Symmetricom

TimeScan
Release 8.7

Administrator's Guide

Revision A – July 2008

Part Number 098-00020-000

Symmetricom, Inc.
2300 Orchard Parkway
San Jose, CA 95131-1017
U.S.A.

http:\\www.symmetricom.com.

Contents

How to Use This Guide

Chapter 1 Introduction

Chapter 2 Managed Object Configuration

Chapter 3 Security Manager

Chapter 4 Alarm Forwarding

Chapter 5 Process Supervisor

Chapter 6 Database Administration

Chapter 7 Fault Management Configuration

Chapter 8 Terminal Application

Chapter 9 Troubleshooting

Chapter 10 SNMP

Figures

Tables

How to Use This Guide

This section describes the format, layout, and purpose of this guide.

In This Preface

Purpose of This Guide

The *TimeScan Administrator's Guide* describes the procedures for installing, using, maintaining, and troubleshooting the Symmetricom TimeScan Release 8.7 (TimeScan). It also includes appendixes that describe alarms and events, the languages that you use to communicate with the TimeScan, default values, and other information.

Who Should Read This Guide

Chapter 1, Introduction, is written for non-technical audiences who need general information about the product. Chapter 2, Managed Object Configuration, and subsequent chapters contain technical information about the product and configuration instructions or details primarily intended for qualified system administrators.

Structure of This Guide

This guide contains the following sections and appendixes:

Chapter, Title	Description
Chapter 1, Introduction	Provides a description of the major components of the TimeScan PC/NT software application.
Chapter 2, Managed Object Configuration	Contains a description of the Managed Object Configuration application and its various functions.
Chapter 3, Security Manager	Provides a description of the Security Manager application and contains information on using the application.
Chapter 4, Alarm Forwarding	Provides a description of the Alarm Forwarding function and explains its uses.
Chapter 5, Process Supervisor	Contains a description of the Process Supervisor and provides information on its uses.
Chapter 6, Database Administration	Provides information on possible maintenance schedules, checking database status, and archiving records.
Chapter 7, Fault Management Configuration	Provides information on the Fault Management Configuration application and describes how to use the application to map alarms and events to unique identities.
Chapter 8, Terminal Application	Contains a description of the Terminal application and provides information on its features.
Chapter 9, Troubleshooting	Provides information on Work-arounds for commonly occurring TimeScan faults.

Chapter, Title	Description
Chapter 10, SNMP	Provides information on installing SNMP and on installing and configuring the NuDesign Multi-product Agent Service.
Index	Provides references to individual topics within this guide.

Conventions Used in This Guide

This guide uses the following conventions:

- **Acronyms and Abbreviations** – Terms are spelled out the first time they appear in text. Thereafter, only the acronym or abbreviation is used.
- **Revision Control** – The title page lists the printing date and versions of the product this guide describes.
- **Typographical Conventions** – This guide uses the typographical conventions described in the table below.

When text appears this way...	... it means:
TimeScan Administrator's Guide	The title of a document.
SSU CRITICAL IOC1	An operating mode, alarm state, status, or chassis label.
Select **File**, **Open**...	Click the Open option on the File menu.
Press **Enter** Press **;**	A named keyboard key. The key name is shown as it appears on the keyboard. An explanation of the key's acronym or function immediately follows the first reference to the key, if required.
`TimeScan Username:`	Text in a source file or a system prompt or other text that appears on a screen.
`AlarmListAddress -list`	A command you enter at a system prompt or text you enter in response to a program prompt. You must enter commands for case-sensitive operating systems exactly as shown.
alarms are received *after* ...	A word or term being emphasized.
Symmetricom ***does not*** recommend...	A word or term given special emphasis.

Warnings, Cautions, Recommendations, and Notes

Warnings, Cautions, Recommendations, and Notes attract attention to essential or critical information in this guide. The types of information included in each are explained in the following examples.

Warning: To avoid serious personal injury or death, *do not* disregard warnings. All warnings use this symbol. Warnings are installation, operation, or maintenance procedures, practices, or statements, that if not strictly observed, may result in serious personal injury or even death.

Caution: To avoid personal injury, *do not* disregard cautions. All cautions use this symbol. Cautions are installation, operation, or maintenance procedures, practices, conditions, or statements, that if not strictly observed, may result in damage to, or destruction of, the equipment. Cautions are also used to indicate a long-term health hazard.

ESD Caution: To avoid personal injury and electrostatic discharge (ESD) damage to equipment, *do not* disregard ESD cautions. All ESD cautions use this symbol. ESD cautions are installation, operation, or maintenance procedures, practices, conditions, or statements that if not strictly observed, may result in possible personal injury, electrostatic discharge damage to, or destruction of, static sensitive components of the equipment.

Electrical Shock Caution: To avoid electrical shock and possible personal injury, do not disregard electrical shock cautions. All electrical shock cautions use this symbol. Electrical shock cautions are practices, procedures, or statements, that if not strictly observed, may result in possible personal injury, electrical shock damage to, or destruction of components of the equipment.

Recommendation: All recommendations use this symbol. Recommendations indicate manufacturer-tested methods or known functionality. Recommendations contain installation, operation, or maintenance procedures, practices, conditions, or statements, that provide important information for optimum performance results.

Note: All notes use this symbol. Notes contain installation, operation, or maintenance procedures, practices, conditions, or statements, that alert you to important information, which may make your task easier or increase your understanding.

Related Documents and Information

Other helpful documents and software tools are listed below. See your Symmetricom representative or sales office for a complete list of available documentation.

Note: Symmetricom offers a number of applicable training courses designed to enhance product usability. Contact your local representative or sales office for a complete list of courses and outlines.

Where to Find Answers to Product and Document Questions

For additional information about the products described in this guide, please contact your Symmetricom representative or your local sales office. You can also contact us on the web at www.symmetricom.com.

What's New in This Guide

This revision of the guide has the following changes from the previous revision:

- Revised Chapter 2, Managed Object Configuration
- Revised Chapter 3, Security Manager
- Revised Chapter 9, Frequently Asked Questions

Chapter 1 Introduction

This chapter provides a brief description of the administration and troubleshooting tools used within the TimeScan suite of applications.

In this chapter:

Managed Object Configuration

Managed Object Configuration is launched by selecting the **Managed Object Configuration** icon from the **TimeScan Administrator item**, on the Windows **Start** menu (Figure 1-1).

Managed Object Configuration (MOC) provides the ability to define new or modify existing, managed elements. See Chapter 2, Managed Object Configuration for a description of how to define the existence of a new element, include a new Network Browser view and make these new objects accessible to the operator.

The TimeScan Server has a protection scheme that prevents unauthorized users from accessing and manipulating the elements managed from the platform. This chapter describes how the Security Manager works and how the sub-system should be maintained.

The Security feature application is launched by selecting **Security Management Configuration** in the **NMS Administrator** directory on the Windows **Start** menu (Figure 1-1). The Security Manager Configuration Tool screen is shown in Figure 1-2.

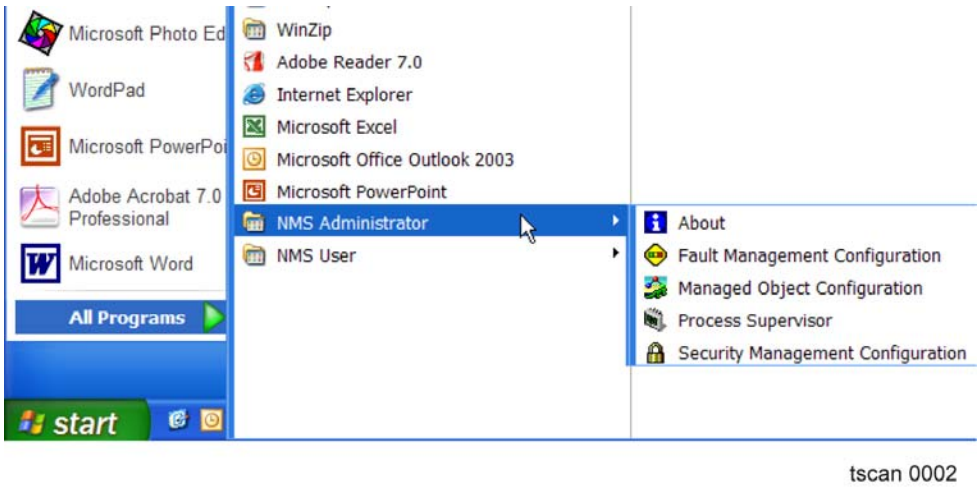


Figure 1-1. Windows Start Menu

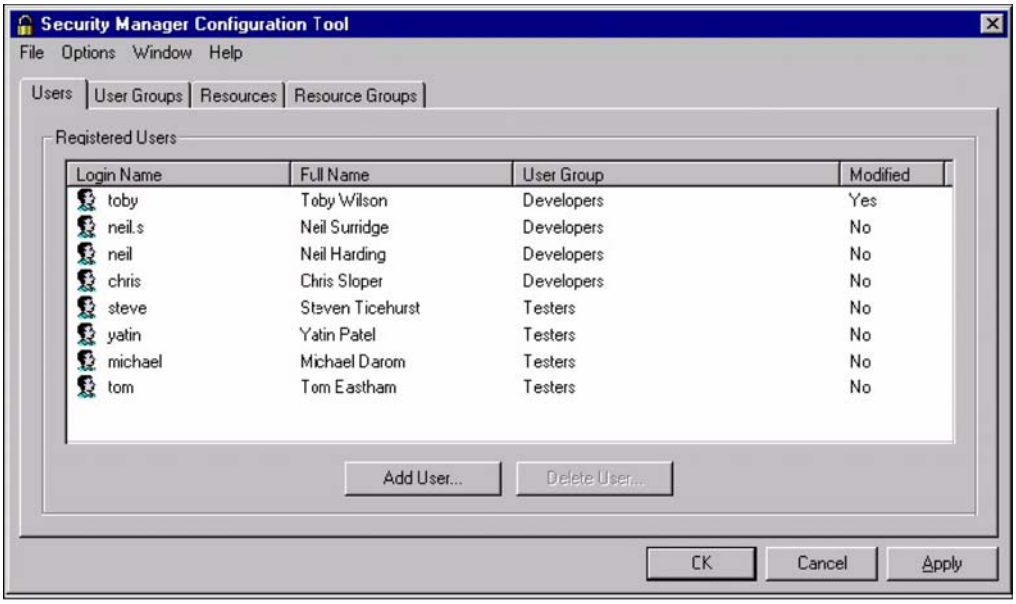


Figure 1-2. Security Manager Configuration Tool

Fault Management Configuration

All alarms within the TimeScan system have an ID and a mapping for severity. Using this facility, you can configure incoming alarm IDs and amend severity mapping. If a mapping is changed it is effective only on new alarms received *after* the amendment has taken place.

Alarm Forwarder

TimeScan can be set-up to forward alarms to an external system. The external system must listen on a TCP/IP socket and receive textual based alarm/event and clearing messages once a connection is established. This document describes how to set-up TimeScan to forward alarms, including criteria that can be set, and the format of the forwarded messages.

Database Administration

Chapter 6, Database Administration discusses archiving of the alarm database as well as viewing archived data. This chapter discusses how to plan and perform basic maintenance tasks. The Maintenance schedule is a list of tasks that must be performed on a regular bases (daily, weekly, monthly), to keep the system running smoothly.

Terminal

Terminal is a versatile application capable of providing command access and event Monitoring for any element type ASCII based command protocol. This application has not been optimized for TL1 and is useful for isolating specific communications protocol problems. The Terminal screen is shown in Figure 1-3.

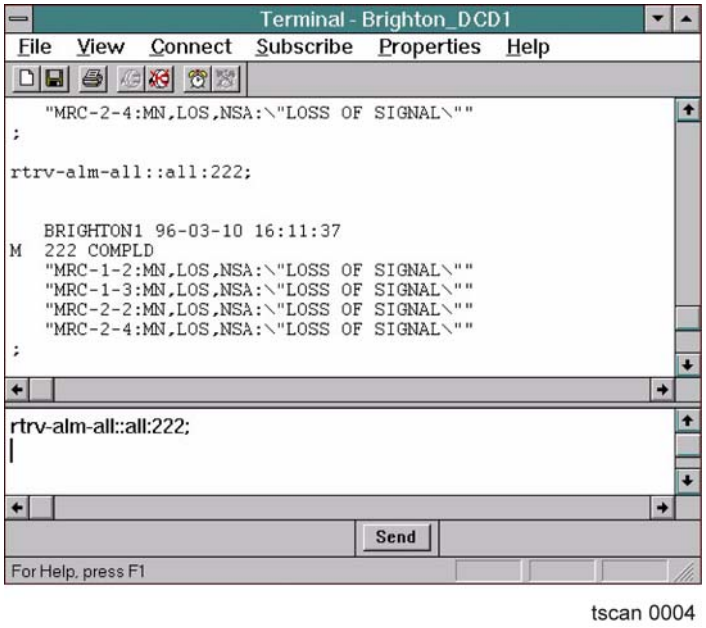


Figure 1-3. Terminal

Troubleshooting

Console

This facility reports internal TimeScan events. If a problem arises with the system, which prevents communication use this console to record any faults. Information recorded should be included when any faults are reported.

Free Text Console

This facility is similar to the console except it reports all output of the TimeScan system and not just alarms and faults.

Chapter 2 Managed Object Configuration

A common requirement of any management system is the ability to define new, or modify existing, managed elements. This chapter provides a step-by-step description of how to define the existence of a new Network Element, include a new Network Browser view, and make these new objects accessible to the operator.

In this chapter:

Opening the Application

The first task in defining a new element is to insert a new entry into the Managed Object Configuration (MOC) Database.

In the **TimeScan Administrator** menu (in the Windows **Start** menu), select **Managed Object Configuration** (see Figure 2-1). Selecting this icon opens the Hierarchy View Window (see Figure 2-5) to provide access to information on all objects defined within the MOC Database.

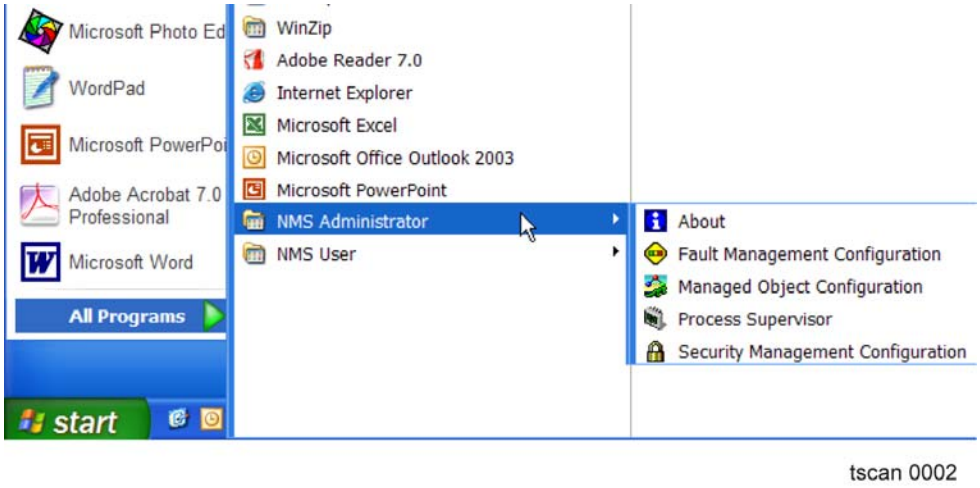


Figure 2-1. Windows Start Menu

The Managed Object Configuration Database

The purpose of the MOC Database is to provide a store for all the information required by the system to realize and manage an arrangement of objects and elements. The distinction is made between objects and elements, because not only does the TimeScan System support the existence of Managed Elements (MEs), it also supports the existence of *virtual objects*, for instance objects that do not have any tangible form.

In general these virtual objects form containers that can contain managed elements or other virtual objects. For example, a network is a virtual container - it contains managed elements.

Virtual objects define logical partitions in a network providing context and rationalization for the user. Consider a network containing 100 elements. The main purpose of any network presentation system is to display the current notification state of all the elements in the network. To attempt this on one graphical view would result in a confusing clutter. However, if elements are grouped together in containers and the containers displayed then the view can be simplified without losing status resolution.

Figure 2-2 provides a typical example of how such a network can be defined.

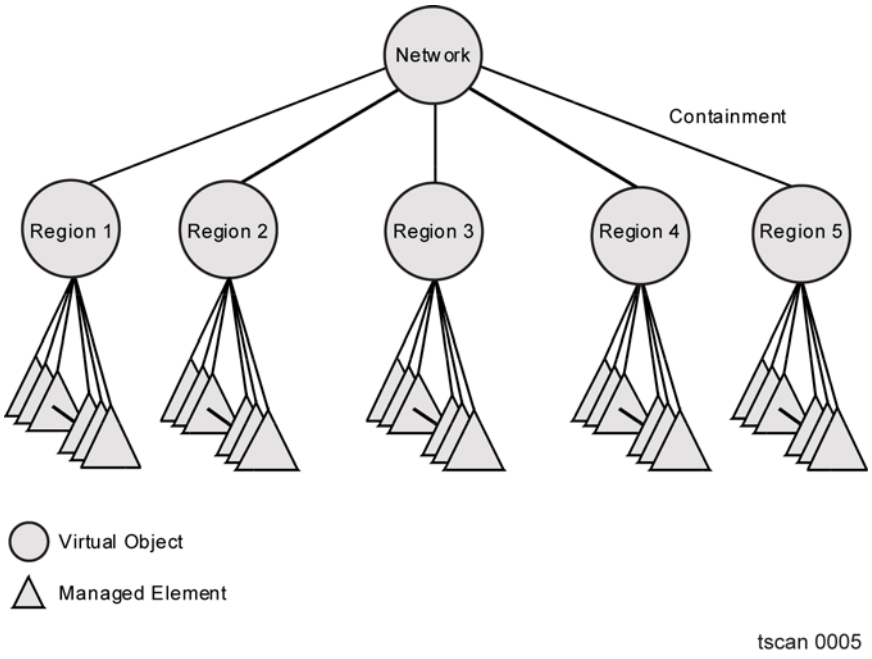


Figure 2-2. Network Definition Example

Six virtual objects are created: **Network** and five **Regions** which in turn contain all the MEs. The task of depicting and understanding the network becomes greatly simplified. These virtual objects are known as Sub-Network Objects because, in general, they represent parts of a network.

Sub-Networks

Sub-Network Objects have a special property that causes them to exhibit the same notification status as all the MEs either directly or indirectly contained within them. Each region depicts a notification status which represents the summation of the notification states of all the managed elements contained within the region.

Any structure of Sub-Networks can be defined. A popular arrangement is to mimic the physical or conceptual containers found in the network, as shown in Figure 2-3 for example:

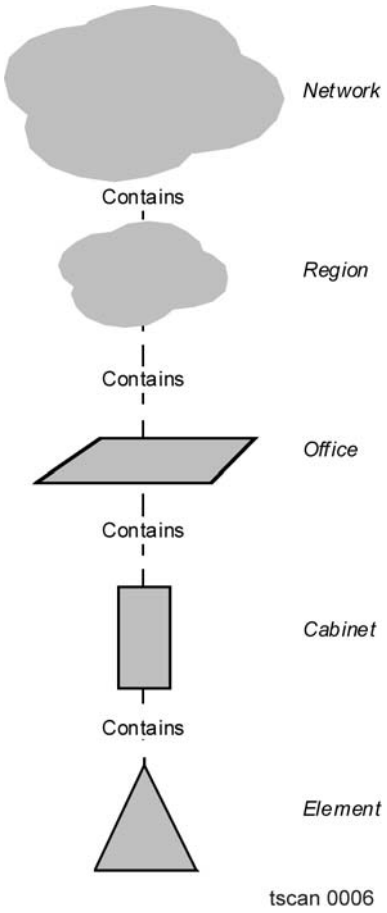


Figure 2-3. Sub-Network Example

There is no limit on how many Sub-Networks can be defined or what is contained within them. It is also perfectly legal to have an object, either a Sub-Network or Element, contained by multiple Sub-Networks.

For example: consider two simple SDH ring structures (see Figure 2-4).

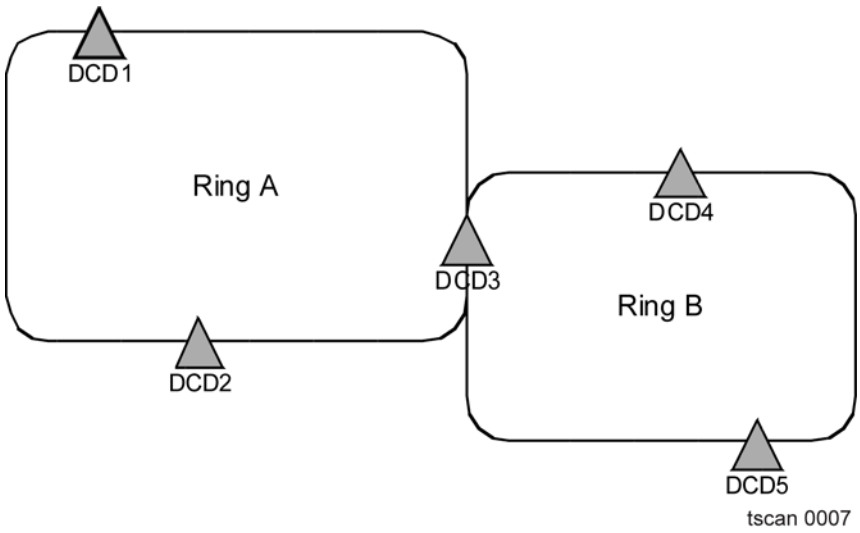


Figure 2-4. SDH Ring Structures

We could define Ring A and Ring B as two Sub-Networks. However, the element DCD3 exists in both rings. This does not cause a problem because DCD3 can be contained within Ring A Sub-Network *and* Ring B Sub-Network. If the notification status of DCD3 changes then the change is propagated to both Ring A and Ring B.

Managed Elements (MEs)

Managed Elements are defined as equipment, for instance DCD Elements, directly managed by the local TimeScan platform. Although it is possible to define a managed element that contains another Managed Element (ME), the notification status is not propagated to the containing managed element.

Managed Object Configuration Hierarchy View

When the MOC application is launched you are presented with the main hierarchy view window (Figure 2-5). This is where you configure the system by adding, deleting and modifying objects in the database.

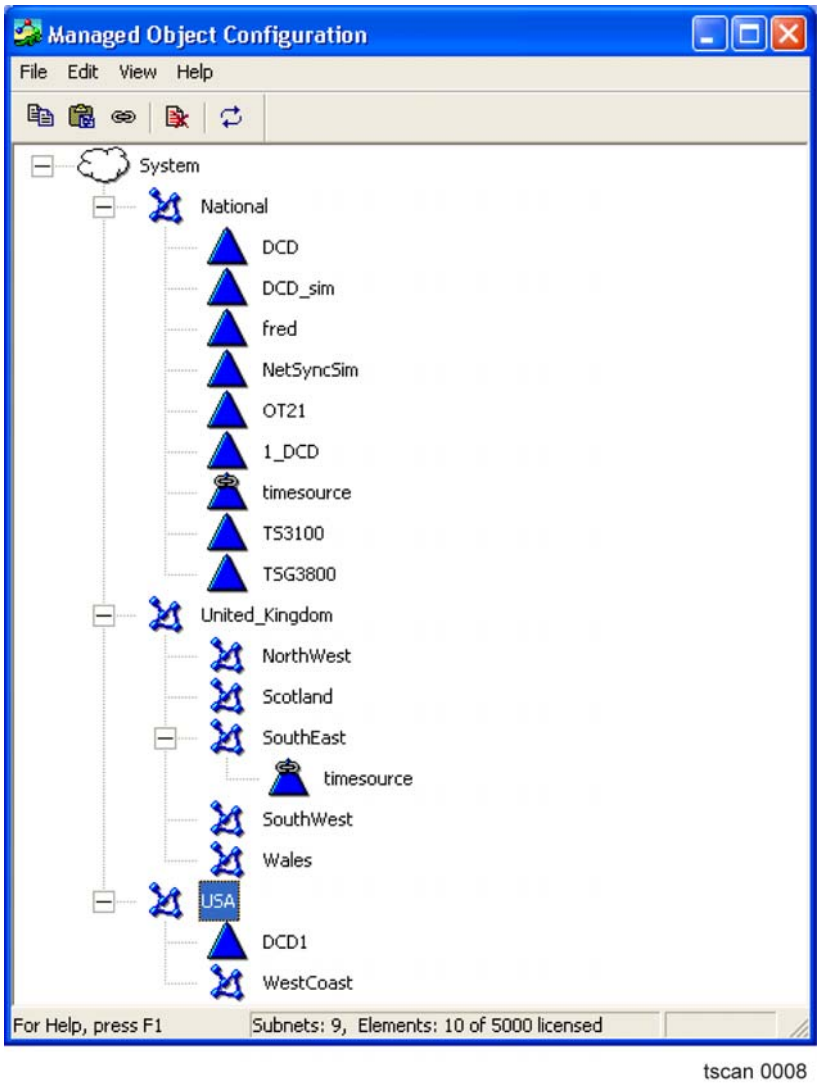


Figure 2-5. Hierarchy View

The Toolbars

There are two toolbars that are used to configure the system. The first is present when the main view (Figure 2-5) is displayed. The second is used when previewing a sub-network.

All of the options that are available through the toolbars are available from the drop-down menus.

Main Toolbar

The options on this toolbar are (from left to right):

Copy object  - This option is only available when an object other than the root is selected. When this button is selected, a copy of the current object is taken for future use (see Paste object and Link object).

Paste object  - Once an object is copied (see Copy object), selection of this button makes a copy of the object at the current location. The new object is prefixed with the words “copy_of_”. This option remains ‘greyed out’ until an object has been copied and the destination is not the root object.

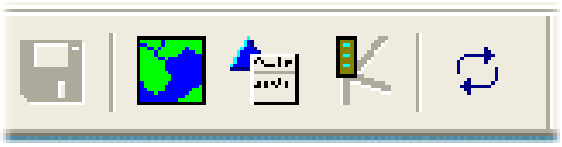
Link object  - Once an object is copied (see Copy object), selection of this button creates a link to the copied object at the current location. Any changes made to the original object are automatically made to the linked object. This option remains ‘greyed out’ until an object has been copied and the destination is not the root object.

Delete object  - Selection of this option deletes the current object from the system, if the object is a sub-network, all contained objects are moved to the root of the system.

Refresh from server  - Selection of this button refreshes the system from the server.

Preview Toolbar

This toolbar is available when the system is in preview mode, accessed by selecting preview from the drop-down menu that appears when a sub-network is selected with the right mouse button.



The available buttons are (from left to right):

Save - When a change is made to the preview, this button becomes active. When selected, the changes that have been made are updated to the database.

Change background image - When this button is selected, a dialog is displayed that allows the selection of a new background image for the preview. Note that the image must be a bitmap file.

Test - When this option is selected, selecting an object allows you to test the currently selected toolbindings, for instance selecting an object with the right mouse button produces a popup menu with the available tools.

Show Connections - Selection of this button either displays or hides the connection line between elements.

Refresh from server - Selection of this button refreshes the system from the server.

Create New Object

To create a new object in the system you must start at the main hierarchy view window.

First select either the root object or a sub-network from the tree in the hierarchy view then bring up the popup menu by selecting with the right mouse button. Then select **Add new...** from the available list of objects (see Figure 2-6).

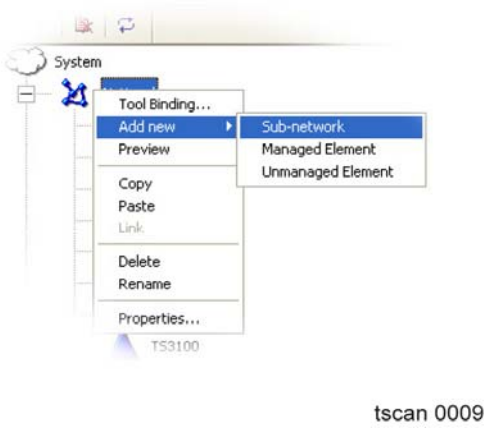


Figure 2-6. Add New Object Menu

The following dialog screen is displayed (Figure 2-7).

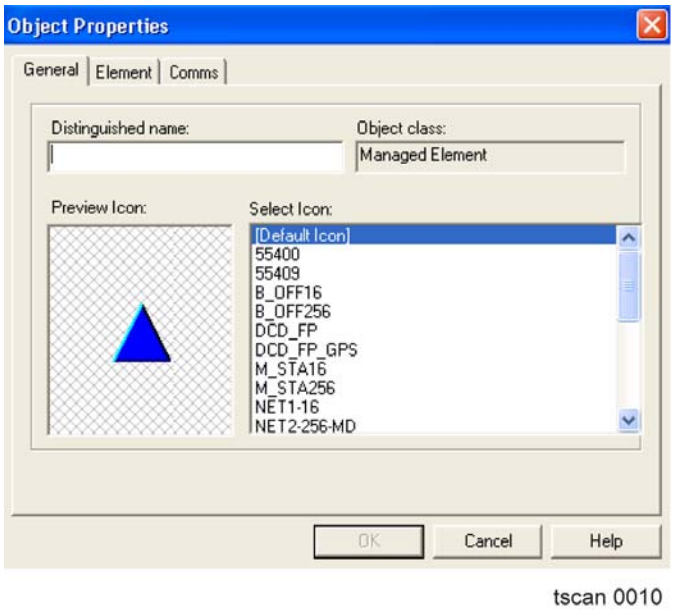


Figure 2-7. Add New Object

You must then enter a unique identifier in the **Distinguished Name** text box. The name must not contain spaces.

You must also select an object class from one of the available options. The dialog changes depending on the choice that is made. These options are discussed in later sections of this document.

Preview Icon specifies the bitmap image (*.bmp) used to depict this object. The system is capable of displaying any size icon image. The icons are bitmap and mask files present in the directory specified by the environment variable `$GRAPHICS_LOCATION_ICONS`.

Attributes for Managed Element (ME)

When **Managed Element** is selected, the **Object Properties** dialog has the **Element** and **Comms** tabs which are specific for MEs. See Figure 2-8 for the **Element Tab** view.

Element Tab

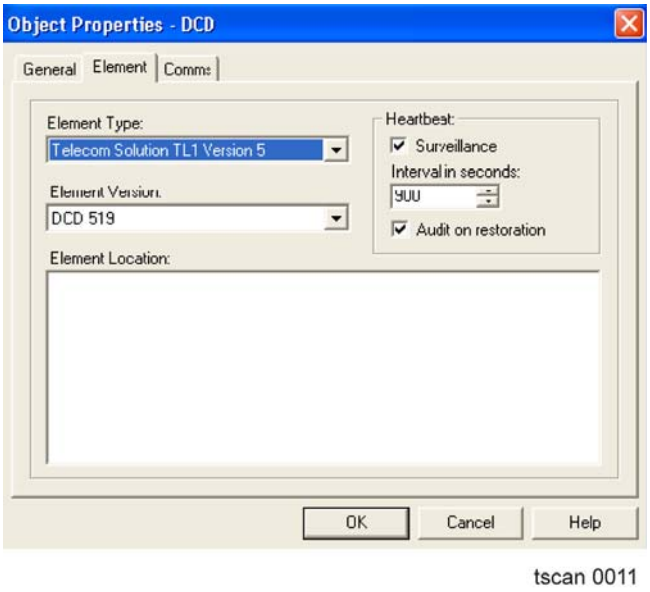


Figure 2-8. Object Properties dialog – Element Tab

Element Type is an attribute that conveys type information for objects of class ‘Managed Element’. If the object is of class ‘Sub-Network’, no type information is required and this field should be left blank. Selecting the Element Type auto-selects the Element Version or scopes the choices.

Element Version is an attribute that conveys variant information for objects of class ‘Managed Element’. If the object is of class ‘Sub-Network’ no variant information is required and this field should be left blank.

Element Location is an optional attribute used to convey the physical location of the object, e.g. “12th Street Office/Rack TQ1-0”.

Heartbeat Surveillance when this box is selected it enables Heartbeat.

Interval in seconds is a user-selectable value that dictates the period, in seconds, that can elapse before the system attempts to Heartbeat the element. The default and recommended value is 900 seconds (15 minutes).

Audit After Restoration when this box is selected, it causes the system to automatically perform an alarm audit on the element when a Heartbeat failure is cleared, for instance when communication with the element is restored. Alarm Audit is described in more detail in the User’s Guide.

Comms Tab

Figure 2-9 shows the Comms Tab view.

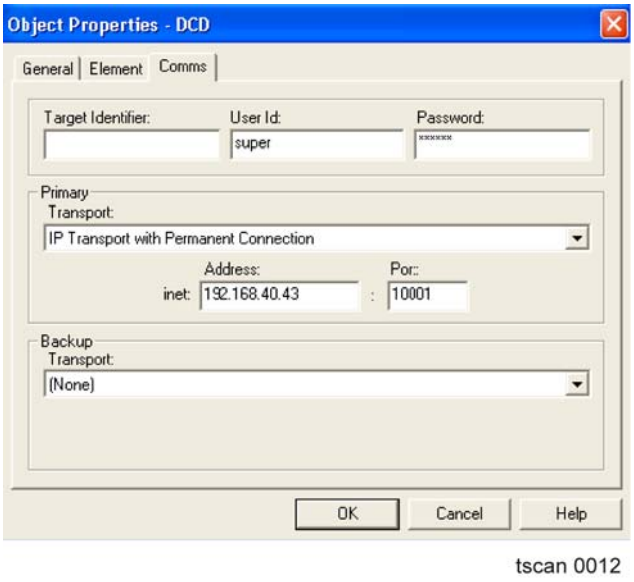


Figure 2-9. Object Properties dialog – Comms Tab

Target Identifier is an attribute that defines the unique identifier string (TID/SID) the element reports to identify itself. This attribute is mandatory for elements that communicate with the local TimeScan server via PSTN modem.

UserId is a mandatory field used to establish communications with the element. A user identity should be selected from the pull-down list provided.

Password is a mandatory field used to establish communications with the element. The password should be the appropriate password for the user identity selected in the UserId field. The password string is not displayed but is implied by a string of asterisk characters.

Primary Transport defines the primary communication method for this element. The TimeScan System supports two basic forms of connection – permanent and session-based.

Permanent connections are recommended for IP and direct serial communication where spontaneous alarm messages are sent over the same communications channel as configuration actions. On system start-up all permanent connections are established. If a permanent connection has failed, periodic attempts are automatically made to re-establish the connection.

Session-based connections are recommended for Modem and X.25 communications, and where the element reports an alarm directly to a TimeScan system. These include TimeSource and NetSync products.

The TimeScan System is capable of supporting two communication transport methods for each managed element. The primary method is always attempted first; if this method fails, the system automatically reverts to the backup method if one is defined. Select the appropriate transport method from the list provided.

Primary Address defines the address of the element associated with the primary transport method.

For IP communications the Address can either be an IP address format or a hostname (see Figure 2-10). The Port is a number which the element uses for incoming TL1 connections. Table 2-1 lists the port numbers associated with the various network elements supported in TimeScan.

Table 2-1. Network Element Port Numbers

Network Element	TL1 Port
NetSync 55400, 55409	7588
OT-21	2000
SSU-2000	2000
TimeSource 3x00	5001 to 5004
TimeProvider	5000
TSG-3800	4000

Note: All TL1 sessions use the TCP protocol and all SNMP sessions use the UDP protocol.

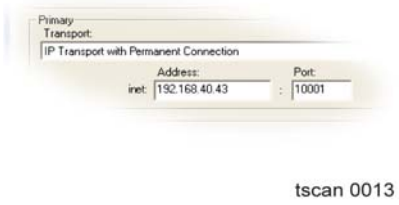


Figure 2-10. IP Communications Example

For X.25 communications the Prime Configuration Management Address is defined as shown in Figure 2-11.

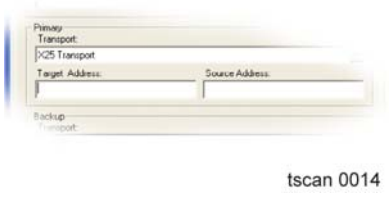


Figure 2-11. X.25 Communications Example

Remote X25 PAD address + port sub-address

Therefore, if the configuration channel of an element is connected to a remote PAD of address 12345 and the port sub-address is 6, then the address is 123456.

The Source Address is the same format as the Target and is used to identify where an alarm originates.

For PSTN (dial-up modem) communications, the Prime Configuration Management Address is defined as shown in Figure 2-12

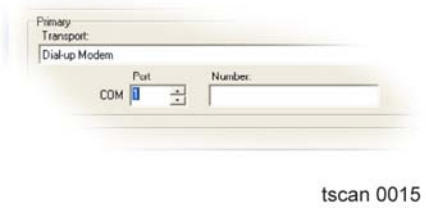


Figure 2-12. PSTN Communications Example

COM + internal port assignment +_+ PSTN number

For RS-232 serial communications, the Prime Configuration Management Address is defined as shown in Figure 2-13.

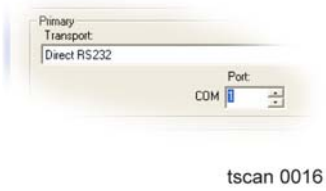


Figure 2-13. RS-232 Serial Communications Example

Backup Configuration parameters are set and stored in exactly the same way as those for the Primary Configuration.

Note: For system configurations where there is no backup communication transport method available, and the prime communication transport method is not based upon permanent connections.

Attributes for Sub-Network (SN)

When Sub-Network is selected, the Object Properties dialog box has a Background tab (Figure 2-14).

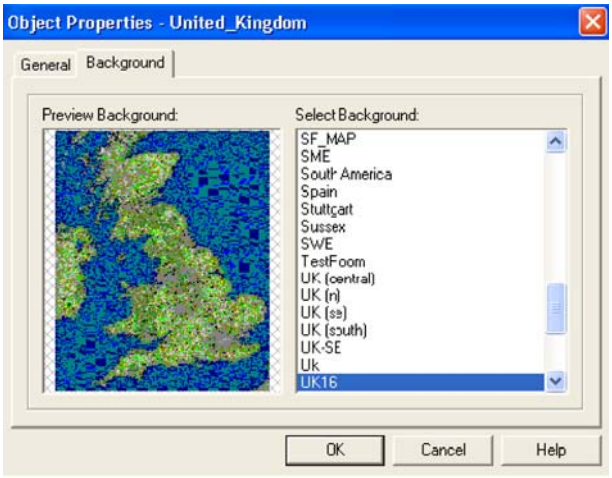


Figure 2-14. Sub-Network Background Tab

Select Background shows a list of images which are bitmap files found in the directory specified by environment variable `$GRAPHICS_LOCATION_MAPS`.

Attributes for Unmanaged Element

Selection of Unmanaged Element allows icons with no other attributes to display in the browser view (Figure 2-15).

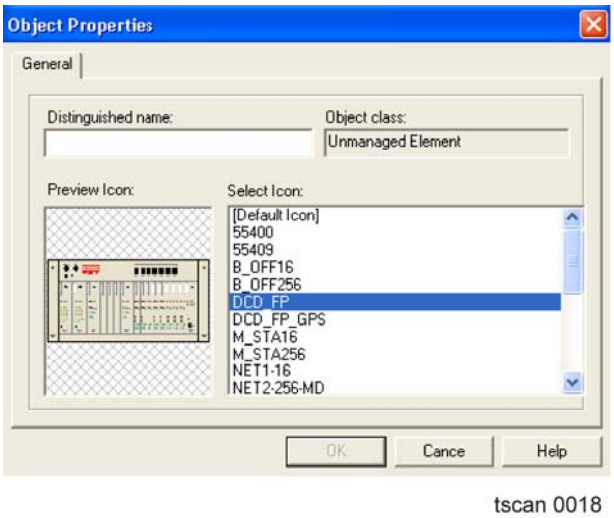


Figure 2-15. Select Unmanaged Element

Tool Bindings

Selecting **Tool Binding...** from the right click menu (available either from the main or preview windows) displays the following dialog box (Figure 2-16).

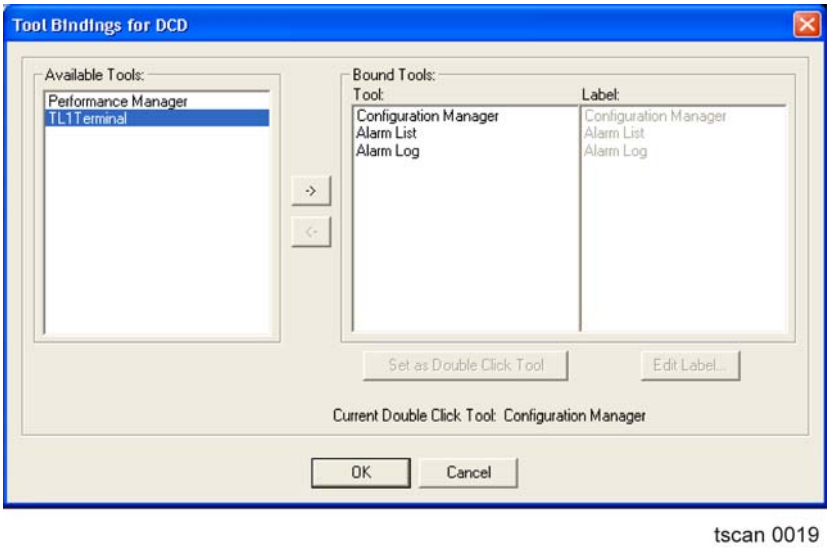


Figure 2-16. Select Tool Bindings

Tool bindings allow you to set the tools that can be selected from the popup menu associated with the element when using the network browser.

The list box entitled **Available Tools** shows a list of the tools that are still available for use on this particular object. Selecting one or more of the tools and then the **->** button binds the tools to the object (shown by the selected tools moving into the **Bound Tools** box. When tools are highlighted in the bound tools box, they can be unbound by pressing the **<-** button.

Highlighting an item in the box titled **Label** and pressing the **Edit Label** button allows you to change the text that is displayed when the popup menu is shown.

Double Click Tool - selecting a bound tool and then clicking on the set as double click tool button changes the currently selected double click tool. This is shown in the caption at the bottom of the box, marked **Current Double Click Tool.**

Remove Object

To remove certain objects from the system, select the object that you wish to delete, then either pressing the **Delete** key (on your keyboard), select **Delete** from the right click popup menu, or press the **Delete** option on the main toolbar.

Edit Object

Edit Object Attributes

To edit the attributes of an object in the system, select the object with the right mouse button and choose the **Attributes...** item from the right click menu. A dialog appropriate for the object is then displayed (see Attributes for Managed Element (ME), on page 31.)

You can edit the attributes for an object in either the main or preview windows.

Edit Object Name

It is possible to edit the name of an object in the system without having to go through the object attributes dialog. Edit the text by selecting **Edit Distinguished Name** (see Figure 2-17) from the right click popup menu or selecting the item text using the left mouse button.

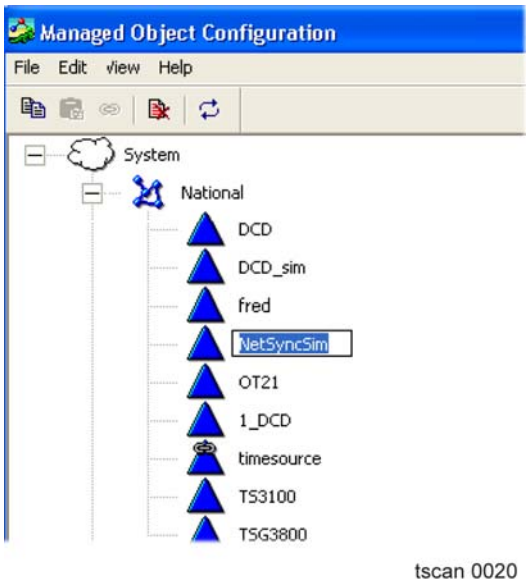


Figure 2-17. Edit Distinguished Name

Move Object

To move objects from one location in the system to another, ensure that you are at the main window and not in the preview window, select the object that you want to move with the left mouse button, then with the left button still depressed ‘drag’ the object to its new location.

A message box is displayed asking you to confirm the operation. If you are happy with the move, select **OK**, otherwise choose **Cancel**.

Copy Object

Copying an object allows you to make an exact duplicate of an object and place it anywhere in the system. Changes made to either object ***are not*** reflected in the other.

When an object is initially copied, the *Distinguished Name* is prefixed with the words “copy_of”. This can be changed once the copy is complete. See Edit Object, on page 38 for details.

To copy an object use the following steps:

1. Select the object that you wish to copy.
2. Choose the *Copy* option from the menu or toolbar.
3. Select the location to copy to (must be a sub-network).
4. Choose the *Paste* option from the menu or toolbar.
5. Confirm the operation by pressing *OK* on the dialog box that is displayed.

Link Object

Linking allows one object to be contained in two or more places in the system, for instance any changes made to the object appear in all of the linked objects.

To copy a link object use the following steps:

1. Select the object that you wish to copy.
2. Choose the *Copy* option from the menu or toolbar.
3. Select the location to copy to (must be a sub-network).
4. Choose the *Link* option from the menu or toolbar.
5. Confirm the operation by pressing *OK* on the dialog box that is displayed.

Preview Network

MOC provides the ability to preview and edit the contents of a sub-network to see how it appears in the network browser.

To enter the preview view simply select **Preview** from the right click menu that is displayed when selecting a sub-network from the main window. A window is displayed as shown in Figure 2-18.

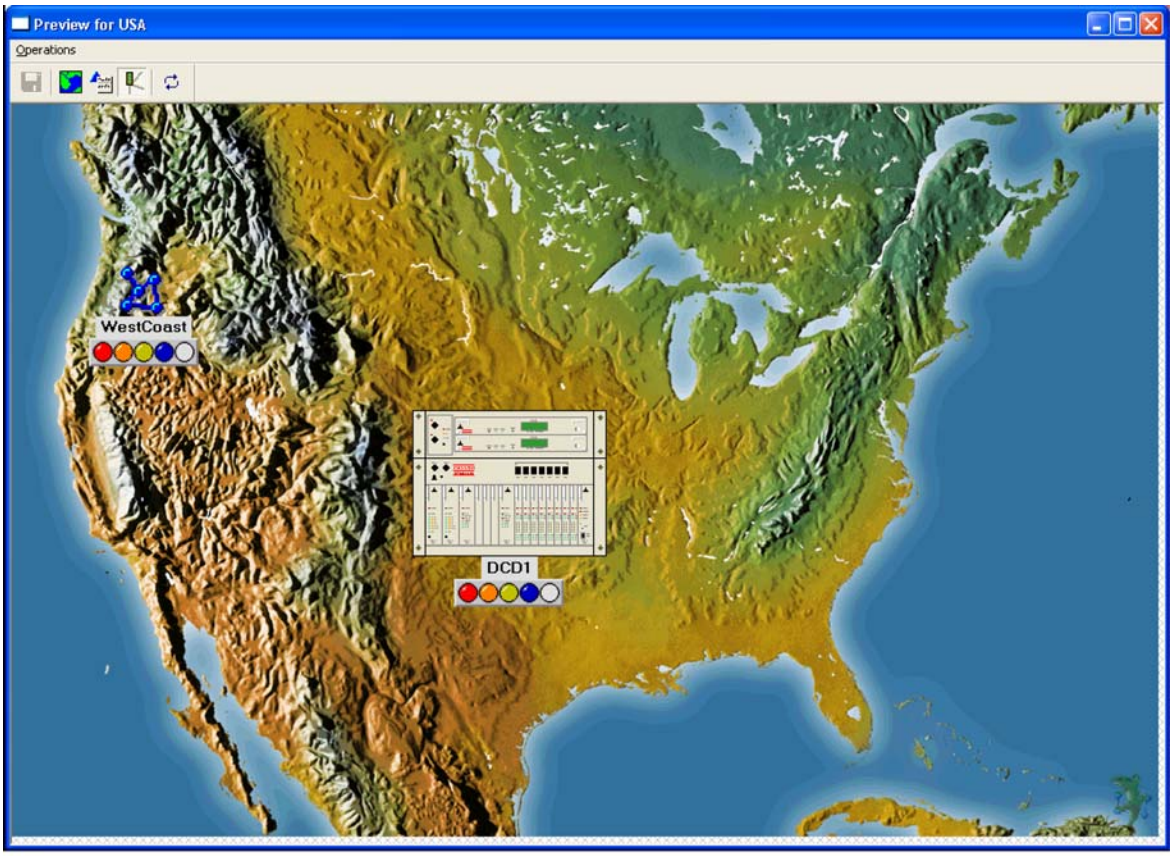


Figure 2-18. Preview Sub-Network

Change Background Image

To change the background image, select **Change background image...** from the operations menu. You can then select a bitmap file and location from the file selection dialog.The window sizes itself to the new image.

Note: You can use only bitmap images for the background image.

Test

When this option is selected, selecting an object allows you to test the currently selected toolbindings. Selecting an object with the right mouse button produces a popup menu with the available tools.

Save

When a change has been made to the preview, the **Save** option becomes active. Selecting the **Save** option saves all of the changes that have been made.

Connections

MOC is used to set up connections between elements. Connections are lines drawn between elements within the Browser. To set up connections between elements, select the object with the right mouse button and choose the “Connections” options (see Figure 2-19).

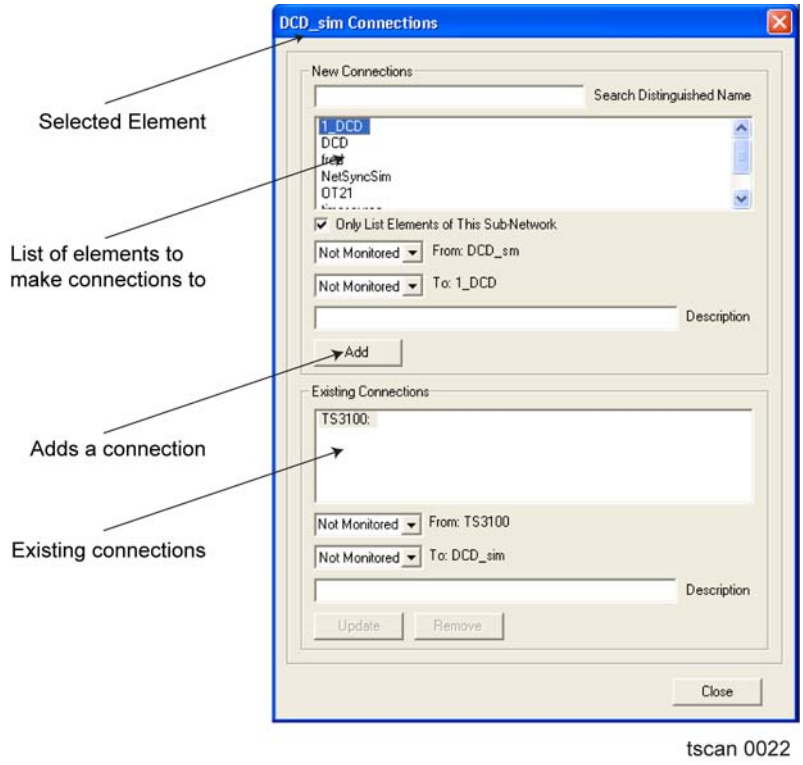


Figure 2-19. Connection dialog

Connections made here can be viewed in the preview window (Figure 2-20).

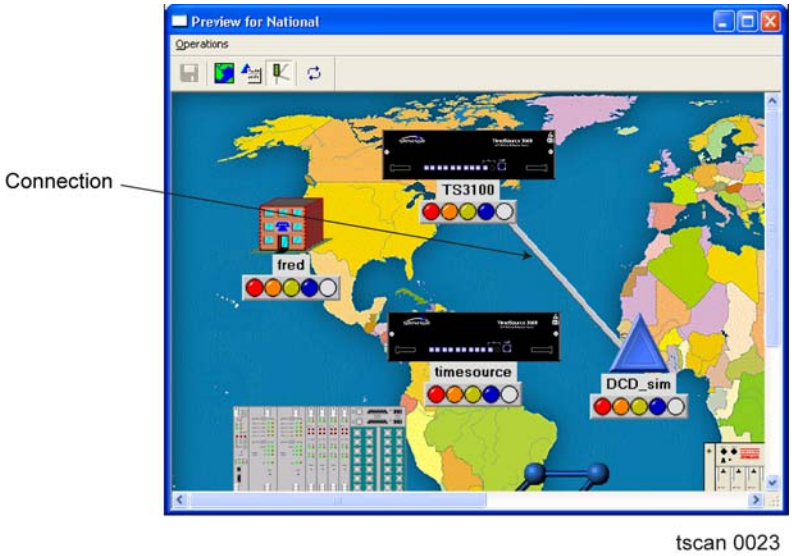


Figure 2-20. Connection Preview

Using Imported Graphics in a Client/Server Setup

The Managed Object Configuration application only looks for the graphics files using the two environment variables `$GRAPHICS_LOCATION_MAPS` and `$GRAPHICS_LOCATION_ICONS`. This can cause a problem when trying to preview an object on a client if the files do not exist in the specified directories.

Chapter 3 Security Manager

This chapter provides information on the security management application with detailed descriptions of set up procedures and operation.

In this chapter:

Overview

The Security Manager keeps your records and applications safe from those who are not authorized to use them. It checks that a given user has the security privileges necessary to complete a particular action.

What Would I Need to Use the Security Manager Application?

The Security Manager can run either as a standalone application or as part of a suite of TimeScan applications. You will need a server (or database) that is already set up to exchange information with the Security Manager to run it effectively. Security Manager comes supplied with a set of templates suitable for Users, Administrators, and Observers of the applications.

What's in This Chapter?

To make full use of the security management subsystem, it is necessary for you to understand the concepts of the security system and how they interrelate. The Notes for Administrators, on page 58 outlines some key concepts needed to exploit the features of the Security Manager, including information about the supplied templates. There is also a step by step guide, Using Security Manager – Overview, on page 46.

Opening the Security Manager Application

The application is launched by double clicking on its icon , found on the Admin menu in the Windows **Start** menu (see Figure 3-1). Once successfully launched, the application displays a list of users registered with the system (Figure 3-2).

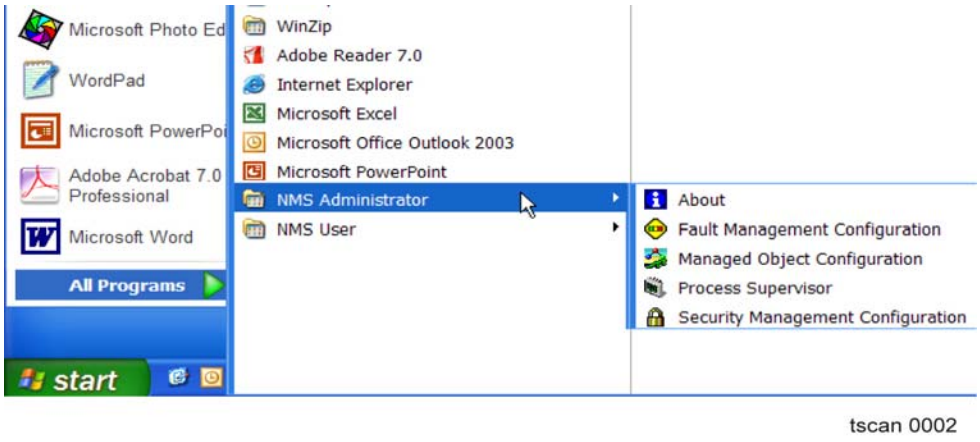


Figure 3-1. Windows Start Menu

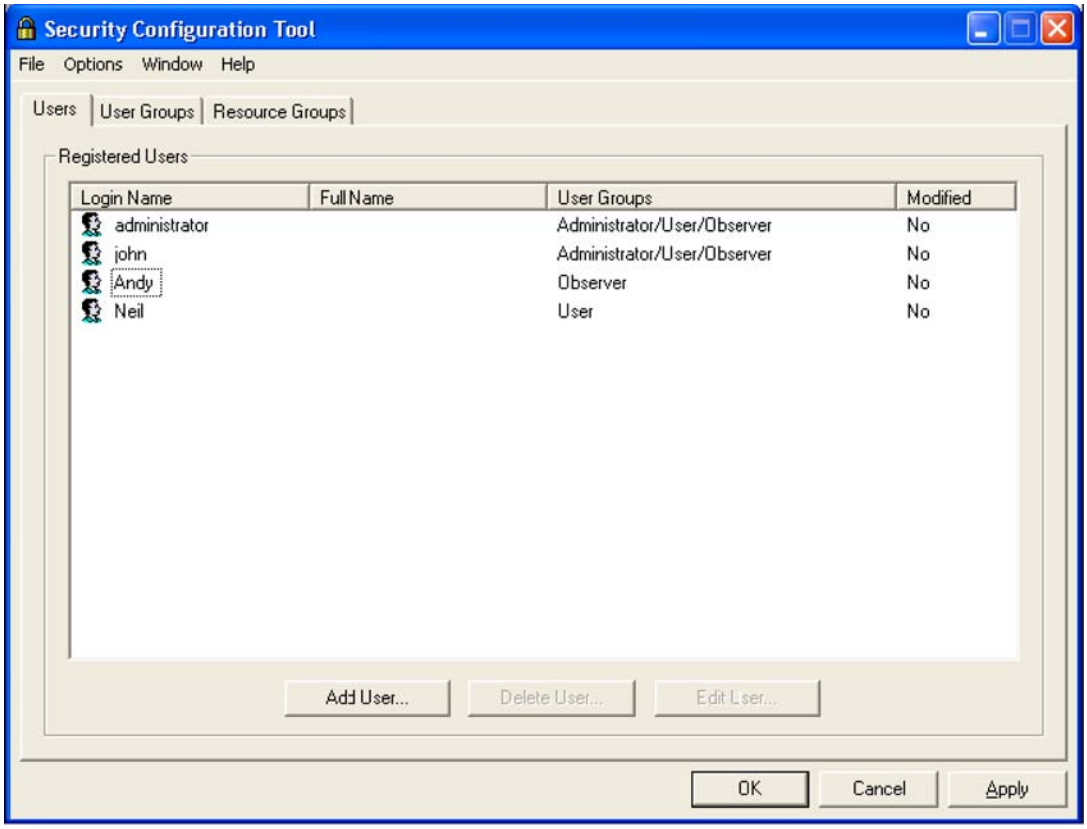


Figure 3-2. Security Manager at Startup

You can also start the Security Manager application by selecting its shortcut from the program group.

Using the Security Manager Application

The Security Manager looks similar to Figure 3-2. It is structured as a series of tabbed pages. You can select any page at any time (although the current page may require you to finish changing data before letting you leave it).

- The **OK** button sends the current security set up to the server and closes the tool.
- The **Cancel** button closes the tool without sending data to the server.
- The **Apply** button updates the server but does not close the tool. This is particularly useful if you want to save changes that you have just made, but are unsure about a set of changes which you are about to attempt.

The Menus

The security configuration tool has four drop-down menus:

- File Menu
- Options Menu
- Window Menu
- Help Menu

File Menu

Import Data File: You can set up and save different security configurations without committing them to the server and consequently having them go ‘live’. The **Import Data File** option is for reloading a previously saved data set.

Export Data File: The export data file option allows you to save the current security set up in the security tool to a data file. This option is also useful for making backups of the security configuration over and above that provided automatically by the security system.

Exit: Selecting this closes the security tool.

Options Menu

Re-Synchronize from Database: This option allows security to verify/add/remove objects (Element/Sub-Networks) in the security system. This option is normally used if a security scheme is imported using the Import Data File option, or after an upgrade from an old version.

Window Menu

Refresh from server: Selecting this item updates the security tool’s local copy of the security data from the server and refresh the window. Any changes made in this session but not yet saved to the server (using the **Apply** button) is lost. A warning to this effect is issued before the refresh is begun.

Help Menu

Contents: The contents item brings up the help contents page.

About: Selecting this item displays the security tool’s **About** box, which shows version and copyright information.

Using Security Manager – Overview

There are three tab pages. They show a list of items with the information arranged as a series of columns containing items. An *Item* is an entry or row in the list on any of the tab pages.

Sorting Security Manager Items

Clicking on each column heading sorts the list based on the data in that column. Clicking the same column twice reverses the data sort order.

Editing Items in Security Manager

To edit any item in the list, double click on it in the left hand column to display an appropriate details dialog box. You can also display this dialog by right clicking on the item and selecting the **Details...** option from the popup menu.

Adding Items to Security Manager

To add a new object, click the **Add** button, or right click in a blank area of the list and select **Add...** from the popup menu. This creates a new object with a default name and brings up the appropriate details dialog to allow you to edit the newly created object. Note that the name of an object is required and must be unique.

Deleting Items from Security Manager

Deleting an object requires selecting the object in the list and clicking the **Delete...** button at the bottom of the page, or right clicking the appropriate object and selecting **Delete...** from the popup menu. There is a confirmation dialog before objects are deleted as this action cannot be undone.

Note: You cannot delete a User Group/Resource Group which still contains a User/Resource.

Filtering Items in Security Manager

Many of the dialog boxes contain filter boxes. These are intended to assist you by decreasing the size of lists which can contain many items. The first item in the filter box is **All**, which displays all of the data, followed by the options that limit the data. These filters only affect the display – they do not change the underlying data or security set up.

Users Page

The users page is the active page when the application first starts (see Figure 3-2). The page consists of four columns.

Login Name Column

The first of these columns is the user's login name. This must be the same as the name with which they identify themselves to the operating system at login time.

Full Name Column

This shows the real name of the user. This is particularly useful if their login is something meaningless, such as fb27.

User Group Column

The next column shows the user group to which the user currently belongs. Users can only belong to one group at a time.

Modified? Column

The final column indicates whether the user has any specific overrides in their security access.

Adding/Editing User Items

Double-clicking an item in the user name column brings up the User Details dialog box. This allows you to change the user's login, full name, and user groups (See Using Security Manager – Overview, on page 46).

To add a new user, either right-click on an empty part of the list and select Add from the popup menu, or click the Add User button at the bottom of the window. An empty version of the User Details dialog box (Figure 3-3) is displayed which you can fill in.

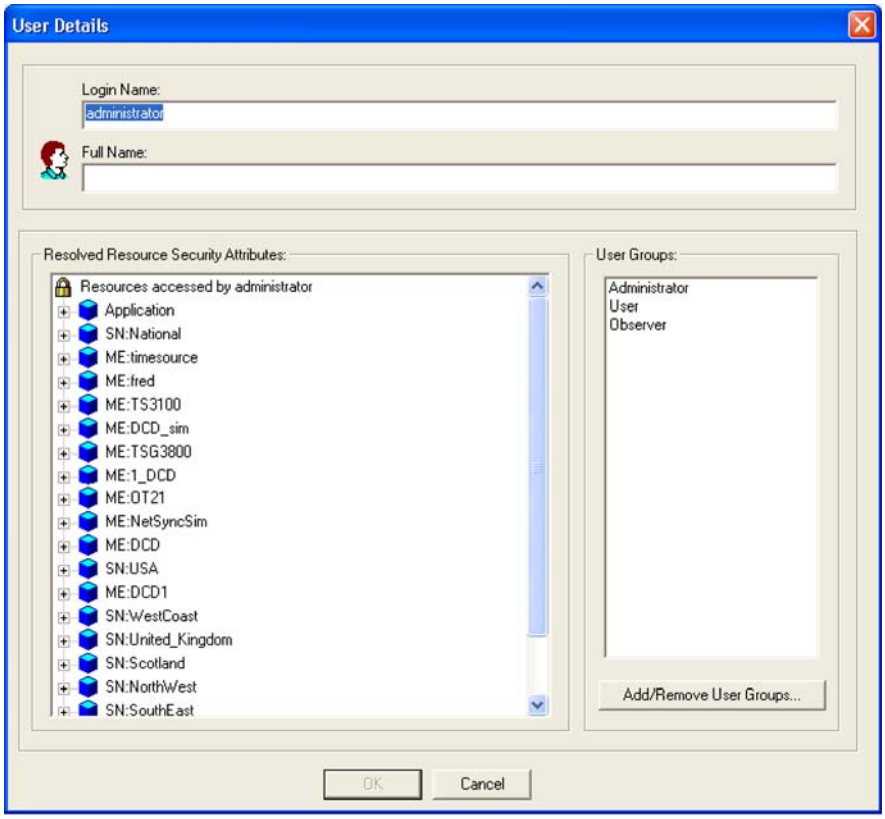


Figure 3-3. User Details dialog Box

Viewing/Modifying Access Levels Available to a User

The resources to which a user has access are also listed in the user details dialog box (Figure 3-3). Expanding a resource, by either double clicking on its name or single clicking on the small + box to its left, shows all of that resource's attributes. The user's default access level for each attribute is marked in brackets, for example *NA-No Access*, as shown next to Application Y in Figure 3-3. This default access is inherited from the User Group to which they belong.

If you wish to override the user's access level to that attribute you can add a modification to the security level. Right clicking on the attribute displays the popup modifications menu. The first item (Add modification) cascades into a further menu that lists access levels. Selecting an access level from this menu sets the modification. Once set, a modification is shown to the right of the original access in angle brackets, e.g. <*FA*>, shown on Application Y in Figure 3-3.

Removing a modification is just as simple. Right click on an attribute with a modification and select **Remove Modification** from the menu.

Click **OK** to set the changes, or **Cancel** to return to the main window without applying them.

Making a New Resource Available to a User

Resources cannot be added directly to the user. If you need a user to have access to a resource which is currently unavailable to them, take the following steps:

- Find out which resource groups the user's user groups can access (system contains all resources).
- Add the resource to one of these resource groups.
- Set the default access level to that resource to *NA* - No Access.
- Modify the individual user's Access Level to this resource as outlined in the previous section.

If this is not desirable, you could consider moving them to a group which does have access to the required resource.

Deleting a User

To delete a user, highlight their name in the list and press the **Delete User** button at the bottom of the window. You could also select **Delete** from the popup menu.

If you wish to commit these changes to the server immediately click **Apply** at the bottom of the main window.

User Groups

The User Groups panel shows the user groups to which this user belongs (Figure 3-4). The security attribute and the resources (elements) to which they apply are directly retrieved from these groups. A user can belong to one or more user groups; these can be changed using the Add/Remove User Group dialog box (Figure 3-5).

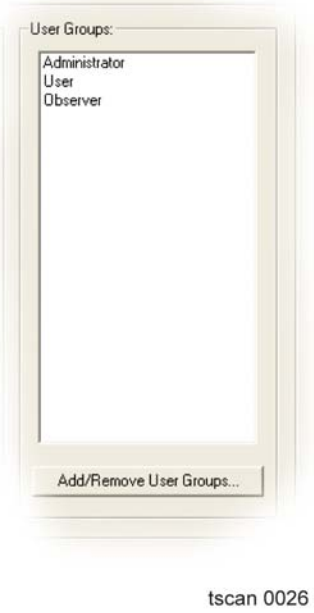


Figure 3-4. User Groups Panel

Figure 3-5. Add/Remove User Group

User Groups Page

The User Groups page is shown in Figure 3-6. There is a column displaying the names of the user groups, and a column displaying an optional description of each user group.

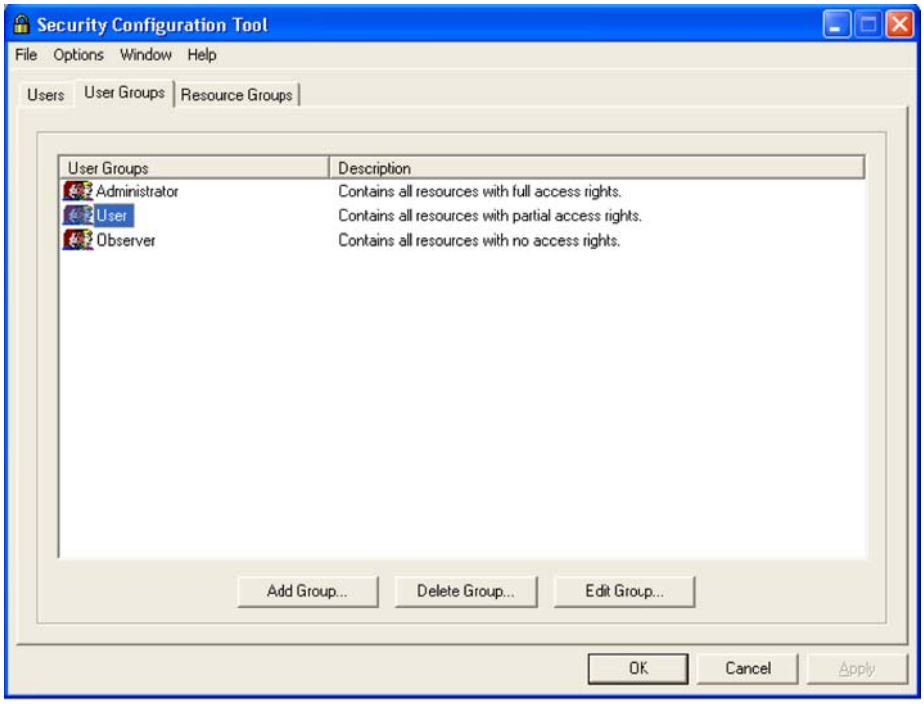


Figure 3-6. User Groups Page

Adding/Editing User Groups

Double click on an item in the **User Group** column to bring up the user group details dialog box for the selected group. Pressing the **Add Group** button also brings up the User Group Details dialog, but in this case it is empty.

The dialog (Figure 3-7) consists of several tabs, each discussed in detail below.

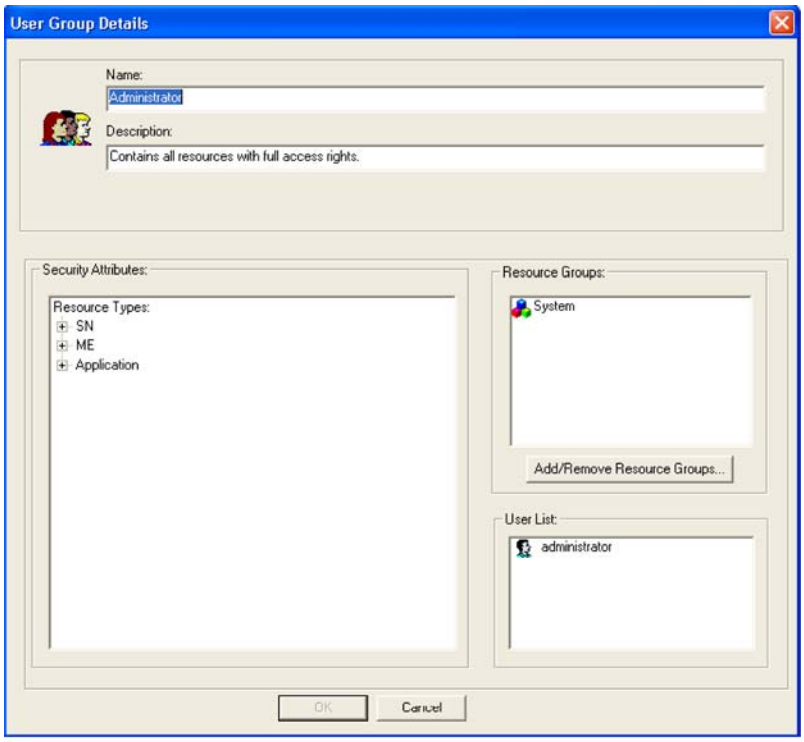


Figure 3-7. User Group Details dialog

Security Attributes

The security attributes define the security for the particular resource types, Sub-Network (SN), Managed Elements (ME), and Applications. Opening the tree shows the value of the attributes (Figure 3-8).

Figure 3-8. Security Attribute Values

The attribute value can be changed using the background menu for each attribute. Changing this affects all users who are members of this group (Figure 3-9).

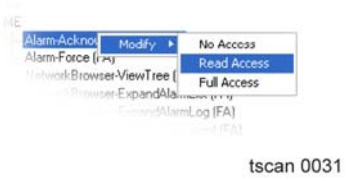


Figure 3-9. Security Attribute Background Menu

Resource Groups Panel

The Resource Groups panel (Figure 3-10) shows which resource group the security attributes apply to.

Figure 3-10. Resource Groups Panel

Resource groups can be added using the dialog shown in Figure 3-11.

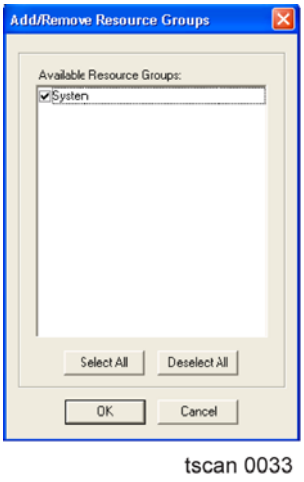


Figure 3-11. Add/Remove Resource Groups

The user panel shows which user belongs to this User Group and is affected by changes to this group.

Resource Groups Page

The Resource Groups page (Figure 3-12) shows all the resource groups in the system. It has two columns showing the name of the resource group and an optional description. Adding, deleting and editing of resource groups is done in the usual way.

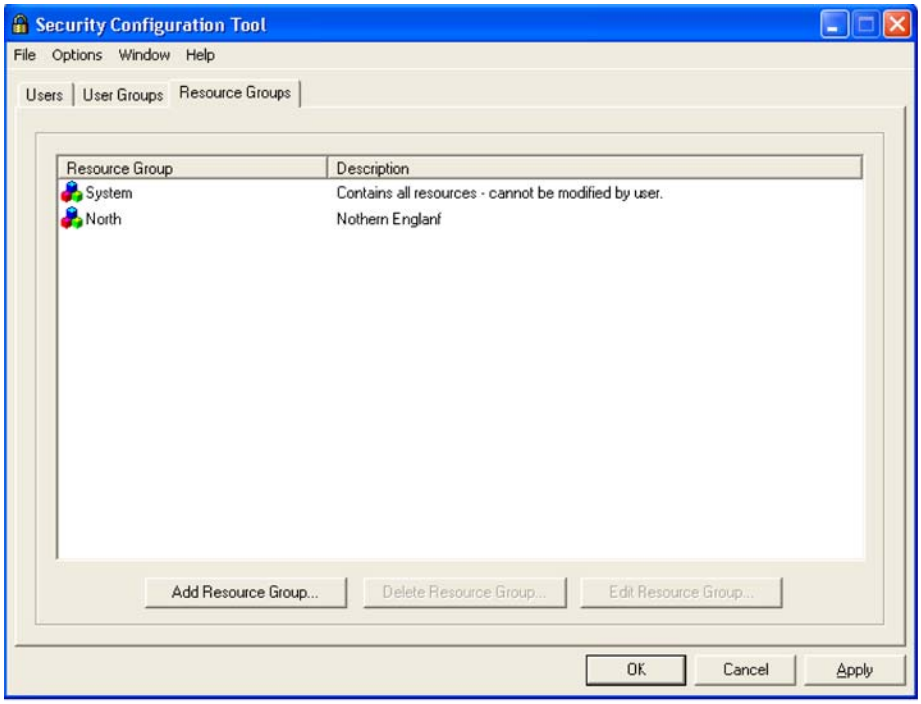


Figure 3-12. Resource Groups Page

Adding a New Resource Group

Either right click on an empty part of the page or click the **Add Resource Group** button at the bottom of the page. Both of these actions brings up the Resource Group details dialog. Fill this in with the Resource Group name (required) and Resource Group description (optional), then follow the instructions for adding resources to a group in the following section, Editing Existing Resource Groups.

Editing Existing Resource Groups

Double-clicking/right-clicking on a Resource Group brings up the Resource Group details dialog box (Figure 3-13).

Note: The Resource Group called *System* is maintained automatically and cannot be modified by you. This group contains all the resources currently administered by the Security Manager application. Providing every user group with differing levels of access to this group (for example, access to Managed Elements) ensures that any new Managed Elements added is automatically available to that user group.

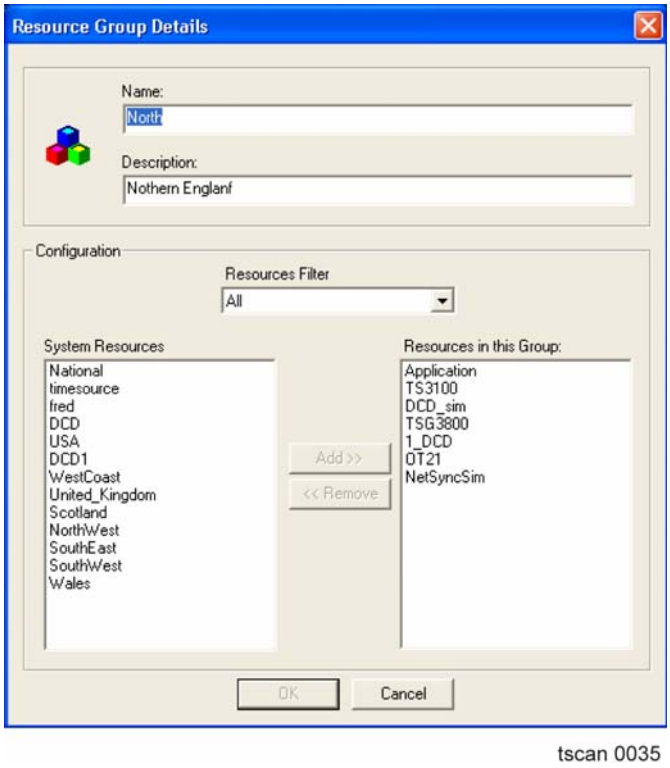


Figure 3-13. Resource Group Details dialog Box

The resource group details dialog box allows the name of the group to be changed, and an optional description to be added or edited. It also allows you to edit the resources that are in the group.

To add a resource, select the one you want to include from the box on the left labelled **System Resources** and click the **Add >>** button. At this point it transfers across to the **Resources In This Group** box.

Resources can be removed from the group by selecting them in the right hand box and clicking the **<< Remove** button.

The **Resources Filter** box can be used to limit which resources are displayed in both of the boxes.

Deleting Resource Groups

To delete a resource group, simply highlight it in the main Resource Group page and press the **Delete Resource Group** button at the bottom of the page. A confirmation dialog is displayed, checking that you really want to do this.

Note: You cannot delete Resource Groups that still contain Resources. Reassign Resources to another Resource Group before deleting a Resource Group.

If you wish to commit these changes to the server immediately, click **Apply** at the bottom of the main window.

Automatic Idle Time Out

Only one copy of the security tool can be open at any one time. Since the server to which the tool connects can be running on a different machine from that of the tool, it is possible that the security tool could inadvertently be left running and prevent other copies being started.

To avoid this, the security tool detects when it has been left idle for five minutes and prepares to close down automatically. Thirty seconds before closing down, Security Manager beeps and displays a dialog. This informs the user that it is about to terminate, that changes are automatically be saved, and it counts down the remaining seconds. To stop the application from shutting down, press the cancel button on the dialog box.

Frequently Asked Questions

1. Q Why can’t I change the System Resource Group?

   A This is not modifiable by the user. It shows all the resources which are currently being managed by the application. When resources are removed from or added to Security Manager, the System Resource Group is automatically updated.

2. Q Why do only some of my changes get saved?

   A To ensure that a modification is saved, press the Apply button once you have completed it. Then the server is updated with any unsaved changes.

3. Q Can I select more than one user/resource at a time?

   A No.

4. Q Why can't I delete a User Group/Resource Group?

   A You cannot delete a User Group or Resource Group which still has members. Reassign these members to another group before attempting to remove the original group.

5. Q Why can't I start a copy of Security Manager?

   A Only one copy of Security Manager can be running at a time. Check that either the home machine, or the server to which it connects, is not already running a copy of Security Manager.

Notes for Administrators

Terms Used in Security Manager

User

A *user* is a person registered with the security system. Their security access is derived from the user group to which they belong.

User Group

User groups are sets of individual users who have the same or similar access privileges. It is in a user group that most of the security access is set up. A user group contains a set of resource groups that specify which resources the user group members can access, and you can assign a set of access templates to act on each resource group.

Resource

A *resource* represents something that is secured. Resources have to be based on a *type definition* (see Type Definition, on page 59) and they inherit the *attribute* (see Attribute, on page 59) of that type. If the definition subsequently changes so does the structure of all resources based on that type.

Resource Group

A *resource group* is simply a collection of resources. There is always one resource group defined, called System. This contains all resources currently supervised by the Security Manager. You can define as many resource groups as you wish. Resource groups can contain as many resources as necessary. Each resource can be included in more than one resource group. One example of a resource group could be to class resources by their geographical location.

Type Definition

A type is intended to model something that can be secured. Types are used as *templates* on which to base resources. They can have a set of attributes (see Attribute, on page 59), each of which can be assigned an *access level* (see Access Levels, on page 59). Attributes can also *contain* attributes, so for example you could have MRC1 as an attribute with ports 1 to 4 as sub attributes.

Another example of a type definition would be to have a *type* called *Application* with an *attribute Run* which would be used to specify who could launch that application.

Access Templates

An *access template* provides a way of specifying a set of *access levels* for a type. For any given type you can define as many access templates as necessary. Each access template can assign a different access level to each attribute. Access templates can be applied to all the resources in a resource group via a user group.

Attribute

An attribute is a specific part of, or action that can be performed on, a resource. Each attribute has an individual access level. Attributes are created in type definitions.

Access Levels

These are levels of access that a user has to a resource, or to one of its attributes. There are three access levels:

- No Access (NA)
- Read access (R)
- Full Access (FA)

Modifications

The security system is designed to allow you to set up the likeliest access scenario for most situations quickly and easily. However in some circumstances you can tweak the specific access provided for a given user or user group. These tweaks are known as *modifications* and can be applied on a per attribute basis to both individual users and user groups.

Supplied Templates

The Security Manager comes with a ready to use set of templates already defined for you, providing you with instant security for the NMS set of applications. They contain the following groupings:

Resource Group

There are two designated Resource Groups:

- **System** – all of the resources controlled by Security Manager.
- **User Resource Group** – the resources which can be accessed by Users.

User Group

There are three designated User Groups with default access levels:

- **NMS Admin** – Full access to all resources in System, and hence all of the resources in the User Resource Group.
- **NMS Users** – Full access to all resources in the User Resource Group, and full access to all SubNetwork and Managed Element (ME) resources. Note that this group also has limited access to the System group, so that any Managed Elements or SubNetworks which are added to Security Manager control.
- **NMS Observers** – Read access to all resources in the User Resource Group.

User

There is one designated User:

- **nms** – A member of the NMS Admin group.

Chapter 4 Alarm Forwarding

This chapter contains information about using the Alarm Forwarding System.

In this chapter:

Overview

This chapter provides information on using the Alarm Forwarding function in TimeScan Release 8.7.

Why Would I Use Alarm Forwarding?

TimeScan can be set up to forward alarms to an external system. The external system must listen on a TCP/IP socket and receive textual based alarm/event and clearing messages once a connection has been established.

Alarm Forwarder Service

A new NMS service “SimpleAlarmForwarder” can now be added to the *SupervisedProcesses.txt* files. This service controls the alarm forwarding function. On start-up the service reads a configuration file (default= *AlarmForwarder.txt*) (Figure 4-1) which defines the forwarding destination, the severity filter, and a regular expression criteria. This file can be found in the *$MONITORHOME/configs* directory.

```
// Simple alarm forwarding configuration file

DestinationAdresss=inet:11.103.41.99:1234567

SeverityFilter=”WARNING” // values
CRITICAL,MAJOR,MINOR,WARNING,NONE

AlarmMatchRE=”.*” // matches all

Acknowledgments=NO // YES/NO

RetryIntervalOnFailedsocket=15000 // timeout in milliseconds

AckTimeout=15 // timeout in seconds

AlarmBufferSize=20 // number of alarms to buffer up in failure situation
```

Figure 4-1. Alarm Forwarder Configuration File

The parameters in the config file have the following format:

- *DestinationAdresss* = inet:<*IP or known hostname*>:<*socket number*>.
- *SeverityFilter* = <*severity value*> from the following list:
  - CRITICAL: Forward only critical alarms

  - MAJOR: Forward only Critical and major alarms
  - MINOR: Forward critical, major, and minor alarm
  - WARNING: Forward critical, major, minor, and warning alarms
  - NONE: Do not forward alarms.

- *AlarmMatchRE = <a valid RE>* this regular expression is matched against the alarm text. If it matches then the alarm is forwarded.
- *Acknowledgments = <YES or NO>* If yes the remote device is expected to send a message after each alarm containing the string *ACK=n* where *n* is the *ACK Number* sent in the alarm. If no acknowledgment is received within <*AckTimeout*> seconds, the socket is shutdown and reopened.
- *RetryIntervalOnFailedsocket =<0-32000>* a timeout in milliseconds that the Alarm Forward is delayed in between connection attempts to the remote socket.
- *AckTimeout =<1-300>* a timeout in seconds. If no acknowledgment is received in the specified number of seconds, the remote socket is shutdown and restarted.
- *AlarmBufferSize =<0-2000>* the number of alarms that are buffered and re-sent to the remote socket if a failure occurs.

The SimpleAlarmForwarder service tries to connect to the destination address specified in the configuration file. If this fails, it retries to connection every 15 seconds (or *RetryIntervalOnFailedsocket* value). Once a connection is established, incoming alarms are compared to the specified criteria, and if matching they are forwarded as text over the socket. If the socket fails, the retry mode is re-entered. Alarms are buffered up to the number specified by *AlarmBufferSize* value when the remote socket is in failure, or the remote end does not acknowledge an alarm.

When *Acknowledgments* is set to *YES*, the SimpleAlarmForwarder expects the remote socket to send a message back to over the socket, containing the *ACK Number* specified in the original alarm message. No more alarms are sent until an *ACK* is received. Instead they are buffered and sent after the *ACK* is received. If no *ACK* is received within *AckTimeout* second of the alarm being sent, the socket is shutdown, then reopened.

Figure 4-2 shows the forwarded alarm format and Figure 4-3 shows the *ACK* message format.

DN=<NMS DistinguishedName>,ACK=<n><CR><LF>>

<Alarm Text>

e.g.

DN=DCD1,ACK=1

TELECOM 2000-01-03 01:24:52

A 217 REPT EVT EQPT

"CLK-2:LOCKED,SC,2000-01-03,01-24-52:/* CLOCK CONVERGED ON REFERENCE INPUT */"

;

Figure 4-2. Forwarded Alarm Format

ACK=<n>

e.g.

ACK=1

Figure 4-3. ACK Message Format

The alarm text can contain white space before first line, depending on the text that was received from the ME.

Regular Expression Format

The regular expression (RE) is constructed as follows:

The following rules (1.1-1.5) determine one-character REs that match a single character:

Table 4-1. Rule 1.1

1.1	Any character that is not a special character (to be defined) matches itself.

Table 4-2. Rule 1.2

1.2	A backslash (\) followed by any special character matches the literal character itself. *i.e., "escapes" the special character.*

Table 4-3. Rules 1.3 and 1.4

1.3	The "special characters" are: + * ? . [ ] ^ $
1.4	The period (.) matches any character except the new line. e.g., ".umpty" matches either "Humpty" or "Dumpty."

Table 4-4. Rule 1.5

1.5	A set of characters enclosed in brackets ([]) is a one-character RE that matches any of the characters in that set. E.g., "[akm]" matches either an "a", "k", or "m". A range of characters can be indicated with a dash. E.g., "[a-z]" matches any lower-case letter. However, if the first character of the set is the caret (^), then the RE matches any character except those in the set. It does not match the empty string. Example: [^akm] matches any character except "a", "k", or "m". The caret loses its special meaning if it is not the first character of the set.

The following rules (2.2-2.4) can be used to build a multi character RE.

Table 4-5. Rule 2.1

2.1	A one-character RE followed by an asterisk (*) matches zero or more occurrences of the RE. Hence, [a-z]* matches zero or more lower-case characters.

Table 4-6. Rule 2.2

2.2	A one-character RE followed by a plus (+) matches one or more occurrences of the RE. Hence, [a-z]+ matches one or more lower-case characters.

Table 4-7. Rule 2.3

2.3	A question mark (?) is an optional element. The proceeding RE can occur zero or once in the string - no more. e.g. xy?z matches either xyz or xz.

Table 4-8. Rule 2.4

2.4	The concatenation of REs is a RE that matches the corresponding concatenation of strings. e.g., [A-Z][a-z]* matches any capitalized word.

Finally, rules 3.1 and 3.2 show how the entire regular expression can be anchored to match only the beginning or end of a line.

Table 4-9. Rule 3.1

3.1	If the caret (^) is at the beginning of the RE, then the matched string must be at the beginning of a line.

Table 4-10. Rule 3.2

3.2	If the dollar sign ($) is at the end of the RE, then the matched string must be at the end of the line.

The following escape codes can be used to match control characters.

Table 4-11. Escape Codes

Code	Description
\b	backspace
\e	ESC (escape)
\f	formfeed
\n	newline
\r	carriage return
\t	tab
\xddd	the literal hex number 0xdd
\ddd	the literal octal number ddd
\^C	Control code. e.g. \^D is “control-D”

Supervised Processes Files

Figure 4-4 shows a example of the *SupervisedProcesses.txt* file which can be found in the *$MONITORHOME/configs* directory. Inserting the last line starts the SimpleAlarmForwarder when the supervised processes are restarted.

```
IS

FM_SERVER

HB_SERVER

TSERVER

TSCV5 UI

SimpleAlarmForwarder
```

Figure 4-4. SupervisedProcesses.txt Example

Chapter 5 Process Supervisor

This chapter provides information on the Process Supervisor, a server application that manages user specified processes.

In this chapter:

Overview

The Process Supervisor is a server application that manages the processes you specify. A process is something which the operating system can run. It is also known as a program or executable file. At startup, the Process Supervisor starts any processes stored within the ini file: PSFiles.ini.

The Process Supervisor User Interface (UI) allows you to view the processes being supervised. You cannot view processes for which you do not have read access, as defined by the NMS Security Manager application.

Why Would I Use the Process Supervisor Applications?

With these programs you can monitor the CPU usage of each supervised process and set a maximum memory usage for it. All supervised processes are continually checked to see if they have crashed or if they are leaking memory. If so, they are restarted automatically.

Note: Processes that crash frequently have a 15-second delay before restarting. Other processes restart immediately.

What Else Would I Need to Use the Process Supervisor Applications?

To run the Process Supervisor, you must be running Windows 2000 or XP.

The Process Supervisor's supervised processes can only be manipulated via requests from the Process Supervisor UI. Only one Process Supervisor UI can be connected to the Process Supervisor server at a time.

The Process Supervisor UI is a client application which allows you to manipulate the running of processes via a connection to the server application Process Supervisor. You can stop a process, start a process, restart a process, stop all processes, start all processes, remove a process and change the set memory usage value for a process.

Opening the Process Supervisor Application

To start the Process Supervisor, type the path and file name on the command line (found in the **Run** item of the **Start** menu).

You can also double-click the Process Supervisor item within Windows Explorer, or select the Process Supervisor icon from the Windows **Start** menu (see Figure 5-1).

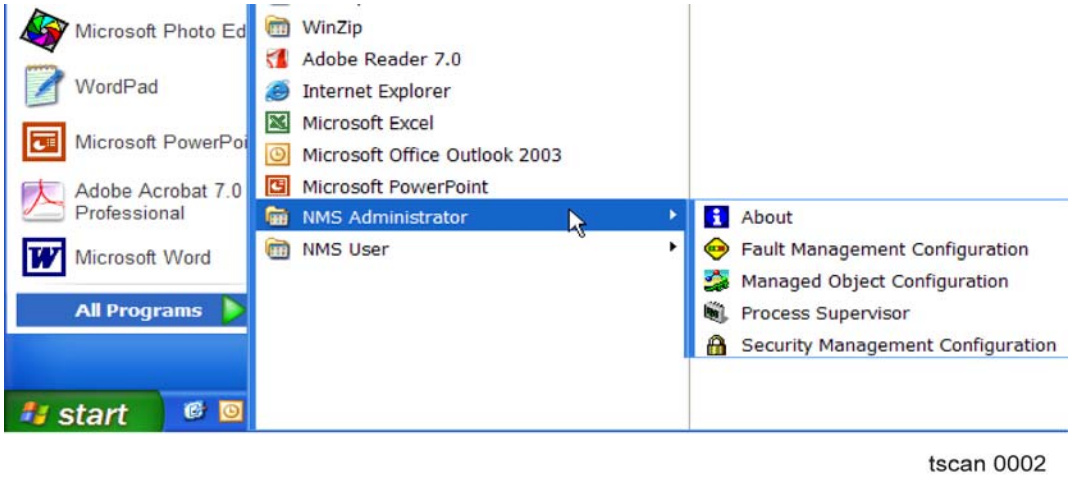


Figure 5-1. Windows Start Menu

Opening the Process Supervisor UI

To start the Process Supervisor UI, type its path on the command line, (found in the **Run** item on the **Start** menu). You must also supply the address of the Process Supervisor *server* application. The syntax for this is as follows:

Application path and name -sv Server Name

or

Application path and name -sv IP Address

For example, if the application needs to connect to Process Supervisor located on a server known as *embersoft1*, the command line instruction would read as follows

PSUI -sv embersoft1.

If no address is supplied, the local machine is checked for the Process Supervisor application.

Another (optional) flag can also be used within the command line. This loads non-English versions of the application. To do this, type in the name and server address, as shown above, followed by -nls and the name of the supplied translation file.

For example, to expand the example given above to include translation files, the translation file is called *language.nls*:

PSUI -sv embersoft1 -nls language.nls

On startup, the Process Supervisor UI first checks your level of user access with the related Security System. There are three levels of access possible shown in the following table:

Security Level	Access Rights
No Access	Unable to run the program.
Read Access	Able to run programme and scan process details, but not to send requests to the server.
Full Access	Able to run the program, scan process details, and send requests to the server.

Press **OK** to display the following window (Figure 5-2).

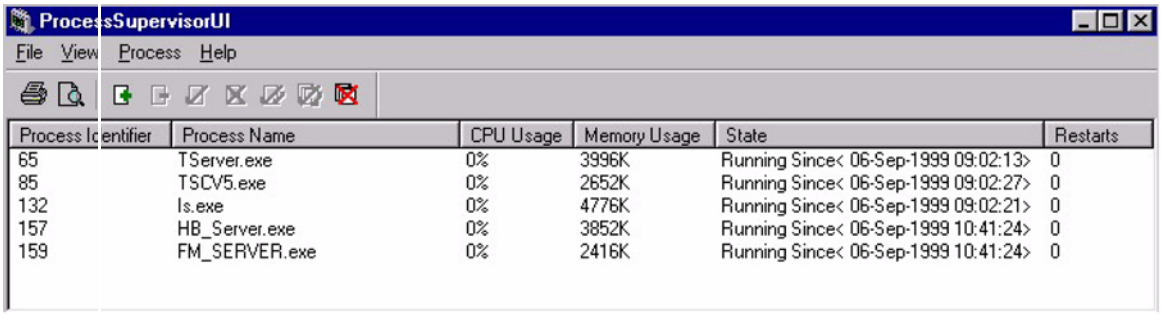


Figure 5-2. Process Supervisor UI Application Main Screen

If the server is supervising any processes at the time you started up the application, they are shown in the main window (see Figure 5-2). If no processes are currently being supervised, the window is empty.

Failure on Startup

If the server name or IP address you have defined cannot be found, a message box is displayed saying *Server Name Specified Not Found*. The program exits when **OK** is pressed.

If the Process Supervisor UI has failed to connect to the server, a message box is displayed saying: *Your Connection Has Been Unsuccessful*.

If another instance of the Process Supervisor UI is already connected to the Process Supervisor than a message box is shown saying: *Connection Unsuccessful: Client Already Exists*.

Security Manager and Security Key failure error messages are also shown.

The Process Supervisor UI Toolbar

Below are the tool bar item titles, with a reference to where further information can be found:

Start All Processes Tool 

This is discussed later. See Starting All of the Supervised Processes, on page 79.

Stop All Processes Tool 

This is discussed later. See Stopping All of the Supervised Processes, on page 80.

Restart Process Tool 

This is discussed later. See Restarting a Supervised Process, on page 79.

Start Selected Process Tool 

This is discussed later. See Starting a Supervised Process, on page 78.

Stop Selected Process Tool 

This is discussed later. See Stopping a Supervised Process, on page 78.

Remove Selected Process Tool 

This is discussed later. See Removing a Process from the Supervised List, on page 79.

Add Process Tool 

This is discussed later. See Adding a Process, on page 75.

Print Tool

This tool prints out a hardcopy version of the list of currently supervised processes.

Print Preview Tool

This tool displays on screen the appearance of a printout.

The Process Record

Each process record contains the following information about a process:

Process ID

This is a unique number allocated by the operating system to each process.

Process Name

The name of the process entered by you in the **Add Process** dialog box (see Figure 5-3).

CPU Usage

A percentage of the totally available processing power that is currently being used by the process.

Memory Usage

The average amount of physical memory used by the process. It is an averaged out from the time the process was last started until the present time. Therefore the longer a process has been running, the more accurate this value is. Expressed in kilobytes.

State

This shows whether the process is currently running and if so, when it was started. If the process is currently stopped, it shows when it was terminated.

Restarts

This shows the total number of restarts made by this programme, either since it was registered by the Process Supervisor or since the Restart value was last set to zero.

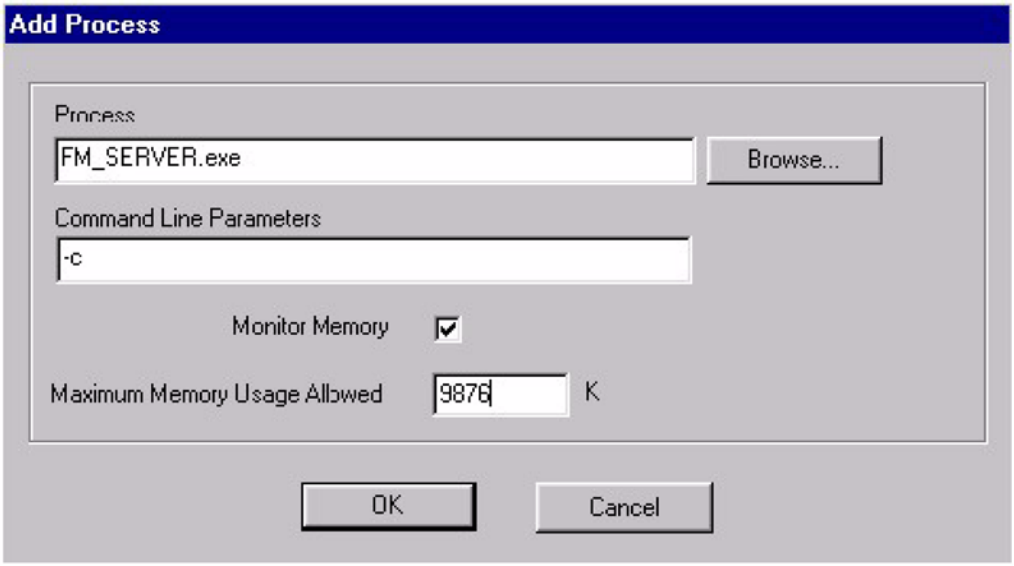


Figure 5-3. Add Process dialog

Sorting Process Records

The process records can be sorted by any column (alphabetically A-Z or numerically in ascending order) by clicking in the column header (where the column title is).

Adding a Process

Either select the **Add Process** item from the **Process** menu or click on the **Add Process** icon in the toolbar. The Add Process dialog (Figure 5-3) is displayed.

Fill in either the name or address of the process in the top text box. If the full path is not known, you can press the **Browse** button and find the file using standard **Open File** box. Use this to find the process you wish to monitor. The name of the selected process is automatically written to the edit box once you have pressed the **Open** button.

If the selected process has any required parameters, these can be inserted within the **Command Line Parameters** box.

Setting the Set Memory Usage Limit when Adding a Process

To set a limit for the amount of memory the process can use, click in the **Monitor Memory** tick box. You cannot insert a value, in kilobytes, in the **Maximum Memory Usage Allowed** box.

Clicking again in the **Monitor Memory** tick box removes the tick and stop memory use being monitored.

Any non-numeric entries within the **Maximum Memory Usage Allowed** box also prevents the memory use of the process being monitored.

Any values set now can be changed once the Process Supervision has been set up (See Changing the Properties of a Process, on page 77).

Press **OK**. If it is started successfully, the process details are entered in the Process Supervisor UI screen.

If the attempt to monitor the process is unsuccessful, the process details are not added to the main screen and a message box appears informing you of this. Common reasons for failure are that a process with the same name and parameters is already being supervised, or the server has failed to start the process.

If it was successful, an entry is inserted in the PSFiles .ini file for the process. This details its name, parameters, set memory usage value and restart value. This is updated as necessary. An example of this is shown in Figure 5-4.

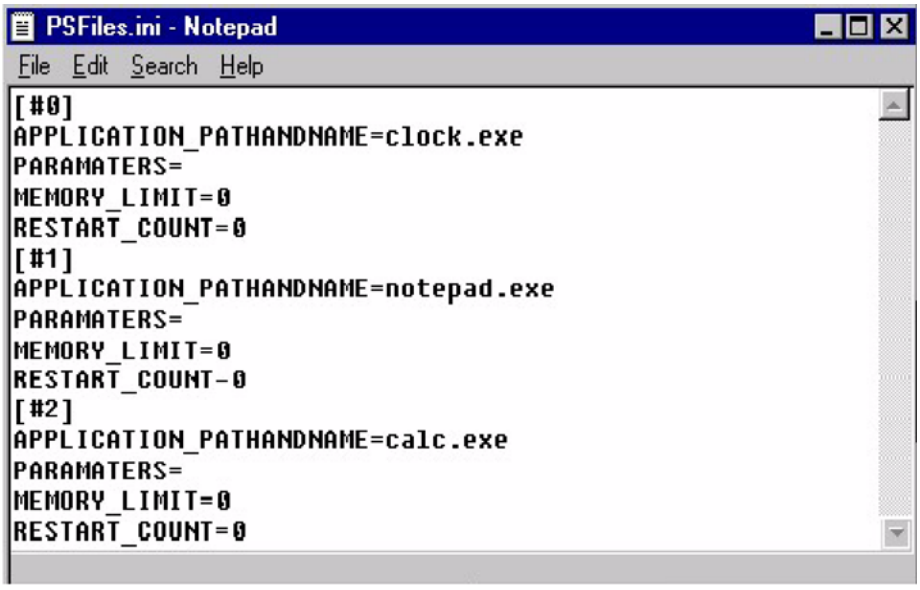


Figure 5-4. PSFiles.ini Editing Window

Changing the Properties of a Process

Once a process has entered supervision, various values can be reset. Either double click on the process whose values you wish to change, or highlight it by single clicking on it and then select **Process Properties** from the **Process** Menu. The *Process Properties* dialog (Figure 5-5) is displayed, showing the current set of values for this process.

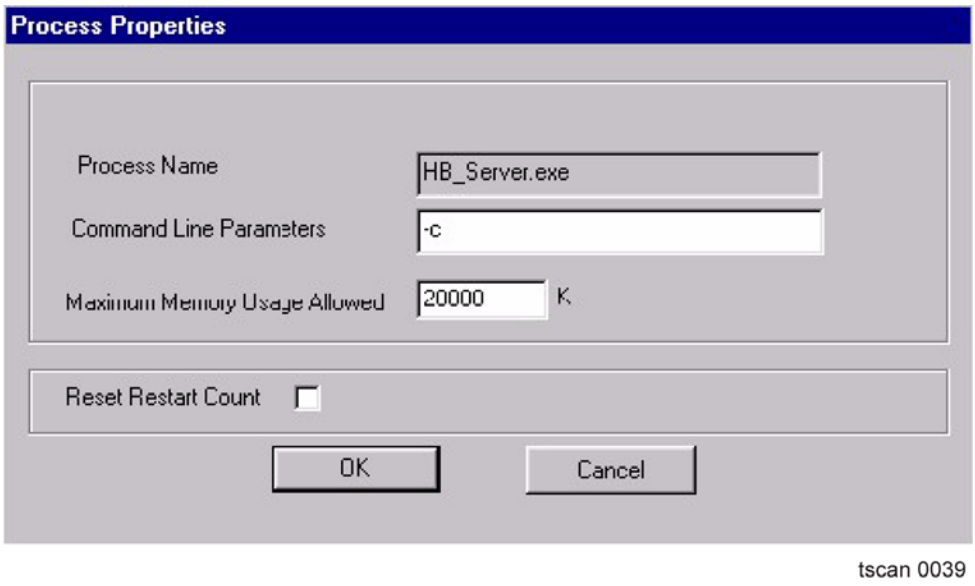


Figure 5-5. Process Properties dialog Box

Changing the Set Memory Usage Value of a Process

The value in the **Memory Usage** box can be either set to zero or changed.

Resetting the Restart Count

The value in the *Restart Count* column can be reset to zero by clicking the **Reset Restart Count** box.

If you do not wish to keep the changes that you have made in the this box, press **Cancel**. Otherwise click the **OK** button.

A **Confirmation of Changes** dialog box (Figure 5-6) is displayed.

Figure 5-6. Confirmation of Changes dialog Box

There are three options available to you:

- **Store Changes:** This stores the changes made in the Process Supervisor ini.files and show them in both the UI and server applications. The new details are shown in this session and retained for future sessions. Tick the box and click the **OK** button to choose this option.
- **Store Changes/Restart Process:** This stores the options as discussed previously. It also restarts the process. Tick the box and click the **OK** button to choose this option.
- **Cancel Changes**. Press the **Cancel** button to discard any changes that you have made in the **Process Properties** box.

Stopping a Supervised Process

Select the process that you wish to stop by clicking on it within the main Process Supervisor UI window. Then either choose the **Stop Selected Process** item from the **Process** menu, or click on the **Stop Supervised Process** icon in the toolbar.

A message appears asking you to confirm that you wish to stop the process. Once you have pressed **OK**, the chosen process is killed and the *State* column shows the time that the process was stopped.

Starting a Supervised Process

First select the process you wish to start by clicking on it within the list box. Then choose the **Start Selected Process** item from the **Process** menu or click on the **Start Selected Process** icon in the toolbar.

A dialog appears asking you to confirm that you wish to start the process. Once you have pressed **OK**, the chosen process is launched.

The *State* column of the Process Supervisor UI main window now shows that the process is running, and the time it was started.

Restarting a Supervised Process

Select the process you wish to re-start by clicking on it within the main Process Supervisor UI window. Then select the **Restart Selected Process** menu item from the **Process** menu, or click on the **Restart Process** icon  from the toolbar.

A dialog appears asking you to confirm that you wish to restart the process. Press **OK** and the chosen process is restarted. This option is only available if the process is already running. The *State* column shows the time at which the process was restarted.

Once the process has been started, the value in the *Restarts* column for the process is increased by one.

Removing a Process from the Supervised List

First select the process that you wish to stop monitoring in the main Process Supervisor UI window. Then choose the **Remove Process** item from the **Process** menu or click on the **Remove Process** icon  in the toolbar. A message box asking you to confirm that you wish to remove the process is displayed.

If the process is currently running, you are also asked whether you wish to leave it running after removing it from supervision.

Click **OK** to remove the process, or **Cancel** to retain it. Once a process is removed, it no longer appears in the Process Supervisor UI window.

Starting All of the Supervised Processes

To do this, either select the **Process** menu at the top of the Process Supervisor UI and then choose the **Start All Processes** item *or* click on the **Start All Supervised Processes** toolbar button  .

A message box appears asking you to confirm that you wish to start all of the processes. To continue, press **OK**, otherwise press **Cancel**.

All processes currently stopped are started. Any running processes are restarted. The *State* Column of the Process Supervisor UI list box now shows the time at which the processes were started/restarted.

The restart count of all the processes is increased by one.

Stopping All of the Supervised Processes

To do this, select the **Stop All Processes** item from the **Process** menu *or* click on the **Stop All Processes** toolbar button  .

A message box appears asking you to verify that you wish to stop all of the processes. To continue press **OK**. All processes that are running are now stopped. The *State* Column of the Process Supervisor UI main window now shows the process stop time.

Shutting Down the Process Supervisor UI

The Process Supervisor UI can be closed either by selecting the **Exit** option from the **Window Menu** *or* by clicking on the X in the right hand corner of the main window.

Print Previewing the Contents of the Process Supervisor Main Window

To print preview the contents of the Process Supervisor UI main window, either select the **Print Preview** item from the **Window** menu or the **Print Preview** icon  from the toolbar. A print preview window is displayed, enabling you to see how the contents of the window would look if printed out. Press **Close** to return to the Process Supervisor UI window.

Printing a List of Supervised Processes

To print the contents of the Process Supervisor UI main window, either select the **Print** item from the **Window** menu or the Print icon  from the toolbar. A standard **Print Setup** dialog box is displayed. Here you can set the number of copies, select a printer from those available, and change the page settings. When you have made your selections, press **OK** to continue printing.

Constructing and Adding to the PSFile.ini

Warning: This action is not recommended unless it is absolutely essential, as making incorrect modifications to your system files could have unpredictable results.

You should not need to alter the .ini file because adding a process enters an entry to it and removing a process deletes an entry from it. However, if you do choose to do this, it is vital to remember the following points:

- Do not leave spaces within the section names of the entries or between the section headings and set values.
- Include a # before the next entry number if adding an entry to the file manually.

Important: Always keep the numbers in order if you have to do this.

- Note that any duplicate entries within the .ini file are ignored.

Note: Refer to Figure 5-4 for an example of a PSFile.ini editing window.

Frequently Asked Questions

1. Q What has happened when I get the error message *'Error ini file Constructed Incorrectly'*?

   A The Process Supervisor has had a problem with reading the PSFiles.ini. The file may have been amended manually and there can be headings missing or spaces included. Both of these problems stop the Process Supervisor from reading the file properly.

   The solutions is to exit the Process Supervisor applications and amend the .ini file so that:

– There are no spaces in any of the section names
– The numbers all follow on from each other with a hash in front
– There are no spaces between the = signs of the heading names

When you've done this, the Process Supervisor is able to read the PSFiles.ini file.

2. Q Why did nothing happen when I requested an action on a process?

   A The socket used to send to the Process Supervisor UI is also used for sending new data to the screen. A result of this is that, occasionally, messages can collide and not reach the Process Supervisor. Simply repeat the request for an action.

3. Q Why did the Process Supervisor not add the process I requested?

   A A process is not added under the following circumstances:

– It is already being supervised
– Process Supervisor fails to start the process. Repeat the request to start the process.
– The process cannot be found at the location you have specified. Recheck the location in the Add Process dialog box.

Check each of the previously listed points. If the process still does not get added, there may have been a collision between messages within the socket, so try resending the request.

Chapter 6 Database Administration

This chapter contains basic information about possible maintenance schedules, checking the status of your database and archiving records. If you need to use the chapter as a quick reference guide, there is a keyword index at the end.

In this chapter:

Overview

This chapter gives advice on the basic procedures needed to keep your System working efficiently and securely. The two main steps that we shall examine are the archiving and purging of records from the database.

In addition to the information contained here, you may need access to the set of help manuals that were provided with your database system.

Why Would I Need to Backup the Database?

It is common practice to backup a database. Not only can hardware/software failure cause data to be lost, but data can be accidentally deleted, wrongly added or corrupted. When you make an organized backup up plan, you are guarding against loss of data, and ensuring that in the event of a major machine disaster to both your database and network you can quickly reconfigure all your elements in a combination that you know has been stable in the past. You are also able to delete records from the active database to keep it working efficiently.

Maintenance Schedule

The TimeScan system collects notifications from various MEs (e.g. DCDs), inserts them into a database and allows you to view the information contained in them in various ways. Over a relatively short period of time, the normal use of this system generates many records in the database. A regular maintenance schedule ensures the continued high performance of your system. Table 6-1 and Table 6-2 outline a possible maintenance plan, but there are also other times at which you should backup your system, shown in the “Non-Routine Backup of Archives” section.

Table 6-1. Weekly Schedule (Full)

Action	Type	User
Backup database	Full	Administrator

Table 6-2. Monthly Schedule

Action	Type	User
Archive Log records	Delete Log records, up to end of LAST month	Administrator

The suggested schedule outlined above may not be suitable for your system, because this depends on individual circumstances. The two main attributes to consider when planning a maintenance schedule are the **number of Managed Elements** (MEs) and the **number of notifications raised** by each ME. Even if there are only a few MEs, if they raise many alarms, you must perform housekeeping activities more frequently than if you have a larger, but less active, system.

As a very rough guideline, performance starts to deteriorate when the total database size is approximately 10 MB, or when there are approximately 10 000 alarm records. At this point you should definitely start removing records from the database. This should be done as soon as you have performed a backup.

To find how large your current database is, take the following steps:

1. Find your current Access database file (**.mde*).
2. Right click on it to open the popup menu.
3. Select the **Properties** item from the menu.

The file size is shown in the resulting information box. Use this information to decide if you need to remove some of the records in the database. If you do, see Removing Log Records, on page 86.

Non-Routine Backup of Archives

As well as backing up your system on a regular basis, there are other events which should prompt you to think about performing an additional backup.

- Changes have been made to the TimeScan system with the MOC program.

Organization of Archives

It is recommended that you give some thought to organisation of your archived data, and ensure that it meets at least the following criteria:

- The saved data sets are copied from the disk on which they are originally saved and stored elsewhere.
- The most recent complete archive from which a successful restore has been made are kept, until it is superseded.

Backing Up the Database

Backing up your database should be done regularly, and as part of a routine. The better planned your system of backing up, the more likely you are to survive a (computer) disaster without significant loss of data. Ideally, the media containing the backup information (disks or tapes) should be stored in a physically separate location to the current database.

Database Backup

To backup your Windows/Access database, perform the following steps:

1. Find the current database file (*rmdata.mde*), whose default location is *net-monitor/db/data* and right click on it.

2. A popup menu appears. Select the **Copy** item from this menu.

3. Move to the chosen backup location, and **Paste** the file into new position (from the right click menu.

4. Rename the file, preferably including the date of backup in the new title.

5. Now move this file to a different physical location to the active database.

6. Once you have performed a backup, you are ready to delete records from the database (see Removing Log Records, on page 86).

Removing Log Records

To maintain your database at a reasonable size (see Maintenance Schedule, on page 84 for sizing information), you must periodically remove some records from the active database and store them elsewhere. If you make backups, these can act as storage for cleared out records. If necessary you could recreate the database at a particular point in time from these backups. (The exactness with which you can recreate the file for a particular point in time depends on how often backups are performed on your system.)

For the TimeScan NMS database, you should archive *Log* (no longer active, usually cleared) records with an initial *Date* that is over three months old. (In the *alarmlog* table on the NMS/TimeScan database, these conditions are shown when the *eventtime* is over three months ago and the *activealarm* value is 0.) Outlined below is a simple method of doing this.

For both systems, it is recommended that you remove records immediately after making a complete backup. Then, if necessary, you can recover records from your backup.

To remove records from the database run the program *ArchiveAlarms*. This is part of the Information Server (IS) program.

Using Alarm Archive AA

Archive Alarms is run from the Windows command line.

Usage: AA [-name DBNAME] [-date dd-mm-yyyy] [-time hh-mm] [-a] [-d]

-name: Name of archive database (database must already exist). Default name = nmsarchive.

-date: Specifies the archive date (dd-mm-yyyy). If not specified, current date is used. If used with -a option, alarms before this date is archived from current database to archive database. If used with -d option, alarms before this date are deleted from current database.

-time: Specifies the archive time (hh-mm). If date is specified but time is not, time is 00-00. If time and date are not specified, current date and current time are used.

-a: Archives alarms from current database to archive database.

-d: Deletes alarms from current database.

e.g. AA -date 18-01-2000 -time 23-00 -d -a

If a name ‘-name’ is not specified, the name of the archive database defaults to nmsarchive. If you wish the alarms to be archived to a database with a different name then add it after the -name command. You can not change the name of the current database, for instance the database from where the alarms are to be copied or deleted.

Decide the cutoff point for records in your database, for example, records which are over three months old. Type this date after the ‘-date’ command. The format for this is dd/mm/yyyy. For example, the 31st of January 2006 would be typed 31/01/2006. If you have a specific time cutoff point add this to the command line after the ‘-time’ command. The format for this is hh-mm. If time and date are not specified, current date and current time are used.

Decide whether you want the alarms archived ‘-a’, copied from the current database to the archive database, or deleted ‘-d’, removed from current database, or both ‘-a -d’ archived and deleted.

Note: This program can take some time to execute, but it can be run as a background task, and does not prevent other database usage.

If you enter an invalid date, time, or command, the AA displays an error and terminates. If successful, the number of alarms are displayed as they are being archived. Once the task is completed, AA displays the number of alarms (Alarms and Alarm acknowledgements) successfully archived and/or deleted.

Restoring Database Records from Previously Saved Sets

There are three main reasons why you might want to restore previously archived data. They are as follows:

- Some data has been lost, due to user or computer error.
- The complete database has been corrupted.
- You wish to view sets of previously archived data.

If the complete database has been lost, follow the instructions for Restore Database from Backup, on page 88).

If you wish to view sets of previously archived records, follow the instructions for Viewing Previously Archived Records, on page 88).

Restore Database from Backup

To restore the complete database from a backup, first find the backup you made following the instructions in the section Database Backup, on page 86. Double click on it to view it using Access. Once you have decided to make it your current (active) database, then simply rename it to "*rmdata.mde*", and move it to location of your current active database (default location: *net-monitor/db/data*). You can import records to it from the NMSArchive database, again using standard Access techniques.

Viewing Previously Archived Records

The records removed from the database using the *ArchiveAlarms* program (see Using Alarm Archive AA, on page 87) are put into a database called *NMSArchive*. Simply double click on this database to view it, then use standard Access filtering techniques to display the required dataset.

Notes for Administrators

Full SQL listing to add alarm log table to nmsarchive database.

```
CREATE TABLE alarmlog (

        recordid INTEGER,
        distinguishedname VARCHAR (50,0),
        eventtime DATETIME YEAR TO FRACTION(3),
        receptiontime DATETIME YEAR TO FRACTION (3),
        event SMALLINT,
        recordtype INTEGER,
        perceiviedseverity INTEGER,
        pstext VARCHAR (9,0),
        alarmid INTEGER,
        slogan VARCHAR (80,0),
        alarmnumber INTEGER,
        likelyorigin VARCHAR (50,0),
        sid VARCHAR (50,0),
        printouttext VARCHAR (255),
        cleartime DATETIME YEAR TO FRACTION (3),
        cleartype INTEGER,
        cleartext VARCHAR (255),
        acknowledge SMALLINT,
        acknowledgetime DATETIME YEAR TO FRACTION (3),
        activealarm SMALLINT,
        originalps INTEGER,
        originalpstext VARCHAR (9,0),
        audittime DATETIME YEAR TO FRACTION(3)
        )
```

Chapter 7 Fault Management Configuration

This chapter provides information on how to use the features of the Fault Management Configuration Application.

In this chapter:

Overview

The Fault Management Configuration application provides a flexible utility which enables alarms and events to be mapped to unique identities. In turn, notifications from given sources can have their perceived severities re-mapped.

What Do I Need to Run Fault Management Configuration?

You would need to have an appropriate information server to link to.

What's in This Chapter?

This chapter provides a description of available tools (see The Fault Management Configuration Toolbar, on page 94) and a step-by-step guide for using the application (see Managing Severity Mapping, on page 95).

Opening the Fault Management Configuration Application

The Fault Management Configuration application can be found in the **NMS Administrator** menu in the Window **Start** menu (Figure 7-1). On start-up, the system determines if you have the authority to access this facility. This decision is based on your user identification.

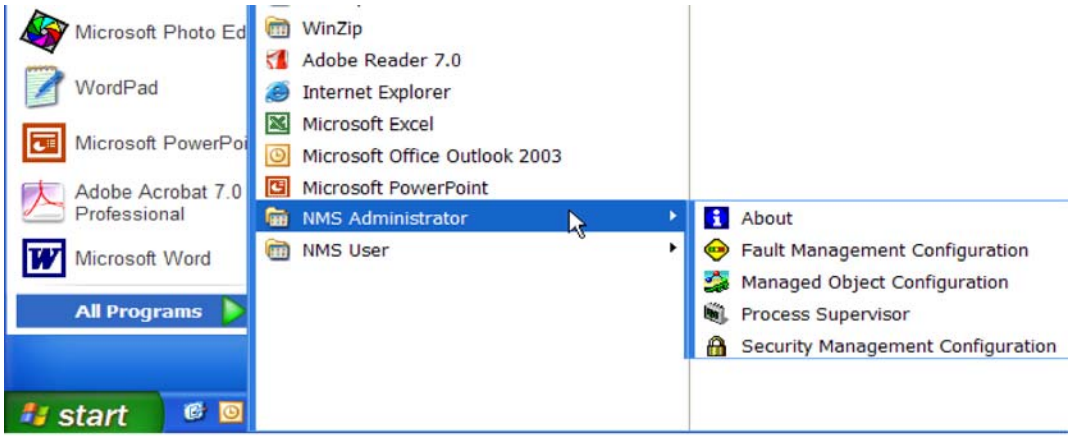


Figure 7-1. Windows Start Menu

If access is granted the Fault Management User Configuration window (Figure 7-2) is displayed.

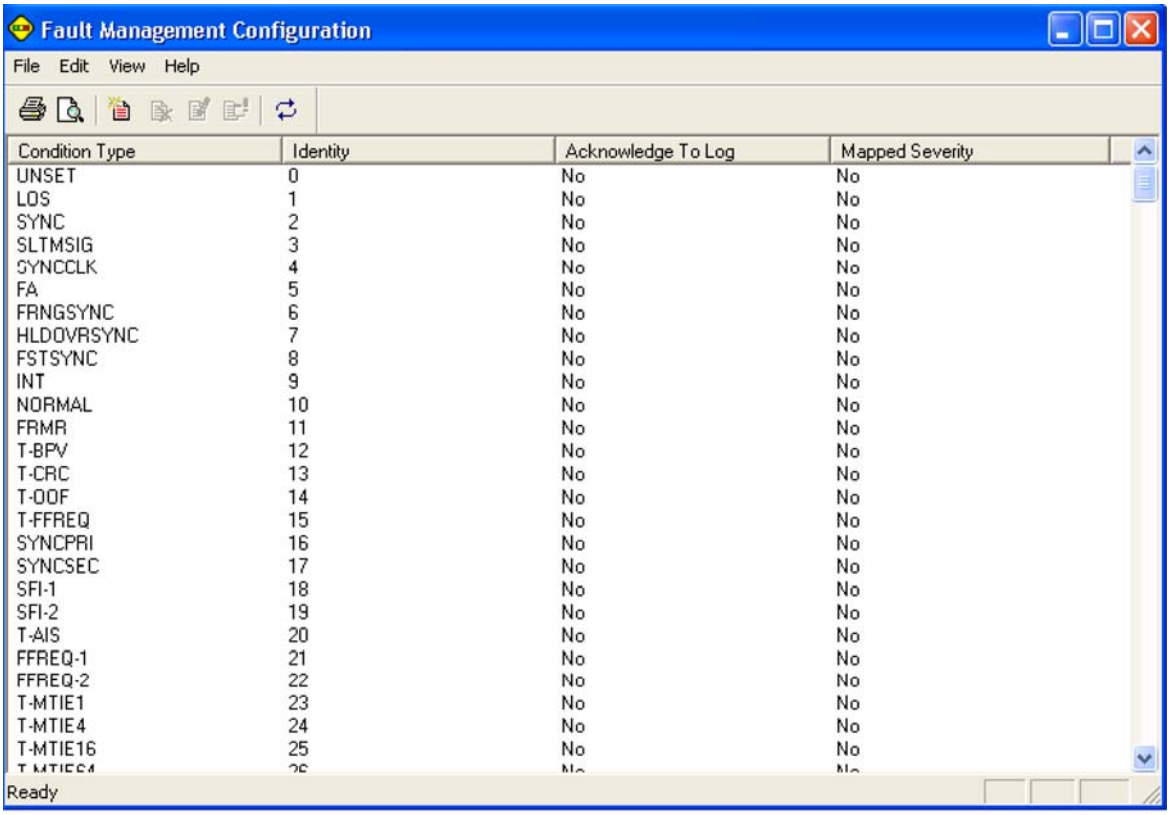


Figure 7-2. Fault Management Configuration User Window

This is the Fault Management Configuration user window. It is composed of four columns which illustrate the notification mapping data already defined in your system.

- The *Condition Type* field contains the condition types, as defined by the interface description of the managed elements. These codes are used as *keys* for the mapping process.
- The *Identity* field contains a numeric identifier which is unique for each mapping entry.
- The *Acknowledge To Log* field shows whether the mapped notification is a revertive or non-revertive condition. If the value is NO, alarms and events move to the log only when they are both *cleared* and *acknowledged*. If the value is YES, alarms and events move to the log only when they are *acknowledged*.
- The *Mapped Severity* field indicates if the perceived severity of this notification has been re-mapped to another severity.

The Fault Management Configuration Toolbar

On startup the Fault Management Configuration application has a toolbar, just above the view illustration, containing seven tools.

This toolbar is dockable so if you are not happy with its position you can pick it up with the mouse and position it where you want around the view. If you drop it outside the window, or place it in the centre, it transforms to a *fly-off* window:

Print Tool

Selection of the **Print** tool causes a hard copy report of the current fault management configuration to be generated.

Print Setup Tool

Selection of the **Print Setup** tool allows you to control the hard copy report generation.

New Alarm Tool

The **New Alarm** tool allows you to create a new mapping entry. This feature is discussed further in the next section.

Delete Alarm Entry Tool

This tool becomes active when a list entry is selected. Selection of this tool removes the selected mapping from the system.

Edit Alarm Entry Tool

This tool becomes active when a list entry is selected. Selection of this tool enables you to edit the selected mapping.

Map Alarm Severities Tool

This tool becomes active when a list entry is selected. Selection of this tool allows you to edit the perceived severity re-mapping of the selected entry.

Refresh List Tool

Selection of the **Refresh** Tool causes the contents of the alarm re-mapping list in the main window to be refreshed from the Fault MIB (Management Information Database) tables.

Managing Severity Mapping

The following section discusses both **adding** and **editing** severity mappings, as these are very similar operations.

To **add** an alarm or event mappings, select the **New Alarm** tool. The following dialog (Figure 7-3) is provided for you to input the required information. To edit an alarm or event, select the **Edit Alarm Entry** tool. A similar dialog is provided, which allows the available fields to be edited.

Figure 7-3. Add Alarm Mapping dialog

For a new mapping, the *Notification Code* must be entered exactly as it is specified in the interface description of the alarm or event. The *Identity* is a mandatory numeric identifier, which is automatically generated by the application. Both the *Notification Code* and *Identity* must be unique to the system. An attempt to enter a non unique value results in a warning message.

If the mapped notification is revertive, for instance has an associated clearing, the **Cleared Event** check box must be checked. To set-up a re-mapping for the perceived severity for the alarm or event, select the **Map** button. The Empty Severity Mapping dialog (Figure 7-4) is provided.

Figure 7-4. Empty Severity Mapping dialog

Multiple perceived severity re-mappings are supported from different source elements and likely origins. All are listed in this dialog.

As this is new mapping, no entries exist as yet. Selecting the **Add** button causes the Add Severity Mapping dialog (Figure 7-5) to appear.

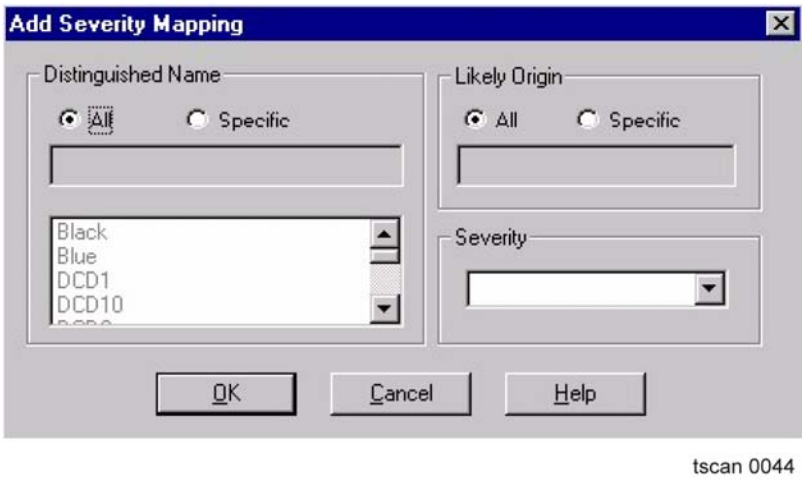


Figure 7-5. Add Severity Mapping dialog

The **Distinguished Name** panel enables you to define the source for the perceived severity re-mapping. With **All** selected, any notification carrying the matching notification code from any source element is re-mapped. If the re-mapping is to be specific to a single element, by selecting the **Specific** control the desired source element can be selected from the list box.

The **Likely Origin** panel enables you to define the origin within the selected sources for the perceived severity re-mapping. With **All** selected, any notification carrying the matching notification code from any likely origin is re-mapped. If the re-mapping is to be specific to a single origin, by selecting the **Specific** control the desired origin can be defined in the edit box.

Finally the **Severity** panel provides a list box containing the mapped perceived severity, Critical, Major, Minor, or Warning.

On selecting the **OK** button, the newly created entry appears in the Severity Mapping dialog list.

NOTE: For conflicting mapping entries the highest perceived severity is taken.

Deleting an Existing Notification Mapping

With a notification entry selected, press the **Delete Alarm Entry** tool. A confirmation dialog is provided. On confirmation, the entry is deleted from the system. Great care must be exercised when deleting mappings as there is no undo facility.

Chapter 8 Terminal Application

This chapter contains all the information you need to know to exploit the features of Terminal. If you need to use the chapter as a quick reference guide, there is a keyword index at the end of this document.

In this chapter:

Overview

Terminal is a versatile application. It is capable of providing command access and event monitoring for any element type supporting an ASCII-based command protocol.

What Would I Need to Use the Terminal Application?

Terminal can only be run as part of the TimeScan suite of programmes.

Opening the Terminal Application

The TimeScan TL1Terminal Application can be accessed from the Network Browser as shown below in Figure 8-1. Right-click on the network element icon and in the popup window select **TL1Terminal**.

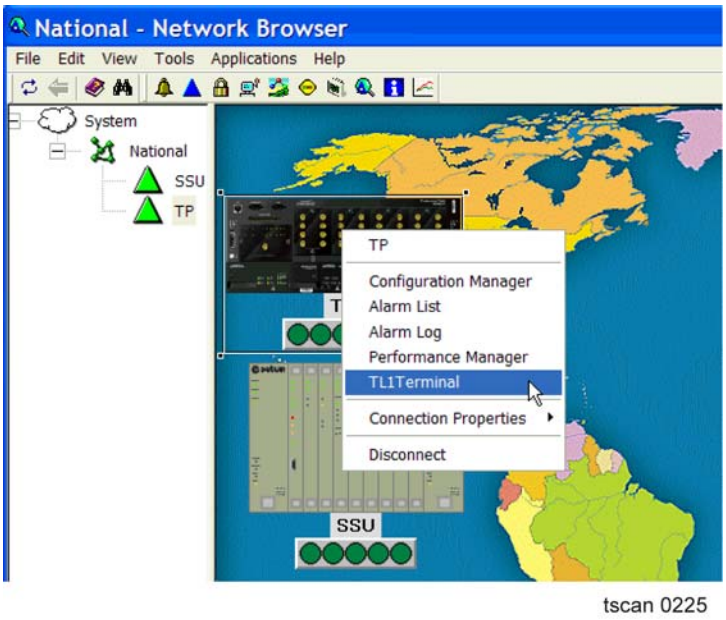
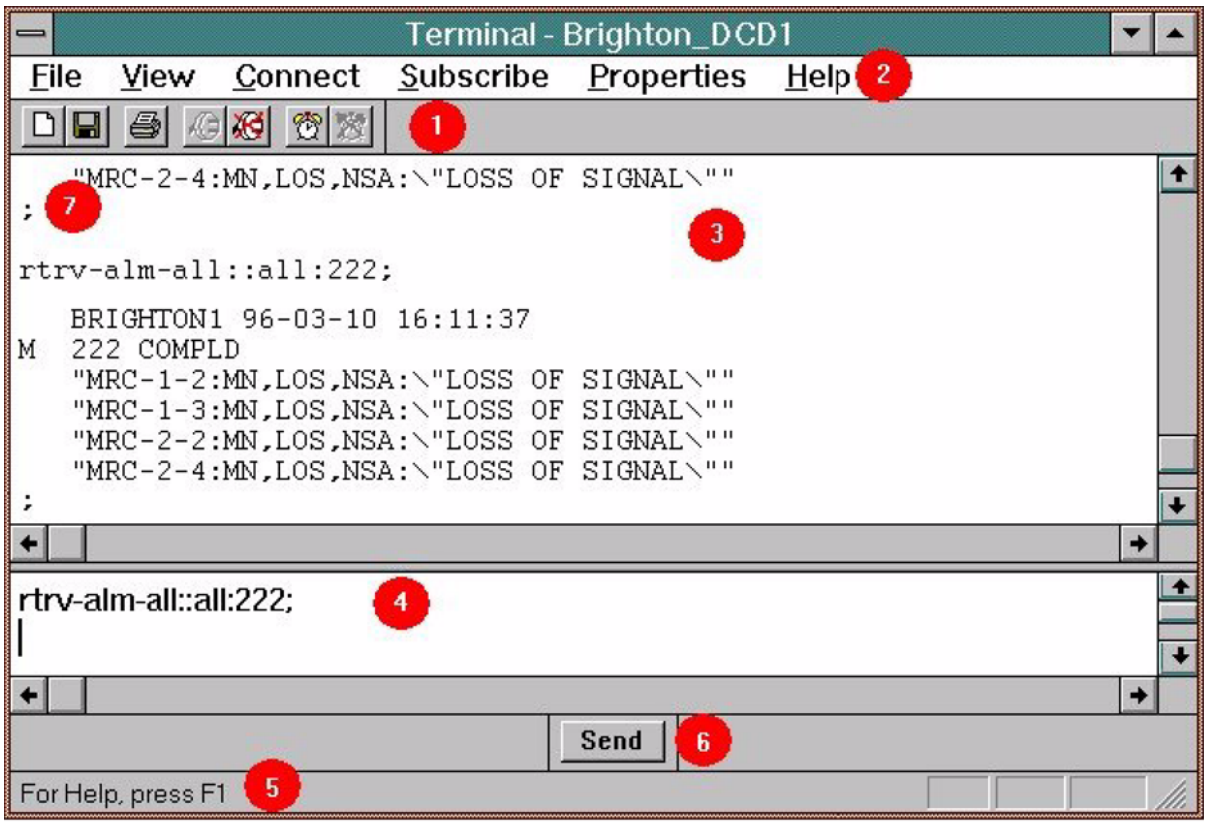


Figure 8-1. Windows Start Menu

A Quick Tour of the Terminal Window

A typical Terminal window is shown in Figure 8-2 and the window elements are listed below.



tscan 0045

Figure 8-2. Typical Terminal Window

1. Menu Bar
2. Tool Bar
3. Response Window
4. Command Window
5. Status Bar
6. Send Button
7. Managed Element Distinguished Name

The **Command Window** accepts input from the console. The **Response Window** displays all responses generated by the element.

Terminal Toolbar Items

Clear Response – This tool deletes the contents of the response window.

Save Response – This tool enables the user to save a snap shot of the response window to file.

Print Response – This tool enables the user to print a hardcopy of the current response buffer.

Connect to Element – This tool makes the request to establish a communication path to the target element.

Disconnect from Element – This tool makes the request to close an established a communication path with the target element.

Subscribe to Alarms – This tool makes the request to establish a subscription on alarms and events sent by the target element.

Un-subscribe to Alarms – This tool makes the request to terminate an alarm subscription on the target element.

Communicating with an Element via Terminal

When the Terminal Application is started from a Network Browser, the Terminal Application automatically gives the distinguished name of the element to communicate with, and any options appropriate to that element type.

If an attempt is made to start a Terminal while there is already a Terminal active towards the same target element on the same work station, the dialog in Figure 8-3 is shown.

Figure 8-3. Communications Failure dialog

Selecting **Show Existing Terminal** button restores the original Terminal if iconized and brings that Terminal window to the front. Selecting the **Open New Terminal** button starts another Terminal window.

On start up, the command and response windows are both blank. To send a command to the element a communication session must first be established. This can be achieved by selecting the **Connect** option from the **Connect** menu, or by selecting the **Connect** tool from the tool bar (see Terminal Toolbar Items, on page 102). To establish a communication session, the platform automatically invokes the correct transport method appropriate to an element, for example: *X.25*, *RS232*, etc. It also performs a user login operation appropriate to the element type, with any access passwords automatically derived.

When a connection is established the message

Connected to Managed Element Distinguished Name

appears in the Response Window. Clicking the mouse in the command window causes an edit cursor to appear. Type a command at the flashing cursor.

It should be noted that commands are not transported to the managed element until the **Send** button is pressed. Therefore, protocols with character echo do not echo key strokes. Rather, the entire command string is echoed once the command has been sent. For protocols that do not support dynamic command line editing, this facility enables you to correct typing errors using backspace etc.

On completion of the command string, press the **Send** button, or **Return** key. The command string is sent to the element. Since only one command can be sent at a time, Terminal disables any further command transmission until a response is received or the response timeout period elapses, (see Terminal Properties, on page 105).

All command response text returned from the element is displayed in the Response Window. To enable the viewing of large response printouts, the Terminal window can be resized. The proportions of the command and response regions can be altered by selecting the dividing bar and dragging in the desired direction.

For protocols that do not support command echo, this feature can be emulated by Terminal. With the **Echo Command** item selected from within the properties window (Figure 8-4), the contents of the command line are automatically echoed to the Response Window.

It is possible to re-transmit a command to the element by placing the cursor on the same line as the command in the command window and pressing the **Send** button or **Return** key. It is also possible to cut strings from either the command or response windows and paste them into the command window as new commands.

Once a command sequence has been completed you can close the communication session to the element by selecting the **Disconnect** option from the **Connect** menu or by selecting the **Disconnect** tool from the toolbar (see Terminal Toolbar Items, on page 102). This action results in a user logout operation appropriate to the element type. If Terminal is left idle with an active communication session then the session is automatically closed after an idle timeout period.

It should be noted that an active communication session blocks other communication sessions to the same distinguished name and hence, prevents command contention.

Using Terminal to Collect Alarm Messages

The Terminal Application can be used to collect and display alarm and event messages from a managed element. To collect alarm messages, an *alarm subscription* must first be established. This can be achieved by selecting the **Subscribe** option under the **Subscribe** menu or by selecting the **Subscription** tool from the tool bar.

When a subscription is established the message:

```
Started subscription to Distinguished Name
```

appears in the Response Window.

On setting up an alarm subscription, the TimeScan System automatically presents alarm messages from the managed element to the Terminal Application. The alarm text is displayed in real time in the response window with the following banner:

Report from Distinguished Name

An alarm subscription can be established at any time and is independent of the existence of a communication session. Alarm subscription does impede the alarm functionality of the TimeScan System.

Terminal Properties

The Terminal Application Properties window is shown in Figure 8-4.

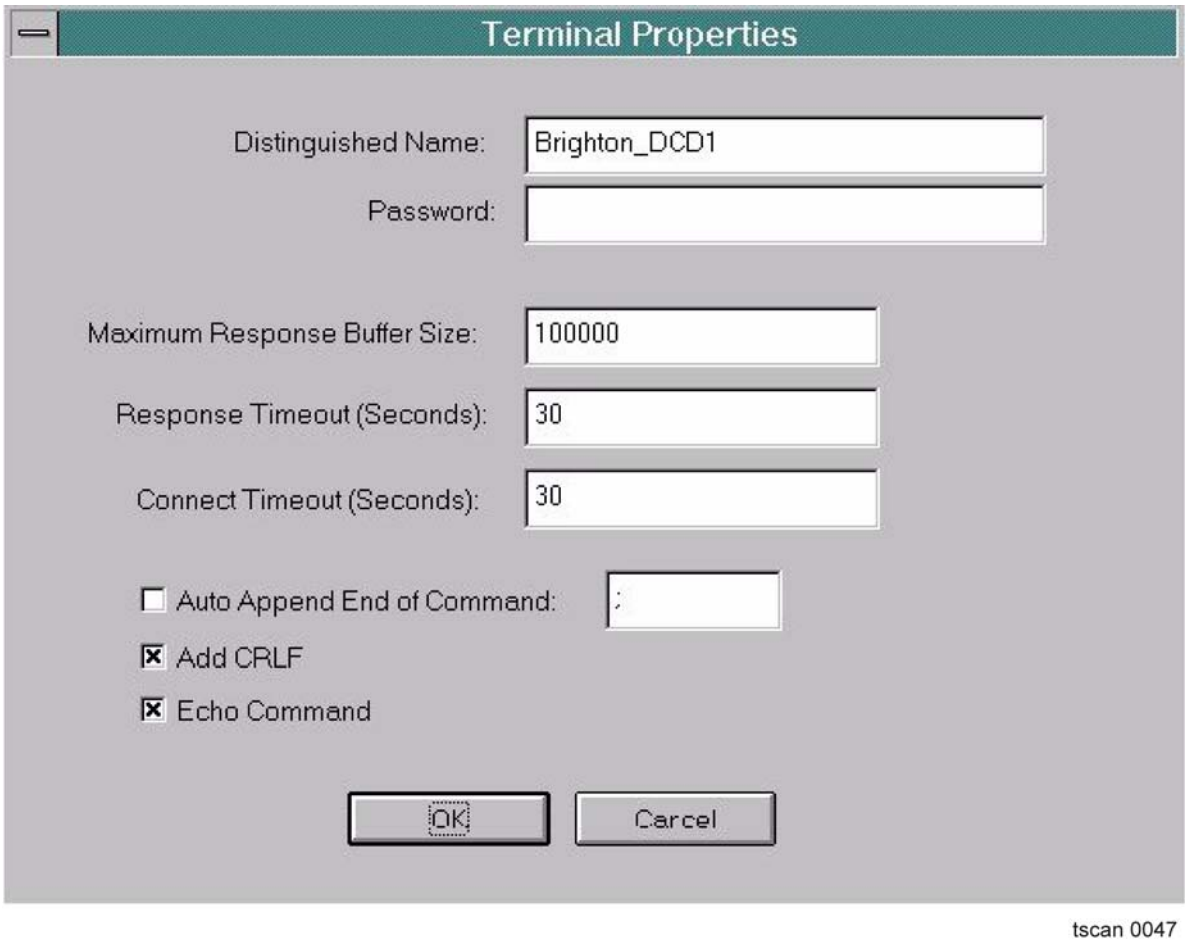


Figure 8-4. Terminal Application Properties Window

The Terminal Application Properties Window provides access to many configurable parameters:

The first field, **Distinguished Name**, specifies the unique identifier of the target element. The field can be edited in order to provide access to another element.

A **Password** field has been made available so that it is possible force the communication system to use an alternative password to that defined in the TimeScan database.

Maximum Response Buffer Size defines the maximum size of the response buffer.

The **Response Timeout** field defines how many seconds the Terminal Application should allow before a command is considered to have failed due to timeout.

The **Connect Timeout** field defines how many seconds the Terminal Application should allow before an attempt to establish a communication with the target element is considered to have failed due to timeout.

The **Auto Append End of Command** field enables the user to define a character that should be automatically appended to the end of a command buffer if not appended by the user. This facility is particularly useful with the TL1 protocol which relies on a terminating semi-colon character. If a semi-colon is defined in this field, it is added to the end of all commands unless it is already present.

Add CRLF automatically appends a carriage return/line feed character pair to the end of every command.

Echo Command automatically inserts the command into the response buffer. This makes the Response Window easier to read and understand.

Notes for Administrators

Location

The correct path and file name of the Terminal Application is as follows:

C:\Program Files\nms\bin\Terminal.exe

Command Line Options

-nc	Suppress appending carriage return, line feed pair to command strings. (Default: append CRLF).
-a "string"	Automatically append *string* to end of all commands if omitted by user. Note *string* can be single character. (Default: no auto append).
-p "password"	Use *password* to establish communication session. (Default: use TimeScan NMS database password).
DistinguishedName	Distinguished name of managed element. (Default: None - use name provided in Properties dialog box.).

Chapter 9 Troubleshooting

The Troubleshooting chapter provides information on Work-arounds for commonly appearing system-wide faults. Faults for specific applications can be found in the relevant User Guides.

In this chapter:

Overview

When trying to sort out a problem, if the solutions are numbered sequentially, as in Q1, then perform the actions outlined in the order given. If the solutions are lettered, as in Q5, choose from between them.

Frequently Asked Questions

1. Q Why can't I communicate to a DCD using X.25?

   A1 If using a permanent connection, first stop NMS Services. Then use XPAD and Windows Terminal (in Accessories Program group) to try to communicate to the remote element. If this is successful (a TL1 command was sent and the correct response was received) the NMS Services should be restarted. If this fails restart the Eicon X.25 card, using commands "eccard stop" and "eccard start". In a "command prompt" the last message from "eccard start" should be "network connect established". If it returns an error, check connection to the packet switch. If XPAD cannot connect to the DCD, the fault is most likely in the X.25 network or the far end. Contact your network administrator for further help.

   A2 If communication is still not established, verify that the communication (X.121) address for the specific DCD is correct.

   A3 If communication is still not established, run the Terminal application from the TimeScan NMS Administrator menu and try to connect to the ME. The resulting error message report should indicate the fault condition.

2. Q Why can't I communicate to a DCD using a modem?

   A1 Use Windows Terminal to try to communicate to remote element. If Terminal cannot connect to the modem, consult the modem installation guide. If you can successfully dial the number but do not connect, verify that the phone number is correct and the DCD end modem is set up correctly.

   A2 If communications still do not work, verify that the communication address (phone number) for the specific DCD is correct.

   A3 If communication is still not established, run the Terminal application from the TimeScan NMS Administrator menu and try to connect to the ME. The resulting error message report should indicate the fault condition.

3. Q Why can't I communicate to a DCD using RS-232?

A1 If using a permanent connection, first stop NMS Services. Then use Windows Terminal to try to communicate with the remote element. If Terminal fails to connect you should check your cabling to the DCD.

A2 If communication is still not established, verify that the communications port (com port e.g. “COM1”) address for the specific DCD is correct.

A3 If communication is still not established, run the Terminal application from the TimeScan NMS Administrator menu and try to connect to the ME. The resulting error message report should indicate the fault condition.

4. Q Why can’t I connect to the DCD using the IP address?

A1 If using a permanent connection, first stop NMS Services. Then, using Telnet, verify that you are able to communicate with the distant device.

A2 Ensure that the IP address is not already in use.

A3 Ensure that the correct port has been correctly specified.

A4 Ensure the Terminal Server is set up correctly.

A5 If communication is still not established, run the Terminal application from the TimeScan NMS Administrator menu and try to connect to the ME. The resulting error message report should indicate the fault condition.

5. Q Programs do not start correctly. Either database corruption or ‘no data found’ errors are reported. Why?

A This error can be one of three causes:

– ODBC Sources. Check ODBC Sources are still present with the correct settings.
– Database corruption. See Repair/Compact Database, on page 112.
– Database corruption and failed repair. If repairing and compacting the database failed, the database should be rolled back to a previous state. See Rollback to Previous Database, on page 112.

6. Q My disk appears to be full of TimeScan NMS files. Why?

A The two parts of the TimeScan NMS system grow over a period of time are the temporary files and the database files. Restarting your machine can clear some temporary files. See Repair/Compact Database, on page 112.

7. Q A disk crash or other major hardware failure has occurred and the system installation has been corrupted. How do I recover?

A If the system is too badly damaged for database repair/rollback, the system may need to be reinstalled from the original CD and the database can be rolled back. See Reinstallation, on page 111.

8. Q How do I recover from a system “lock up” after using all virtual memory?

   A Restart the machine. See Restarting Machine, on page 111.

9. Q Why are alarms reported on the wrong ME?

   A It is possible to configure to ME with the same primary communications address. If this occurs, alarms reported on one DCD can appear on another DCD with the same address. This can apply across transport types, i.e., if, for a given ME, both a permanent connection and modem receiver have been set up to use COM1. The Database Administration form can be used to see if this is your problem.

10. Q Why are alarms reported to an “UNKNOWN” distinguished name?

    A The source of an alarm can be determined in a number of ways:

    – A connection (permanent or transitory) is made to the ME. All alarms on this channel are associated with the connected ME.
    – The communications source address is used and compared to the FM address (works with X.25).
    – The alarm SID is used to match the SID defined in CM database (modems).

If all of the above fail, the alarm is raised against an “UNKNOWN” distinguished name. This is most common with modems, and the cause is normally that the SID has not been configured in the CM database. Use MOC to set the SID correctly.

11. Q Why did I receive the message “The desired vendor daemon is down”?

    A FLEXlm License Manager is unable to start due to no or invalid license file.

    – Ensure a valid license file (license.lic) is located in the directory C:\Program Files\nms\license.

    A FLEXlm License Manager is started but Vendor daemon MONITOR.exe is not started.

    – Ensure that your computer is properly connected to the network
    – Restart the FLEXlm License Manager service and ensure that MONITOR.exe is running (Processes in the task manager).

12. Q Why did I receive the message “Component comdlg32.ocx or one of its dependancies not correctly registered: a file is missing” when running

Performance Manager on a Vista system?

A The comdlg32.ocx file is a visual basic runtime file that does not come by default with Vista and must be manually registered by the user as follows:

– Copy comdlg32.ocx (from instllation CD / any other vista machine) into System directory (C:\Windows\System32).

– Click Start->Command Prompt->Right Click->Run As Administrator.

– cd to C:\Windows\System32.

– Type the command `regsvr32 comdlg32.ocx` and press **Enter**.

Repair Actions

The following are a list of repair actions available for the *TimeScan NMS Platform*. The previous section, “Frequently Asked Questions”, has referred to these actions.

Reinstallation

Reinstallation is not a trivial task. A good knowledge of your operating system and the *TimeScan NMS* system are required. If you are uncertain you should not continue!

An installation guide is distributed with each system. This should be consulted before the installation. Before this installation takes place the old system should be removed, if possible using the following actions:

- Using the *Add/Remove* program application from the control panel to remove the TimeScan NMS system.
- Use the **Remove Access Run Time** item to remove all ODBC sources.
- Run the following command “C:\net-monitor\bin\supervisorservice -remove”
- Delete the “C:\net-monitor” directory

Some of these actions can fail depending on how much of the system remains on your hard disk. Once completed, installation can continue as specified in the installation guide. After a successful installation follow Rollback to Previous Database, on page 112.

Restarting Machine

Some applications with unsaved data require you to save or discard the data before you can restart the system.

If, after a period of 5 minutes after requesting shutdown, you still have a blank screen, the hardware **Reset** button on the computer can be used.

Restart “Supervisor Service”

After restarting your computer, the *NMS Services* facility is automatically restarted. You can check that it is running by looking at your Task Manager.

Rollback to Previous Database

During routine maintenance operations the database files are backed up. See the Operational Management chapter for more advice on this. If the database is damaged too badly for repair, these files can be used to recover the database

For more information on Restoring your database files, see both the Operational Management chapter, and your own proprietary database help.

Repair/Compact Database

An tool is provided in the *TimeScan NMS Administrator* program group to repair and compact the database file. All programs must be shutdown, including stopping the *NMS Services* application, then the “Compact Database” programs should be run. A pop-up verifying that the Database was repaired successfully is displayed on completion.

Chapter 10 SNMP

This chapter contains the information you need to install and configure the SNMP agent service.

In this chapter:

Overview

The SNMP agent is an extension agent which allows alarms/events monitored by TimeScan to be sent to a superior Network Manager using SNMP Traps.

What Do I Need to Use the SNMP

You need a license form Symmetricom and to follow the installation procedure described in this chapter.

Installing SNMP

If you have not already done so, install TimeScan/NMS.

You must have a software license to run TimeScan SNMP. If you do not have a software license, contact your vendor.

TimeScan SNMP uses the NuDesign Multiprotocol Agent Service, which replaces the Microsoft SNMP Service. Check if the Microsoft SNMP Service is installed and disable it if so by following these steps:

1. Open the control panel. (For Windows 2000, click **Start**, point to **Settings**, and then click **Control Panel**. For Windows XP, click **Start** and then click **Control Panel**.)

2. Open the **Services** dialog from the control panel by double clicking on **Administrative Tools** and then double clicking on **Services**.)

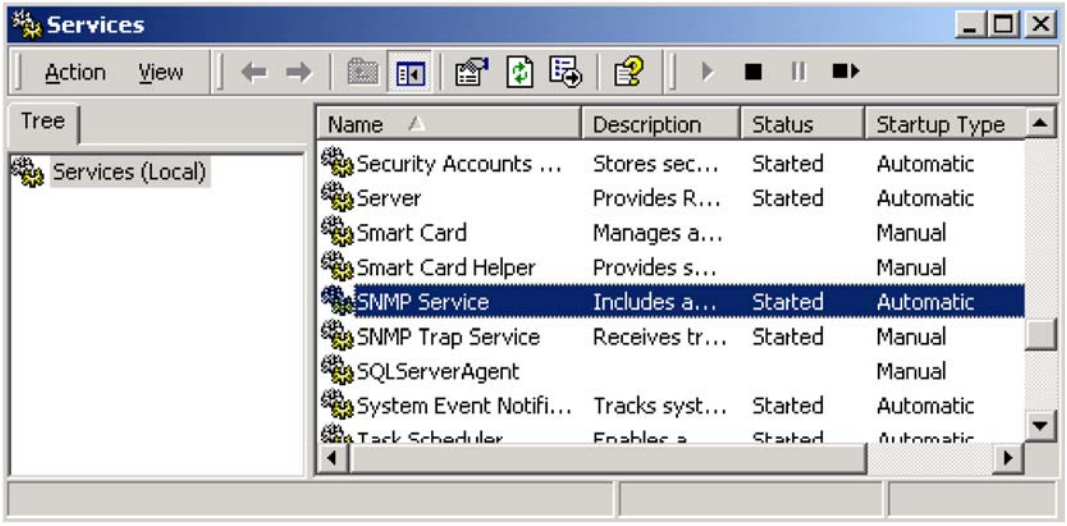


Figure 10-1. Service Control

3. Scroll through the list of services to find the **SNMP Service**. The list can be sorted alphabetically by name to make this easier.

4. If the **SNMP Service** is listed, double click on it to open the **SNMP Service Properties** dialog**.**

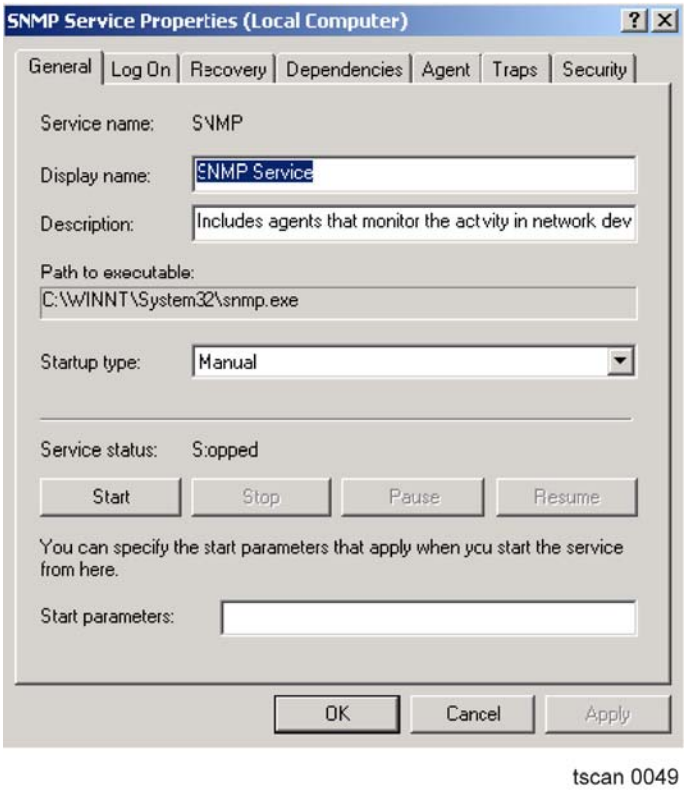


Figure 10-2. SNMP service

5. Change the **Startup type** to **Manual** and then click the **Stop** button. When the SNMP Service has stopped click the **OK** button.

Registering the TimeScan SNMP Agent

Update the registry with **TimeScanSNMPAgent.reg**, which can be found by using Windows Explorer. Navigate to the directory in which TimeScan/NMS was installed and then look in the **configs** directory. Double click this file and press **YES** on the confirmation message. (The exact message varies depending on where TimeScan/NMS was installed.)

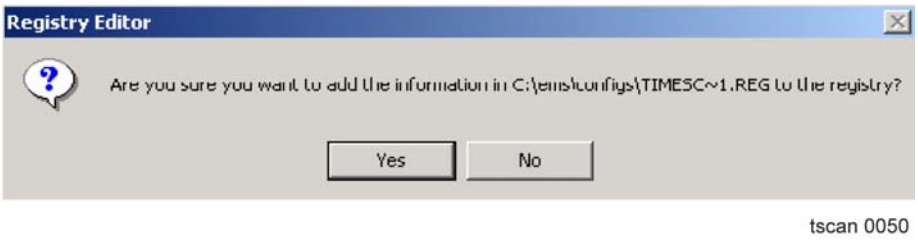


Figure 10-3. Registry Confirmation

Installing the NuDesign Multiprotocol Agent Service

Use the following steps to install the NuDesign multiprotocol agent service in either Windows 2000 or Windows XP.

For WinNT

1. Use Windows Explorer to navigate to the directory in which TimeScan/NMS was installed, open the **apps\NuDesign** directory and then double click **NuDesign_EAgSrv031.exe** (the exact filename can vary slightly). This starts the installation wizard. Follow the on-screen instructions.

2. Start the Network Control Panel Applet (by double clicking the **Network** icon in the Control Panel).

3. Click on the **Services** tab to make it active.

4. Click on the **Add...** button. The **Select Network Service** dialog appears.

5. Click on the **Have Disk** button. The **Insert Disk** dialog should appear.

6. Type in the path to the directory where the NDSnmpAgent setup files were extracted (this is the target directory used in the installation wizard in step 1, e.g. C:\Program Files\NuDesign Tools\SNMPv3 & HTTP Agent Service) then click **OK**.

7. The **Select OEM Option** should appear. The only one option is:

   NuDesign Multiprotocol (SNMPv3/HTTP) Agent Service. Select that option and click the **OK** button.

8. **NuDesign Multiprotocol (SNMPv3/HTTP) Agent** should appear in the **Network Services** list.

9. Click on the **Close** button

10. Reboot the computer if instructed to.

For Win2000

1. Use Windows Explorer to navigate to the directory in which TimeScan/NMS was installed, open the **apps\NuDesign** directory and then double click **NuDesign_EAgSrv031.exe** (the exact filename can vary slightly). This starts the installation wizard. Follow the on-screen instructions.

2. Start Network Control Panel Applet (by double clicking the **Network** icon in the Control Panel.

3. Double click on **Network & Dial up Connection** to make it active.

4. Double click on **Local area Connection**.

5. Click on the **Properties** button.

6. Click on the **Install...** button.

7. Select **Service** from the list box, then press the **Add...** button.

8. Click the **Have Disk...** button.

9. Use the **Browse...** button to select the directory where the NDSnmpAgent setup files were extracted (this is the target directory used in the installation wizard in step 1, e.g. C:\Program Files\NuDesign Tools\SNMPv3 & HTTP Agent Service).

10. Click the **OK** button.

11. Select **NuDesign Multiprotocol (SNMPv3/HTTP) Agent Service**.

12. Click the **OK** button to finish the Service installation.

13. Quit the Control Panel by pressing the **OK** button.

14. Reboot the computer if instructed to.

For WinXP

1. Use Windows Explorer to navigate to the directory in which TimeScan/NMS was installed, open the **apps\NuDesign** directory and then double click **NuDesign_EAgSrv031.exe** (the exact filename can vary slightly). This starts the installation wizard. Follow the on-screen instructions.

2. Press the **Start** button and select **Control Panel**.

3. Select the **Network and Internet Connections** link.

4. From the **Pick a task....** window select the **Network Connections** link in the **or pick a Control Panel icon** section.

5. From the **Network Connections** window, right click on the **Local Area Connector**. If you have more than one, select the first one. Select the **Properties** item.

6. From the **Local Area Connection Properties** window, press the **Install...** button.

7. Select **Service** from the list box, then press the **Add...** button.

8. Press the **Have Disk...** button.

9. Use the **Browse...** button to select the directory where the NDSnmpAgent setup files were extracted (this is the target directory used in the installation wizard in step 1, e.g. C:\Program Files\NuDesign Tools\SNMPv3 & HTTP Agent Service).

10. Click the **OK** button.

11. Select **NuDesign Multiprotocol (SNMPv3/HTTP) Service**.

12. Click the **OK** button to finish the Service installation.

13. Close the **Local Area Connection Properties** window, by pressing **close**.

14. Close the control panel window.

15. Reboot the computer if instructed to.

Configuring the NuDesign Multiprotocol Agent Service for TimeScan SNMP

1. Open the **NuDesign SNMPv3/HTTP Agent Service Configuration** window by double clicking **NuDesign SNMPv3/HTTP Agent** in the Control Panel.

2. In the left hand area click on **SNMP**.

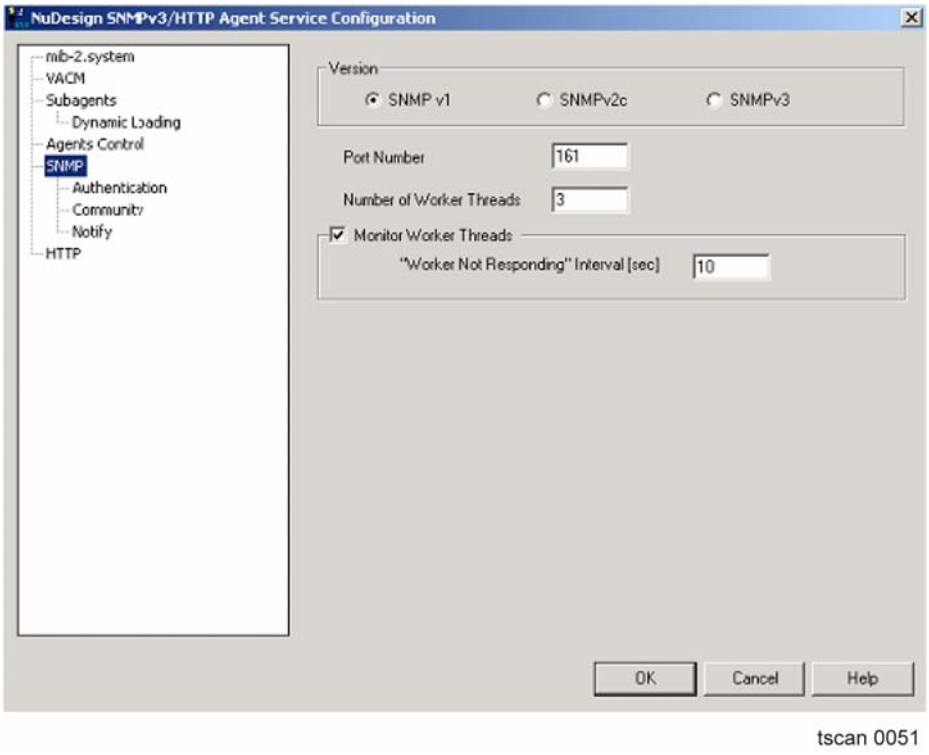


Figure 10-4. NuDesign SNMP Configuration Window

3. In the right hand area select the required SNMP version. Options are **SNMPv1**, **SNMPv2c** or **SNMPv3**.

4. In the left hand area click on **Notify**. The right hand area changes to show notify settings. The format varies depending on the version of SNMP selected in step 3. The following example relates to SNMPv1 and SNMPv2c:

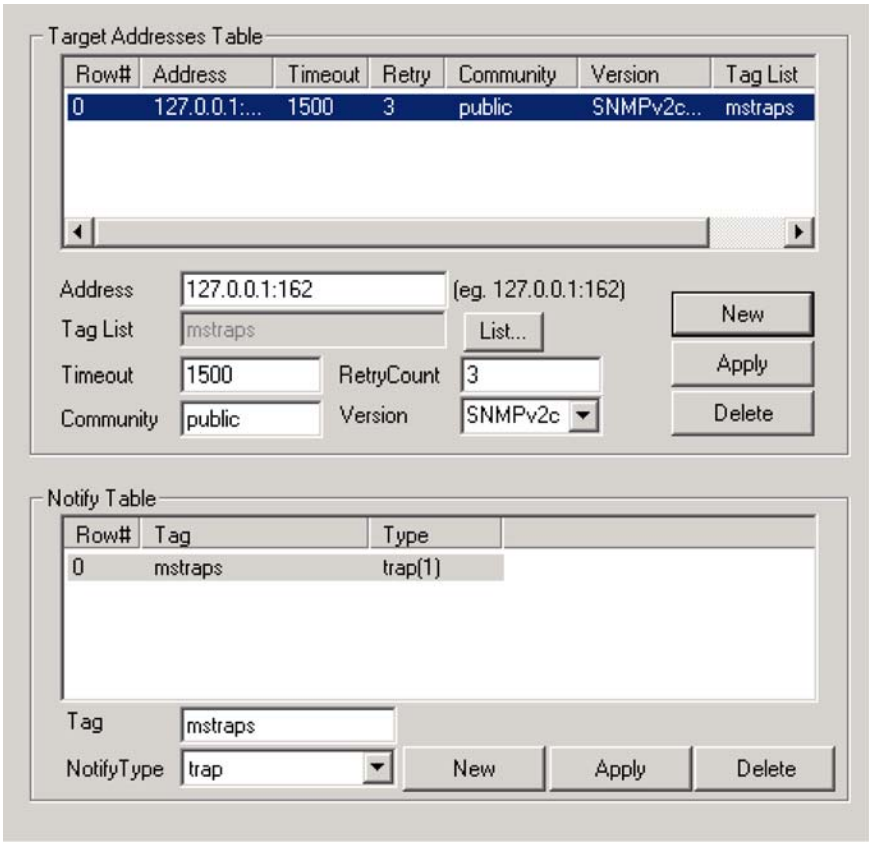


Figure 10-5. SNMP Trap Configuration

5. Press the **New** button in the Target Addresses Table area. In the **Address** field, Enter the IP address of the SNMP manager followed by a colon and the port number used by the manager to receive traps (usually 162). Enter values for **Timeout** (e.g. 1500), **Retry Count** (e.g. 3), **Community** (e.g. public) and **Version** (normally the version used in step 3).

6. Press the **List...** button in the Target Addresses Table area (located above the retry count).

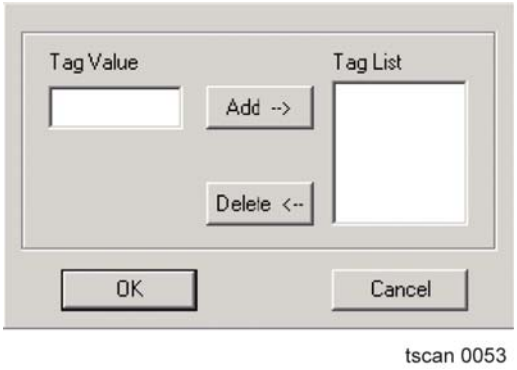


Figure 10-6. SNMP Trap Configuration Continued

7. Enter a tag value (e.g. mstraps) and then click the **Add** button. Press **OK**.

8. When all values have been entered press the **Apply** button in the Target Addresses Table area then the **OK** button at the bottom of the **NuDesign SNMPv3/HTTP Agent Service Configuration** window.

More information can be found by pressing the Help button at the bottom of the **NuDesign SNMPv3/HTTP Agent Service Configuration** window.

Notes for Administrators

1. From the **NuDesign SNMPv3/HTTP Agent Service Configuration** window (opened from the control panel), select **Subagents**. A list of subagents should appear in the right hand side. Scroll through the list looking in the registry column for 'SOFTWARE\Symmetricom\TimeScanSNMPAgent\CurrentVersion'. If it is not there the most likely cause is that the registry has not been updated. To fix this, press the **Add** button, navigate to the directory where TimeScan/NMS was installed and look in the **dlls** directory. Find **TimeScanSNMPAgent.dll**, select it and press the **Open** button. Press the **Apply** button.

2. Open the **Services** window as described in the section **Getting Started**. Look for the **NuDesign Multiprotocol (SNMPv3/HTTP) Agent**. Ensure that it is there and is started. If it is not there repeat the section **Installing the NuDesign Multiprotocol Agent Service** from step 2.

3. Use Windows Explorer to navigate to the directory in which TimeScan/NMS was installed and open the **logs** directory. Look for a file called **TimeScanSNMPAgent.log**. This is a text file that is created the first time TimeScanSNMPAgent is run and updated as it is used. Open the file into a text editor (e.g. notepad) to see if there is any error information. In particular, check that a software license has been found and that the alarm subscription has started. If the alarm subscription has not started check that TimeScan/NMS is running.

System Event Types

HeartBeat

The agent sends a regular heartbeat in the form of a trap two fields:

Message - with value "HEARTBEAT".

timeStamp -with value as the time of notification.

The heartbeat interval is read from the file TimeScanSNMPAgent.txt which gets installed in the configs directory. The value stored in the file is 600 seconds (10 minutes) when first installed but can be changed as required. A value of zero turns the heartbeat off. If the file cannot be read, the heartbeat interval defaults to 10 minutes.

AuditNotifications

An SNMP manager can retrieve all active alarms by sending a Get request to the getAllActiveAlarms attribute. The agent then broadcasts the active alarms. The format of the alarms output is the same as those that are forwarded as they are produced. The alarms come from the TimeScan/NMS database rather than from the elements themselves. No communication with the elements is initiated by this request.

AuditNotifications which can be used to mark the start and end of the list of traps received. The markers are additional traps which have the following format:

Message - with value = "START OF AUDIT" or "END OF AUDIT".

timeStamp -with value as the time of notification.

Licensing (extremely rare)

This should be extremely rare, because at the TimeScan synchronization EMS system installation time, a correct license is always installed. The agent requires a flexLM license (it does not work with a TimeScan/NMS dongle). The agent does not interfere with other SNMP agents on the same computer even if the license is not present.

If no valid license is present the agent responds to all Get, GetNext and Set requests with an error of type SNMP_ERRORSTATUS_GENERR. Also, a notification is transmitted on startup (type = systemEvent) informing the manager that the agent has no license. This notification is also transmitted if a Get request is made on the attribute getAllActiveAlarms.

The notification of no license contains the following fields:

EventAid - with value NMS-INTERNAL

conditionType - with value NOLICENSE

trapSeverity - with value not alarmed (1)

eventNature - with value Not Service Affecting (1)

message - with value No license found for TimeScan SNMP Agent

timeStamp - with value as the time of notification

When a valid license is installed, you must restart the SNMP service to make the agent work.

Trap Descriptions

Table 10-1 provides a list of trap names, IDs, sources, status, severity, and descriptions. The traps have the base OID: 1.3.6.1.4.1.9070.1.2.1.1.14. Trap ID, the severity, and condition are controlled by variable binds of traps. For specific alarm or event types, please refer to the TL1 command reference in the TimeSource 3600 GPS Primary Reference Source User's Guide part number 097-72060-01.

Table 10-1. Trap Descriptions

Name	Trap Id	Source	Status	Severity	Description
System Alarm	22	TimePictra or TimeScan SNMP Agent		Critical Major Minor	This notification type is used by agent to emit traps if the following conditions are satisfied. (1). The event should be generated by timePictra system. (2). The event severity should be either major, minor or critical.
System Event	23	TimePictra or TimeScan SNMP Agent		Clear Noalarm None	This notification type is used by agent to emit traps if the following conditions are satisfied.(1). The event should be generated by timePictra system. (2). The event severity should be either none, noalarm or clear.

Table 10-1. Trap Descriptions

Name	Trap Id	Source	Status	Severity	Description
neAlarm	24	Network Element		Critical Major Minor	This notification type is used by agent to emit traps if the following conditions are satisfied.(1). The event should be generated by the Network Element (2). The event severity should be either major, minor or critical.
neEvent	25	Network Element		Clear Noalarm None	This notification type is used by agent to emit traps if the following conditions are satisfied.(1). The event should be generated by the Network Element. (2). The event severity should be either none, noalarm or clear.
neCreation	26	TimePictra or TimeScan SNMP Agent		None	This trap is used to report creation of a new NE in the database.
neDeletion	27	TimePictra or TimeScan SNMP Agent		None	This trap is used to report deletion of an NE from the database.
AttributeValueChange	28	TimePictra or TimeScan SNMP Agent			This notification type is used by agent to emit traps if the following conditions are satisfied. (1).Set on a single attribute in the database
allAttributeValuesChange	29	TimePictra or TimeScan SNMP Agent			This notification type is used by agent to emit traps if the following conditions are satisfied. (1).Set on a list of attributes by the manager
errorMesg	30	TimePictra or TimeScan SNMP Agent			This trap is emitted by the agent when the GES interface to timepictra returns an error during GET/SET.
agentUp	31	TimePictra or TimeScan SNMP Agent			This trap is emitted by the agent once it complete its initialization.
agentDown	32	TimePictra or TimeScan SNMP Agent			This trap is emitted by the agent before it goes down.

SNMP option FAQ — Frequently Asked Questions and Answers

1. Where is the list of Traps/Alarms/Events?

TimeScan ***does not*** keep any internal list of alarms for NEs. The name of the alarm/event comes from the NE itself (in the autonomous TL1 messages), and this name is contained in the “conditionType” objects within the trap/alarm. Refer to the hardware NE manuals to get a list of all the alarm/events names that the NEs can send. TimeScan has only four generic types of traps:

- neAlarm - Alarms generated by the network elements
- neEvent - The non-alarmed events generated by network elements
- systemAlarm - Alarmed events generated by TimeScan
- systemEvent - Non-alarmed events generated by TimeScan

Please refer to the MIB for more information on them.

2. Where do I look for documentation of the SNMP agent?

Contact Symmetricom support/sales to get the following:

- TimeScan SNMP Agent Manual

- TimeScan SNMP MIB (you can get this after signing an NDA agreements with Symmetricom)

You can also refer to NuDesign's SNMP Agent and related documentation on Windows NT, Windows 2000, and Windows XP at the following web address:

http://ndt-inc.com/index.html

3. What version of SNMP is supported (1, 2x or 3)?

All three versions are supported. Required versions can be selected by configuring NuDesign Multi Protocol Agent Service. (See Configuring the NuDesign Multiprotocol Agent Service for TimeScan SNMP, on page 118.

4. What is the MIB Syntax version?

TimeScan MIB uses SNMPv2 SMI

5. What is the definition of the transport level?

You can access the TS Agent through the NuDesign Agent Service. The default UDP port number is 161, but it can be modified. See the following web address for related documentation:

http://ndt-inc.com/index.html

6. Does this version support Synchronization of Alarms?

Managers can request alarm synchronization by sending a simple Read/Get request on a MIB object, for instance getAllActiveAlarms. Check the MIB for more details.

7. What is the Physical and Software Architecture?

The agent is a part of TimeScan, which is an EMS, and the agent works as a proxy for the device. The agent is designed as an extension agent to the NuDesign Mutliprotocol Agent Service. There is only one TimeScan agent as an extension to the NuDesign Agent Service.

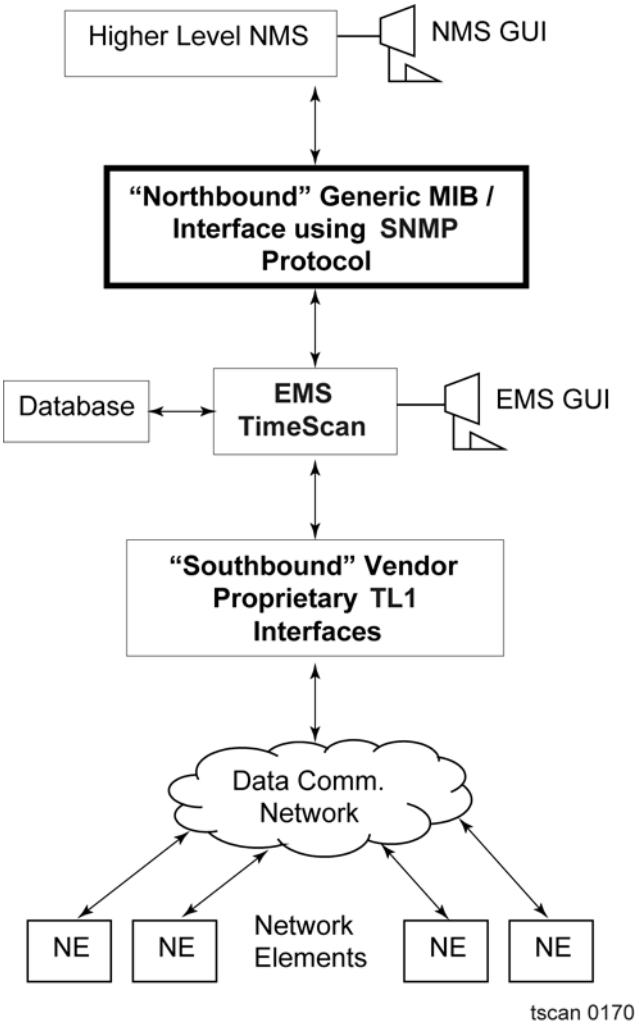


Figure 10-7. Physical and Software Architecture

8. What fields can be used to correlate alarms?

Following fields can used to correlate alarms/events:

- conditionType: contains the name of alarm/event. This name comes directly from the NE
- eventAid: access identifier of the network element that identifies the sub-unit (card, rack, input/output ports, etc.) in the NE
- eventNeClli: is the unique name of NE itself. For correlation purposes, eventNeId (unique numeric id for NE) can also be used in place of eventNeClli

9. What are the systemEvent types in TimeScan SNMP?

- HeartBeat

The agent sends a regular heartbeat in the form of a trap two fields:

Message with value “HEARTBEAT”

timeStamp with value as the time of notification

The heartbeat interval is read from the file TimeScanSNMPAgent.txt which gets installed in the configs directory. The value stored in the file is 600 seconds (10 minutes) when first installed but can be changed as required. A value of 0 turns the heartbeat off. If the file cannot be read, the heartbeat interval defaults to 10 minutes.

- AuditNotifications

An SNMP manager can retrieve all active alarms by sending a Get request to the getAllActiveAlarms attribute. The agent then broadcasts the active alarms. The format of the alarms output is the same as those that are forwarded as they are produced. The alarms come from the TimeScan/NMS database rather than from the elements themselves. No communication with the elements is initiated by this request.

AuditNotifications can be used to mark the start and end of the list of traps received. The markers are additional traps which have the following format:

Message with value = “START OF AUDIT” or “END OF AUDIT”

timeStamp with value as the time of notification

- Licensing (extremely rare)

This should be ***extremely rare***, because at the TimeScan synchronization EMS system installation time, the correct license is always installed. The agent requires a flexLM license; it does not work with a TimeScan/NMS dongle. The agent does not interfere with other SNMP agents on the same computer even if the license is not present.

If no valid license is present, the agent responds to all Get, GetNext and Set requests with an error of type SNMP_ERRORSTATUS_GENERR. Also, a notification is transmitted on startup (type = systemEvent) informing the manager that the agent has no license. This notification is also transmitted if a Get request is made on the attribute getAllActiveAlarms.

The notification of no license contains the following fields:

EventAid with value “NMS-INTERNAL”

conditionType with value “NOLICENSE”

trapSeverity with value not alarmed (1)

eventNature with value Not Service Affecting (1)

message with value "No license found for TimeScan SNMP Agent"

timeStamp with value as the time of notification

When a valid license is installed, you must restart the SNMP service to make the agent work.

Index

I

L

M

N

O

P

R

S

T

U

V

W

X