be access either using the Tools -> Network Tools menu or by right clicking a device in the left tree-view. You can use it to trace back all hops between your machine and a remote machine. The results are displayed in a Listview, and you can see detailed output in a large textbox at the bottom part of the window. It contains a few options that are similar to the ones that are provided in the System tracert command. The TraceRoute Dialog can be opened multiple times, so you can run multiple tracerts at the same time. For details, see the screenshot below:

Figure 1: TraceRoute Form

IP / Hostname

The hostname or IP you want to TraceRoute.

Maximum hops

The maximum number of hops you want to trace. Default is 25, and it is very seldom that this value is reached.

TimeOut

The value in milliseconds for which the TraceRoute waits for a response from the hop. This can be maximum 60000 milliseconds.

Resolve hostnames

If enabled, the TraceRoute tries to resolve the DNS name of each hop.

TraceRoute

Hit this button to start the TraceRoute operation. Once it starts, you can abort it with

the cancel button, or by closing the window.

Cancel

Use this button to abort the TraceRoute operation.

3.2.4.3   Ping Tool

This tool can be used to ping a host over the ICMP Protocol. It can be accessed either using the Tools -> Network Tools menu or by right clicking a device in the left tree-view. It contains a few options that are similar to the ones that are in the system ping command. The Ping Dialog can be opened multiple times, so you can run multiple pings at the same time. For details, see the screenshot below:
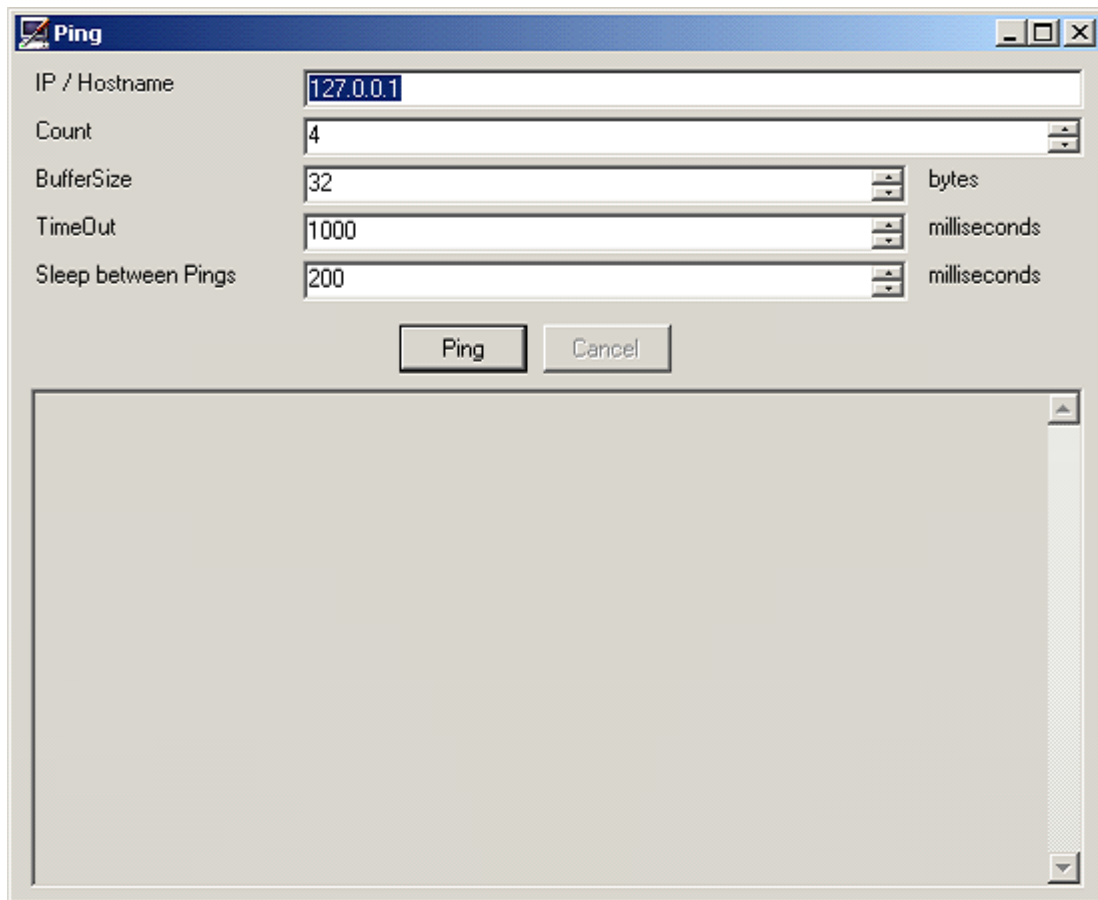

Ping Settings Form

IP /Hostname

The hostname or IP Address which you wish to ping.

Count

The number of Pings you want to do. Enter zero for continuous pinging.

BufferSize

The data size, which is sent to the target. By default, this is 32 bytes. This can be up to 10240 bytes (10 Kbytes).

TimeOut

The value in milliseconds for which the ping waits for a response from the target. Its maximum value can be 60000 milliseconds.

Sleep between Pings

Just like the real System Ping command, you can specify a wait time between each ping. This can be maximum 60000 milliseconds.

Ping

Hit this button to start the ping operation. Once started, you will be able to abort it by clicking the cancel button, or closing the window.

Cancel

Use this button to abort the ping operation.

3.2.5   The Devices Module

A Device refers to any piece of hardware or gadget that is hooked up to the network and reports or logs events/messages using some well-defined mechanisms like Syslog or NT Event log etc. MonitorWare Console provides an easy and user-friendly way to track all such reporting devices in the system.

The Devices module allows users to add, update, delete or discover device(s). Apart from these features, user can associate a knowledge base article with specific device/devices, which can later help in troubleshooting or tracking device specific issues and information.

3.2.5.1   Device Manager

Device manager can be opened using one of the following ways:

1). Click on the Devices button in the main tool bar.
2). Click the Managers Menu in the menu bar and then click on Device Manager.
3). Click the Devices node in the tree view.

After the user has selected one of the above-mentioned ways, then a form similar to the one shown in the next figure would be displayed:
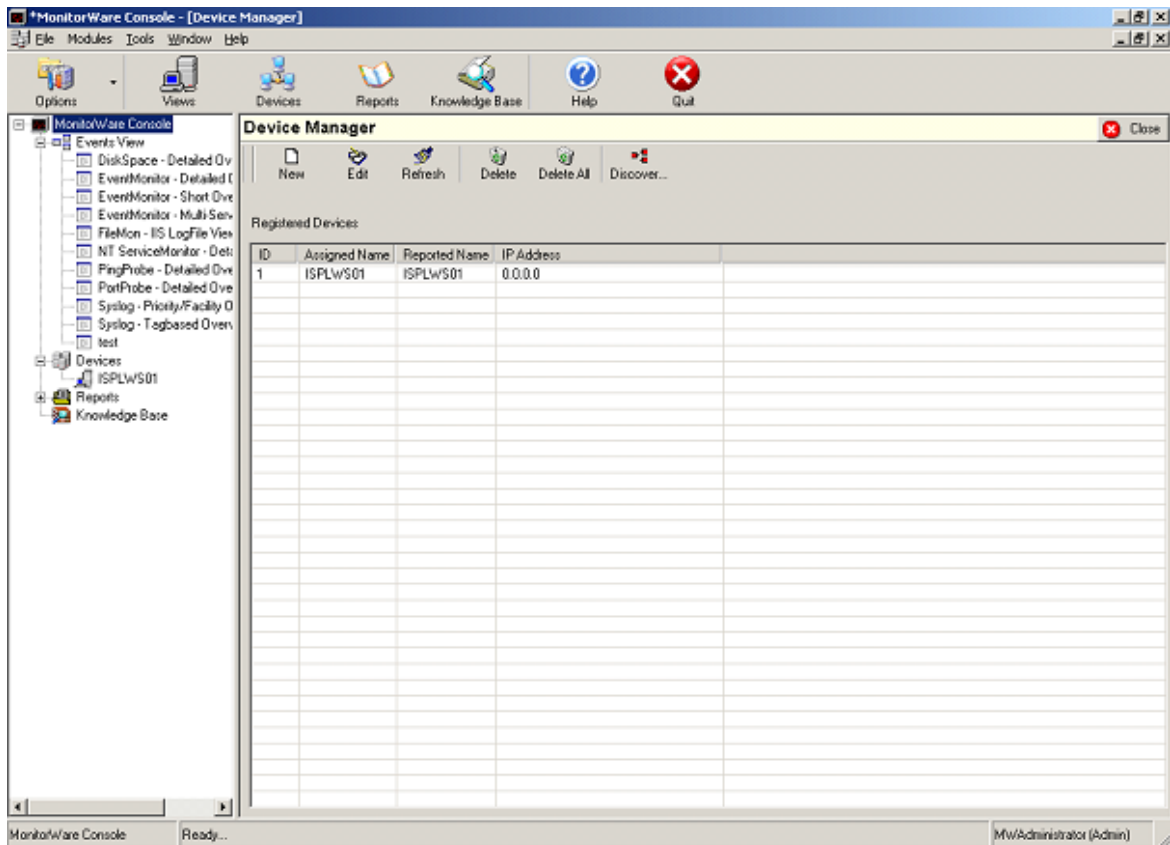
Figure 1: Device Manager

Device Manager displays a list of all the registered devices in the list view. On top of the Device Manager, there is a tool bar having new, edit, refresh, delete, delete all, discover and close button. Details of all of the Device Manager's features are given in the coming sub-sections.

Refreshing Device Manager

If new devices have been added by other users, or device details have been changed, you will not notice this immediately. You need to refresh device manager to see these changes. To refresh, do either of these:

1). Press F5 key on the keyboard.
2). Press Refresh button on Device Manager's tool bar.
3). Right click on the list view and select refresh.
4). Right click on the Device Node in the tree view and click on refresh.

Once the user has selected one of the above-mentioned ways, the device manager would be refreshed from the database and will display fresh entries.

3.2.5.2 Creating a new Device

The form for creating a new device can be displayed in one of the following ways.

1). Click on the new button in Device Manager's tool bar.
2). Right click on the Device Manager's list view and click on New sub menu item.
3). Right click on Devices Node in the tree view and click on add.

After the user has selected one of the above-mentioned ways, a form similar to the one shown in the next figure is displayed:

Figure 1: Device Information Form

Device Reported Name is the name of the device and Device Assigned Name is some useful name that can also be associated with this device. Rest of the fields on this form are self-explanatory.

The tool bar in this form contains New KB (Knowledge Base) Article, Save, Clear, Search KB and Close button. A brief description of all of them is given below.

New KB Article: If the user clicks on this button, a form, as shown in figure 2 is displayed. This form will now be used to create a Knowledge Base (KB) article that is related to this device.

Note: that the same KB article can also be related with other devices as well.
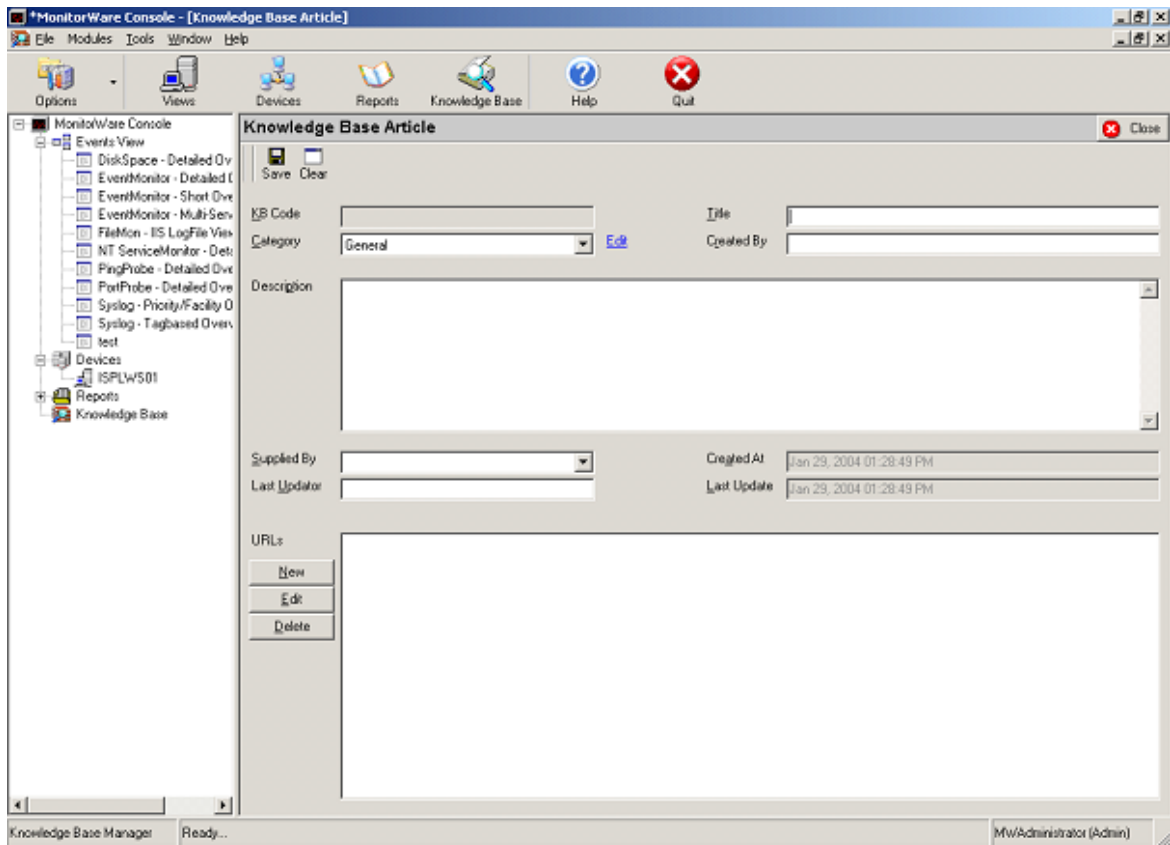
Figure 2: New KB Article

For information about this form, refer to "Editing a Knowledge Base Article" sub section in "Knowledge Base Module".

Save: This button will save the information that the user has entered in the form.

Clear: This button is used to clear all the fields that are there on the form.

Search KB: This button will open up the Knowledge Base Manager that will display all the articles that are associated with this device.

Close: This button will simply close the form.

3.2.5.3 Discovering Devices

Form for discovering devices can be opened in one of the following ways:

1). Click on the Discover Devices button in Device Manager's tool bar
2). Right click on Device Manager's list view and select Discover.

Once the user has selected one of the above-mentioned ways, a form similar to the one shown below, would be opened:
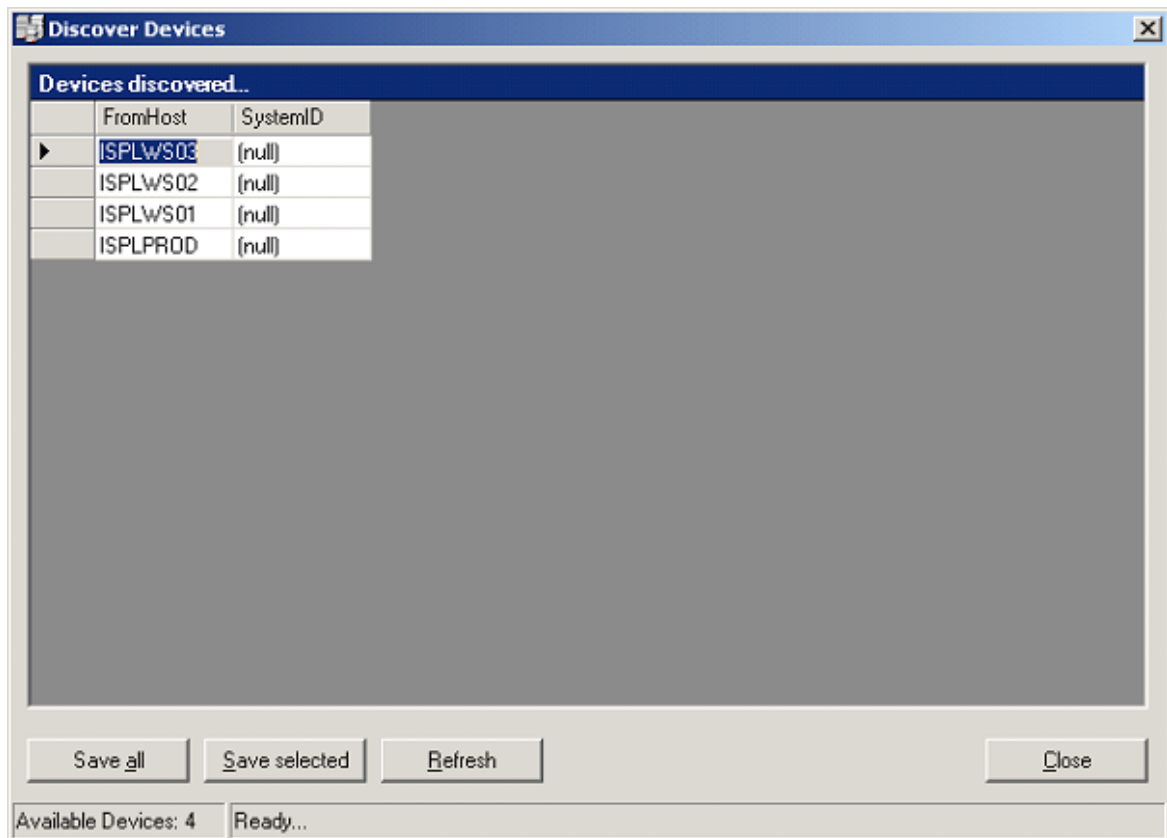
Figure 1: Discover Devices Form

This form displays a list of all of the devices that are yet to be discovered.

1). **Save All:** This button will discover all the devices and after this action, all the devices that were initially there in the list view of Discover Devices form will now be shifted to the Device Manager's list view. In other words, they have been discovered.
2). **Save Selected:** This button will discover only those devices that have been selected from the list view in the Discover Devices form.
3). **Refresh:** Simply refreshes this list from the database. If a new device has logged some data in the database after this form was opened, then pressing the refresh button would also bring that device in the list view of figure 1.
4). **Close:** Closes the form shown in figure 1.

3.2.5.4   Editing a Device

Form for editing a device can be opened up in one of the following ways:

1). Select the device that you want to edit and press the edit button in Device Manager's tool bar. If more than one device has been selected, then the last selected device would be opened for editing.
2). Right click on any device in the list view of Device Manager and click on edit.
3). Select a device from the list view and press enter key on the keyboard.

After the user has selected one of the above-mentioned ways, a form will open up and all of the fields would have the values that are associated with this opened device. If any of the value is changed and the save button is pressed, the opened device is modified to the fresh entries. Note that a new device would not be created in this way. For creating a new device, refer to "Creating a new device" sub section of this module.

3.2.5.5 Deleting Devices

Deleting one or some Devices

Device or Devices could be deleted in one of the following ways.

1). Select Device(s) to be deleted and press the DEL key on the keyboard.
2). Select Device(s) to be deleted and press the Delete button in Device Manager's tool bar.
3). Select Device(s) to be deleted and right click on the selection. Select Delete.
4). Select a specific device from the tree view. Right click on it and press delete.

Once the user has selected one of the above-mentioned ways, then the device would be deleted from the device list.

Note: that you can discover this deleted device once again using the Discover device button that is explained in the coming sub sections.

Deleting all Devices

All of the devices can be deleted in one of the following ways:

1). Press the Delete All button in Device Manager's tool bar
2). Right click on the list view and click Delete All
3). Right click on Devices node in the tree view and click Delete All

After the user has selected one of the above-mentioned ways, all the devices would be deleted but you can discover them later using the Discover Devices button, which is explained in the "Discovering Devices".

3.2.5.6 Running Tools on Selected Device

As mentioned in the section of tools, there are three network tools in MonitorWare Console.

1). Ping Tool
2). TraceRoute Tool
3). PortScan Tool

You can right click on any device that is displayed in the tree view and select the network tool that you want to run on that device.

Note: You will only be able to run these tools if you have a valid license for "Network Scanning Tools"

3.2.6   The Knowledge Base Module

Knowledge Base Manager is a very useful component of MonitorWare Console. It contains a collection of articles that are related either with one or more devices or with one or more event rows. With the passage of time, user can enhance the articles repository by adding articles to it. This repository will help the user during troubleshooting.

3.2.6.1   Knowledge Base Manager

When the Knowledge Base Node in the tree view is clicked, Knowledge Base Manager would open up as shown in the figure:
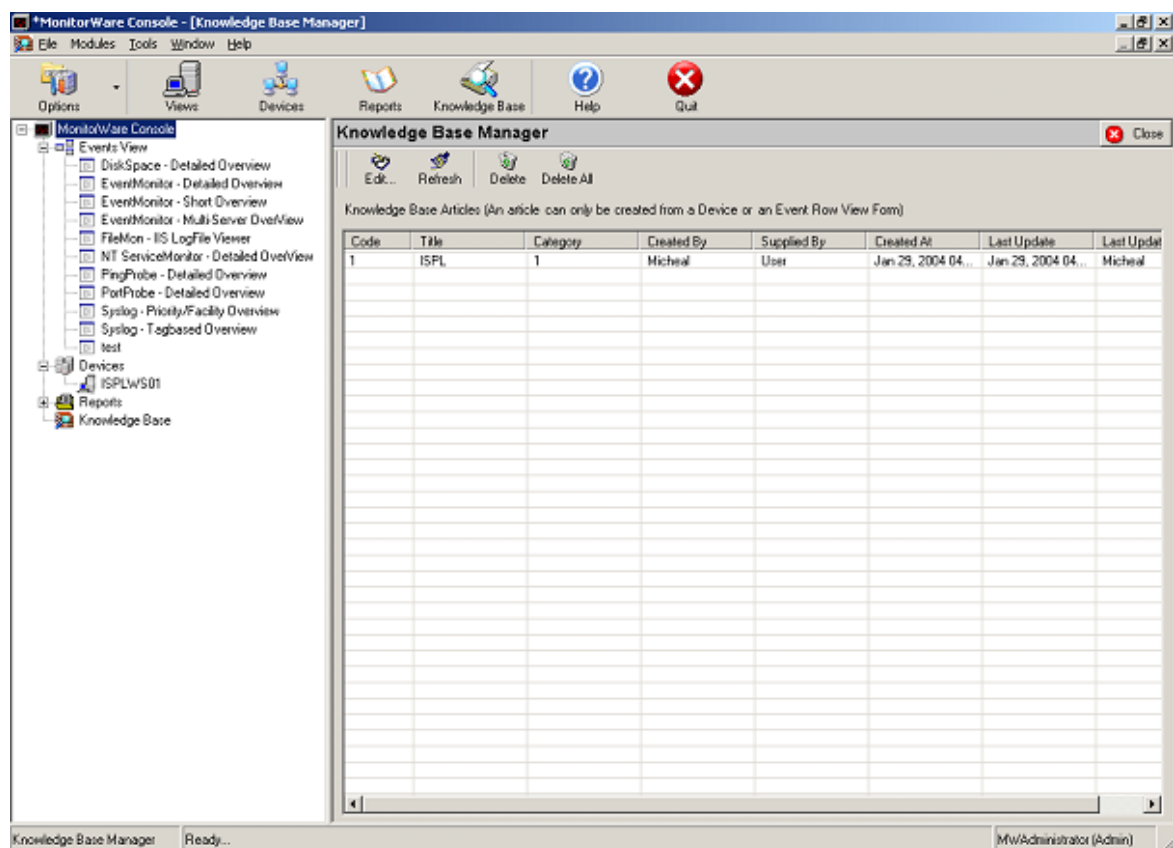
Figure 1: Knowledge Base Manager

Knowledge Base Manager displays the complete repository of Knowledge Base articles that have been added by various users so far. For each article, it displays its code, title, category, created by, supplied by, created at, last update and last updater.

Edit Link

If Category combo box is to be updated, edit link is pressed and it opens up a small form, as shown below, which can be used to insert, update or delete a category.
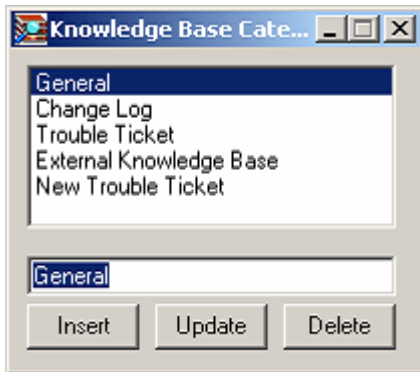
Figure 2: Knowledge Base Category Form

New Button

When this button is pressed, a small form, as shown below, is displayed in which the user can enter the URL and its description.
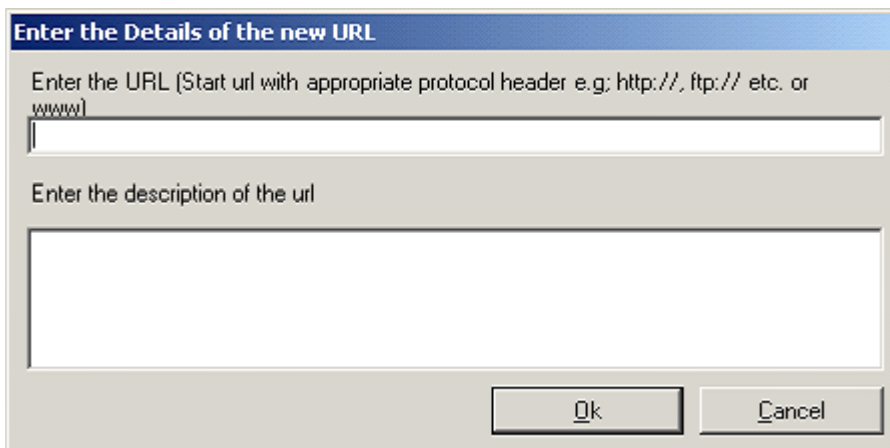
Figure 3: URL Form

Note: Start URL with appropriate protocol header e.g. http://, ftp:// etc or start the URL with www.

Edit Button

Select at most one URL and click the edit button. It will open up the same form as displayed above. User can modify this URL using this button.

Delete Button

Select the check boxes adjacent to the URLs and press this button. This will delete all selected URLs from this article.

3.2.6.2 Editing a Knowledge Base Article

To edit a Knowledge Base Article, A Knowledge Base Article can be opened for editing in one of the following four ways:

1). Select at most one article at a time and then press the add button in the tool bar of Knowledge Base Manager.
2). While the focus is on some article, press Enter key.
3). Right click on any article, and click Update
4). Double click on any article.

Once any of the above-mentioned steps has been performed, a form for that Knowledge Base Article would open up as shown in the following figure:

Figure 1: Knowledge Base Article Form

In this form user can make the changes in all the fields except for the KB Code, Created At and Last Update field because all of them are automatically generated.

3.2.6.3 **Deleting Articles**

Deleting a specific Article

A specifc article can be deleted in one of the following three ways.

1). Select an article and press the Delete key on the keyboard.
2). Right click on an article and click delete.
3). Select an article and click on delete button in Knowledge Base Manager's tool bar.

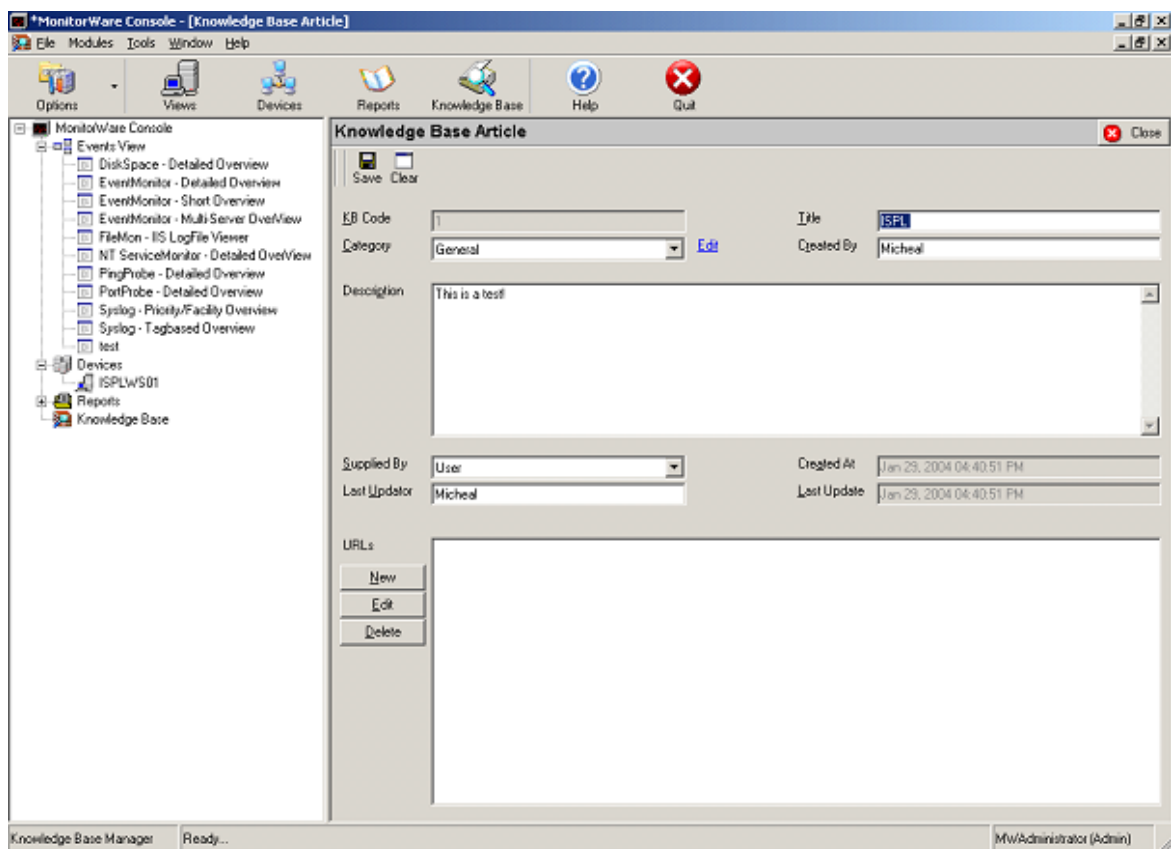**Deleting all Knowledge Base Article**

All the Knowledge Base Articles can be deleted by using one of the following options:

1). Click the Delete All button in the tool bar.
2). Right click on the list view in Knowledge Base Manager and click on delete all.

3.2.6.4 **Refreshing Articles**

Knowledge Base Manager can be refreshed in one of the following three ways.

1). Click the refresh button in Knowledge Base's tool bar.
2). Press F5 key from the keyboard.
3). Right click on list view and click on refresh.

This action will update the Knowledge Base Manager from the database. In other words if another user has added some knowledge base articles, they would also be visible after this action.

4 Getting Help

In the event you experience problems, find here how to solve them.

Please note that all options (except priority support) are also open to evaluating customers. So do not hesitate to try them. Help is available in English and German language. Our local resellers may provide local language support. Please check with them.

Frequently asked Questions

For a current list of Frequently Asked Questions (FAQ), please visit http://www.mwconsole.com/en/FAQ/. The FAQ area is continuously being updated

MonitorWare Console Web Site

Visit the support area at http://www.mwconsole.com for further information. If for any reason that URL will ever become invalid, please visit www.adiscon.com for general information.

Support Forum

Share questions and answers with your peers! The forum is also monitored by Adiscon support staff. To access the forum, point your browser at
http://forum.adiscon.com/viewforum.php?f=2

Customer Support System

Our customers service and support system is available at
http://custservice.adiscon.com. With it, you can quickly open a support ticket via a web-based interface. This system can be used to place both technical support calls as well as general and sales questions. We would appreciate if you select the appropriate category when opening your ticket.

Please note: the customer service system asks you for a userid and password when you open it. If you do not have a userid yet, you can simply follow the "register" link (in the text part) to create one. You can also open a ticket without registering first, in which case the system will create one for you. You will receive the generated userid as part of the email notifications the system generates.

Why using the customer support system? As you see further below, we also offer support by email. In fact, email is just another way to create a ticket in the customer support system. Whenever we reply to your ticket, the system automatically generates an email notification, which includes a link to your ticket as well as the answer we have provided. So for the most cases, you can use email, only. However, there are some situations where the support system should be used:

- Email notifications do NOT include attachments. If we provide an attachment, you must login to the ticket in order to obtain this. For your convenience, each email notification contains an active link that allows you to login immediately.
- **If you seem to not receive responses from us, it is a very good idea to check the web interface.** Unfortunately, anti-SPAM measures are being setup more and more agressive. We are noticing an increasing number of replies that simply do not make it to your mailbox, because some SPAM filter considered it to be SPAM and removed it. Also, it may happen that your support question actually did not get past our own SPAM filter. We try very hard to avoid this. If we discard mail, we send a notification of this, so you should at least have an indication that your mail did not reach us. Using the customer support system via its own web interface removes all SPAM troubles. So we highly recommend doing this if communication otherwise seems to be distrubed. In this case, please remember that notification emails may also get lost, so it is a good idea to check your ticket for status updates from time to time.

Subscription

We have set up an announcement mailing list for MonitorWare Console. It will carry news on upcoming releases and hotfixes. It is a low-volume list and we guarantee it will NOT send any marketing via it (except, if you consider a new release announcment as marketing).

You can subscribe yourself at: http://lists.adiscon.net/cgi-bin/mailman/listinfo/mwcon

Email

Please address all support requests to support@adiscon.com. An appropriate subject line is highly appreciated.

Online Seminars

Adiscon offers a selection of online seminars. This selection is continuously being expanded. All available seminars can be found at
http://www.adiscon.com/Common/SeminarsOnline/

Please note: Windows Media Player is required to view the seminars.

Phone

Phone support is limited to those who purchased support incidents. If you are interested in doing so, please email info@adiscon.com for further details.

Fax

Please direct your faxes to

+49-9349-928820

Toll free in the US: 1-888-900-3772

with "+" being the international dialing prefix, e.g. 011 in the US and 00 in most other countries.

Software Maintenance

Adiscon's software maintenance plan is called UpgradeInsurance. It offers unlimited free upgrades and priority support during its duration. It can be purchased for a period between 1 and 5 years.

To learn more about UpgradeInsurance, please visit

http://www.adiscon.com/Common/en/products/upgrade-insurance-details.asp

Non-Technical Questions

Please address all non-technical questions to info@adiscon.com. This email alias will answer all non-technical questions like pricing, licensing or volume orders.

Please note: we have increasingly often problems with too-agressive SPAM filtering, resulting in loss of our replies. If you do not receive a response from us within two working days latest, we highly recommend re-submitting your question via the customer support system.

Product Updates

The MonitorWare line of products is being developed since 1996. New versions and enhancements are made available continuously.

Please visit www.mwconsole.com for information about new and updated products.

5 Purchasing MonitorWare Console

All MonitorWare Console features can be used for 30 days after installation without a license.

The License

The end user license agreement is displayed during setup. If you obtained a ZIP file with the product, there is also a file license.txt inside that ZIP file. If you need to receive a copy of the license agreement, please email info@adiscon.com.

Pricing & Ordering

Please visit http://www.mwconsole.com/en/intermediate-order.asp to obtain pricing information. This form can also be used for placing an order online. If you would like to place a purchase order, please visit http://www.adiscon.com/Common/en/OrderByPO.asp to obtain details.

If you would like to receive assistance with your order or need a quote, please contact info@adiscon.com.

6 References

Following links will help you in getting further information on MonitorWare Console

- MonitorWare Console Main Web Site
- Windows' Reports Description
- PIX's Reports Description
- Version History

7 Copyrights

Adiscon GmbH copyrights this documentation as well as the actual MonitorWare Console product. To learn more about other Adiscon products, please visit www.adiscon.com/en/products/.

Please note that MonitorWare Console is part of the MonitorWare line of products. Please visit the MonitorWare site www.monitorware.com to receive updates and information on all members of the family. The site also does have information on combining the individual components to build a complex distributed configuration.

8 Glossary of Terms

The Glossary of Terms is also available on the Web:

http://www.adiscon.com/Common/en/glossary/

8.1 EventReporter

EventReporter is Adiscon's solution to forward Windows NT/2000/XP event log entries to central system.
These central systems can be either WinSyslog's, other syslog daemons (e.g. on UNIX) or MonitorWare Agents. EventReporter is part of Adiscon's MonitorWare line of products.

More Information about EventReporter:
http://www.adiscon.com/Common/en/glossary/eventreporter.asp

8.2 Millisecond

A millisecond is a thousand of a second. It is abbreviated as "ms". As such, 500ms mean half a second.
Inside the MonitorWare line of products, many timers are expressed in milliseconds as a fine control over the services and actions is provided to the administrator.

More Information about Milliseconds:
http://www.adiscon.com/Common/en/glossary/Millisecond.asp

8.3 Monitor Ware Line of Products

Adiscon's MonitorWare line of products includes monitoring and operations management tools. It consists of several components, each of which can be used either individually or as a complete solution. As of this writing, the following products are available:

- Adiscon Logger (www.monitorware.com/logger/)
- ActiveLogger (www.activelogger.com)
- EventReporter (www.eventreporter.com)
- IISLogger (www.iislogger.com)
- MoniLog (www.monilog.com)
- MonitorWare Agent (www.monitorware.com)

- MonitorWare Console (www.mwconsole.com)
- WinSyslog (www.winsyslog.com)

There is also an open source syslog library available for programmers whishing to integrate syslog into their C/C++ programs:

- liblogging (www.liblogging.org)

New products are continously being added - please be sure to check www.monitorware.com from time to time for updates.

More Information about the MonitorWare Line of Products:
http://www.adiscon.com/Common/en/glossary/MonitorWare-Line-of-Products.asp

8.4   Resource ID

The resource ID is an identifier used by the MonitorWare line of products. It is a simple, administrator assigned string value. It can be used to correlate different events - even from different source - to a specific resource.
For example, on a Windows server running Microsoft Exchange, all Exchange events could be assigned to a resource id of "Exchange Server".

In MonitorWare Agent 1.0 and WinSyslog 4.0 support for Resource IDs is limited. The field is present and can be persisted to the database or stored in XML files, but besides this there is no value in it.

Later releases of the MonitorWare Line of Products will much broader support the Resource ID.

More Information about the Resource ID:
http://www.adiscon.com/Common/en/glossary/Resource-ID.asp

8.5   SMTP

The "Simple Mail Transfer Protocol". This is an Internet standard for sending email messages. Virtually all major email systems are either based on SMTP or at least offer gateways to SMTP capable systems.

SMTP is used for sending email. It can not be used to pick up email messages. For this purpose, protocols like POP3 or IMAP4 are required.

SMTP is highly standardized. As such, a standard email client can work with all SMTP compliant servers. In the public Internet, almost all providers offer SMTP compliant mail servers for their customer's use.

More Information about SMTP:
http://www.adiscon.com/Common/en/glossary/SMTP.asp

8.6   SETP

SETP is the "Simple Event Transfer Protocol". SETP allows reliable delivery of events between SETP supporting systems. WinSyslog and MonitorWare Agent support SETP WinSyslog works as SETP client, only. As such, it can forward events generated and gathered by them to central or intermediary SETP servers. The MonitorWare Agent can operate both as a SETP server and client and as such also as a relay. It plays a vital role in a complex, distributed environment.

SETP was developed for MonitorWare. It allows synchronous communication between SETP clients and servers. With SETP, an event can be forwarded exactly as it was on the original event generating system. For example, if a syslog message is received on a remote system, that exact syslog message can be forwarded via as many SETP relays as is configured. During that relaying, no information from the original message is altered or lost. As such, each of the relays as well as the final SETP server will see the original source address, time stamps and message.

Furthermore, SETP guarantees reliable delivery. It is based on TCP, so each of the SETP peers know exactly that the communication partner can successfully receive and process the message. SETP guarantees that new events are only forwarded after the previous ones were successfully received and processed. SETP also checks for on the wire errors. Due to its characteristics, SETP can successfully be used in barely or occasionally connected environments like radio connected systems.

The SETP design is influenced by many industry standard movements, most notably the BEEP protocol and XML. However, SETP is optimized to have a very lightweight footprint. As such, it can be implemented even in low powered devices with little overhead.

More Information about SETP:
http://www.adiscon.com/Common/en/glossary/SETP.asp

8.7   Syslog Facility

Syslog Facility is one information field associated with a syslog message. It is defined by the syslog protocol. It is meant to provide a very rough clue from what part of a system the message originated from.

Tradidionally, under UNIX, there are facilities like KERN (the OS kernel itself), LPD (the line printer daemon) and so on. There are also the LOCAL_0 to LOCAL_7 facilities, which were traditionally reserved for administrator and application use.

However, with the wide adaption of the syslog protocol, the facility field contents has become a little less clear. Most syslog enabled devices nowadays allow configuring any value as the facility. So it is basically left to distinguise different classes of syslog messages.

The facility can be very helpful to define rules that split messages for example to different log files based on the facility level.

More Information about Syslog Facility:
http://www.adiscon.com/Common/en/glossary/Syslog-Facility.asp

8.8   TCP

A reliable IP transport protocol. TCP communication ensures that no packets are lost in transit. As such, it is most useful in low-bandwidth or unreliable environments. Examples are slow WANs or packet radio networks.

More Information about TCP:
http://www.adiscon.com/Common/en/glossary/TCP.asp

8.9   UDP

A non-reliable IP transport protocol. It provides best effort delivery. Typically, in LAN environments UDP packets are never lost. However, in WAN scenarios or with heavily loaded LANs, UDP packets might be lost.

More Information about UDP:
http://www.adiscon.com/Common/en/glossary/UDP.asp

8.10 Upgrade Insurance

UpgradeInsurance is Adiscon's software maintenance plan. It offers free major upgrades as well as priority support. UpgradeInsurance is available for all Adiscon products and can be purchased for a period between 1 and 5 years.

More Information about Upgrade Insurance:
http://www.adiscon.com/Common/en/products/upgrade-insurance-details.asp

8.11 UTC

UTC is the so-called "universal coordinated time". UTC was formerly referred to as "GMT" (Greenwich Mean Time) and is the basis of the international time zone system. For example, New York, USA is 5 hours behind UTC. So if it is 12 noon in New York, the UTC time is 5pm.

The MonitorWare line of products often uses UTC. UTC has the fast advantage of providing one consistent time notation, even if devices are across multiple time zones. This is extremely valuable if a centrel location is to consolidate events from senders in multiple time zones.

Using UTC might not be appropriate if a whole system is contained within a single time zone. As such, most time parameters inside the MonitorWare line of products can be configured to work with local time instead of UTC.

More Information about UTC:
http://www.adiscon.com/Common/en/glossary/UTC.asp