Client Services for Netfinity Manager

User’s Guide

Client Services for Netfinity Manager

User’s Guide

Note

Before using this information and the product it supports, be sure to read the general information under Appendix G, "Notices" on page 187.

First Edition (June 1998)

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

This publication was developed for products and services offered in the United States of America. IBM may not offer the products, services, or features discussed in this document in other countries, and the information is subject to change without notice. Consult your local IBM representative for information on the products, services, and features available in your area.

Requests for technical information about IBM products should be made to your IBM reseller or IBM marketing representative.

Contents

About This Book

This book provides detailed information on how to use each of the services included with Client Services for Netfinity Manager. For information on how to install and configure Client Services for Netfinity Manager, see *Client Services for Netfinity Manager Quick Beginnings.*

Who Should Read This Book

This book is for anyone who will be using Client Services for Netfinity Manager for local hardware systems management. It can also be used for quick reference by users of individual services. However, detailed online helps are available for all Netfinity services.

You should have general knowledge of your operating system.

Chapter 1. Netfinity Product Description

Netfinity is a family of distributed applications designed to enhance the system monitoring and management capabilities of a network. Netfinity has a flexible, modular design that allows for a variety of system-specific configurations. You can install only those program files that are necessary for the individual system's designated function within a network environment or as a stand-alone system. Netfinity's modularity also enables you to update and add new services without reinstalling the base product. Netfinity combines the power and flexibility you want today with the expandability you'll need in years to come.

Client Services for Netfinity Manager enables your network administrator to effectively monitor and manage systems remotely without interrupting any work. Running the Netfinity programs in the background does not interfere with work being done on the system. However, it enables your network administrator to monitor the status of systems in the network, anticipating and correcting problems before they become serious.

Client Services for Netfinity Manager also includes the Serial Connection Control service. With this service, an Netfinity Manager can remotely access and manage your system using your system's modem. Now, you don't even have to be attached to a network for your systems administrator to monitor, manage, and troubleshoot your system. Just configure the Serial Connection Control service, and a Netfinity Manager can dial into your system and access any of the Netfinity services that they are permitted access to by the Security Manager service, just as if they were accessing your system over a network.

You can also use Client Services for Netfinity Manager to manage and monitor your own system, regardless of whether it is attached to a LAN or not. Client Services for Netfinity Manager features several installation configurations that provide users with varying degrees of access to their own system's Netfinity services.

Depending on the hardware configuration of your system and the installation configuration selected during installation, some or all of the following Netfinity Services will be available for use on your system:

- Alert Manager
- Critical File Monitor
- Security Manager
- Serial Connection Control
- Software Inventory
- System Information Tool
- System Monitor
- User Profile
- ECC Memory Setup (requires ECC memory)
- System Partition Access (requires a System Partition)
- Predictive Failure Analysis (requires a PFA-enabled hard disk drive)
- RAID Manager (requires a RAID adapter)
- DMI Browser (requires DMI Service Layer)

Instruction on how to use each of these services is provided in this book.

Chapter 2. Starting Netfinity

To start Netfinity:

1. Open the Netfinity folder or program group.

   During installation of the Client Services for Netfinity Manager, a Netfinity folder (OS/2 and Windows 95 only) or a Netfinity program group (Windows and Windows NT only) was added to your desktop. The Netfinity folder or program group contains the Netfinity Service Manager object.

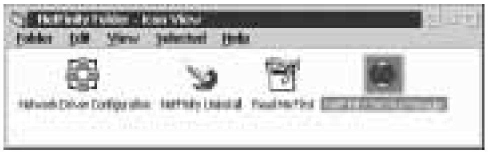


Figure 1. The Netfinity Folder

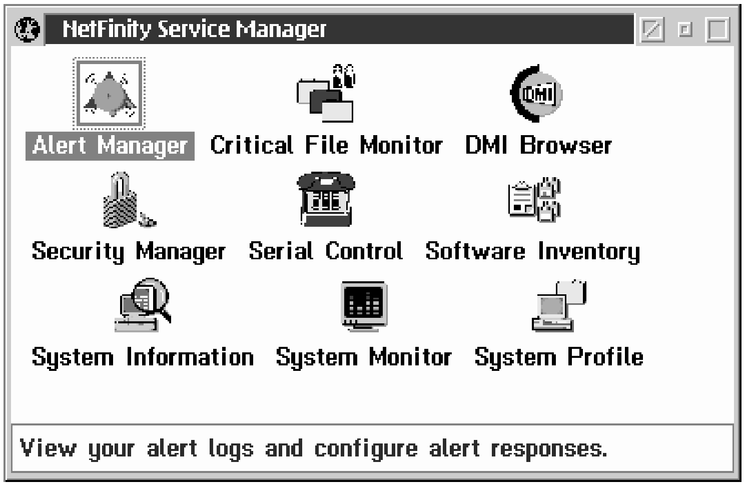
   Note: In your Netfinity folder or program group is a document titled *Read Me First*, which contains information about Netfinity that might not be covered in your documentation. The Netfinity folder also contains the Network Driver Configuration object, which allows you to reconfigure your network protocols and system keywords.

2. Start the Netfinity Service Manager.

   To start the Netfinity Service Manager, use mouse button 1 to double-click on the Netfinity Service Manager object.

Netfinity Service Manager

All Netfinity services that are supported by your system can be started from the Netfinity Service Manager window. The services that are available for use depend on the installation configuration you selected during installation (see Appendix A, “Installation Configurations” on page 149).



View your alert logs and configure alert responses.

Figure 2. Netfinity Service Manager. The services shown are installed when the “Active Client Installation” installation configuration is selected.

To start any Netfinity service that appears in your Service Manager window, double-click on the icon for that service.

Netfinity Service Descriptions

Each Netfinity service consists of a base program and a graphical user interface (GUI). The service base programs enable the individual services to be accessed remotely by the Netfinity Manager, but do not allow for local access. The service GUIs, when functioning along with their respective base program, enable the local user to access the service.

Some services are available only on systems with certain system configurations. These services are:

- DMI Browser (requires an installed and functional DMI Service Layer)
- ECC Memory Setup (requires ECC memory)
- Predictive Failure Analysis (requires a PFA-enabled hard disk drive)
- RAID Manager (requires a RAID hard disk drive subsystem)

- System Partition Access (requires a built-in System Partition)

Brief descriptions of each of the Netfinity services follow. Complete instructions on how to use each of these services can be found in the service-specific chapters of this book.

Alert Manager

The Alert Manager is an extendable facility that allows receiving and processing of application-generated alerts. A variety of actions can be taken in response to alerts, including logging alerts, notifying the user, forwarding the alert to another system, executing a program, playing a WAV file (available only on multimedia systems), generating an SNMP alert message, dialing out to a digital pager service (available only on systems that have a modem), or taking an application-defined action. Actions are user-definable, using a highly flexible action management interface.

Also, an extensive, detailed log is kept of all alerts received by the Alert Manager. Logged information available from the log includes date and time the alert was received, type and severity of the alert, the ID of the application that generated the alert, as well as any text that was generated and any action taken by the Alert Manager. Individual or multiple alerts can be selected from the log and printed for later reference, or deleted once problems are corrected. This service is available for both stand-alone and network use.

Critical File Monitor

Critical File Monitor enables you to be warned whenever critical system files on your system are deleted or altered. Critical File Monitor makes it simple for you to generate Netfinity alerts when an important System File (such as the CONFIG.SYS file) changes date, time, size, or when it is deleted or created . Critical File Monitor can also be used to monitor any other files that reside on a Netfinity system.

DMI Browser

DMI Browser enables you to examine information about the DMI-compliant hardware and software products installed in or attached to your system.

ECC Memory Setup

The ECC Memory Setup allows for monitoring of ECC memory single-bit errors, and can automatically “scrub,” or correct, the ECC memory when errors are detected. Also, you can keep a running count of single-bit errors, and can set a single-bit error threshold that will cause a nonmaskable interrupt (NMI) if the ECC single-bit error threshold is exceeded. This service is available for both stand-alone and network use by any system that has ECC memory.

Predictive Failure Analysis

The Predictive Failure Analysis (PFA) service enables you to continually monitor and manage PFA-enabled hard disk drives. A PFA-enable hard disk drive features hardware designed to help detect drive problems and predict drive failures before they occur, thus enabling you to avoid data loss and system downtime.

RAID Manager

The RAID Manager service enables you to monitor, manage, and configure an assortment of Redundant Arrays of Independent Disk (**RAID**) adapters and arrays without requiring you to take the RAID system offline to perform maintenance. Use the RAID Manager to gather data about your system’s RAID array and RAID adapter, rebuild failing drives, add (or remove) logical drives, perform data integrity tests, and many other RAID system tasks. This service is available for both stand alone and network use by any system that has a supported RAID adapter.

Security Manager

The Security Manager can prevent unauthorized access to some or all of your Netfinity services. It uses incoming user ID and password combinations, and is available for network use only.

Note: If your system is configured for network operations (that is, you selected the Active Client or Passive Client installation configuration), several program names that you may not recognize will appear in your Security Manager. These programs are support programs for remote system management. If you have any questions about setting incoming user ID and password combinations on these services, see your network administrator.

Serial Connection Control

The Serial Connection Control service enables remote Netfinity Managers to access your system through a phone line and modem. With the Serial Connection Control service, you don't have to be attached to a network to benefit from Netfinity's outstanding remote system access, monitoring, and management capabilities.

Note: Your system *must* have a properly installed and configured modem that supports at least 9600 baud for the Serial Connection Control service to function.

Software Inventory

Enables you to create and manage software product dictionaries that can be used to easily maintain an inventory of all application programs installed on your system.

System Information Tool

The System Information Tool enables you to quickly and conveniently access detailed information on the hardware and software configurations of your system. System Information Tool gathers information about almost any computer; however, the most detail is provided when this service is used with IBM computers. This service is available for both stand-alone and network use.

System Monitor

The System Monitor provides a convenient method of charting and monitoring the activity of a number of components in a system, including processor usage, disk space used, and ECC memory errors. These convenient monitors are detachable and scalable, enabling you to keep only the monitors you need available at all times. You can use System Monitor's Threshold Manager to set threshold levels for any of the monitored components. When exceeded, these thresholds will generate user-configured alerts.

Data is continually collected from the time the system starts. A sophisticated data-handling technique is used to weigh the individual values, average concurrent samples, and post single values that accurately reflect long-term system activity. This technique allows you to maintain system activity records without creating enormous data files. This service is available for both stand-alone and network use.

System Partition Access

The System Partition Access allows for greatly simplified System Partition file handling, both locally and remotely. Individual files and entire directories can be renamed or deleted from the System Partition. Individual files can be renamed, deleted, or copied into the System Partition. Also, the entire partition can be backed-up, restored, or deleted. This service is available for both stand alone and network use by any system that has a System Partition.

System Profile

The System Profile provides a convenient notebook of pertinent data about a particular user or system. It features many predefined fields for extensive user-specific data, including name, address, office number and location, and phone number. System Profile also includes many predefined fields for system-specific data that might not be available to System Information Tool, including model and serial numbers and date of purchase. Finally, there are many user-definable “miscellaneous” fields that can be used to hold any data the user or administrator requires.

Delaying Netfinity Startup on OS/2 Systems

In some cases, it might be necessary for you to delay the automatic startup of the Netfinity Network Interface (NETFBASE.EXE) in order to allow other time-sensitive applications to start up correctly or to allow your system to fully configure itself prior to beginning network operations. NETFBASE.EXE includes a parameter (WAIT) that enables you to specify the number of seconds that NETFBASE.EXE will wait before starting.

During Netfinity installation, the Netfinity Network Interface object is placed in the Startup folder. To configure Netfinity to wait a specified number of seconds before starting:

1. Shut down the Netfinity Network Interface if it is running.
2. Open the Startup folder.
3. Using mouse button 2, click on the Netfinity Network Interface object. This will open the Netfinity Network Interface context menu.
4. Select **Settings** to open the Netfinity Network Interface **Settings** notebook.
5. Type in the **Parameters** field

   ```
   WAIT:x
   ```

   where *x* is the number of seconds that you want the Netfinity Network Interface to wait before starting.
6. Close the Netfinity Network Interface **Settings** notebook.

With the WAIT parameter set to *x*, whenever you start your system, the Netfinity Network Interface will wait *x* seconds before starting.

Note: This feature is available only on systems that are running OS/2.

Chapter 3. Alert Manager

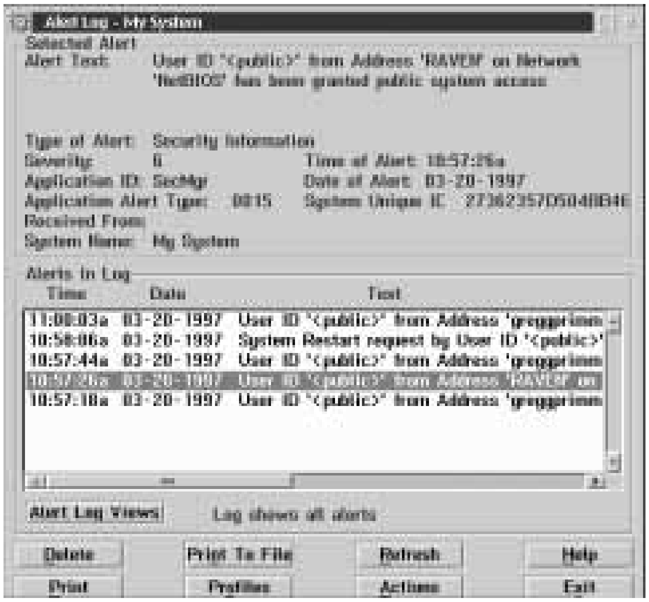
Netfinity Alert Manager enables your system to receive and automatically respond to alerts generated by other Netfinity services. Using a variety of alert-specific information (including the severity of the alert, the name of the Netfinity service that generated the alert, the type of alert, and the network address of the system that generated the alert), Netfinity alerts are categorized into alert profiles. Profiles can be bound to one or more Alert Manager actions (such as logging the alert or executing a command). Once a profile is bound to an action, the action will be performed whenever an alert that fits the profile is received.

Netfinity Alert Manager includes actions that do the following:

- Log the alert to a file
- Display the alert in a pop-up window
- Forward the alert to another workstation
- Execute a command
- Execute a minimized command
- Send a *simple network management protocol* (SNMP) version of the alert (not available for local use on systems running Windows 3.1 or Windows 95.)
- Send a mapped SNMP version of the alert (similar to the standard SNMP version of the alert, but featuring specific Enterprise ID values for each of the various alert types; not available for local use on systems running Windows 3.1 or Windows 95)
- Play a waveform (WAV) sound file (requires multimedia support)
- Send a message to a digital pager through a modem (requires modem attached to system)
- Send the alert information to an alphanumeric pager through a modem (requires modem attached to system)
- Send the alert to another user using TCP/IP SENDMAIL (available only on systems running OS/2; requires TCP/IP for OS/2 2.0 or later)
- Send an email version of the alert using Vendor Independent Messaging (VIM) (requires VIM support)
- Send a *messaging application programming interface* (MAPI) version of the alert (requires MAPI support)
- Export the alert information to a Netfinity database

- Export the alert information to a Lotus Notes database
- Generate a Desktop Management Interface (DMI) event and send it to the DMI Service Layer (requires DMI support)
- Display the alert on PC Server 720 front panel (available only on IBM PC Server 720 systems)
- Add an error condition to the system
- Remove the error condition from the system

  Note: Error conditions are used by the Netfinity Manager to help quickly identify remote systems that have reported a problem. For information about error conditions, see the *Netfinity Manager User's Guide* or your network administrator.



Alert Text: User ID '<public>' from Address 'RAVEN' on Network 'NetBIOS' has been granted public system access

```
Type of Alert:  Security Information
Severity:       6                          Time of Alert: 10:57:26a
Application ID: SecMgr                     Date of Alert: 03-20-1997
Application Alert Type:  0015              System Unique ID:  27362357D5048B4E
Received From:
System Name:    My System
```

```
  Time       Date                        Text
11:00:03a  03-20-1997  User ID '<public>' from Address 'greggrimm
10:58:06a  03-20-1997  System Restart request by User ID '<public>'
10:57:44a  03-20-1997  User ID '<public>' from Address 'greggrimm
10:57:26a  03-20-1997  User ID '<public>' from Address 'RAVEN' on
10:57:18a  03-20-1997  User ID '<public>' from Address 'greggrimm
```

Log shows all alerts

Figure 3. Alert Manager Service

Alert Manager performs two essential systems management functions:

1. Maintains a log of all received and logged alerts that can be viewed with configurable filters.

The Alert Log lists all alerts that are currently recorded in the Alert Log file. The Alert Log can be configured to display:

- All logged alerts
- Alerts that were received and logged within a specified time or date range
- Alerts that were received and logged and that fit specified alert profiles
- Alerts that were received within a specified time or date range *and* that fit specified alert profiles.

Note: Only alerts that have been received and entered into the Alert Log using the **Add the alert to log file** alert action will appear in the **Alerts in Log** field. For information on this and other alert actions, see “Netfinity Alert Actions” on page 19.

For information on configuring the Alert Log views, see “Alert Log Views” on page 15. For information on alert profiles, see “Alert Profiles” on page 29.

2. Automatically responds to the alerts it receives with user-specified actions.

   You can use Alert Manager manager to select one or more alert profiles and bind them to one of Alert Manager’ alert actions. Once one or more profiles are bound to an alert action, this action will automatically execute whenever an alert is received that fits a profile to which it is bound. For information on alert profiles, see “Alert Profiles” on page 29. For information on binding alert profiles to alert actions, see “Binding Profiles to Actions” on page 38.

The Alert Log

The Alert Log window is the first window that you see when you start the Alert Manager service. Any alerts that have been logged using the **Add alert to log file** action, appear in the **Alerts in Log** field in the bottom half of the Alert Log window.

Select an alert from the **Alerts in Log** to display information about the alert in the upper half of the Alert Log window.

Note: You can select multiple alerts for the purposes of deleting multiple files or printing reports, but only the currently highlighted alert in the log will have its alert-specific information displayed at the top of the screen.

Information displayed about the selected alert includes:

- Alert Text
- Type of Alert
- Severity
- Application ID
- Application Alert Type
- System Received From
- System Name
- Time of Alert
- Date of Alert
- System Unique ID

Alert Text

The Alert Text includes the name of the alert, as well as any textual commentary included by the application that generated the alert.

Type of Alert

This is the application-specified alert type. A Type of Alert consists of an alert sender ID followed by an alert type value. The alert sender ID describes the nature of the device that generated the alert, and the alert type value describes the content of the alert itself.

The possible alert sender IDs are:

- System
- DASD
- Network
- Operating System
- Application
- Device
- Security

An alert sender might also be unspecified, in which case an alert sender ID will not be displayed.

The possible alert type values are:

- Failure
- Error
- Warning
- Information

An alert type can also be unspecified, in which case an alert type value will not be displayed.

Severity

The alert Severity is a value from 0 to 7, with 0 being the most severe. For example, an alert Severity of 0 could be assigned to a disk failure, while a value of 7 could simply represent a system going offline at the end of a day. Alert Severity is determined by the application that generates the alert.

Application ID

The Application ID is the name of the application that sent the specified alert to the log.

Application Alert Type

The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application that generated the alert.

Received From

The Received From value is the network address of the system that generated the alert. The Received From value could be the local system or a remote system that has been instructed to relay alerts to the local error log.

System Name

The System Name value is the name of the system that generated the alert. This name is specified by the user during Netfinity installation.

Time of Alert

The Time of Alert is the time of day when the alert was generated and logged.

Date of Alert

The Date of Alert is the calendar date on which the alert was generated.

System Unique ID

The System Unique ID is a random 16 character identification string that is assigned to the system when Netfinity is installed. It is stored in the NFUNIQUE.ID file in the Netfinity directory of the system that generated the alert. The System Unique ID is primarily used for the identification and management of systems that frequently change network addresses (such as when DHCP is used).

Alert Log Views

You can configure Alert Manager to filter the alerts that will be visible in the **Alerts in Log** field. The current Alert Log View is shown beside the **Alert Log Views** button. The available Alert Log Views are:

- Log shows all alerts

  All alerts contained in the Alert Log are shown in the **Alerts in Log** field.

- Log is currently viewed by time

  The alerts shown in the **Alerts in Log** field have occurred within a specified time frame.

- Log is currently viewed by profile

  The alerts shown in the **Alerts in Log** field fit selected alert profiles.

- Log is currently viewed by time and profile

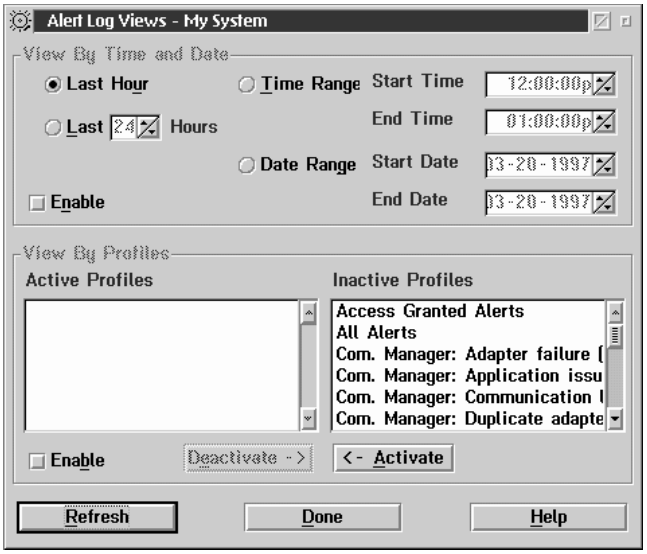
  The alerts shown in the **Alerts in Log** fit selected alert profiles *and* have occurred within a specified time frame.

Note: Only alerts that have been received and entered into the Alert Log using the *Add the alert to log file* alert action will appear in the **Alerts in Log** field. For information on this and other alert actions, see "Netfinity Alert Actions" on page 19.

To change the Alert Log view:

1. Select **Alert Log Views**.

   This opens the View Alert Log window (see Figure 4).



Alert Log Views - My System

View By Time and Date

● Last Hour

○ Last 24 Hours

○ Time Range Start Time 12:00:00p End Time 01:00:00p

○ Date Range Start Date 03-20-1997 End Date 03-20-1997

□ Enable

View By Profiles

Active Profiles

Inactive Profiles

Access Granted Alerts
All Alerts
Com. Manager: Adapter failure (
Com. Manager: Application issu
Com. Manager: Communication l
Com. Manager: Duplicate adapte

□ Enable

Figure 4. The View Alert Log window.

2. Enable (or disable) Alert Log view filters.

   There are two Alert Log view filters:

   - View by Time and Date
   - View by Profiles

   To enable the View by Time and Date filter:

   a. Select the radio button that describes the time and date range for alerts that will appear in the **Alerts in Log** field. The available selections are:

      - Last Hour

Only alerts logged in the last hour will appear in the **Alerts in Log** field.

- Last (1—48) Hours

  Only alerts logged within the number of hours that you specify will appear in the **Alerts in Log** field.

- Time Range

  Only alerts logged within the time range specified in the **Start Time** and **End Time** fields, on the date specified in the **Start Date** field, will appear in the **Alerts in Log** field.

- Date Range

  Only alerts logged within the date range specified in the **Start Date** and **End Date** fields will appear in the **Alerts in Log** field.

b. Select **Enable**.

To enable the View by Profiles filter:

a. Select one or more alert profiles from the **Inactive Profiles** field.

   Select only the alert profiles that correspond to the alerts that you want to appear in the **Alerts in Log** field.

b. Select **Activate**.

   Selected alert profiles are removed from the **Inactive Profiles** field and appear in the **Active Profiles** field.

c. Select and remove any unwanted alert profiles from the **Active Profiles** field.

   If there are any alert profiles contained in the **Active Profiles** field, select them and then select **Deactivate** to remove them from the **Active Profiles** field. They then appear in the **Inactive Profiles** filed.

d. Select **Enable**.

Alert log entries that correspond to one or more of the selected profiles will appear in the **Alerts in Log** field.

3. Select **OK** to save these changes and close the View Alert Log window.

To close this window without saving any changes, select **Cancel**.

To disable the View by Time and Date filter or the View by Profiles filter, deselect **Enable** in the filter's button group.

Alert Manager Functions

Alert Manager functions are activated from push buttons in the Alert Manager window. These buttons are:

- Delete
- Print
- Print to File
- Profiles
- Refresh
- Actions
- Help
- Exit

Information on each of the Alert Manager functions follows.

Delete

Select **Delete** to delete any selected alerts from the Alert Log. To use this function, select the alerts that you want to discard from the Alert Log and select **Delete**.

Print

Select **Print** to print a hardcopy of all selected alerts (and all specific alert information for the selected alerts) within the Alert Log.

Print to File

Select **Print to File** to save all selected alerts to a user-specified file.

Profiles

Select **Profiles** to configure, edit, or delete alert profiles. For detailed instructions on how to create, edit, or delete profiles, see “Alert Profiles” on page 29.

Refresh

Select **Refresh** to add any alerts that have been generated since the Alert Log window was displayed.

Actions

Select **Actions** to bind alert actions to any configured alert profiles. Alert actions can also be configured to respond to individual alerts that are not included in an Alert Manager alert profile. For instructions on how to bind alert actions to alert profiles, see “Binding Profiles to Actions” on page 38. For instructions on how to configure an alert action to respond to an alert that is not part of an alert profile, see “Binding Actions to Individual Alerts” on page 41. For information on alert actions, see “Netfinity Alert Actions.”

Help

Select **Help** to access the online help for Alert Manager. Detailed information is available for all of Alert Manager’s functions.

Exit

Select **Exit** to exit Alert Manager.

Netfinity Alert Actions

Alert Manager includes alert actions that do the following:

- Add the alert to log file

  Puts the alert into the Alert Log. This alert action does not require that you provide additional information.

- Display the alert in a pop-up window

  Displays a small window with all alert-specific information. This alert action does not require that you provide additional information.

- Forward the alert to another workstation

  Sends the alert to another user over a specified network. Once received, the alert is treated as though it were generated locally. When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Network Type
  The network type that will be used to forward the alert. The network type **must** be entered as NETBIOS, TCPIP, IPX, or SERIPC (for serial connections).

  Note: To forward an alert to a remote system using SERIPC (a serial connection), the serial connection must be active. This alert action will forward the alert to a remote system using SERIPC only if a serial connection to the remote system exists. To forward alerts to remote systems using a serial connection that is not currently active, use the “Send alert to remote system through serial connection” alert action.

  <P2>: Network Address
  The network type-specific address used by the remote system to which the alert will be forwarded.

  If you are unsure of the remote system’s network type or network address, see your network administrator.

- Execute a command

  Executes a single command. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Command Line
  The command that will be executed on the system.

  This action includes special command strings (or *macros*) that enable you to imbed alert-specific data in the command. This data can then be used by the application that is started by the command line. These macros are:

Macro	Imbedded Information
%TXT	Alert text
%TIM	Alert time
%DAT	Alert date
%SEV	Alert severity
%SND	Alert sender (for example, "NETBIOS::USER1")
%TYP	Alert type
%APP	Alert application ID
%AT	Alert application-specific type
%SYS	System Name
%P1–%P9	Alert-specific text strings that are imbedded in the Alert Text. The content of these parameters is dependent on the alert itself. For more information, see Appendix F, "Netfinity Alerts" on page 165.

- Execute a minimized command

  Executes a single, minimized command. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Command Line
  The command that will be executed on the system.

  This action includes special command strings (or *macros*) that enable you to imbed alert-specific data in the command. This data can then be used by the application that is started by the command line. These macros are:

Macro	Imbedded Information
%TXT	Alert text
%TIM	Alert time

%DAT	Alert date
%SEV	Alert severity
%SND	Alert sender (for example, “NETBIOS::USER1”)
%TYP	Alert type
%APP	Alert application ID
%AT	Alert application-specific type
%SYS	System Name
%P1–%P9	Alert-specific text strings that are imbedded in the Alert Text. The content of these parameters is dependent on the alert itself. For more information, see Appendix F, “Netfinity Alerts” on page 165.

- Send SNMP Alert through TCP/IP

  Uses an SNMP agent to generate an SNMP version of the alert. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Community String
  The community string name used by SNMP applications in your network.

  Notes:

  1. This action requires IBM TCP/IP for OS/2 version 2.0 or later in an OS/2 environment.

  2. This action is not available for local use on systems running Windows 3.1 or Windows 95.

  3. Netfinity’s management information base (MIB) file for use with SNMP management applications is found on the Netfinity CD in the SNMP_MIB directory. It is named NETFIN.MIB. For information on how to use NETFIN.MIB with your SNMP-based systems management software, see the documentation that was supplied with your SNMP agent or with your systems management product.

4. Netfinity's management information base (MIB) file for use with OS/2 SNMP management applications is found on the Netfinity CD in the SNMP_MIB directory. It is named MIB2.TBL. You can append this file to your existing MIB2.TBL file, or replace your MIB2.TBL with this file.

- Map Alert to SNMP Trap

  Uses an SNMP agent to generate an SNMP trap featuring an Enterprise OID value for use by SNMP-based management applications. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Community String
  The community string name used by SNMP applications in your network.

  Notes:

  1. This action requires IBM TCP/IP for OS/2 version 2.0 or later.
  2. This action is not available for local use on systems running Windows 3.1 or Windows 95.
  3. Netfinity's management information base (MIB) file for use with SNMP management applications is found on the Netfinity CD in the SNMP_MIB directory. It is named NETFIN.MIB. For information on how to use NETFIN.MIB with your SNMP-based systems management software, see the documentation that was supplied with your SNMP agent or with your systems management product.
  4. Netfinity's management information base (MIB) file for use with OS/2 SNMP management applications is found on the Netfinity CD in the SNMP_MIB directory. It is named MIB2.TBL. You can append this file to your existing MIB2.TBL file, or replace your MIB2.TBL with this file.

- Play a WAV file (requires multimedia support)

  Plays a specified waveform (WAV) audio file in response to the alert. When configuring this action, you must specify the following parameter:

Parameter Description

<P1>: Waveform file name
The fully-qualified filename of the waveform that will be played in response to the alert.

- Activate a numeric pager using a modem (requires a 100% Hayes-compatible modem attached to the system)

  Uses a modem attached to the system to dial out to a digital pager service. After the modem connects to the pager service, it will send all numeric data entered in the **Digital Pager Display** field. If your digital pager service requires that you press the pound sign (#) to send a page, be sure to type the # in the **Digital Pager Display** field after the numeric data. When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Modem COM port
  The COM port that the modem is configured to use. The COM port **must** be entered as COM*x*, where *x* is the number of the COM port.

  <P2>: Pager number
  The telephone number that will be dialed by the modem to transmit the information to the pager.

  <P3>: Digital pager display
  The numeric data that will be displayed on the pager.

  Note: Depending on your paging service, you might need to increase the amount of time that this alert action waits after dialing the telephone number in field **<P2>** before it transmits the numeric data in field **<P3>**. To increase the amount of time that will pass before the numeric data is transmitted, add one or more commas (“,”) to the end of the telephone number in field **<P2>**. Each comma will cause the modem to wait two seconds before transmitting the numeric data.

- Send alert to alphanumeric pager through TAP using a modem (requires a 100% Hayes-compatible modem attached to the system)

  Uses a modem attached to the system to dial out to an alphanumeric pager service. After the modem connects to the alphanumeric pager service, it will send all alert information.

  Parameter Description

  <P1>: Modem COM port
  The COM port that the modem is configured to use. The COM port **must** be entered as COM*x*, where *x* is the number of the COM port.

  <P2>: TAP access number
  The telephone number that will be dialed by the modem to transmit the information to the pager.

  <P3>: Pager ID
  The identification number of the pager to which the data will be sent.

  <P4>: Additional text to send
  Any additional text that you want to send along with the alert data. This parameter is optional.

  Notes:

  1. This action will work only with pager services that use the telocator alphanumeric protocol (TAP).
  2. You must provide your pager's Pager ID.

- Send alert as TCP/IP mail (available only on systems running OS/2; requires TCP/IP for OS/2 2.0 or later)

  Uses the TCP/IP SENDMAIL program to send the Netfinity alert as a note to a specified email address. When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Target user ID
  The TCP/IP ID of the system to which the alert will be sent.

<P2>: Target host address
The TCP/IP host address of the target user's system.

- Send alert as TCP/IP Web mail (available only on systems running OS/2; requires TCP/IP for OS/2 2.0 or later)

  Uses the TCP/IP SENDMAIL program to send the Netfinity alert as a note to a specified email address. The alert text will be marked up with HTML tags. When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Target user ID
  The TCP/IP ID of the system to which the alert will be sent.

  <P2>: Target host address
  The TCP/IP host address of the target user's system.

- Send to E-Mail via VIM interface (requires VIM support)

  Uses the Vendor Independent Messaging (VIM) interface to generate a VIM-version of the alert that can be sent to any properly configured system that is 32-bit VIM-compliant, such as Lotus Notes.

  The requirements for a system running Lotus Notes are identical to the requirements for a system to export data to a Lotus Notes database. For more information, see see "Lotus Notes Database Support" in *Netfinity Manager Quick Beginnings*.

  When configuring this action, you must specify the following parameters:

  Parameter Description

  <P1>: Mail System Password
  The password that must be used to enable access to the VIM mail system.

  <P2>: E-Mail Address
  The email address of the system to which the alert information will be sent.

- Send to E-Mail via MAPI interface (requires MAPI support)

Uses the MAPI interface to generate a MAPI-version of the alert that can be sent to any system that is MAPI-compliant. When configuring this action, you must specify the following parameters:

Parameter Description

<P1>: Mail System Password
The password that must be used to enable access to the VIM mail system.

<P2>: E-Mail Address
The email address of the system to which the alert information will be sent.

<P3>: Profile Name
Some MAPI-compliant applications require a Profile Name to properly process MAPI data. If the MAPI-compliant application to which this alert will be sent requires a Profile Name, type it in this field. If your MAPI-compliant application does not require a Profile Name, leave this field blank.

- Send DMI Event through DMI Service Layer (requires DMI support)

  Converts the alert into a DMI event, which is then forwarded to the DMI Service Layer. Once it is received by the DMI Service Layer, it can be used by other DMI-compliant management applications. This alert action does not require that you provide additional information.

- Display on PC Server 720 Front Panel (available only on IBM PC Server 720 systems)

  Displays the alert-specific information on the PC Server 720's front panel LED screen. This alert action does not require that you provide additional information.

- Set error condition for sending system

  Adds an Error Condition to the sending system's Error Condition log. A system's Error Condition log is accessed with the Netfinity Manager's Remote System Manager service. Error conditions are used by the Netfinity Manager to help quickly identify remote systems that have reported a problem. When configuring this action, you must specify the following parameter:

Parameter Description

<P1>: Error Condition
The name that will be used to identify this error condition in the Error Condition log.

For information about error conditions, see the *Netfinity Manager User's Guide* or your network administrator.

- Clear error condition for sending system

  Removes a previously generated Error Condition from the sending system's Error Condition log. When configuring this action, you must specify the following parameter:

  Parameter Description

  <P1>: Error Condition
  The name of the error condition that will be removed from the Error Condition log.

  p.For information about error conditions, see the *Netfinity Manager User's Guide* or your network administrator.

- Remove the error condition from the system

  Removes a previously generated Error Condition from the system's Error Condition log. A system's Error Condition log is accessed with the Netfinity Manager's Remote System Manager service. Error conditions are used by the Netfinity Manager to help quickly identify remote systems that have reported a problem. For information about error conditions, see the *Netfinity Manager User's Guide* or your network administrator.

- Send alert to remote system through serial connection

  Uses a previously defined serial connection to send the alert to a Netfinity system that can be accessed using Netfinity's Serial Connection Control service (see Chapter 10, "Serial Connection Control" on page 87). When configuring this action, you must specify the following parameter:

Parameter Description

<P1>: Connection Name
The name of serial connection as defined in Serial Connection Control.

- Send alert to host via APPC

  Converts the Netfinity alert to a network management vector transport (NMVT) alert for use by host-based management applications (such as NetView for MVS). This alert action does not require that you provide additional information.

  Notes:

  > The NMVT.INI file, found in the Netfinity directory, contains alert descriptions that map standard Netfinity alerts to NMVT-style alerts that can then be properly passed to a host system using APPC and the "Send alert to host via APPC" alert action. If you define new Netfinity alerts (using, for example, Netfinity's GENALERT command), you must make changes to this file for the alerts to be converted properly. For more information, see "Adding GENALERT Alert Descriptions to the NMVT.INI File" on page 157.

- Add event to Windows NT Event Log (available only on systems running Windows NT)

  This action adds information about the alert to the Windows NT Event Log. This alert action does not require that you provide additional information.

- Forward alert to FFST/2 (available only on systems running OS/2)

  This action sends a version of the Netfinity alert to FFST/2. This alert action does not require that you provide additional information.

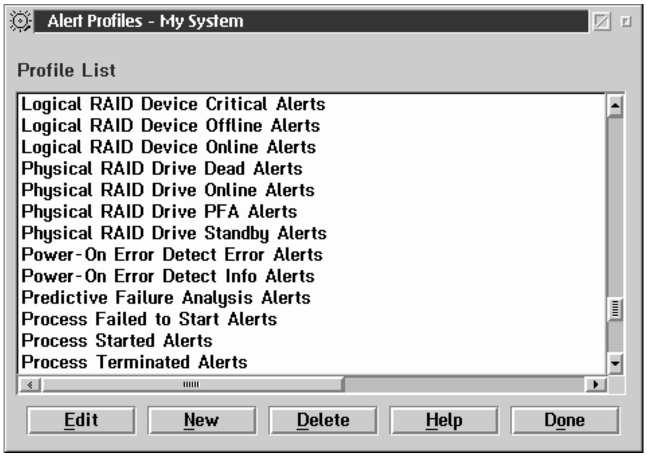
Alert Profiles

Alert profiles are simple filters that enable you to better manage alerts received by your system. Using alert-specific information a profile describes a class, or set of classes, of alerts. With alert profiles you can classify alerts by service or application, by responsible person, or simply by urgency. Alert profiles can be bound to Alert Manager actions, enabling you to react automatically to alerts generated by Netfinity systems in your network. Alert profiles can also be used to filter the type of alerts that are shown in the Alert Log (see “Alert Log Views” on page 15).

Netfinity Alert Manager comes with many predefined alert profiles that will meet the needs of most users. Using these predefined alert profiles, you will be able to quickly and easily configure Alert Manager to respond and react to received alerts automatically. See “Predefined Alert Profiles” on page 34 for more information on Netfinity’s predefined alert profiles.

Select **Profiles** from the Alert Log window to open the Alert Profiles window (see Figure 5). The Alert Profiles window displays a list of all available profiles. You can select individual profiles for editing or deleting, or create completely new profiles.

- To create a new alert profile, see “Creating New Alert Profiles” on page 31.
- To edit an alert profile, see “Editing Alert Profiles” on page 34.
- To delete an alert profile, see “Deleting Alert Profiles” on page 34.



Logical RAID Device Critical Alerts
Logical RAID Device Offline Alerts
Logical RAID Device Online Alerts
Physical RAID Drive Dead Alerts
Physical RAID Drive Online Alerts
Physical RAID Drive PFA Alerts
Physical RAID Drive Standby Alerts
Power-On Error Detect Error Alerts
Power-On Error Detect Info Alerts
Predictive Failure Analysis Alerts
Process Failed to Start Alerts
Process Started Alerts
Process Terminated Alerts

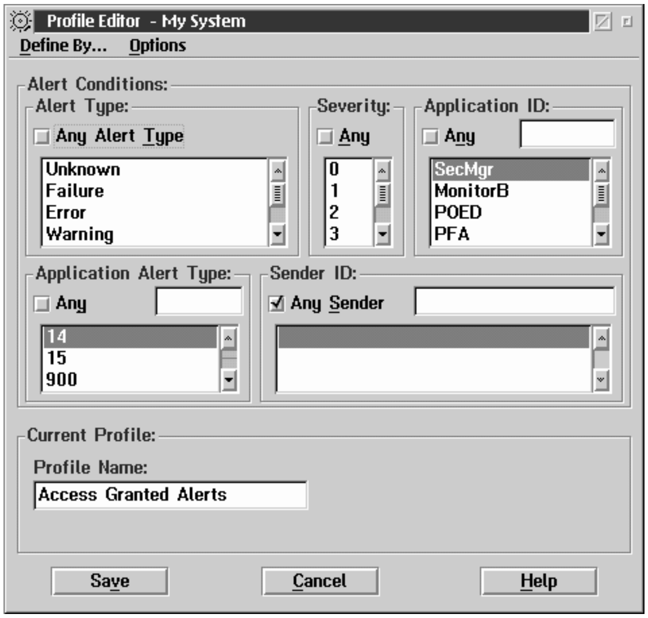
Figure 5. The Alert Profiles window.

Creating New Alert Profiles

To create a new alert profile:

1. Select **New**.

   This opens the Profile Editor window (see Figure 6). Use the Profile Editor to specify the alert-specific information (called *alert conditions*) that will determine whether a received alert fits the alert profile.



Alert Type: □ Any Alert Type — Unknown, Failure, Error, Warning

Severity: □ Any — 0, 1, 2, 3

Application ID: □ Any — SecMgr, MonitorB, POED, PFA

Application Alert Type: □ Any — 14, 15, 900

Sender ID: ☑ Any Sender

Profile Name: Access Granted Alerts

Figure 6. The Profile Editor window.

2. Set the **Alert Conditions**

   When creating an alert profile action, you must first specify the alert conditions that must be met for the received alert to fit a specific alert profile. As alerts are received, the Alert Manager checks each of these conditions to see if they meet the specifications for a defined alert profile. If *all* alert conditions are met, the alert fits the alert profile. If an alert fits an alert profile, any actions that are bound to that profile will be executed. For instructions on how to bind alert actions to alert profiles, see “Binding Profiles to Actions” on page 38.

There are five alert conditions that are used by the Alert Manager to determine whether an alert fits an alert profile. For an alert to fit an alert profile, it must meet all of the alert conditions for the action. These five alert conditions are:

- Alert Type
- Severity
- Application ID
- Application Alert Type
- Sender ID

To specify the alert conditions for this alert profile:

a. Select an Alert Type.

   The Alert Type is a brief description of the generated alert. It describes the nature of the alert (unknown, failure, error, warning, information), and can also contain a general description of the source of the alert (system, disk, network, operating system, application, device, or security).

   To check incoming alerts for specific Alert Types, select one or more Alert Types from the selection list. If you do not want to check for specific Alert Types, select the **Any** check box above the selection list.

b. Select a Severity.

   The Severity is a number from 0 through 7 that indicates how serious a generated alert is. A severity of 0 represents a very serious alert, while a severity of 7 is relatively minor.

   To check incoming alerts for specific Severity values, select one or more Severity values from the selection list. If you do not want to screen for specific Severity values, select the **Any** check box above the selection list.

c. Select an Application ID.

   The Application ID is the alphanumeric identifier of the application that generated the alert.

To check incoming alerts for specific Application IDs, you can choose one or more from the Application ID selection list. If an Application ID that you require is not available from the list, you can add it to the list by typing the ID in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Application IDs, select the **Any** check box above the selection list.

d. Select an Application Alert Type.

   The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application itself.

   To check incoming alerts for specific Application Alert Types, you can choose one or more from the Application Alert Type selection list. If an Application Alert Type that you require is not available from the list, you can add it to the list by typing it in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Application Alert Types, select the **Any** check box above the selection list.

e. Select a Sender ID.

   The Sender ID is the network address of the system that generated the alert.

   To check incoming alerts for specific Sender IDs, you can choose one or more from the Sender ID selection list. If a Sender ID that you require is not available from the list, you can add it to the list by typing it in the entry field above the selection list and pressing **Enter**. If you do not want to check for specific Sender IDs, select the **Any** check box above the selection list.

3. Name the alert profile.

   This is the name that will appear in the Alert Profile window **Profile List** field. Type in the **Profile Name** field a name for the Alert Profile. This name can be up to 64 characters long.

4. Save the Alert Profile.

Select **Save** to save the Alert Profile. This Alert Profile will now appear in the Alert Profile window **Profile List** field.

Select **Cancel** to close this window without saving any alert profile information.

Editing Alert Profiles

To edit a previously defined alert profile:

1. Select from the **Profile List** the name of the alert profile you want to edit.
2. Select **Edit**.

   This opens the Profile Editor window (see Figure 6 on page 31).
3. Change alert conditions, if necessary.

   If you are editing this alert profile to alter the alert conditions that must be met for the received alert to fit the alert profile, select the appropriate new Alert Type, Severity, Application ID, Application Alert Type, or Sender ID values as necessary.
4. Change the profile name, if necessary.

   If you want to rename this alert profile, type in the **Profile Name** field the new profile name.
5. Save this alert profile.

   Select **Save** to save the changes you've made to this alert profile.

Select **Cancel** to close this window without changing any alert profile information.

Deleting Alert Profiles

To delete an alert profile, select an alert profile from the **Profile List** field, and then select **Delete**.

Predefined Alert Profiles

Alert Manager includes many predefined alert profiles. A list of predefined alert profiles that will be installed on *all* Netfinity systems, and a brief description nature of the alert-specific information that fits the profile, follows:

Profile Name **Alert Description**

Power-On Error Detect Error Alerts
POST error detected by Power-On Error Detect on a Netfinity system.

Power-On Error Detect Information Alerts
System Partition access during startup detected by Power-On Error Detect on a Netfinity system.

Predictive Failure Analysis Alerts
Imminent failure of a PFA-enabled hard disk drive reported by Predictive Failure Analysis.

File Changed Alerts
Critical File Monitor detected that a monitored file has been changed.

File Deleted Alerts Critical File Monitor detected that a monitored file has been deleted.

File Created Alerts Critical File Monitor detected that a monitored file has been created.

Process Terminated Alerts
Process Manager detected that a monitored process has ended.

Process Started Alerts
Process Manager detected that a monitored process has started.

Process Failed to Start Alerts
Process Manager detected that a monitored process has failed to start.

System Online Alerts
Remote System Manager has reported that a specific remote system is online and functional.

System Offline Alerts
Remote System Manager has reported that a specific remote system is offline or unreachable.

Access Granted Alerts
Security Manager allowed a remote user that provided a User ID/Password combination access to the system.

Public Access Granted Alerts
Security Manager has allowed a remote user Public access to the system.

System Access Denied Alerts
Security Manager has denied a remote user access to the system.

System Restart Initiated Alerts
Security Manager has detected and permitted a system restart request by a remote user.

System Restart Rejected Alerts
Security Manager has detected and rejected a system restart request by a remote user.

Service Start Request Alerts
Service Manager has allowed use of a Netfinity service by a remote user.

Service Start Rejected Alerts
Service Manager has denied use of a Netfinity service by a remote user.

Threshold Error Alerts
A System Monitor error threshold condition has been met.

Threshold Warning Alerts
A System Monitor warning threshold condition has been met.

Threshold Return to Normal Alerts
A previously registered System Monitor warning or error threshold condition has returned to normal.

Physical RAID Device Online Alerts
A physical RAID device attached to the system has changed state to **Online**.

Physical RAID Device Standby Alerts
A physical RAID device attached to the system has changed state to **Standby**.

Physical RAID Device Dead Alerts
A physical RAID device attached to the system has changed state to **Dead**.

Logical RAID Device Online Alerts
A logical RAID device attached to the system has changed state to **Online**.

Logical RAID Device Critical Alerts
A logical RAID device attached to the system has changed state to **Critical**.

Logical RAID Device Offline Alerts
A logical RAID device attached to the system has changed state to **Offline**.

Physical RAID Drive PFA Alerts
A physical RAID device attached to the system has reported the imminent failure of a PFA-enabled hard disk drive in the RAID array.

Severity 0 Alerts A severity 0 alert has been received.

Severity 1 Alerts A severity 1 alert has been received.

Severity 2 Alerts A severity 2 alert has been received.

Severity 3 Alerts A severity 3 alert has been received.

Severity 4 Alerts A severity 4 alert has been received.

Severity 5 Alerts A severity 5 alert has been received.

Severity 6 Alerts A severity 6 alert has been received.

Severity 7 Alerts A severity 7 alert has been received.

All Alerts An alert has been received.

Many additional alert profiles will be installed if your system uses specific software or communications products (such as Communications Manager or LAN Server).

To create new alert profiles, see "Creating New Alert Profiles" on page 31. To edit an existing alert profile, see "Editing Alert Profiles" on page 34.

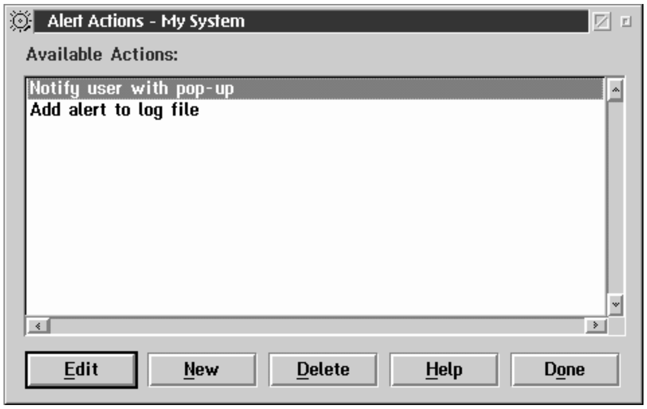
Binding Profiles to Actions

To enable Alert Manager to automatically respond to received alerts, you must bind alert profiles to alert actions. Once an alert profile is bound to an alert action, the alert action will be performed automatically whenever Alert Manager receives an alert that fits the profile. Multiple profiles can be bound to individual alert actions, and an individual alert profile can be bound to multiple alert actions.

To bind an alert profile to an alert action:

1. Select **Actions** from the Alert Log window.

   This opens the Alert Action window (see Figure 7 on page 39). This window contains a list of all currently configured alert actions.

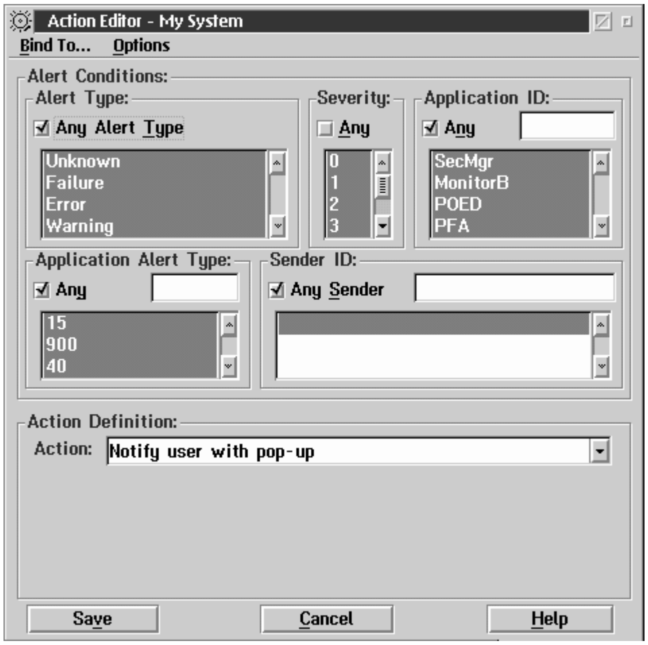


Notify user with pop-up
Add alert to log file

Figure 7. The Alert Actions window.

2. Select **New**.

   This opens the Action Editor window (see Figure 8).



Alert Type: ☑ Any Alert Type — Unknown, Failure, Error, Warning

Severity: □ Any — 0, 1, 2, 3

Application ID: ☑ Any — SecMgr, MonitorB, POED, PFA

Application Alert Type: ☑ Any — 15, 900, 40

Sender ID: ☑ Any Sender

Action: Notify user with pop-up

Figure 8. The Action Editor window.

3. Select **Profiles** from the **Bind To...** pull-down menu. This switches the Action Editor window to the Profiles view.

4. Bind one or more alert profiles to an alert action.

   To bind alert profiles to an alert action, you must first select the profiles that will trigger the action, and then select the alert action and provide any necessary defining information.

   a. Select one or more alert profiles to bind to an action.

      All currently available and unused alert profiles are listed in the **Other Profiles** field. Select one or more alert profiles from this list, and then select **Trigger By**. All selected profiles will then appear in the **Triggering Profiles** field. Received alerts that fit any of the profiles listed in the **Triggering Profiles** field will cause Alert Manager manager to perform an alert action.

      Note: To remove alert profiles from the **Triggering Profiles** field, select the profiles that you want to remove and then select **Do Not Trigger By**. Selected profiles are then moved to the **Other Profiles** field.

   b. Select an alert action.

      Use the spin buttons at the right of the **Action** field to see the available alert actions.

   c. Enter additional information, if necessary.

      Some alert actions will require you to provide additional information (to whom alerts should be sent, what command to execute, and so on). If additional information is required, the parameter will be displayed in the Action field group as <P#>, where # is the number of the parameter. An Action Definition parameter field appears for each required parameter, along with a brief description of the information that is required. Enter the necessary information in each field.

5. Label this action.

   Type in the **Action Label** field a brief description of this alert profile and alert action combination. This description can be up to 32 characters. When you finish binding the alert profiles and the alert action, the Action Label will appear before the name alert action in the **Available Actions** field in the Alert Actions window.

6. Finish binding the alert profiles to the selected alert action.

   Select **Save** to finish binding the alert profiles to the selected action. The Action Editor window will close, and the Action Label, followed by the name of the alert action that you selected, appears in the **Available Actions** field in the Alert Actions window.

Select **Cancel** to close this window without saving any information.

Binding Actions to Individual Alerts

To enable Alert Manager to automatically respond to individual alerts that are not part of a defined Alert Profile, you must bind the desired action to specific specific alert conditions. Once an alert profile is bound to specific alert conditions, the alert action will be performed automatically whenever Alert Manager receives an alert that contains **all** of the specified conditions.

Configuring an action is a two-step process. First, you must set the Alert Conditions that Alert Manager will look for. Then, you must set an Action Definition to define what action the Alert Manager will take in response to the received alert. Detailed descriptions of this process follow.

1. Select **Actions** from the Alert Log window.

   This opens the Alert Action window (see Figure 7 on page 39). This window contains a list of all currently configured alert actions.

2. Select **New** from the Alert Actions window.

   This opens the Action Editor window.

3. Select **Alert Conditions** from the **Bind To...** pull-down menu.

4. Set the **Alert Conditions**

   When defining an action, you must first specify the Alert Conditions that must be met for the Alert Manager to execute a defined action. As alerts are received, the Alert Manager checks each of these conditions to see if they meet the specifications for a defined action. If *all* Alert Conditions are met, the defined action is executed.

There are five Alert Conditions that are used by the Alert Manager to determine appropriate action responses. For an alert to trigger an action, the alert must meet all of the alert conditions for the action. These five alert conditions are:

- Alert Type
- Severity
- Application ID
- Application Alert Type
- Sender ID

To specify the **Alert Conditions**:

a. Select an Alert Type.

   The Alert Type is a brief description of the generated alert. It describes the nature of the alert (unknown, failure, error, warning, information), and can also contain a general description of the source of the alert (system, disk, network, operating system, application, device, or security).

   To screen incoming alerts for specific Alert Types, select one or more Alert Types from the selection list. If you do not want to screen for specific Alert Types, select the **Any** check box above the selection list.

b. Select a Severity.

   The Severity is a number from 0 through 7 that indicates how serious a generated alert is. A severity of 0 represents a very serious alert, while a severity of 7 is relatively minor.

   To screen incoming alerts for specific Severity values, select one or more Severity values from the selection list. If you do not want to screen for specific Severity values, select the **Any** check box above the selection list.

c. Select an Application ID.

   The Application ID is the alphanumeric identifier of the application that generated the alert.

   To screen incoming alerts for specific Application IDs, you can choose one or more from the Application ID selection list. If an Application ID that you require is not available from the list, you can add it to the list by entering the ID in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Application IDs, select the **Any** check box above the selection list.

d. Select an Application Alert Type.

   The Application Alert Type is a numeric value assigned to an individual alert by the application that generated it. This value is often used by the application itself.

   To screen incoming alerts for specific Application Alert Types, you can choose one or more from the Application Alert Type selection list. If an Application Alert Type that you require is not available from the list, you can add it to the list by entering it in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Application Alert Types, select the **Any** check box above the selection list.

e. Select a Sender ID.

   The Sender ID is the network address of the system that generated the alert.

   To screen incoming alerts for specific Sender IDs, you can choose one or more from the Sender ID selection list. If a

Sender ID that you require is not available from the list, you can add it to the list by entering it in the entry field above the selection list and pressing **Enter**. If you do not want to screen for specific Sender IDs, select the **Any** check box above the selection list.

5. Set an Action Definition.

   You must select a specific action, and supply any necessary information for the completion of the action.

   a. Select an Action.

      An action is a program that is executed in response to an alert that meets the Alert Conditions that you have specified. Use the spin buttons at the right of the **Action** field to see the available action handlers.

   b. Enter additional information, if necessary.

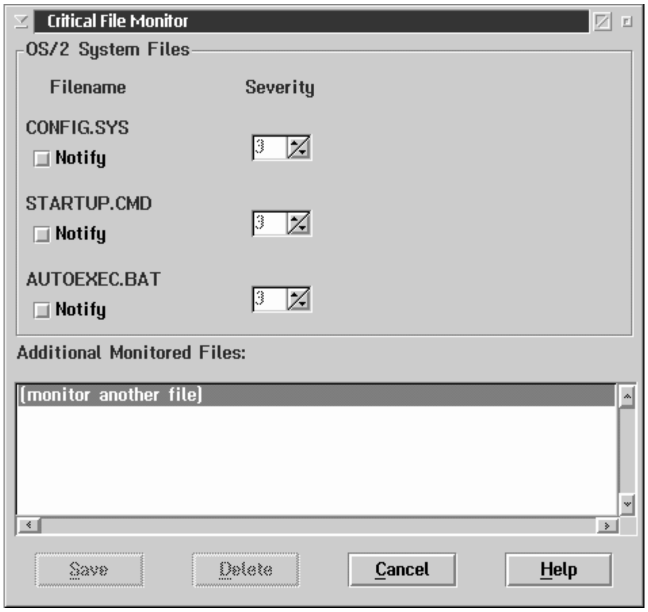
      If additional information is required, the parameter will be displayed in the **Action** field as <P#>, where # is the number of the parameter. An Action Definition parameter field appears for each required parameter, along with a brief description of the information that is required. Enter the appropriate information in each field.

6. Save the defined action.

   Once all Alert Conditions and Action Definition information has been entered, select **Save** to save the configured action. This action will now appear in the Available Actions field of the Alert Actions window. After you select **Save**, the Alert Manager window closes automatically.

Chapter 4. Critical File Monitor

Critical File Monitor can warn you whenever critical system files on the systems in your network are deleted or altered. The Critical File Monitor service makes it simple for you to generate Netfinity alerts when an important system file (such as the CONFIG.SYS file) changes date, time, size, is deleted (when it was present previously), or is created (when it was not present previously). Critical File Monitor can also be used to monitor any other files that reside on a Netfinity system.



Critical File Monitor

OS/2 System Files

Filename Severity

CONFIG.SYS
□ Notify 3

STARTUP.CMD
□ Notify 3

AUTOEXEC.BAT
□ Notify 3

Additional Monitored Files:

(monitor another file)

Figure 9. Critical File Monitor

Monitoring System Files

The system files that can be monitored by the Critical File Monitor are operating-system-specific. The name of the operating system that is in use by the system that you are accessing appears in the title area of the System Files field group. The names of the system files that can be monitored appear beside the check boxes.

Notes:

1. You can use Critical File Monitor to monitor *any* file on the system. The system files that appear at the top of the Critical File Monitor window are important files that you would be most likely to want to monitor. To monitor other files, see "Monitoring Other Files" on page 47.
2. Files located on network drives cannot be monitored.

OS/2 System Files

The OS/2 system files that appear in the System File field group are:

- CONFIG.SYS
- STARTUP.CMD
- AUTOEXEC.BAT

Windows 3.1, Windows for Workgroups, and Windows 95 System Files

The Windows system files that appear in the System File field group are:

- CONFIG.SYS
- AUTOEXEC.BAT
- WIN.INI
- SYSTEM.INI

Windows NT System Files

The Windows NT system files that appear in the System File field group are:

- WIN.INI
- SYSTEM.INI

NetWare System Files

The NetWare system files that appear in the System File field group are:

- AUTOEXEC.NCF
- STARTUP.NCF
- VOL$LOG.ERR
- SYS$LOG.ERR

To monitor one or more system files:

1. Select the system files that you want to monitor.

   Select the check boxes beside the names of the system files that you want to monitor. A check mark appears in the box.

2. Select a Severity.

   Each system file in the System File field group has a Severity field beside its name. Use the spin buttons to select a Severity value for each of the system files that you want to monitor. This severity value will be assigned to the Netfinity alert that will be generated if the system file is created, deleted, or changed. You can choose a severity value from 0 (most severe) to 7 (least severe).

3. Select **Save** to save the Critical File Monitor settings.

To close Critical File Monitor without saving any changes, select **Cancel**.

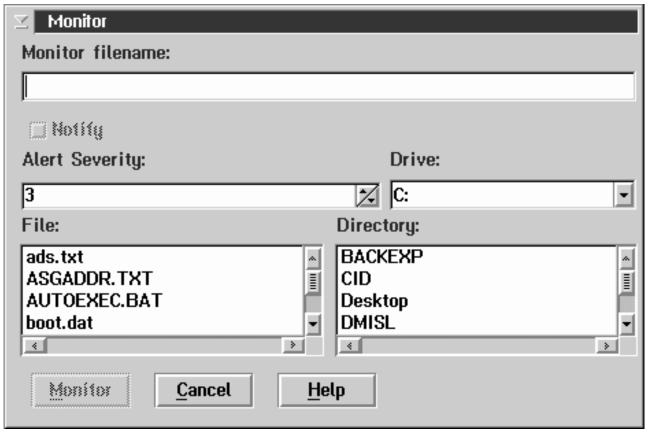
Monitoring Other Files

Critical File Monitor can monitor any file on the Netfinity system that you are accessing. The **Additional Monitored Files** field contains a list of all other files that are currently being monitored.

To select a file to monitor:

1. Select **(monitor another file)** from the **Additional Monitored Files** field (see Figure 9 on page 45).

   This will open the Monitor window (see Figure 10 on page 48).



Monitor

Monitor filename:

□ Notify

Alert Severity: 3

Drive: C:

File:
ads.txt
ASGADDR.TXT
AUTOEXEC.BAT
boot.dat

Directory:
BACKEXP
CID
Desktop
DMISL

Figure 10. Critical File Monitor — Monitor window

2. Select from the **Drive** list the drive letter that contains the file that you want to monitor.
3. Select from the **Directory** field the directory that contains the file that you want to monitor.
4. Select from the **File** list the name of the file that you want to monitor.
5. Use the spin buttons beside the **Severity** field to set the Severity of the alert that will be generated if the selected file is altered or deleted.
6. Select **Monitor** to initiate the monitoring process on the selected file.

To close the Critical File Monitor service without saving any changes, select **Cancel**.

Note: Critical File Monitor can be set to alert you if a specific file that does not exist on the system is created. For more information, see "Monitoring for File Creation" on page 49.

Monitoring for File Creation

Critical File Monitor can also generate alerts when specified files are created. To configure the Critical File Monitor to generate an alert in this case:

1. Select from the **Drive** field the letter of the disk drive that you want to monitor for file creation.
2. Type in the **Monitor Filename** field the fully qualified path and name of the file that you want to monitor.

   For example, if you want the Critical File Monitor to generate an alert if a file named ERROR.LOG appears in the directory named PROGRAM, you would type in the **Monitor Filename** field

   ```
   PROGRAM\ERROR.LOG
   ```
3. Use the spin buttons beside the **Severity** field to set the Severity of the alert that will be generated if the file is created.
4. Select **Monitor** to initiate the monitoring process on the specified file.

Chapter 5. DMI Browser

You can use the Netfinity Desktop Management Interface (DMI) Browser Service to examine information about the DMI-compliant hardware and software products (called *DMI components*) installed in or attached to the system.

You can use the DMI Browser to:

- View information about DMI components
- Receive notification of problems or errors with products from the DMI Service Layer
- View the log of problems or errors concerning DMI components

Notes:

1. This service is available only on systems that have the DMI Service Layer installed and operational. DMI Service Layers are available for most of the operating systems that are supported by Netfinity. If a DMI Service Layer is not installed and operational on your system when you install Netfinity, neither the DMI Browser nor the Netfinity-specific DMI components will be installed on your system. If you install a DMI Service Layer after you install Netfinity, you must reinstall Netfinity in order to install and use Netfinity's DMI Component Instrumentation.
2. The Netfinity DMI Browser service is a special version of the DMI Browser that comes with the DMI Service Layer. Some functions that are available with the DMI Browser are not available in Netfinity’s DMI Browser service.

What is DMI?

The Desktop Management Interface (DMI) is an industry standard that simplifies management of hardware and software products attached to, or installed in, a computer system. The computer system can be a standalone desktop system, a node on a network, or a network server. DMI is designed to work across desktop operating systems, environments, hardware platforms, and architectures.

DMI provides a way to provide or obtain, in a standardized format, information about hardware and software products. Once this data is obtained, desktop and network software applications can use that data to manage those computer products. As DMI technology evolves, installation and management of products in desktop computers will become easier, and desktop computers will become easier to manage in a network.

How Does DMI Work?

The complete DMI structure consists of three separate elements:

- DMI components
- DMI Service Layer
- DMI-compliant management applications

DMI Components

Each DMI component contains information about the product with which it is associated. This information is organized into product-specific groups. This information is contained in a Management Information File (*MIF*). The MIF describes the manageable attributes of the DMI component or product.

Each group contains a variety of group-specific attributes. The attributes that are found within a group are entirely dependent on the group itself. For example, the Component ID group for a software product might include the following attributes:

- Manufacturer
- Product
- Version
- Serial Number
- Installation
- Verify

However, the attributes found in the Processor group included in a PC system’s component might contain these attributes:

- Type
- Processor Family
- Version Information

- Maximum Speed
- Current Speed
- Processor Upgrade

Each of a group's attributes is fully defined by a series of data items. The items available for a group vary according to the type of product, but most attributes include the following data items:

ID
The attribute's **ID** is a sequential number unique to the attribute's group.

Type
The data **type** can be one of eight defined by DMI. These data types are:

- Integer
- 64-Bit Integer
- Counter
- 64-Bit Counter
- Gauge
- Display String
- Octet String
- Date

Access
The ways in which this attribute's data can be accessed. Access values can be:

- Read-Only
- Read-Write
- Write-Only

Note: Attributes that have Read-Write or Write-Only access values can have certain other attributes changed. For more information, see “Changing Attribute Information” on page 57.

Name
The **name** of the attribute is derived from DMI standards or is provided by the manufacturer.

Value
A **value** is a specific occurrence of an attribute. For example, an attribute value of 2.1 could be provided for the version number of an application. In a few cases, a value is read-only and will never change. The value can be specified directly in the MIF file. However, most values will change over time.

Updating usually occurs automatically, managed by programs supplied by the manufacturer of the component.

A value can also be an enumeration value (ENUM), indexing into a table of possible values defined in the MIF file.

Description The **description** of the component is technical information supplied by the manufacturer.

Netfinity DMI Component Instrumentation

The Netfinity DMI Component Instrumentation provides DMI-based management applications with information from Netfinity's Remote System Manager, System Monitors, and System Information Tool. The MIF files required by DMI-based management applications are installed as part of Netfinity's DMI Instrumentation when Netfinity is installed.

Notes:

1. If a DMI Service Layer is not installed and operational on your system when you install Netfinity, neither the DMI Browser nor the Netfinity-specific DMI components will be installed on your system.
2. DMI-based Netfinity data is available to other DMI-based application only when the Netfinity Support Program is running.

DMI Service Layer

The DMI Service Layer is a program that gathers and organizes the DMI component information into a standardized format. Once this data has been organized and is available, a DMI-compliant component agent (Netfinity’s DMI Browser service, for example) can access the DMI service layer and request information about any of the DMI components.

Note: Your system *must* have the DMI Service Layer installed and operational for Netfinity’s DMI Browser to function.

The DMI Service Layer gathers configuration information from the installed MIF files, builds a database, and, upon request, passes the information to management applications. Management applications are programs that are capable of receiving data from the DMI Service Layer and providing this data for desktop or network management purposes.

In addition to gathering and configuring the MIF data, the DMI Service Layer also collects information about problems or errors that the various DMI components have encountered. You can use the Netfinity DMI Browser to receive notification of problems or errors concerning your DMI components and to view a log of problems or errors concerning your DMI components.

The Netfinity DMI Browser works with the following DMI Service Layers:

Operating System	**Supported DMI Service Layer**
OS/2 Warp 3.0 or later	IBM SystemView Agent version 1.4.2 or later
Windows NT 3.51 with Service Pak 5 or later	IBM SystemView Agent version 1.3.2 for WIN32, Intel DMI Service Provider 2.0
Windows 95	IBM SystemView Agent version 1.3.2 for WIN32, Intel DMI Service Provider 2.0
Windows 3.1	Intel® DMI SDK version 2.0 or later

Management Applications

A management application is any DMI-compliant systems-management application that is capable of interfacing with the DMI Service Layer in order to gather and make use of the DMI component information.

Using the DMI Browser

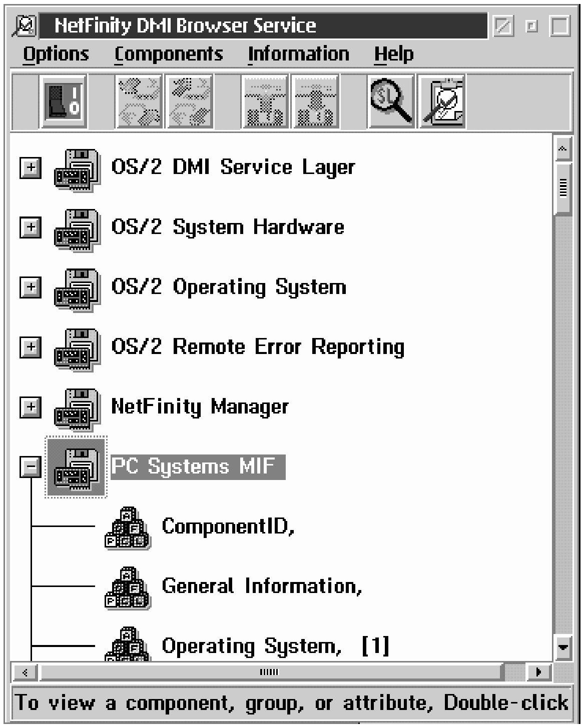
The Netfinity DMI Browser service enables you to:

- View information about DMI components, groups, and attributes of installed DMI-compliant products
- Receive notification of problems or errors with your products from the DMI Service Layer
- View the log of problems or errors concerning your DMI components

The DMI Browser functions can be accessed by selecting menu choices from the menu bar, or by selecting the function's corresponding objects from the fast-path icon bar.

The menu bar includes the following functions:

- Options: View the event log or exit the DMI Browser service.
- Information: Display version information for the Service Layer and copyright notices for the DMI Browser.



To view a component, group, or attribute, Double-click

Figure 11. The DMI Browser window

For quickest operation, use the mouse to select the menu bar icon that you want. The alternative is to select a menu choice and then select a choice from the menu that drops down. If you are unsure about the meaning of an icon, just move the mouse pointer over it. A brief explanation of the icon will appear at the bottom of the window.

Viewing DMI Component Information

Using mouse button 1, double-click on the DMI component that you want to open. This will open the Component Information window.

When you are finished, select **Close** to close the Component Information window.

Viewing Group Information

To view information about one of a DMI component's individual groups:

1. Using mouse button 1, click on the plus sign (+) beside the DMI component that contains the group data that you want to view.
2. Using mouse button 1, double-click on the name of the group that you want to view. This will open a window that contains a list of the group's attributes.

Viewing Attribute Information

To view information about one attribute of a single group:

1. Using mouse button 1, click on the plus sign (+) beside the DMI component that contains the group data that you want to view.
2. Using mouse button 1, double-click on the name of the group that you want to view. This will open a window that contains a list of the group's attributes.
3. Using mouse button 1, double-click on the name of the attribute that you want to view. This will open the Attribute Information window.

Changing Attribute Information

You can configure attributes that have Access values of *Read-Write* or *Write Only*. To change attribute information:

1. Using mouse button 1, double-click on the specific attribute that you want to change. This will open the Attribute information window.
2. Enter the new Attribute information. Note that not all Attribute information items can be changed.
3. Select **Apply** to change the attribute information.

If you decide not to make a change, select **Reset** to restore the attribute information to its last-saved value.

Select **Cancel** to close this window without saving any changes.

Receiving Notification of Problems or Errors

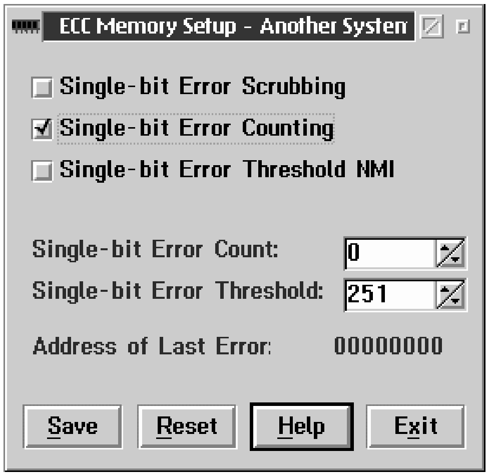
Upon request, the Service Layer notifies management applications of the occurrence of a problem or error. These problem and error messages are called *events.* The events are then stored in the Event Log, where they can be examined later to help rectify the problem or error.

The DMI Browser service automatically receives notification of DMI component events from the DMI Service Layer. If an event message is received by the DMI Browser service, a telephone object appears in the DMI Browser icon bar. Select the telephone icon (or select **View event log...** from the **Options** pull-down menu) to open the DMI Browser Event Log.

Chapter 6. ECC Memory Setup

You can use the Netfinity ECC Memory Setup to monitor and manage ECC memory. Options are:

- Single-Bit Error Scrubbing
- Single-Bit Error Counting
- Single-Bit Error Threshold Nonmaskable Interrupt (NMI)



ECC Memory Setup - Another System

□ Single-bit Error Scrubbing

☑ Single-bit Error Counting

□ Single-bit Error Threshold NMI

Single-bit Error Count: 0

Single-bit Error Threshold: 251

Address of Last Error: 00000000

Figure 12. ECC Memory Setup

To configure the ECC Memory Setup:

1. Select the actions that you want ECC Memory Setup to perform.

   - Activate the Single-Bit Error Scrubbing option to automatically correct any single-bit errors that might occur. Selecting this option might cause slight performance delays on some systems, but ensures greater data integrity. Check your system documentation for more information.

   - Activate the Single-Bit Error Counting option to keep a running count of all ECC memory errors that occur.

   - Activate the Single-Bit Error Threshold NMI option to cause a nonmaskable interrupt (NMI) if the number of single-bit errors exceeds the user-specified threshold.

     Note: If an NMI occurs, it might halt your system.

2. Change the Single-Bit Error Count, if desired.

   The **Single-Bit Error Count** field displays the number of single-bit errors that have been detected by the ECC Memory Setup during the current session.

   Note: The single-bit error count is for the current session *only*. The count is reset to 0 when the computer is restarted. To carry a count over from a previous session, you must enter the error count manually from the configuration screen.

3. Set a Single-Bit Error Threshold value if you have chosen the Single-Bit Error Threshold NMI option.

   The **Single-Bit Error Threshold** field displays the number of ECC single-bit errors that will be allowed before a nonmaskable interrupt (NMI) will be triggered.

   Note: An NMI will occur only if the Single-Bit Threshold NMI option is activated.

4. Select **Save** when you are satisfied with the selections you have made.

5. Select **Exit** when you have finished configuring ECC Memory Setup.

Chapter 7. Predictive Failure Analysis

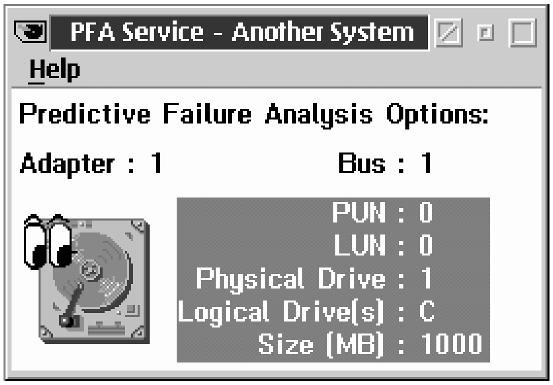
Use the Predictive Failure Analysis (PFA) service to monitor all PFA-enabled disk drives installed locally on your system. With this service, you will instantly be notified when a PFA-message is generated by a PFA-enabled drive. Also, you can configure this service to automatically generate a Netfinity Alert when a PFA message is received.

Note: PFA-messages generated by PFA-enabled disk drives that are in use as part of a RAID array **cannot** be detected by the Predictive Failure Analysis service. However, PFA-messages can be monitored and reported by using the System Monitor service's attribute monitors for the PFA-enabled disk drive. For more information, see "Attribute Monitors" on page 135.

The Predictive Failure Analysis Window

Each PFA-enabled physical drive is represented by an object in the Predictive Failure Analysis window. Predictive Failure Analysis service uses two objects to help you quickly determine the status of each disk drive. These objects are:

Object	**Description**
Solid disk drive	Normal: The drive has not reported any predictive failure analysis messages.
Shattered disk drive	Warning: The drive has reported one or more predictive failure analysis messages and might be failing.



Predictive Failure Analysis Options:

Adapter : 1 Bus : 1

PUN : 0
LUN : 0
Physical Drive : 1
Logical Drive(s) : C
Size (MB) : 1000

Figure 13. The Predictive Failure Analysis service. The PFA Drive shown represents a drive that has not reported any predictive failure analysis messages.

Information that will help you identify the drive is listed beside its icon. This information includes:

- Adapter

  The **Adapter** is the value of the adapter card that the disk drive is connected to.

  When Predictive Failure Analysis detects PFA-enabled hard disk drives in your system, it also scans your system for SCSI hard disk drive controllers. The **Adapter** value is the number of the SCSI adapter to which the PFA-enabled hard disk drive is attached. For example, if your system has two SCSI hard disk drive adapters installed, and each SCSI adapter has one PFA-enabled disk drive attached, you will two PFA-enabled disk drive objects in the PFA Service window. The first PFA-drive object would have an Adapter value of 1, because it is the first SCSI hard disk drive adapter detected by Predictive Failure Analysis. The second PFA-drive object would have an Adapter value of 2, because it is the second SCSI hard disk drive adapter detected by Predictive Failure Analysis.

- PUN and LUN

  The physical unit number (PUN) and logical unit number (LUN) are values assigned to the hard disk drive to uniquely identify it within a system.

Note: If an individual physical drive is partitioned into two or more logical drives, each logical drive will have the same PUN, LUN, and physical drive value.

- Physical Drive value

  The **Physical Drive** value is a numeric value assigned to each hard disk drive in your system. These values begin with 0 and increase with each additional hard disk drive installed (for example, if you have two hard drives in your system, their Physical Drive values will be 0 and 1).

- Logical Drive values

  The **Logical Drive** value is a letter assigned to each hard disk drive or partition you create on a hard disk drive. For example, if you have a 1 GB[*] drive, and you divide this drive into 5 partitions of 200 MB each, they will have **Logical Drive** values of C, D, E, F, and G. However, each **Logical Drive** will share the same PUN, LUN, and Physical Drive values.

- Size

  The **Size** value is the capacity of the physical drive.

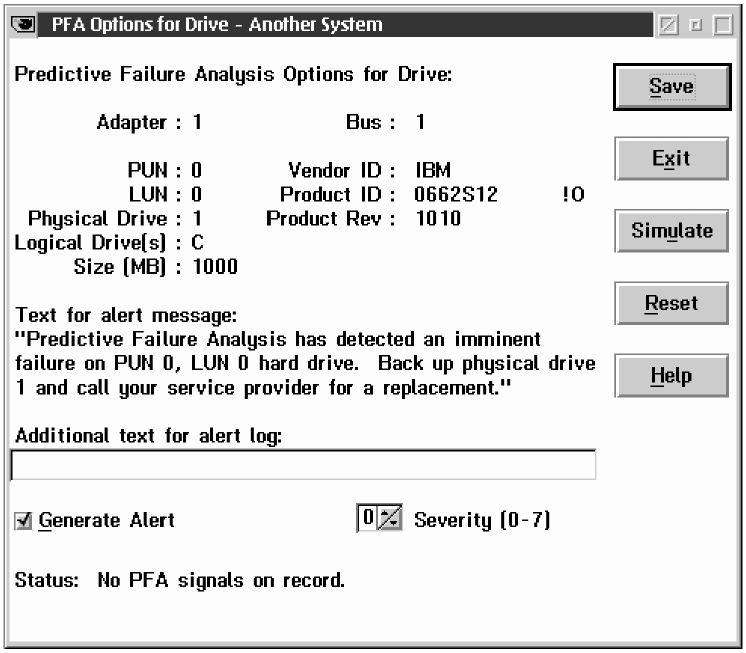
  Note: **Size** does *not* represent space remaining on the individual drive.

To obtain more detailed information on an individual PFA-enabled drive, or to configure Predictive Failure Analysis service options for an individual drive, select the drive from the Predictive Failure Analysis window. This will open the PFA Options for Drive window (see Figure 14 on page 64).

The PFA Options for Drive Window

Use the PFA Options for Drive window to view additional information about the selected PFA-enabled drive, and to configure Predictive Failure Analysis service options specific to the selected drive.

[*] When referring to hard-disk-drive capacity, GB means 1 000 000 000 bytes; total user-accessible capacity may vary depending on operating environment.



Predictive Failure Analysis Options for Drive:

```
        Adapter : 1              Bus :  1

            PUN : 0        Vendor ID :  IBM
            LUN : 0       Product ID :  0662S12       !O
 Physical Drive : 1      Product Rev :  1010
Logical Drive(s) : C
      Size (MB) : 1000
```

Text for alert message:
"Predictive Failure Analysis has detected an imminent failure on PUN 0, LUN 0 hard drive. Back up physical drive 1 and call your service provider for a replacement."

Additional text for alert log:

☑ Generate Alert   0 Severity (0-7)

Status: No PFA signals on record.

Figure 14. The PFA Options for Drive window

Detailed Disk Drive Information

The PFA Options for Drive window duplicates the drive-specific information from the Predictive Failure Analysis window, and also provides the following additional information:

- Vendor ID

  The Vendor ID is the name of the drive manufacturer reported by the disk drive.

- Product ID

  The Product ID is the drive-specific product number reported by the disk drive.

- Product Revision

  The Product Revision is the product revision level reported by the disk drive.

- Status

  The Status shows the most recent information reported by the disk drive. If a PFA message has been generated by the disk drive, the Status data will show the day, date, and time at which the PFA message was generated.

Predictive Failure Analysis Options

In addition to providing detailed drive information, the PFA Options for Drive window enables you to:

- Configure Predictive Failure Analysis' alert generation options for this drive.
- Simulate a Predictive Failure Analysis warning message for this drive.
- Reset the drive from "Warning" status to "Normal" status.

Generating Alerts

Select the **Generate Alert** check box to enable Predictive Failure Analysis to generate a Netfinity alert whenever this disk drive generates a Predictive Failure Analysis message. You can customize some of the alert-specific information.

- Alert Text

  The standard Alert Text that will appear in the generated alert appears in the center of the window. If you would like to add information to this text, type it in the **Additional text for alert log** field.

- Severity

  Use the spin buttons beside the **Severity** field to set the alert severity value. This value can be an integer from 0 (most severe) to 7 (least severe).

Simulating a Predictive Failure Analysis Message

To simulate a Predictive Failure Analysis failure warning message for this drive, select **Simulate**. The Predictive Failure Analysis service will behave exactly as if an actual warning message had been received (it will change the drive status in the Predictive Failure Analysis window and in the PFA Options for Drive window, and will generate an alert if **Alert Generation** is selected). However, both the Status reported in the PFA Options for Drive window and the Alert Text will state that the PFA message was simulated and was not caused by a real PFA message.

Resetting a Drive's Status

Select **Reset** to change the drive's status from "Warning" to "Normal."

Chapter 8. RAID Manager

RAID (*redundant array of independent disks*) is a technology whereby several physical storage devices are grouped into an array that appears to the operating system as one or more physical drives. Using RAID technology, you can configure the RAID array drives into a variety of data configurations. These configurations (called *RAID levels*) provide varying levels of data-integrity protection and storage capacity. Some RAID levels provide greater data integrity through the use of data mirroring.

Ordinarily, you must take your RAID system offline in order to perform most RAID management tasks. However, with Netfinity's RAID Manager service, you can easily gather information about your system's RAID adapter, physical drives in the array, and virtual drives that are defined by the array. You can also perform a variety of important RAID management tasks quickly and easily. These tasks include:

- Scrubbing virtual drives
- Formatting and rebuilding RAID physical devices
- Gathering data about all RAID adapters, devices, virtual drives, and enclosures

Notes:

1. Irresponsible use of RAID Manager can seriously harm your system and its data. Use RAID Manager only if you are familiar with RAID arrays and RAID systems management.

2. RAID Manager is not designed to operate simultaneously with other RAID management utilities. Running other RAID management utilities while running RAID Manager may cause your system to become unstable.

3. This service is available for use only on systems that have a supported RAID adapter installed. For a list of supported RAID adapters, see Appendix C, "Supported RAID Adapters" on page 152.

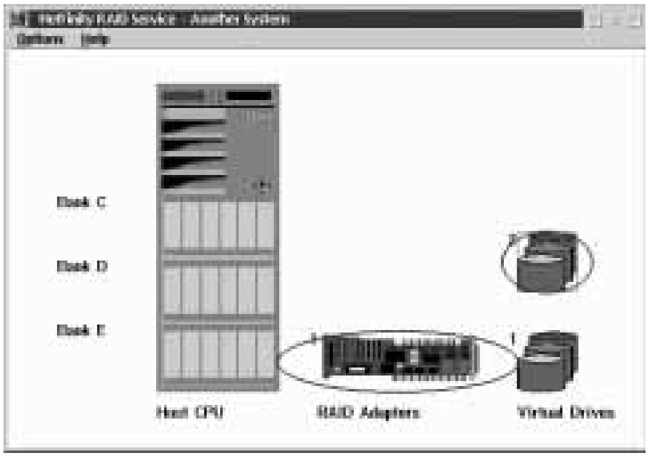


Figure 15. The RAID Manager service

RAID Manager Window Options

The RAID Manager window shows a graphical representation of your RAID system enclosure, RAID adapters, and logical disk drives. You can:

- Change the scale of the graphical representations
- Change the number of virtual drives that are shown in each column
- Change the enclosure configuration
- Refresh the current information

Changing the Viewing Scale

To change the scale of the graphics shown in the RAID Manager window:

1. Select **Viewing Scale** from the Options pull-down menu.
2. Use the spin buttons to select a scale for the RAID Manager graphics.
3. Select **OK** to apply this change.

The RAID Manager graphics are resized according to the scale you have specified.

Changing the Virtual Drives Representation

To change the number of virtual drives shown per column:

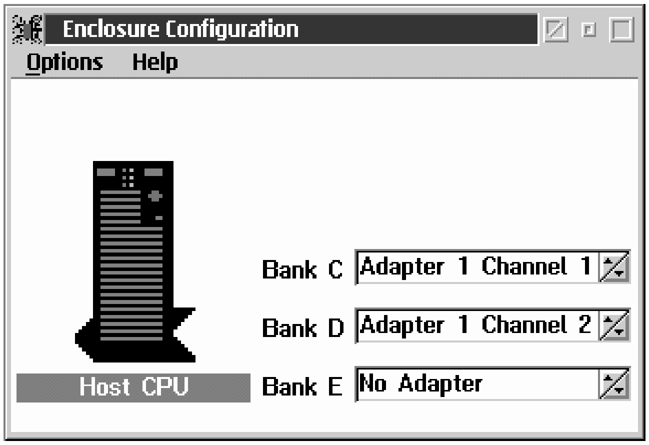
1. Select **Virtual Drive Representation** from the Options pull-down menu.
2. Use the spin buttons to select the number of virtual drives that will be shown in each column.
3. Select **OK** to apply this change.

The number of virtual drives in each column will be adjusted according to the value you selected.

Changing the Enclosure Configuration

Select **Enclosure Configuration** from the Options pull-down menu to open the Enclosure Configuration window (see Figure 16 on page 70). From this window, you can:

- Add an enclosure
- Delete an enclosure
- Configure the bank and adapter configuration for your enclosures
- Configure the device numbers for each bank in your enclosures



Bank C Adapter 1 Channel 1

Bank D Adapter 1 Channel 2

Bank E No Adapter

Figure 16. The Enclosure Configuration window

Adding an Enclosure

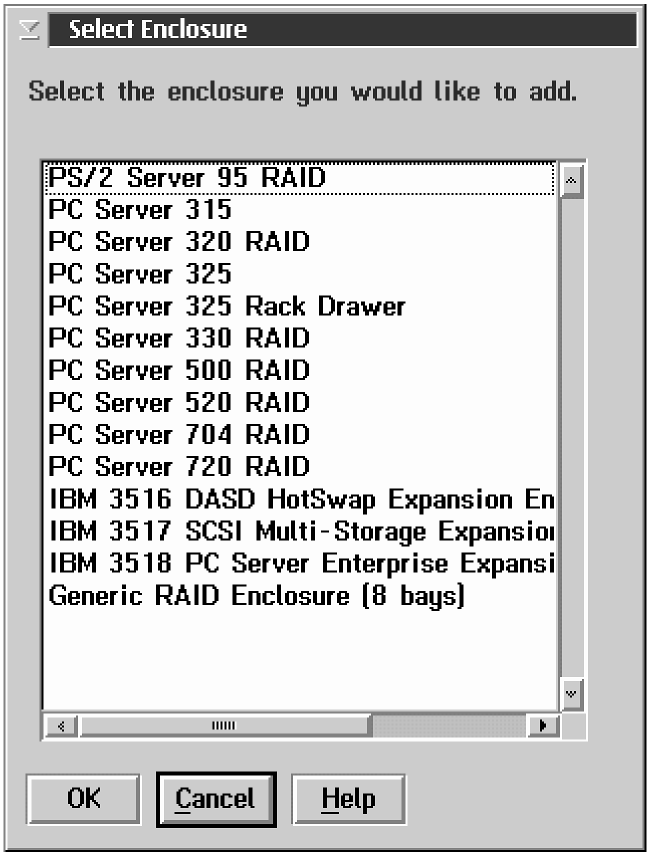
To add an enclosure:

1. Select **Enclosure Configuration** from the Options pull-down menu in the RAID Manager window.

   This opens the Enclosure Configuration window.

2. Select **Add Enclosure** from the Options pull-down menu in the Enclosure Configuration window.

   This opens the Select Enclosure window (see Figure 17 on page 71).



Select Enclosure

Select the enclosure you would like to add.

PS/2 Server 95 RAID
PC Server 315
PC Server 320 RAID
PC Server 325
PC Server 325 Rack Drawer
PC Server 330 RAID
PC Server 500 RAID
PC Server 520 RAID
PC Server 704 RAID
PC Server 720 RAID
IBM 3516 DASD HotSwap Expansion En
IBM 3517 SCSI Multi-Storage Expansio
IBM 3518 PC Server Enterprise Expansi
Generic RAID Enclosure (8 bays)

Figure 17. The Select Enclosure window

3. Select the name of the enclosure you want to add.

4. Select **OK**.

Deleting an Enclosure

To delete an enclosure:

1. Select **Enclosure Configuration** from the Options pull-down menu in the RAID Manager window.

   This opens the Enclosure Configuration window.

2. Using mouse button 2, select the enclosure that you want to delete.

This opens a context menu for the elected enclosure.

3. Select **Delete Enclosure** from the context menu.

Configuring RAID

To specify which RAID adapter controls which bank of RAID drives in your enclosure:

1. Select **Enclosure Configuration** from the Options pull-down menu in the RAID Manager window.

   This opens the Enclosure Configuration window.

2. Use the spin buttons beside each **Bank** field to specify which adapter and channel controls the bank.
3. When you have finished configuring the enclosure bank, close the Enclosure Configuration window to save your new settings.

Configuring RAID Bank Device Numbers

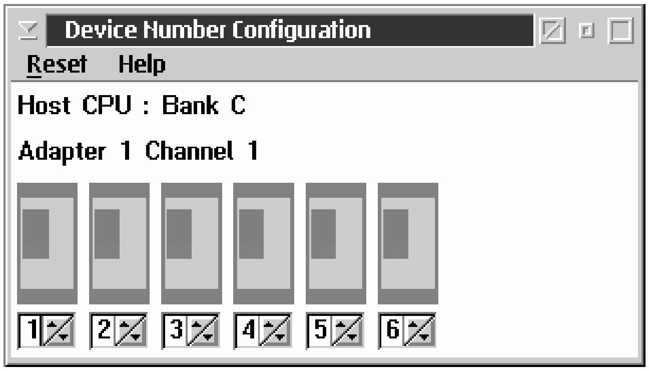
To specify the device numbers for each RAID device in a selected bank:

1. Select **Enclosure Configuration** from the Options pull-down menu in the RAID Manager window.

   This opens the Enclosure Configuration window.

2. Select the **Bank** field for the bank that contains the devices for which you want to specify a device number configuration.
3. Select **Configure Device Numbers** from the Options pull-down menu.

   This opens the Device Number Configuration window (see Figure 18 on page 73).



Host CPU : Bank C

Adapter 1 Channel 1

Figure 18. The Device Number Configuration window

4. Use the spin buttons associated with each device in the bank to specify a device number for that device.
5. When you have finished configuring the device numbers, close the Device Number Configuration window to save your new settings.

Refreshing RAID Information

Select **Refresh** from the Options pull-down menu to update all information displayed in the RAID Manager window.

Viewing RAID Information

You can use RAID Manager to view general information on your RAID system's devices, including the RAID enclosure, physical RAID devices, RAID adapters, and logical RAID drives.

Viewing Enclosure Information

Use RAID Manager to quickly gather information about any RAID enclosures attached to this system. Available information includes:

- Enclosure model
- Enclosure manufacturer
- Number of RAID adapters
- Enclosure function

To view information about a RAID enclosure:

1. Use mouse button 2 to select the enclosure that you want to examine. This opens the enclosure's context menu.
2. Select **View Enclosure** from the enclosure's context menu.

Select **OK** to close the Enclosure Information window.

Viewing Physical Device Information

Use RAID Manager to gather a variety of information about the physical devices that are part of your RAID array. Available information includes:

- Device status
- Device number
- Channel number
- Device type
- Device size
- Sectors
- Manufacturer
- Model, version
- Serial number

To view information about a physical RAID device:

1. Use mouse button 2 to select the device that you want to examine. This opens the adapter's context menu.
2. Select **View Device** from the device's context menu.

Select **OK** to close the Standard Device Information window.

Viewing General Adapter Information

Use RAID Manager to quickly gather information about any installed RAID adapters. Available information includes:

- Adapter identifier
- Slot
- Buses available
- Configured devices
- Device I/O
- Host bus

- Adapter status
- Manufacturer
- Model
- Serial number (if available)

To view information about a RAID adapter:

1. Use mouse button 2 to select the adapter that you want to examine. This opens the adapter's context menu.
2. Select **View Adapter**.
3. Select **General Info**.

Select **OK** to close the Adapter Information window.

Viewing Adapter-Specific Information

Use RAID Manager to quickly gather more detailed information about any installed RAID adapters. Available adapter-specific information includes:

- Stripe size
- Rebuild control
- Parity storage
- Read Ahead

To view adapter-specific information:

1. Use mouse button 2 to select the adapter that you want to examine. This opens the adapter's context menu.
2. Select **View Adapter**.
3. Select **Specific Info**.

Select **OK** to close the Adapter-Specific Information window.

Viewing Virtual Drive Information

Use RAID Manager to quickly gather information about any virtual drives defined by your RAID adapters. Available information includes:

- Virtual drive number
- Virtual drive size

- Virtual drive status
- Virtual drive RAID level
- Virtual drive write policy

To view information about a virtual drive:

1. Use mouse button 2 to select the virtual drive that you want to examine. This opens the virtual drive's context menu.
2. Select **View Virtual Drive Information**.

Select **OK** to close the Virtual Drive Information window.

RAID Device Management

Use RAID Manager to manage the storage devices that make up your RAID array. Use RAID Manager to:

- Add a device
- Remove a device
- Replace a device
- Rebuild a device
- Rebuild to another device
- Stop a device
- Set a device to standby
- Set a device to Hot Spare

To perform any of these RAID device management functions, use mouse button 2 to select the RAID device from the RAID Manager window, and then select the RAID Management function from the selected device's pop-up menu.

RAID Adapter Configuration Backup

You can use RAID Manager to back up the configuration of your RAID adapter. To back up your RAID adapter configuration:

1. Use mouse button 2 to select the adapter you want to back up.
2. Select **Backup Configuration** from the adapter's context menu.
3. Insert a blank, formatted diskette and select **OK**.

RAID Virtual Drive Management

Use RAID Manager to alter a variety of virtual drive parameters. The following logical drive management options are available:

- Initialize virtual drives
- Scrub virtual drives

Initializing Virtual Drives

Select **Initialize** to write binary zeroes to all bits on the logical drive and recompute proper parity information. This operation is required for RAID Level 1 and RAID LEvel 5 virtual drives.

Note: This feature is not available on RAID systems running NetWare.

Scrubbing Virtual Drives

Select **Scrub** to recompute the parity information on a RAID Level 1 or RAID Level 5 virtual drive. The data on the drive is not changed.

Chapter 9. Security Manager

The Netfinity Security Manager is designed to limit remote access to some or all of the Netfinity services installed on your system. Irresponsible or careless use of the Netfinity services can lead to data loss or system damage. To avoid this, you might want to limit remote access to some or all of these services on your system.

Note: The following Netfinity services pose the most potential risk if used irresponsibly:

- Remote System Manager
- System Partition Access
- File Transfer
- Remote Session
- Process Manager
- RAID Manager

These services are not available for use with Client Services for Netfinity Manager, and therefore instructions on how to use these services do not appear in this book. However, a remote Netfinity Manager can use these services when accessing your system.

The Netfinity Security Manager uses a User ID/Password combination to determine security clearance on a system. Incoming User ID/Password combinations determine which of your Netfinity services are available to a remote user that is using Netfinity Manager to access your system.

Security Manager features a default incoming User ID/Password feature. It is called the <PUBLIC> setting, and automatically allows access to any services that you select. For more information on the <PUBLIC> incoming User ID/Password, see “Setting Incoming User ID/Password Combinations” on page 79.

Once you have established incoming and outgoing User ID/Password combinations on your system, security operates passively. When a remote user uses Netfinity Manager to attempt to gain access to your system, the remote user’s outgoing User ID/Password combination is automatically checked against any incoming User ID/Password combinations you have configured. If the outgoing and incoming User ID / Password combinations match, the remote user is granted access to your system.

Netfinity Security Manager generates alerts to help you maintain a record of who has accessed or attempted to access your system. For more information on the alerts generated by the Security Manager, see "Security Alerts" on page 82.

Setting Incoming User ID/Password Combinations

If the Security Manager has not been preconfigured, there will be a User ID called <PUBLIC>. This is a general-security-access default setting. It allows any system using the <default> outgoing User ID / Password combination to access all Netfinity services on your system.

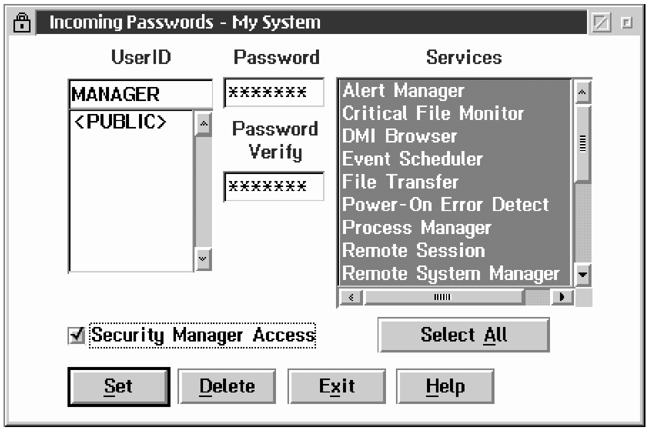
If a remote system user attempts to use the Remote System Manager Login System action to access your system and fails to match a corresponding incoming User ID / Password combination, the user will be given access to any services in your <PUBLIC> configuration.

Initially, *all* Netfinity services are available for <PUBLIC> access. To edit the list of services available from the <PUBLIC> User ID / Password combination:

1. Double-click on **Edit/Display Incoming Passwords** to open the Incoming Passwords window.
2. Select <PUBLIC> from the User ID selection list.
3. Deselect the services you do not want available for public access.
4. Deselect the **Security Manager Access** check box to restrict public access to Security Manager.
5. Select **Set** to save your configuration.

Note: If you do not have a <PUBLIC> default configured as part of your incoming User ID / Password security configuration, only users with valid outgoing User ID / Password combinations will be able to access the Netfinity services on your system.

If an invalid User ID / Password combination is used when a user attempts to access your system, an alert is generated by the Security Manager. However, if you maintain a <PUBLIC> default on your system, users who attempt to access your system using an invalid outgoing User ID / Password combination will automatically be granted access to your <PUBLIC> services. This will also generate an alert. For more information on alerts generated by the Security Manager, see “Security Alerts” on page 82.



UserID: MANAGER

<PUBLIC>

Password: *******

Password Verify: *******

Services:
- Alert Manager
- Critical File Monitor
- DMI Browser
- Event Scheduler
- File Transfer
- Power-On Error Detect
- Process Manager
- Remote Session
- Remote System Manager

☑ Security Manager Access

Figure 19. Incoming User ID/Password Configuration

To set a new incoming User ID / Password combination, and determine access to services:

1. Start Security Manager.
2. Select **Edit/Display Incoming Passwords**.
3. Enter a User ID.

   Enter the User ID that you are allowing access. You may select an ID from the User ID selection list, or enter a new ID in the entry field.

4. Enter a password.

Type in the **Password** field a password that, when used in combination with the User ID you have specified, will allow access to all selected Netfinity services. The password must be from 1 to 8 characters in length. This password will not be displayed.

5. Verify the password.

   Type in the **Password Verify** field the same password that you typed in the **Password** field. These two passwords **must** match to successfully create an incoming User ID / Password combination.

6. Select the accessible services.

   Select one or more services from the Services selection list. The selected services will be available to users who provide the User ID and password you have entered in the corresponding fields.

7. Determine access to the Security Manager.

   Select the **Security Manager Access** check box to allow access to your Security Manager.

   Note: Allowing access to the Security Manager enables the remote system to alter your incoming and outgoing User ID / Password combinations, and will also enable the Remote System Manager's Restart System action on your system. This will enable the remote user to restart your system on demand.

8. Save your incoming security configuration

   Select **Set** to save your configuration.

Deleting an Incoming User ID/Password Combination

To delete a previously set User ID / Password combination:

1. Start Security Manager.
2. Select **Edit/Display Incoming Passwords**.
3. Select the User ID you want to delete.

4. Select **Delete**. The User ID and its corresponding password are then deleted from your incoming User ID/Password combination configuration.

Security Alerts

Security Manager automatically generates a variety of alerts in response to access attempts. These alerts are provided to aid you in tracking which users are accessing what systems, as well as to provide a record of users who have attempted to access others systems using invalid User ID/Password combinations. Alerts are also generated when a remote Netfinity Manager attempts (successfully or unsuccessfully) to use Remote System Manager's System Restart action to restart your system.

These alerts are received by the Netfinity Alert Manager, which can then be configured to take specific actions in response to these alerts. For more information on alerts, see "The Alert Log" on page 12.

Each of the alerts generated by Security Manager contains additional macro parameter strings imbedded in the alert's Alert Text. These parameter strings are described beneath each alert's description.

Security Access Alerts

The Security Manager can generate three alerts in response to specific security access conditions. These alerts are:

- Access Granted Alert

  Generated when Security Manager allows non-public access to a remote user.
- Public Access Granted Alert

  Generated when Security Manager allows public access to one or more services to a remote user.
- System Access Denied Alert

  Generated when Security Manager denies access to the system to a remote user.

Detailed descriptions of the contents of each of these alerts follows.

Access Granted Alert

Explanation	Generated by the Security Manager service when access to one or more services is granted to a remote user that has used a UserID/Password combination to gain access.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been granted system access
Type of Alert	Security Information
Severity	7
Application ID	SecMgr
Application Alert Type	20

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

If you have not altered the default configuration for your Alert Manager, this alert will not trigger an action. However, you can create a new action response to this specific alert.

Public Access Granted Alert

Explanation	Generated by the Security Manager service when **Public** access to one or more services is granted to a remote user.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been granted public system access
Type of Alert	Security Information
Severity	6

Application ID	SecMgr
Application Alert Type	21

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

If you have not altered the default configuration for the Alert Manager, this alert will not trigger an action. However, you can create a new action response to this specific alert.

System Access Denied Alert

Explanation Generated by the Security Manager service when access to the system is denied to a remote user.

Alert Text Logon attempt by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been rejected

Type of Alert	Security Warning
Severity	5
Application ID	SecMgr
Application Alert Type	22

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

If you have not altered the default configuration for the Alert Manager, this alert will be added to the Alert Manager's log file. You can create additional action responses to this specific alert.

System Restart Alerts

The Security Manager can generate two alerts in response to System Restart attempts. These alerts are:

- System Restart Initiated Alert
- System Restart Request Rejected Alert

Detailed descriptions of the contents of each of these alerts follows.

System Restart Initiated Alert

Explanation Generated by the Security Manager service when a remote Netfinity Manager uses the Remote System Manager's Restart System option to restart your system.

Alert Text System Restart initiated by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*'.

Type of Alert Security Information

Severity 5

Application ID SecMgr

Application Alert Type 41

Note: This alert supports the following macro parameter strings:

%P1 User ID requesting system restart

%P2 Network Address of system requesting restart

%P3 Network Type of system requesting restart

If you have not altered the default configuration for the Alert Manager, this alert will be added to the Alert Manager's log file. You can create additional action responses to this specific alert.

System Restart Request Rejected Alert

Explanation Generated by the Security Manager service when a remote Netfinity Manager attempts to use the Remote System Manager's Restart System option to

	restart your system, but does not have adequate security access to do so.
Alert Text	System Restart request by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' rejected rejected.
Type of Alert	Security Error
Severity	3
Application ID	SecMgr
Application Alert Type	40

Note: This alert supports the following macro parameter strings:

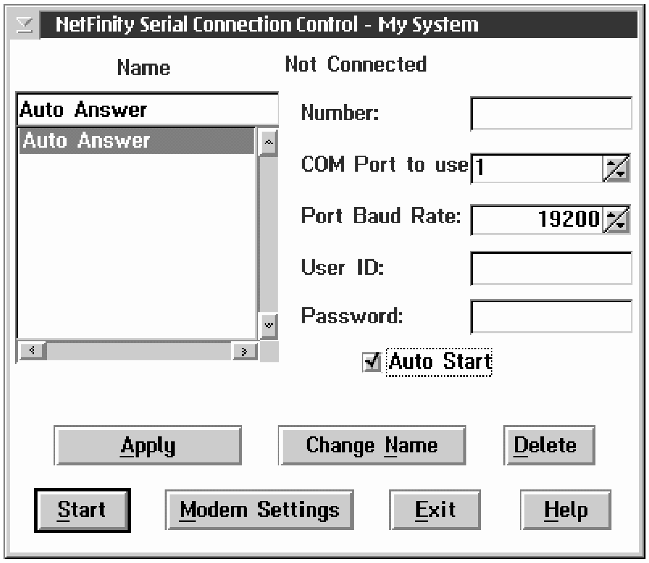
%P1	User ID requesting system restart
%P2	Network Address of system requesting restart
%P3	Network Type of system requesting restart

If you have not altered the default configuration for the Alert Manager, this alert will be added to the Alert Manager's log file **and** will generate a pop-up window notifying you of the System Restart attempt. You can create additional action responses to this specific alert.

Chapter 10. Serial Connection Control

The Netfinity Serial Connection Control service enables a Netfinity Manager to access and manage your system by dialing in to your system's modem. Once properly configured, the Serial Connection Control service will enable remote Netfinity Manager users to access and manage your system just as if they were attached to a LAN.

Note: Your system *must* have a properly installed and configured modem that supports at least 9600 baud for the Serial Connection Control service to function.


NetFinity Serial Connection Control - My System

Name: Auto Answer

Not Connected

Number:

COM Port to use: 1

Port Baud Rate: 19200

User ID:

Password:

☑ Auto Start

Figure 20. The Serial Connection Control service

Modem Configuration

Before you can use the Serial Connection Control service to enable remote access of your system through your modem, you must ensure that your modem is properly configured.

To configure your system's modem:

1. Select **Modem Settings** from the Serial Connection Control window.

This will open the Netfinity Modem Settings window (see Figure 21 on page 88).

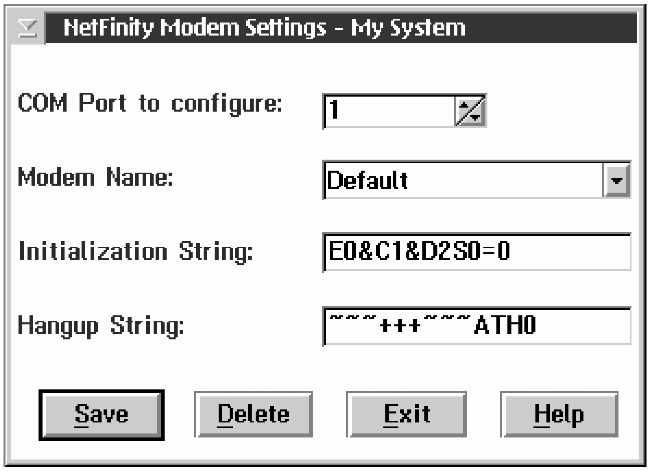
2. Select the **COM Port** for the modem that you are configuring.

   Use the spin buttons beside the **COM Port** field to select the modem's COM port.

3. Select a **Modem Name**, or type in a new one.

   Select from the **Modem Name** field the name of your system's modem, or type in a new one. Netfinity comes preconfigured with settings for some popular modem types. However, if your modem is not listed in the **Modem Name** field, or if you do not know what kind of modem your system has, select **Default**. If your modem does not function properly when using the **Default** settings, see "Initialization String Guidelines" on page 90.

   Note: Selecting a preconfigured Modem Name or **Default** will automatically fill in the other modem configuration information.



COM Port to configure: 1

Modem Name: Default

Initialization String: E0&C1&D2S0=0

Hangup String: ~~~+++~~~ATH0

Figure 21. Serial Connection Control — The Netfinity Modem Settings window

4. Type in the proper **Initialization String** for your system's modem.

If you selected one of the preconfigured Modem Names, this field will be filled in for you. However, you might need to edit this field if Netfinity did not come with preconfigured settings for your modem. If you need more information, see "Initialization String Guidelines" on page 90.

5. Type in the proper **Hangup String** for your system's modem.

   The **Hangup String** field contains the command that will be sent to the modem to instruct it to close the connection to the phone line. A default hangup string is provided by Serial Connection Control. This string will function properly on most modems. If your modem does not respond correctly to the default hangup string, see the documentation that came with your modem for more information.

6. Select **Add/Change/Use** to save these settings and enable this modem to be used by the Serial Connection Control service.

Enabling Remote Access

Once you have configured your modem for use with Serial Connection Control, you must grant access to your system to your network administrator or other authorized users. Authorized users can then use Serial Connection Control to access your system. To grant access to your system:

1. Set the Serial Connection Control service to AutoAnswer mode.
2. Use Security Manager to configure a User ID / Password combination for the authorized user to use when logging on to your system.

For information on how to configure a User ID / Password combination to enable remote access to your system, see "Setting Incoming User ID / Password Combinations" on page 79.

To set the Serial Connection Control service to AutoAnswer mode:

1. Start the Netfinity Serial Connection Control service.

   Open the Serial Connection Control object.

2. Select **AutoAnswer** from the Serial Connection Control window's **Name** field.

The AutoAnswer setting will enable the Serial Connection Control service to automatically answer incoming phone calls through the modem. Once it has answered the telephone, it will attempt to establish a link with the calling system.

3. Set the Serial Connection Control User ID and Password.

   Type in the **User ID** and **Password** fields the user ID and password that a remote system, using Serial Connection Control, must provide in order to gain access to your system using Serial Connection Control.

4. Select **Start**.

   Once you select **Start**, the Serial Connection Control service will begin waiting for an incoming call. Once "Waiting for call" appears in the Serial Connection Control window status field, you can select **Exit**. Serial Connection Control will continue to wait in the background for incoming calls.

   Note: If you want the Serial Connection Control service to automatically start and begin waiting for incoming calls when Netfinity is started, select **AutoAnswer**, and then select the **Auto Start** check box.

Initialization String Guidelines

Although most modems share similar initialization string codes, there are differences from modem to modem. Therefore, it is very difficult to provide appropriate initialization strings for *all* modems. In some cases you might need to create your own initialization string for your modem. If you do, consult the documentation that comes with your modem for the appropriate initialization string codes.

- Required Initialization Codes

  For a modem to operate correctly with the Netfinity Serial Connection Control service, the initialization string must configure the modem as follows:

  - Command echoing OFF
  - Online character echoing OFF
  - Result codes ENABLED

  - Verbal result codes ENABLED
  - All codes and connect messages with BUSY and DT detection
  - Protocol ind added - LAPM / MNP / NONE V42bis / MNP5
  - Normal CD operations
  - DTR ON-OFF hangup, disable AA and return to command mode
  - CTS hardware flow control
  - RTS control of received data to computer
  - Queued and nondestructive break, no escape state
  - Auto-answer off

  Example: The initialization string for a U.S. Robotics Sportster modem using only the settings required for correct operation would be:

  ```
  E0F1Q0V1X4&A3&C1&D2&H1&R2&Y3S0=0
  ```

- Additional Initialization Codes

  In addition to the required initialization codes, you can optimize the operation of the Netfinity Serial Connection Control service by configuring your modem with the following settings:

  - Speaker ON until carrier detected
  - Software flow control disabled
  - Auto-error control
  - Variable data rate

  Example: The initialization string for a U.S. Robotics Sportster modem using all the required and additional settings would be:

  ```
  E0F1M1Q0V1X4&A3&C1&D2&H1&I0&K1&M4&
  N0&R2&Y3S0=0
  ```

Chapter 11. Software Inventory

You can use Software Inventory to quickly and easily scan any Netfinity system for the presence of installed software products. Its flexible scanning methods can be used to search for specific products, types of products (for example, word processors or graphics viewers), or to compile a record of all recognized software on a system. Reports can be printed to a file, sent to your printer, or exported to a Netfinity database.

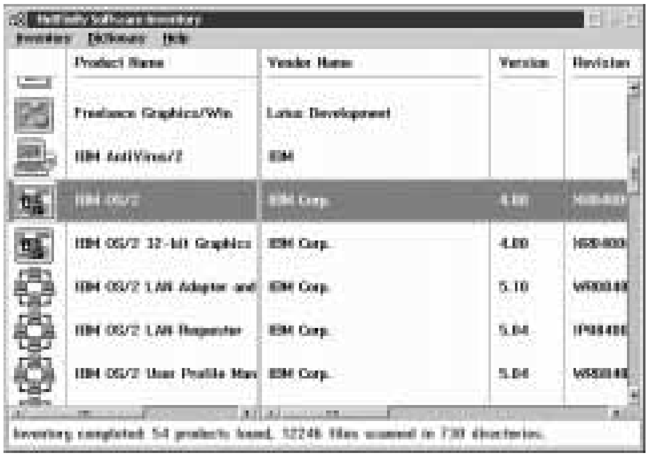
System Inventory comes complete with a dictionary file with many predefined software product profiles (called *product definitions*), so you can start keeping track of the software installed on your networked systems right away.

Software Inventory is designed with a simple graphical interface that enables you to add or edit product definitions quickly and easily. Products can be defined and identified by the presence of specified file names (including files that are of a specific size or that were created on specific date, enabling you to search for only certain versions of software) or by the presence of a SYSLEVEL file.

Software Inventory is designed to work with other IBM and non-IBM systems management software applications. Software Inventory provides a mechanism to integrate a workstation's existing software inventory information into the NetView Distribution Manager/6000 or NetView DM for NetWare software distribution database, if the appropriate NetView DM agent software is installed on the workstation. This is accomplished by the creation of the NetView DM FNDSWINV software change history import file, which contains a listing of the NVDM change object names that where discovered on that workstation by the Software Inventory service.

Software Inventory also provides a software dictionary import function for existing QSoft dictionary files (used by IBM's Network Door/2 product), NetView DM inventory list files (used by the INVSCAN utility), SPAudit dictionaries (a publicly available dictionary, used with the Software Publishers Association SPAudit tool. This dictionary can be obtained on the World Wide Web at http://www.spa.org), and other Software Inventory dictionaries (enabling you to easily combine multiple Software Inventory dictionaries).

Software Inventory can also be used in conjunction with the Remote System Manager. With Software Inventory, you can assign keywords to specific applications. If an application that has a defined application keyword is found during a dictionary search, the application keyword can be added to the list of other keywords that are currently defined for this system. Once an application keyword has been added to the list of system keywords, a Netfinity Manager can use the Remote System Manager discovery feature to add only systems that have specified application keywords to a system group. For example, using an application keyword a Netfinity Manager could create a group that contains only systems that have a specific word processor program that needs upgrading. For more information on keyword assignment and the discovery process, see *Netfinity Manager User's Guide* or consult your network administrator..



Product Name	Vendor Name	Version	Revision
Freelance Graphics/Win	Lotus Development		
IBM AntiVirus/2	IBM		
IBM OS/2	IBM Corp.	4.00	[illegible]
IBM OS/2 32-bit Graphics	IBM Corp.	4.00	XR0400
IBM OS/2 LAN Adapter and	IBM Corp.	5.10	WR0840
IBM OS/2 LAN Requester	IBM Corp.	5.04	IP08400
IBM OS/2 User Profile Man	IBM Corp.	5.04	WR0840

Inventory completed: 54 products found, 12246 files scanned in 730 directories.

Figure 22. The Software Inventory service

The Software Inventory Dictionary File

Software Inventory uses a software product data file (called the *dictionary file*) to determine the presence of a software product on a system. The dictionary file contains the names of many software products and *matching attributes.* Matching attributes are characteristics of the software product that enable Software Inventory to identify the software product when the specified attributes are found. Software Inventory uses two kinds of matching attributes:

- File names (can include file size and file date)
- SYSLEVEL files (can include SysID and Component ID)

As Software Inventory searches your hard disk drives, it checks for the presence of specified files or SYSLEVEL files. If it finds a SYSLEVEL file or other file that is defined as a matching attribute in the loaded dictionary file, it reports the product as installed on the system.

Loading a Dictionary File

To load a Software Inventory dictionary file:

1. Select **Open...** from the Dictionary pull-down menu in the Software Inventory window.

   This opens the Open Existing Dictionary... window.

2. Type in the **Open filename** field the fully qualified path and file name of the dictionary file that you want to open, **or** select from the appropriate fields the drive and directory that contain the dictionary file, and then select the dictionary file name.

3. Select **OK**.

Creating a New Dictionary File

To create a new dictionary file:

1. Select **New...** from the Dictionary pull-down menu in the Software Inventory window.

   This opens the New Dictionary... window.

2. Type in the **Save as filename** field the name of the new dictionary file.

3. Select from the **Drive** and **Directory** fields the drive and directory where the new dictionary file will be created.

4. Select **OK**.

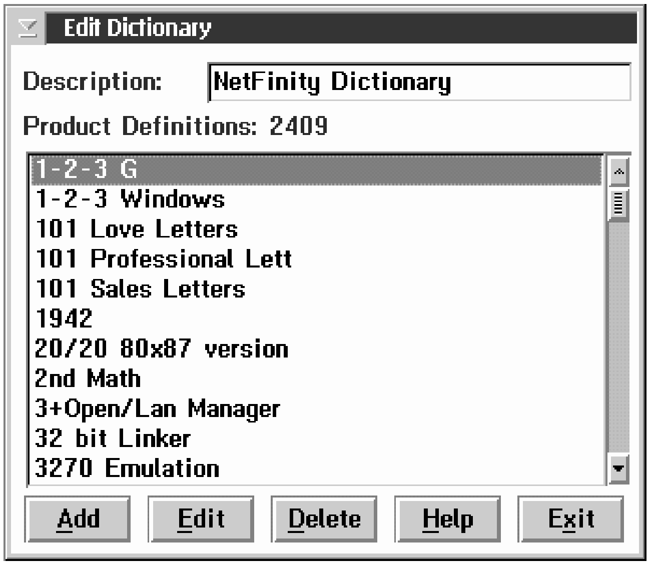
Editing the Dictionary File

To edit the currently loaded Software Inventory dictionary file, select **Edit...** from the Dictionary pull-down menu. This opens the Edit Dictionary window (see Figure 23 on page 96). From this window, you can:

- Change the dictionary description.

  The dictionary file description appears at the bottom of the Software Inventory window and can be used to help you identify the contents of the currently loaded dictionary file. The description is for your use only, and can be anything at all.

  To change the dictionary file description, type in the **Description** field the new description for the dictionary file and then select **Exit**.



Description: NetFinity Dictionary

Product Definitions: 2409

1-2-3 G
1-2-3 Windows
101 Love Letters
101 Professional Lett
101 Sales Letters
1942
20/20 80x87 version
2nd Math
3+Open/Lan Manager
32 bit Linker
3270 Emulation

Figure 23. The Edit Dictionary window

- Add a Product Definition.

  For information on how to add a product definition, see "Adding a Product Definition."

- Edit a Product Definition.

  For information on how to edit a product definition, see "Editing a Product Definition" on page 108.

- Delete a Product Definition.

  To delete a product definition form the dictionary file, select the product definition from the **Product Definitions** selection list, and then select **Delete**.

Adding a Product Definition

Select **Add** to add a new product definition to the currently loaded Software Inventory dictionary file. This opens the New Product Definition Type window (see Figure 24 on page 97). Product definitions can be added based on either of two criteria:

- Product defined by one or more required files

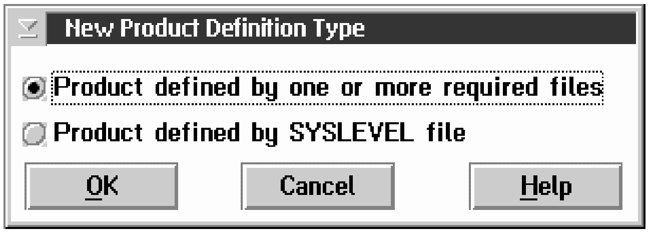
  Select **Product defined by one or more required files** to configure a Software Inventory product definition that will determine whether a product is installed on a system by checking for one or more files of your choosing. In addition to the name of the file or files that Software Inventory will search for, you can specify minimum (or maximum) file size and exact date or date ranges for the file.

  To add a product definition by defining one or more required files, see “File-List Product Definitions.”

- Product defined by SYSLEVEL file

  Select **Product defined by SYSLEVEL file** to configure a Software Inventory product definition that will determine whether a product is installed on a system by checking for a specified SYSLEVEL file. In addition to the name of the SYSLEVEL file, you can specify a SysID Value or Component ID.

  To add a product definition by requiring the presence of a specified SYSLEVEL file, see “SYSLEVEL File Product Definitions” on page 103.



● Product defined by one or more required files

○ Product defined by SYSLEVEL file

Figure 24. The New Product Definition Type window

File-List Product Definitions

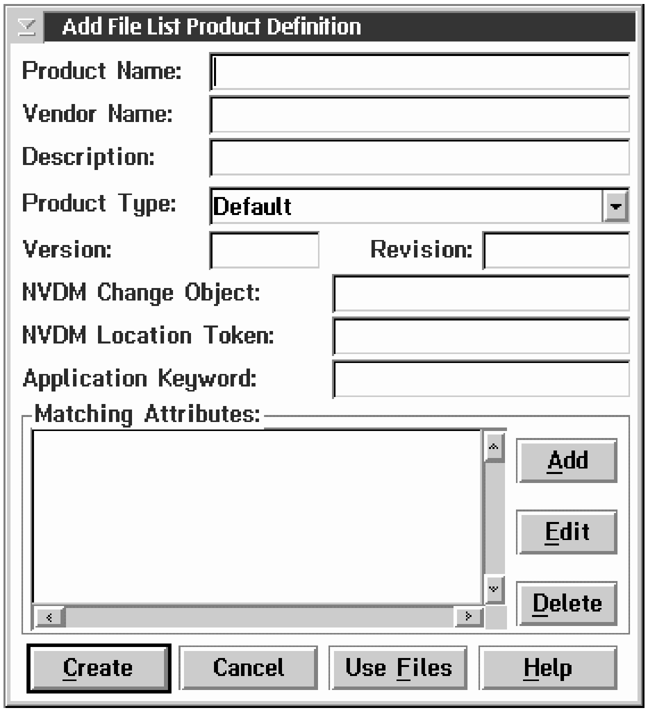
A file-list product definition enables Software Inventory to search your system's drives for specific files that are found in specific products. If the files are found, then the Software Inventory service will report that the software package that contains the files is installed on the system.

To add a file list product definition to the currently loaded Software Inventory dictionary file:

1. Select **Edit** from the Dictionary pull-down menu in the Software Inventory window.

2. Select **Add** from the Edit Dictionary window.

3. Select **Product defined by one or more required files** from the New Product Definition Type window, and then select **OK** to open the Add File List Product Definition window (see Figure 25).



Product Type: Default

Figure 25. The Add File List Product Definition window

4. Fill in the product data fields and select a **Product Type**.

   This information will appear in the Software Inventory window and in any reports Software Inventory generates when the product is found during a search. The Product Type can also be used by the Software Inventory service when Search by Product Type searches are performed. For more information on Search by Product Type searches, see “Search by Product Type” on page 110.

The product data fields include:

- Product Name

  This is the name of the software product.

- Vendor Name

  This is the name of the manufacturer of the software product.

- Description

  This is a brief description of the software product.

- Product Type

  This is a brief description of what function the software product performs. The selections available are:

  - Default
  - Network
  - Communications
  - Word Processing
  - Desktop Publishing
  - Database
  - Mail
  - Server
  - Spreadsheet
  - Financial
  - Entertainment
  - Multimedia
  - Graphics Viewer/Editor
  - Education
  - Operating System
  - Software Development
  - Presentation Graphics
  - System Management
  - Documentation
  - CAD/CAM

- Version

  This is the software product version number.

- Revision

  This is the software product revision number.

- NetView DM Change Object (NetView DM users only)

  This is the NetView Distribution Manager change object that will be added to the workstation's installation history. It does not have to match an existing change object in the NetView DM server's database, but it should follow your naming conventions for change objects. After the invocation of Software Inventory on a workstation, this change object name will be added to your NetView DM catalog if it does not already exist.

  Note: This data is used only for the **Update NetView DM Inventory** function. For more information on the NetView DM Change Object, see “Updating a NetView Distribution Manager Inventory” on page 113, or see your NetView DM documentation.

- NetView DM Location Token (NetView DM users only)

  This is the NetView Distribution Manager location token string for use with the software product you are defining. This is commonly used to denote where the application is installed on the workstation. For example, if you are creating a product definition for Netfinity, you would enter a location token of NETFINDIR. The maximum length allowed is 11 characters. This field is optional.

  Note: This data is used only for the **Update NetView DM Inventory** function. For more information on the NetView DM Change Object, see “Updating a NetView Distribution Manager Inventory” on page 113 or your NetView documentation.

- Application Keyword

  The application keyword, when used in conjunction with the Remote System Manager, enables a Netfinity Manager to discover only systems that have specified applications installed on them. For more information on using application keywords, see "Using Application Keywords" on page 115.

Although you do not need to fill in all of these fields, fill in as many as possible in order to maximize the information available to you when a product is found by the Software Inventory service.

5. Specify the Matching Attributes

   Matching Attributes are the data items used by the Software Inventory service in order to detect whether the software product you are defining is installed on a system. Because you are creating a File List Product Definition, the Matching Attributes will be one (or more) specified files. You can Add, Edit, or Delete files from the **Matching Attributes** field.

   To add a file:

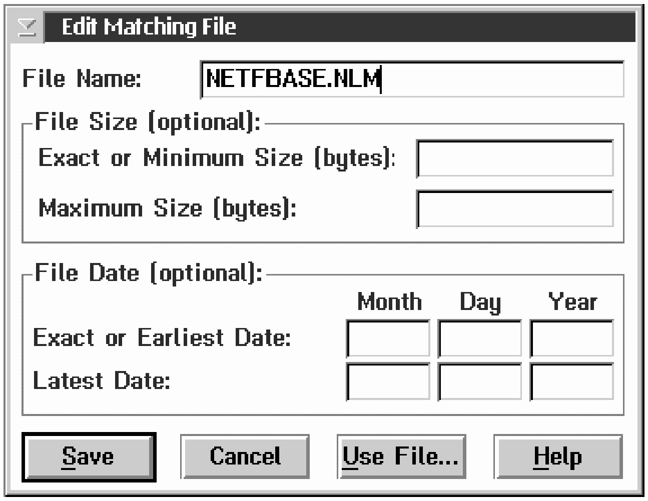
   - If you have the product that you are defining on your system:

     a. Select **Use Files**.

     b. Select the **Drive** and **Directory** where the files that Software Inventory will search for are located. Then, select a **File** and select **OK**.

        This will add the selected file to the **Matching Attributes** field, and then reopen the Use File for Matching File window so you can add other files from this directory. When you have finished adding files, select **Cancel**.

     c. **Optional:** In order to differentiate between different releases or versions of an individual product, you might need to specify that particular files were created on or after a specific date, or that the file is a certain size or within a range of sizes. If you want Software Inventory to look for files that are a specified size or within a range of sizes, or that were created on a specific day or during a specific date range, select the file from the **Matching Attributes** field and then select **Edit** to open the Edit Matching File window (see Figure 26 on page 102). Specify the **File Size** and **File Date** information, and then select **Save** to continue.



File Name: NETFBASE.NLM

Figure 26. The Edit Matching File window

d. Select **Create** to save this Product Definition to the currently loaded Software Inventory dictionary file.

- If you do *not* have the product that you are defining on your system:

  a. Select **Add** to open the Add Matching File window.

  b. Type in the **File Name**, **File Size** data (optional), and **File Date** data (optional).

     In order to differentiate between different releases or versions of an individual product, you might need to specify that a particular file was created on or after a specific date, or that the file is of a certain size or within a certain range of sizes. If you want Software Inventory to look for files that are a specified size or within a range of sizes, or that were created on a specific day or during a specific date range, specify the **File Size** and **File Date** information.

c. Select **Save** to add this file to the Matching Attributes list.

   Repeat this process until you have added as many Matching Attributes as you want.

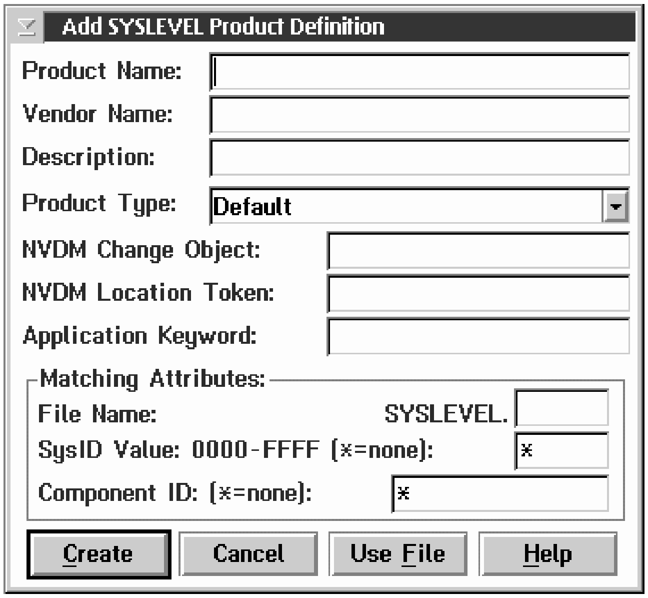
d. Select **Create** to save this Product Definition to the currently loaded Software Inventory dictionary file.

SYSLEVEL File Product Definitions

A SYSLEVEL file product definition enables Software Inventory to search your system's drives for a specific SYSLEVEL file that is found in a specific product. If the SYSLEVEL file is found, then the Software Inventory service will report that the software package that contains the SYSLEVEL is installed on the system.

To add a SYSLEVEL file list product definition to the currently loaded Software Inventory dictionary file:

1. Select **Edit** from the Dictionary pull-down menu in the Software Inventory window.
2. Select **Add** from the Edit Dictionary window.
3. Select **Product defined by SYSLEVEL file** from the New Product Definition Type window, and then select **OK** to open the Add SYSLEVEL Product Definition window (see Figure 27 on page 104).



Product Type: Default

SysID Value: 0000-FFFF (*=none): *

Component ID: (*=none): *

Figure 27. The Add SYSLEVEL Product Definition window

4. Fill in the product data fields and select a **Product Type**. This information will appear in the Software Inventory window and in any reports Software Inventory generates when the product is found during a search. The Product Type can also be used by the Software Inventory service when Search by Product Type searches are performed. For more information on Search by Product Type searches, see "Search by Product Type" on page 110.

   The product data fields include:

   - Product Name

     This is the name of the software product.

- Vendor Name

  This is the name of the manufacturer of the software product.

- Description

  This is a brief description of the software product.

- Product Type

  This is a brief description of what function the software product performs. The selections available are:

  - Default
  - Network
  - Communications
  - Word Processing
  - Desktop Publishing
  - Database
  - Mail
  - Server
  - Spreadsheet
  - Financial
  - Entertainment
  - Multimedia
  - Graphics Viewer/Editor
  - Education
  - Operating System
  - Software Development
  - Presentation Graphics
  - System Management
  - Documentation
  - CAD/CAM

- NetView DM Change Object (NetView DM users only)

  This is the NetView Distribution Manager change object that will be added to the workstation's install history. It does not have to match an existing change object in the NetView DM server's database, but it should follow your naming conventions for change objects. After the invocation of Software Inventory on a workstation, this change object name will be added to your NetView DM catalog if it does not already exist.

Note: This data is used only for the **Update NetView DM Inventory** function. For more information on the NetView DM Change Object, see "Updating a NetView Distribution Manager Inventory" on page 113, or see your NetView DM documentation.

- NetView DM Location Token (NetView DM users only)

  This is the NetView Distribution Manager location token string for use with the software product you are defining. This is commonly used to denote where the application is installed on the workstation. For example, if you are creating a product definition for Netfinity, you would enter a location token of NETFINDIR. The maximum length allowed is 11 characters. This field is optional.

  Note: This data is used only for the **Update NetView DM Inventory** function. For more information on the NetView DM Change Object, see "Updating a NetView Distribution Manager Inventory" on page 113, or see your NetView DM documentation.

- Application Keyword

  The application keyword, when used in conjunction with the Remote System Manager, enables a Netfinity Manager to discover only systems that have specified applications installed on them. For more information on using application keywords, see "Using Application Keywords" on page 115.

Although you do not need to fill in all of these fields, fill in as many as possible in order to maximize the information available to you when a product is found by the Software Inventory service.

5. Specify the Matching Attributes

   Matching Attributes are the data items used by the Software Inventory service in order to detect whether the software product you are defining is installed on a system. Because you are creating a SYSLEVEL File Product Definition, the Matching Attributes will be the SYSLEVEL file name, the SysID, and the Component ID.

   To add Matching Attributes for a SYSLEVEL file:

   - If you have the SYSLEVEL file for the product you are defining on your system:

     a. Select **Use File**.

     b. Select the **Drive** and **Directory** where the SYSLEVEL file is located, select the SYSLEVEL **File** and then select **OK**.

     c. Select **Create** to save this Product Definition to the currently loaded Software Inventory dictionary file.

   - If you do **not** have the SYSLEVEL for the product you are defining on your system:

     a. Type in the **File Name** field the three character file name extension for the product's SYSLEVEL file.

     b. If possible, type in the **SysID Value** and the **Component ID**.

        Note: These values are stored in the SYSLEVEL file, and can be difficult to obtain without the SYSLEVEL file itself.

     c. Select **Create** to save this Product Definition to the currently loaded Software Inventory dictionary file.

Editing a Product Definition

Software Inventory dictionary file product definitions can be edited in much the same as they are added. To edit a product definition:

1. Select **Edit** from the Dictionary pull-down menu in the Software Inventory window.
2. Select from the **Product Definitions** field the name of the product whose definition you want to edit, and then select **Edit**.
   - If the selected product definition is a File List Product Definition, the Edit File List Product Definition window opens.
   - If the selected product definition is a SYSLEVEL File Product Definition, the Edit SYSLEVEL Product Definition window opens.
3. Edit the product information and Matching Attributes as needed.

   The process used to edit the product information and Matching Attributes is the same as that used when adding a new product definition. See "File-List Product Definitions" on page 97 and "SYSLEVEL File Product Definitions" on page 103 for more information.
4. Select **Save** to save the changes to this product definition.

Performing a Search

Software Inventory can perform three types of software searches on the system. The three kinds of searches are:

- Full Dictionary Search
- Search by Drive
- Selected Product Search
- Search by Product Type

Full Dictionary Search

Software Inventory's Full Dictionary Search enables you to search for any software product that is defined in the currently loaded Software Inventory dictionary file. Depending on the speed of your system, the number of files on your system, the products installed on your system, and the number of products defined in the currently loaded Software Inventory dictionary file, the Full Dictionary Search can take from just seconds to several minutes to complete. Once the search is complete, results will be displayed in the Software Inventory window.

To perform a Full Dictionary Search, select **Full Dictionary Search** from the Inventory pull-down menu in the Software Inventory window.

For information on generating reports or exporting this information to a database, see “Generating Reports and Exporting Data” on page 112.

Search by Drive

Software Inventory enables you to perform full dictionary searches on specified hard disk drives. If you want to search to for products only on one disk drive on a system, select **Search by Drive...** from the Inventory pull-down menu in the Software Inventory window, and then select the letter of the disk drive you want to search. Software Inventory will then search for any products defined in the currently loaded Software Inventory dictionary on only the specified disk drive.

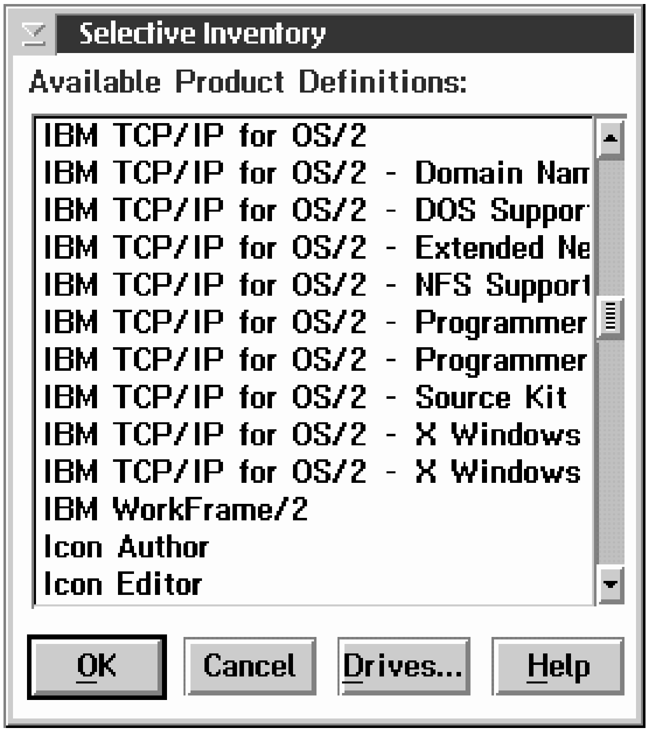
Once the search is complete, results will be displayed in the Software Inventory window. For information on generating reports or exporting this information to a database, see “Generating Reports and Exporting Data” on page 112.

Selected Product Search

In some cases, you might want to search for specific software products on your networked systems. To search for one or more specific products:

1. Select **Selected Product Search...** from the Inventory pull-down menu in the Software Inventory window.

   This opens the Selective Inventory window (see Figure 28 on page 110).


Selective Inventory

Available Product Definitions:

IBM TCP/IP for OS/2
IBM TCP/IP for OS/2 - Domain Nam
IBM TCP/IP for OS/2 - DOS Suppor
IBM TCP/IP for OS/2 - Extended Ne
IBM TCP/IP for OS/2 - NFS Support
IBM TCP/IP for OS/2 - Programmer
IBM TCP/IP for OS/2 - Programmer
IBM TCP/IP for OS/2 - Source Kit
IBM TCP/IP for OS/2 - X Windows
IBM TCP/IP for OS/2 - X Windows
IBM WorkFrame/2
Icon Author
Icon Editor

Figure 28. The Selective Inventory window

2. Select from the **Available Product Definitions** window the names of all products that you want to search for.
3. Select **OK** to begin the search for the selected products.

Once the search is complete, results will be displayed in the Software Inventory window. For information on generating reports or exporting this information to a database, see "Generating Reports and Exporting Data" on page 112.

Search by Product Type

When defining products for use with the Software Inventory dictionary file, you can specify a Product Type. This is a brief description of the product's main function. For example, Netfinity's Product Type is *Systems Management*. Software Inventory enables you to search your networked systems for all products of the same Product Type.

To search only for specified Product Types:

1. Select **Search by Product Type** from the Inventory pull-down menu in the Software Inventory window.

   This opens the Search by Product Type window.

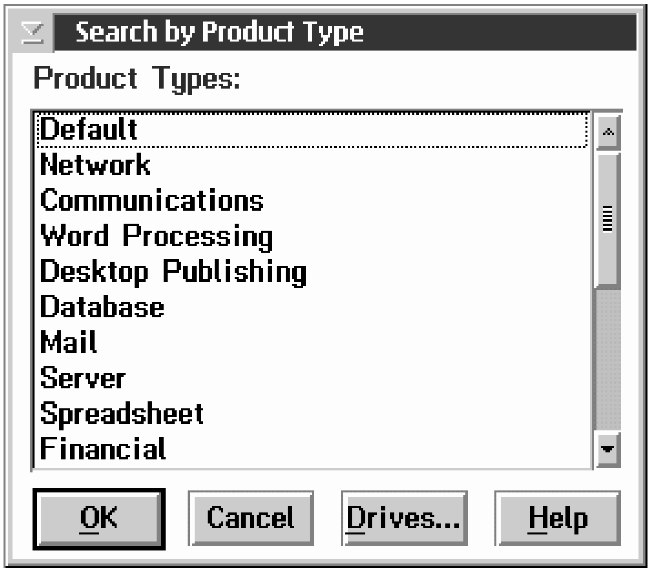


Figure 29. The Search by Product Type window

2. Select from the **Product Type** list one or more product types.

3. Select **OK** to initiate your search.

Once the search is complete, results will be displayed in the Software Inventory window. For information on generating reports or exporting this information to a database, see “Generating Reports and Exporting Data” on page 112.

Generating Reports and Exporting Data

The information gathered by Software Inventory can be:

- Printed to a file
- Printed to a printer
- Exported to a Netfinity database

Print to File

To save the information gathered by Software Inventory to a file:

1. Initiate a Software Inventory search.
2. When the search is complete, select **Print to File** from the Inventory pull-down menu.
3. Name the file, select a drive and directory to which it will be saved, and then select **OK**.

Print to Printer

To print the information gathered by Software Inventory on a printer attached to your system:

1. Initiate a Software Inventory search.
2. When the search is complete, select **Print to Printer** from the Inventory pull-down menu.

The information is then sent to the default printer attached to your system.

Export to Database

To export the information gathered by Software inventory to a Netfinity database, or to save the data to a supported database format file:

1. Initiate a Software Inventory search.
2. When the search is complete, select **Export to Database...** from the Inventory pull-down menu.

3. Select the type of database export you want to perform (export the data to an attached database, or save the data to a database file).

4. Select **OK** to export or save the data.

Updating a NetView Distribution Manager Inventory

You can use Software Inventory to create the NetView Distribution Manager (*NetView DM*) software inventory import file. If your system is running NetView DM agent software, select **Update NetView DM Inventory...** from the Inventory pull-down menu. Software Manager will scan the currently loaded dictionary file for any product definitions that include an NetView DM Change Object and add them to the NetView DM software inventory import file (FNDSWINV). The location token information will be written into the NetView DM agent software base path into a file called FNDTKINV.

This enables a user-written exit routine to then invoke the appropriate NetView DM INV and NetView DM UPDTG commands to move the data in this import file into that workstation’s NetView DM software change history database.

Note: This choice is only available if NetView DM agent software is installed and running on the system.

Importing Software Dictionaries

Software Inventory provides a software dictionary import function for existing QSoft dictionary files (used by IBM's Network Door/2 product), NetView DM inventory list files (used by the INVSCAN utility), SPAudit dictionaries (a publicly available dictionary, used with the Software Publishers Association SPAudit tool. This dictionary can be obtained on the World Wide Web at http://www.spa.org), and other Software Inventory dictionaries (enabling you to easily combine multiple Software Inventory dictionaries).

To import a software dictionary file:

1. Open the Software Inventory dictionary file to which new data will be imported.

   To open a Software Inventory dictionary file, select **Open...** from the Dictionary pull-down menu, select a dictionary file, and then select **OK**.

2. Select an import function from the Dictionary pull-down menu.

   The following software dictionary import functions are available:

   - Import from Software Inventory Dictionary...

     Select **Import from Software Inventory Dictionary...** to import all data from another Software Inventory dictionary file into the currently loaded Software Inventory dictionary file.

   - Import from SPAudit Dictionary...

     Select **Import from SPAudit Dictionary...** to import all data from an SPAudit dictionary file into the currently loaded Software Inventory dictionary file.

   - Import from QSoft Dictionary...

     Select **Import from QSoft Dictionary...** to import all data from a QSoft dictionary file into the currently loaded Software Inventory dictionary file.

   - Import from Dictionary...

     Select **Import from NetView DM Inventory List...** to import all data from a NetView DM Inventory List into the currently loaded Software Inventory dictionary file.

Notes:

1. Depending on the speed of your system and the size of the dictionary file you are importing, import functions can take a considerable amount of time to complete.

2. Import functions import **all** data in the file you select, including entries that could already exist in the loaded Software Inventory

dictionary file. Importing identical product definitions will result in multiple, identical entries for products in your dictionary file and will also result in single products being discovered multiple times. To remove identical entries from your Software Inventory dictionary file, edit the dictionary file using the Software Inventory dictionary edit function (for more information see "Editing the Dictionary File" on page 95).

Using Application Keywords

Software Inventory enables you to add application keywords to specific software applications. Once defined, these keywords can then be used by Remote System Manager to create system groups that contain only systems that have specified applications installed.

To add an application keyword to a product definition in your Software Inventory dictionary file:

1. Load a Software Inventory dictionary file.

   To load a dictionary file select **Open** from the Dictionary pull-down menu, select the dictionary file you want to load, and then select **OK**.

2. Edit the Software Inventory dictionary file.

   Select **Edit...** from the Dictionary pull-down menu to edit the currently loaded dictionary file.

3. Edit the Product Definition.

   Select the product to which you will assign an application keyword from the **Product Definitions** field and then select **Edit**.

4. Assign an application keyword.

   Type in the **Application Keyword** field the keyword that will be used to identify this product. The application keyword can be up to 12 characters long.

5. Select **Save** to save this information to the dictionary file.

Products with application keywords that are discovered on a system following a dictionary search will have the application keyword displayed along with other software product information in the Software Inventory window following the dictionary search. Once a product that has an application keyword defined is discovered on a system, the application keyword can be added to the system's keyword list. To update the system keyword list with application keywords for discovered and defined products, select **Update Application Keywords** from the Inventory pull-down menu.

Notes:

1. To differentiate application keywords from other system keywords, the application keyword will has the characters APP: added to the beginning of the application keyword. Remote System Manager system groups that use the application keyword as part of the group's system discovery criteria must include APP: as well as the text that is entered in the **Application Keyword** field to successfully discover the system.

   For example, if a product definition uses the application keyword SOFTWARE, the keyword that must be used by Remote System Manager to discover systems using the product that is defined using this application keyword would be APP:SOFTWARE.

2. The **Update Application Keywords** function adds only application keywords that are currently displayed in the Software Inventory window to the system's keyword list. If you add an application keyword to the product definition of an application that is installed on your system, the application keyword will not be added to the keyword list until you perform another dictionary search and then select **Update Application Keywords**.

Chapter 12. System Information Tool

System Information Tool is designed to gather and display a broad variety of information about the hardware and software configuration of your system. System Information Tool is primarily designed for use on IBM systems, but many features will function on systems from other manufacturers.

System Information Tool Features

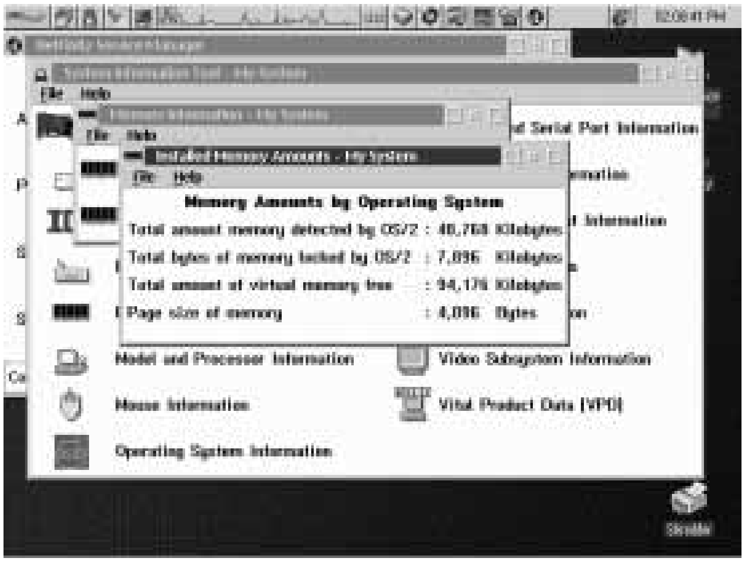
The System Information Tool gathers hardware and software configuration information. This information can be viewed online or directed to a file or printer.

Note: System Information Tool supports export of collected data to a Netfinity database. However, database export can be performed only by the Netfinity Manager. No database export functions are available for local use on systems running Client Services for Netfinity Manager.

Depending on your system's hardware, software, or operating system configuration, System Information Tool provides information on some or all of the the following system features:

- Pentium® processor information, including automatic detection of flawed Pentium processors
- Micro Channel, EISA, and PCI adapter identity, with configuration information available on many common adapters
- Drive information, including file-system type, available space on the disk drive, disk drive size, and partition layout
- Error log display and interpretation
- Keyboard information
- Memory configuration, including total physical memory, installed single inline memory module identification, and supported memory upgrades
- Mouse type and settings
- Operating system information, including version, DOS support, session limits, current task list, and CONFIG.SYS information

- Model and microprocessor information, including model name, processor type and speed, and BIOS date
- Parallel and serial port configuration
- Video system information, including adapter type, screen resolution, and video display identification
- Printer configuration, including data on installed printer drivers
- SCSI, ESDI, IDE/ST506, or other disk adapter information, including devices attached, device sizes, and adapter data
- System security features, including power-on password and secondary security features
- RAID subsystems
- VPD data
- PCMCIA devices
- Plug and Play configuration
- Network (NDIS) devices and data (available only on systems running OS/2)


Netfinity Service Manager
System Information Tool - My System
File
Help
Memory Information - My System
File
Help
Installed Memory Amounts - My System
File
Help
d Serial Port Information
Model and Processor Information
Video Subsystem Information
Mouse Information
Vital Product Data (VPD)
Operating System Information

Memory Amounts by Operating System

```
Total amount memory detected by OS/2 : 40,768 Kilobytes
Total bytes of memory locked by OS/2 : 7,096  Kilobytes
Total amount of virtual memory free  : 94,176 Kilobytes
Page size of memory                  : 4,096  Bytes
```

Figure 30. System Information Tool

Using System Information Tool

To display information gathered by System Information Tool, select the object or name of the component from the System Information Tool window. This action opens a window that contains more specific information regarding the component you selected.

If more information is available, one or more words or objects within the new window will be highlighted. You may then select another object or topic to open a window with more device-specific information. If there is no further information available, no highlighted items will appear within the window.

System Information Tool provides you with three options for generating output of the gathered and displayed data. To access these options, select the **File** pull-down menu at the top of the System Information Tool window, and then do the following:

- Select **Print All System Data To File** to generate a textual report of all of the system configuration data which has been collected by the System Information Tool, and then save the report to a user-selected file. You are given a standard file window to select the file name.
- Select **Print All System Data To Printer** to generate a textual report of all of the system configuration data that has been collected by the System Information Tool, and then send the report to the default printer.
- Select **Generate History File** to create a binary file that contains all of the information displayed in the program as well as the current time and date. The history file can be viewed later by using the **/F** command-line parameter when starting the System Information Tool from a command-line. For more information on System Information Tool's command-line functions, see "System Information Tool Command Line Operations" on page 158.

Protecting Confidential System Data

In addition to extensive hardware configuration information System Information Tool gathers detailed operating system information. The data collected is operating system-dependent, and typically includes the contents of the system's CONFIG.SYS or AUTOEXEC.BAT files. Depending on your system's configuration, these files might contain confidential information. For example, your CONFIG.SYS file might contain the following command, used to logon to a network-accessible disk drive:

```
LOGON MY_USER_ID /D:MY_DRIVE /P:MY_PASSWORD
```

To automatically protect sensitive or confidential system data, create an ASCII file named SIKEYWD.INI in your Netfinity directory. This file should contain one or more alphanumeric strings. If this file is present, System Information Tool will automatically replace all alphanumeric characters (other than the keyword itself) that are on any line that contains one of the keywords specified in the SIKEYWD.INI file with asterisks.

Using the previous example, if your SIKEYWD.INI file contains the keyword LOGON the CONFIG.SYS information shown above would appear to the user as

```
LOGON**************************************
```

Notes:

1. The SIKEYWD.INI file can contain as many keywords as needed. Keywords must be separated by a space.
2. SIKEYWD.INI string entries are case-sensitive. Only strings that exactly match the SIKEYWD.INI entries will be replaced in the System Information Tool data.
3. Because of the additional processing that must be done, adding keywords to the SIKEYWD.INI file can degrade System Information Tool performance. Users should add keywords to the SIKEYWD.INI file with care.

Chapter 13. System Monitor

The System Monitor provides a convenient method of charting and monitoring the activity of a number of components in your system. Standard features include:

- Continuous monitoring of systems, including:
  - Locked memory use
  - Virtual memory use
  - Microprocessor use
  - DASD space available and space remaining
  - DASD use
  - TCP/IP protocol functions
  - Processes running
  - Threads running
  - Pentium processor computations
  - RAID device attributes
  - Read/write errors (Netfinity Manager only)
- Detachable, scalable, and user-configurable monitors
- User-definable thresholds that will generate Netfinity alerts when exceeded
- Alerts that are generated when previously exceeded threshold return to an acceptable or normal state
- Choice of line-graph, text, and real-time graphic representations of system activity

Note: System Monitor supports export of collected data to a Netfinity database. However, database export can be performed only by the Netfinity Manager. No database export functions are available for local use on systems running Client Services for Netfinity Manager.

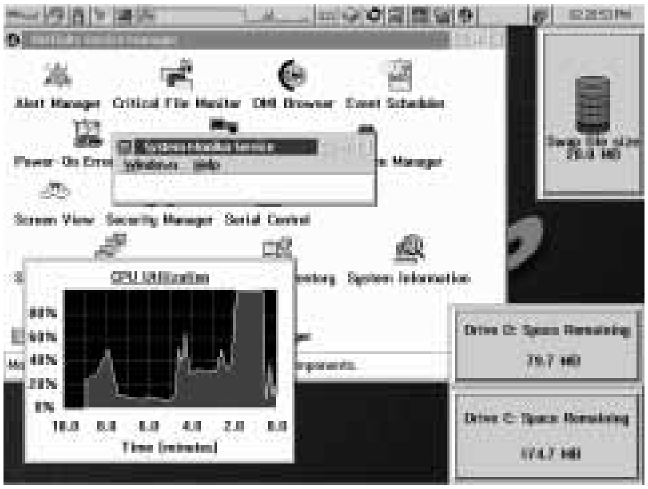


Figure 31. System Monitor Service

Note: System Monitor uses a data-handling technique that allows for both long-term, system activity profiles and short-term, high-resolution system activity monitoring.

As samples of system activity are taken, they are stored and displayed. However, after a number of samples have been taken, their individual values are weighed, several concurrent samples are averaged, and they are posted as a single, long-term value.

Primarily, this is done to prevent System Monitor data files from taking up a large amount of space on a system. This data-handling technique also allows for a more reasonable measurement of average long-term system load values without sacrificing short-term monitoring abilities. This data-handling technique accounts for the initial “spiking” you may see on line graphs when the System Monitor is started.

If you do not need records of a monitor’s previous activity, or do not want to use disk drive space to maintain these records, you can use the System Monitor’s Record Data option to disable record keeping.

The System Monitor Service Window

When the System Monitor service is started, all monitors currently set to be visible appear on your display, along with the System Monitor Service window.

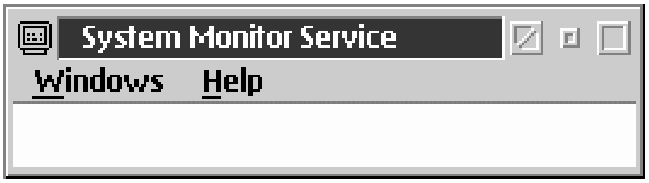


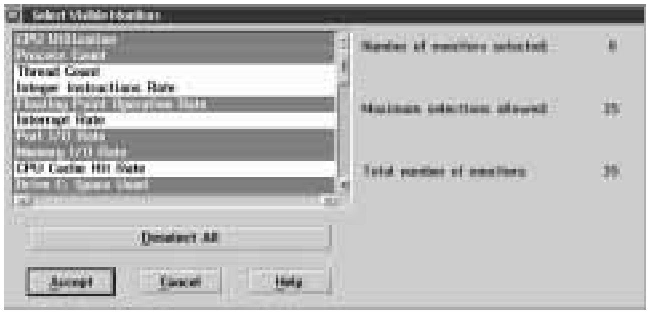
Figure 32. The System Monitor Service window

The System Monitor Service window controls the service as a whole. If the System Monitor Service window is closed, all of the monitors will close as well.

Use the choices in the System Monitor Service window's **Windows** pull-down menu to:

- Show monitors that are available

  Select **Show Monitors** to open the Select Visible Monitors window. Use this window to select which of the System Monitors you want to be visible on your Desktop.



CPU Utilization
Processor Speed
Thread Count
Integer Instructions Rate
Floating Point Operations Rate
Interrupt Rate
Disk I/O Rate
Memory I/O Rate
CPU Cache Hit Rate
Drive C: Space Used

Number of monitors selected: 6

Maximum selections allowed: 35

Total number of monitors: 35

Figure 33. The Select Visible Monitors window

To select the monitors that will be visible on the Desktop:

1. Select the monitors that you want to have visible on the Desktop.

   To select *all* available monitors, click on **Select All**. If all monitors are currently selected and you want to deselect all monitors, click on **Deselect All**.

   There is no enforced limit to the number of monitors that can be active at one time. However, due to system restraints, a default maximum of 50 monitors can be displayed at a time. The maximum number of monitors visible can be changed by setting a system environment variable as follows:

   ```
   SET NF_MAX_MON_DISP=n
   ```

   where *n* is an integer greater than zero. The manner in which the environment variable is set depends on your operating system.

   – To set this environment variable on an OS/2 or Windows 95 system, add the variable to your CONFIG.SYS file and then restart your system.

   – On NT systems:

     a. Open the Windows NT Control Panel, then double-click on **System**.

     b. Click on the **Environment** tab.

     c. Click anywhere in the **System Environment Variables** field.

     d. Type in the **Variable** field

        ```
        NF_MAX_MON_DISP
        ```

     e. Type in the **Value** field the *n* value (an integer greater than zero).

     f. Select **Set**.

     g. Select **Apply**.

     h. Select **OK**.

     i. Shutdown and restart the Netfinity Support Program.

Note: If you increase the number of monitors that can be displayed at a time, you system could run out of resources. To prevent this problem, display only as many monitors as needed.

2. If any monitors are selected that you do not want to be visible on the Desktop, deselect them.

3. Select **Accept** to display or hide monitors as appropriate.

- Bring specific monitors to the foreground

  Select the name of the monitor you want to bring to the foreground. If a monitor is not currently hidden, you can select the monitor's name to bring it to the foreground. If a monitor is hidden, its name will be grayed out. Hidden monitors cannot be brought to the foreground.

Monitor Pop-Up Menus

Each monitor has a number of monitor-specific options that can be accessed from the monitor's pop-up menu. To open a monitor's pop-up menu, use mouse button 2, and click on the monitor. This opens the monitor's pop-up menu. Use the selections in individual monitor's pop-up menu to:

- Configure System Monitor thresholds

  Select **Thresholds** to open the Thresholds page of the individual monitor's notebook. For more information see "Setting Thresholds" on page 128.

- Change System Monitor settings

  Select **Settings** to open the Settings page of the individual monitor's notebook. For more information see "Monitor Settings" on page 131.

- Change the System Monitor that is displayed

  Select **View** to choose the appearance of monitor that will is displayed. The available monitor types are:

  – Line Graph

  – Real Time

  – Text Display

  For more information on the available monitor types see "Changing Monitor Views" on page 132.

- Bring the Main Window to the foreground

  Select **Main Window** to bring the System Monitor Service window to the foreground.

- Enable or disable recording of data

  Select **Record Data** to enable System Monitor to keep records of this monitor's previous activity. If this option is not selected, monitor data is not saved and line-graph monitors are not available. Disabling this option on monitors that you do not use frequently, or from which you do not need long-term data, can help you save space on your disk drive.

- Access online help

  Select **Help** to access System Monitor's online help facility.

- Move

  Select **Move** to move the selected monitor around the Desktop. When you have moved the selected monitor to the new location, click again to drop it. Monitors can also be moved by dragging the monitor to a new location.

- Size the monitor

  Select **Size** to resize the selected monitor. After you select **Size**, move the mouse until the window outline is the size that you want the selected monitor to be. Then, click again to resize the monitor. You can also resize monitors by dragging the sides or corners of the monitor windows.

Note: If you make a monitor too small for the monitor's text to be shown fully, the text will disappear. However, this has no effect on the monitor's function.

- Hide the monitor

  Select **Hide** to make the selected monitor invisible. The monitor will continue to function and collect data, but it will not be seen on the Desktop. To make a monitor that you have hidden visible again, you must open the System Monitor Service window, and then select **Show Monitors...** to open the Select Visible Monitors window. For more information on the Show Visible Monitors window see "The System Monitor Service Window" on page 123.

System Monitor Notebooks

Use each monitor's System Monitor notebook to:

- Set thresholds at which alerts will be generated.

  For more information on setting thresholds, see "Setting Thresholds" on page 128.

- Configure monitor-specific settings. For more information on configuring monitor settings, see "Monitor Settings" on page 131.

To open the System Monitor notebook:

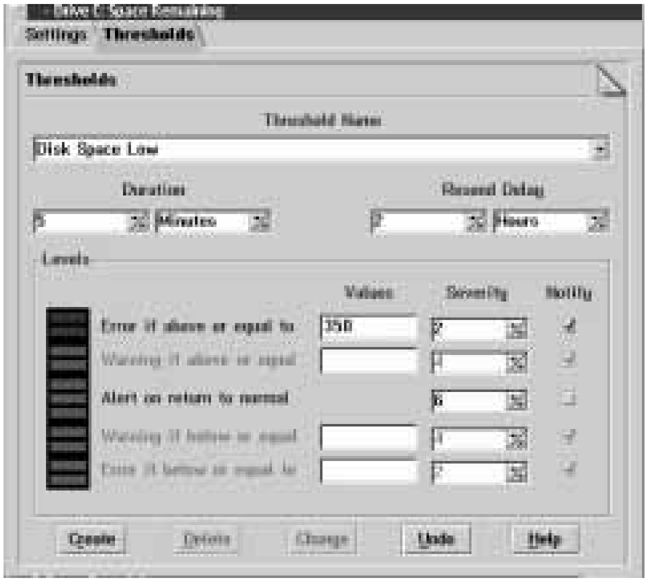
1. Open the individual monitor's context menu (using mouse button 2, click on the monitor).
2. Select **Open**.
3. Select the page of the notebook you want to open:
   - Select **Thresholds** to open the notebook to the Thresholds page.
   - Select **Settings** to open the notebook to the Settings page.

Setting Thresholds

The Thresholds page of the System Monitor notebook enables you to set threshold values for this monitored system component. If the monitored value of this system component falls outside of the configured threshold values, the System Monitor will generate a Netfinity alert. You can also configure System Monitor to generate an alert when a previously exceeded threshold has returned to a normal or acceptable state.

System Monitor also automatically monitors any *redundant arrays of independent disks* (RAID) subsystems that may be present on your system. You can monitor RAID subsystems and other attribute-based devices with System Monitor's Attribute Monitors. For more information on Attribute Monitors, see "Attribute Monitors" on page 135.

System Monitor will automatically generate alerts if a RAID system malfunction is detected. For more information on RAID alerts, see Appendix D, "RAID Alerts" on page 153.



Threshold Name: Disk Space Low

Duration: 5 Minutes

Resend Delay: 2 Hours

	Values	Severity	Notify
Error if above or equal to	350	2	✓
Warning if above or equal		4	✓
Alert on return to normal		6	□
Warning if below or equal		4	✓
Error if below or equal to		2	✓

Figure 34. The System Monitor Notebook Threshold Page

To create (or edit) a threshold for this system component:

1. Open the System Monitor notebook to the Threshold page.

   Using mouse-button 2, click on the monitor for which you will create the threshold. Then, select **Open**, and then **Thresholds** from the monitor's pop-up menu.

2. Name the threshold (or select the Threshold Name to be edited).

   Type the name of the threshold in the **Threshold Name** field. If you are editing an existing threshold, select the threshold from the **Threshold Name** selection list.

3. Set the threshold's duration.

   Type a number and select a unit of measurement (for example, "seconds") to create a duration value. This will specify the length of time that the monitor's threshold value must be exceeded before an alert is generated.

4. Set the resend delay.

   Type a number and select a unit of measurement (for example, "seconds") to create a resend delay value. This will specify the length of time that the System Monitor will wait, after sending an alert, before resending a duplicate alert if the threshold Value continues to be violated.

5. Set the threshold's values.

   Enter one or more threshold Values for this monitor. You can set up to four different threshold Values, each of which will generate a different Netfinity alert.

   - Error if above or equal to

     The threshold value entered in the **Error if above or equal to** field is the minimum value that will trigger an alert. If the parameter being monitored is greater than or equal to this value, System Monitor will generate and "Error" alert type. The threshold value must be less than or equal to the maximum value for this system component (for example, 100.0 for CPU Utilization or 214.0 for the space on a 214 MB logical drive), and must be greater than or equal to the **Warning if above or equal to**, **Warning if below or equal**

to, and **Error if below or equal to** Values (if any). If the entered value does not conform to these requirements, System Monitor will “beep” and reject the entered value.

- Warning if above or equal to

  The threshold value entered in the **Warning if above or equal to** field is the minimum value that will trigger an alert. If the parameter being monitored is greater than or equal to this value, System Monitor will generate and “Warning” alert type. The threshold value must be less than or equal to the maximum value for this system component (for example, 100.0 for the CPU monitor), less than or equal to the value (if any) assigned for **Error if above or equal to**, and must be greater than or equal to the assigned values (if any) for **Warning if below or equal to** and **Error if below or equal to**. If the entered value does not conform to these requirements, System Monitor will “beep” and reject the entered value.

- Warning if below or equal to

  The threshold value entered in the **Warning if below or equal to** field is the maximum value that will trigger an alert. If the parameter being monitored is less than or equal to this value, System Monitor will generate and “Warning” alert type. The threshold value must be less than or equal to the maximum value for this system component (for example, 100.0 for the CPU monitor), less than or equal to the value (if any) assigned for **Error if above or equal to** and **Warning if above or equal to**, and must be greater than or equal to the assigned value (if any) for **Error if below or equal to**. If the entered value does not conform to these requirements, System Monitor will “beep” and reject the entered value.

- Error if below or equal to

  The threshold value entered in the **Error if below or equal to** field is the maximum value that will trigger an alert. If the parameter being monitored is less than or equal to this value, System Monitor will generate and “Error” alert type. The threshold value must be less than or equal to the maximum value for this system component (for example, 100.0 for the CPU monitor), and less than or equal to the values (if any) assigned for **Error if above or equal to**, **Warning if above or equal to**, and **Warning if below or equal to**. If the entered value does not conform to these requirements, System Monitor will “beep” and reject the entered value.

6. Set the threshold’s severity

   A default severity is provided for each of the threshold Values. You can adjust these values by selecting the spin buttons at the right of the field.

7. Select Notify (optional).

   Select **Notify** to cause a pop-up window to appear on this system whenever this threshold is exceeded. If you do not select **Notify**, the threshold will be saved and will be active, but a pop-up window will not automatically inform you if the threshold is exceeded.

8. Select Alert on return to normal (optional).

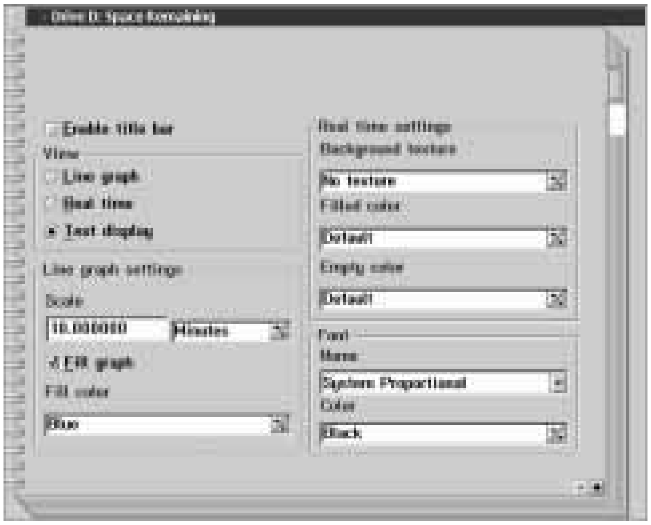
   Select **Alert on return to normal** to configure System Monitor to generate an alert with the user-specified severity when a threshold value that was previously exceeded returns to an acceptable value.

9. Save the threshold.

   If you have been configuring a new threshold, select **Create** to save these threshold values. If you have been editing a previously configured threshold, select **Change** to save the new threshold values.

Monitor Settings

Use the Settings page of the System Monitor notebook to enable of disable the title bar for this monitor, select the type of monitor that is displayed, to configure the line-graph settings for this monitor, to set the background and colors used in the real-time monitor view, or to select a font for use with this monitor.



Drive D: Space Remaining

□ Enable title bar

View
○ Line graph
○ Real time
● Text display

Line graph settings
Scale
10.000000 Minutes
✓ Fill graph
Fill color
Blue

Real time settings
Background texture
No texture
Filled color
Default
Empty color
Default

Font
Name
System Proportional
Color
Black

Figure 35. The System Monitor Notebook Settings Page.

Enabling and Disabling the Title Bar (available on OS/2 systems only)

Select the **Enable Title Bar** check box to activate a title bar on this monitor. This title bar shows the name of the monitor (for example, “CPU Utilization Monitor”). If you do not want a title bar on this monitor, deselect the **Enable Title Bar** check box.

To save the new Settings, close the notebook by double-clicking in the upper-left corner.

Changing Monitor Views

Select the type of monitor that will be displayed from the View button group. The available monitor types are:

- Line graph

  Select **Line graph** to display a “heartbeat-style” chart of this system component’s activity using user-specified Line-Graph Settings to determine the length of the graph and the units in which it is measured. For more information on line-graph monitors, see “Configuring Line-Graph Settings” on page 133.

Note: If you have disabled the Record Data option (found in the monitor's pop-up menu), line-graph monitors will not be available.

- Real time

  Select **Real time** to display a graphic representation of this system component's current status. The real time monitor that is displayed depends on what system component it is meant to represent. For example, the CPU monitor uses a speedometer-style real time monitor to show percentage of CPU utilization, while hard disk drive Space Used monitors use a cylinder to depict how "full" the disk drive is.

- Text display

  Select **Text display** to display a textual readout of the system component's current activity, without any graphical representation.

To save the new Settings, close the notebook by double-clicking in the upper left corner.

Configuring Line-Graph Settings

Use the selections available in the Line graph settings field group to configure this component's line-graph monitor. This field group enables you to:

- Set the Line-Graph Scale

  Use the **Scale** fields to configure the length of time graphed when viewing this monitor's line graph. Enter a number in the first **Scale** field, and then use the spin buttons to the right of the second **Scale** to select the unit of time that the line graph will use to graph component activity. The available units of time are:

  - Seconds
  - Minutes
  - Hours
  - Days
  - Weeks

- Enable / disable line-graph fill

Select **Fill graph** if you want to fill in this monitor's line-graph with a specified color. If **Fill Graph** is not selected, the line graph will show only a white line against the dark background. If you select **Fill graph**, you can then select from the **Fill color** field the color with which the line graph will be filled.

- Select the line-graph fill color

  Use the spin buttons at the right side of the **Fill color** field to select the color with which the line graph will be filled.

To save the new Settings, close the notebook by double-clicking in the upper left corner.

Configuring Real-Time Settings

Use the selections available in the Real-time settings field group to configure this component's real-time monitor. This field group enables you to:

- Select a background texture (available on OS/2 systems only)

  Use the spin buttons at the right side of the **Background texture** field to select a bit map for use as a background texture for this monitor window.

- Select the filled color

  Use the spin buttons at the right side of the **Filled Color** field to select the color that will be used for the foreground of the real-time monitor.

- Select the empty color

  Use the spin buttons at the right side of the **Empty Color** field to select the color that will be used for the background part of the real-time monitor.

To save the new Settings, close the notebook by double-clicking in the upper left corner.

Configuring Font Settings

Use the selections available in the Font field group to select the font and font color for use with all text in all views for this monitor. This field group enables you to:

- Select a font

  Use the spin buttons at the right side of the font **Name** field to select the font that will be used for text in each of this component's views.

- Select a font color (available on OS/2 systems only)

  Use the spin buttons at the right side of the **Color** field to select the color of the font that will be used for text in each of this component's views.

To save the new Settings, close the notebook by double-clicking in the upper left corner.

Attribute Monitors

Attribute Monitors are used where a numerical value is meaningless. For example, the current status of a RAID device is expressed as a descriptive word (Online, Offline, or Defunct), rather than as a numeric value. Attribute Monitors enable you to view the current status of such a device, and to assign thresholds based on changes in state. Attribute monitors can also have a variety of settings assigned to them.

Note: Attribute monitors are similar to, but not the same as, the RAID alerts described in Appendix D, "RAID Alerts" on page 153. RAID alerts are automatically generated by Netfinity whenever a RAID device changes state, but offer no simple way for you to visually check the current state of a RAID device. Attribute monitors enable to you visually monitor the current state of any RAID device and to create additional thresholds for these devices, if necessary.

Attribute Monitor Thresholds

Attribute monitor thresholds are set from the Attribute Monitor notebook's Threshold page. To open the notebook, using mouse button 2 to click on the monitor for which you want to set a threshold to open the monitor's context menu, select **Open**, and then select **Thresholds**.

To configure a threshold for an Attribute Monitor:

1. Select the attribute that you want to monitor.

   Each Attribute Monitor will contain one or more attributes that can be monitored. The names of these attributes are determined by the type of device. Select from the **Attribute to Monitor** field the name of the attribute that you will monitor.

2. Name the threshold.

   Type in the **Threshold Name** filed a name for this threshold and then press **Enter**.

3. Set the threshold’s duration.

   Type a number and select a unit of measurement (for example, “seconds”) to create a duration value. This value specifies the length of time after the monitored attribute changes state before the alert is generated.

4. Set the resend delay.

   Type a number and select a unit of measurement (for example, “seconds”) to create a resend delay value. This value specifies the length of time that the System Monitor will wait, after sending an alert, before resending a duplicate alert if the attribute’s state remains unchanged.

5. Select a violating state.

   Select from the **State** field the name of the state which, if reported by the the monitored **Attribute**, will generate an alert.

6. Select a severity value.

   Select a **Severity** for the alert that will be generated if the specified **State** is reported.

7. Specify an Application Alert Type value.

   The **Application Alert Type** is a four digit numeric value assigned to the generated alert. It can be used by the Alert Manager to differentiate this alert from other alerts for Alert Action responses. Type in the **Application Alert Type** field a four digit value to be used when this monitor’s alert is generated.

8. Select an Alert Type.

The **Alert Type** is a descriptive term assigned to the generated alert. It can be used by the Alert Manager to differentiate this alert from other alerts for Alert Action responses, and helps to describe the nature of the problem that caused the alert to be generated. Select from the **Alert Type** list an Alert Type to be used when when this monitor's alert is generated.

9. Select Notify (optional).

   Select **Notify** to cause a pop-up window to appear on this system whenever the violating state is reported. If you do not select **Notify**, the threshold will be saved and will be active, but a pop-up window will not automatically inform you if the violating state is reported.

10. Select **Create** to save these threshold values. If you have been editing a previously configured threshold, select **Change** to save the new threshold values.

Attribute Monitor Settings

Attribute Monitor settings are set from the Attribute Monitor notebook's Settings page. To open the notebook, use mouse button 2 to click on the monitor for which you want to set a threshold. From the monitor's context menu, select **Open**, and then select **Settings**.

Use the Attribute Monitor's Settings notebook to:

- Enable or disable the title bar (available on OS/2 systems only)

  Select the **Enable Title Bar** check box to activate a title bar on this monitor. This title bar shows the name of the monitor. If you do not want a title bar, deselect the **Enable Title Bar** check box.

- Enable or disable bit maps (available on OS/2 systems only)

  When the **Enable Bit Maps** check box is selected, a small icon will appear before each monitored attribute. This icon will indicate the attribute's current state.

- Change the monitor's view

  The following views are available for the Attribute Monitor:

- Attribute History

  The Attribute History view shows the state reported by the attribute monitor over a specified period of time.
- Real Time

  The Real Time view shows only the current state of the monitored device.

- Change the monitor's font

  Use the selections available in the Font field group to select the font and font color for use with all text in all views for this monitor. This field group enables you to:

  - Select a font

    Use the spin buttons at the right side of the **Font** field to select the font that will be used for text in each of this component's views.

  - Select a font color (available on OS/2 systems only)

    Use the spin buttons at the right side of the **Color** field to select the color of the font that will be used for text in each of this component's views.

To save the new Settings, close the notebook by double-clicking in the upper-left corner.

IBM PC Server 720 Monitors

Netfinity also includes several additional monitors that are specifically designed for use with the IBM PC Server 720. If Netfinity is installed on an IBM PC Server 720, you can use additional monitors that enable you to keep track of the:

- Power supply temperature (Celsius/Fahrenheit)
- System temperature (Celsius/Fahrenheit)
- Planar temperature (Celsius/Fahrenheit)
- Power supply voltage (+5v, +12v, -12V, and +3.3c)

Chapter 14. System Partition Access

The Netfinity System Partition Access allows for greatly simplified System Partition file handling on IBM computers. This service features:

- Extensive file-level manipulation
- Initial machine load (IML) image updating
- Adapter description program (ADP), adapter description file (ADF), and diagnostic (DGS) updating
- Set Configuration program updating
- User-confirmation security to prevent accidental deletion of the System Partition

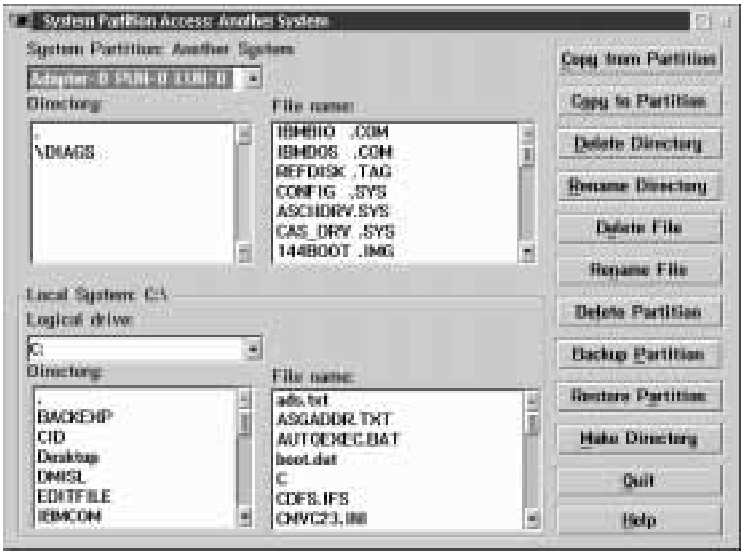
The System Partition is a section of the hard drive on some IBM systems that contains the system's power-on self test (POST), basic input/output system (BIOS), and some system utility programs. If you are not using an IBM system that has a System Partition, you will not have access to, or a need for, this service.

Note: System Partition Access cannot access or manage the System Partitions on *enhanced small device interface* (ESDI) systems.

Netfinity System Partition Access offers a variety of System Partition file-manipulation actions. Available actions are:

- Copy from partition
- Copy to partition
- Delete directory
- Rename directory
- Delete file
- Rename file
- Partition backup
- Partition restore
- Delete partition
- Make directory
- Quit

The following sections provide detailed information on each available action.



System Partition Access: Another System

System Partition: Another System

Adapter: 0 PUN: 0 LUN: 0

Directory:
.
\DIAGS

File name:
IBMBIO .COM
IBMDOS .COM
REFDISK .TAG
CONFIG .SYS
ASCIIDRV.SYS
CAS_DRV .SYS
144BOOT .IMG

Local System: C:\

Logical drive:
C:

Directory:
.
BACKEXP
CID
Desktop
DMISL
EDITFILE
IBMCOM

File name:
ads.txt
ASGADDR.TXT
AUTOEXEC.BAT
boot.dat
C
CDFS.IFS
CNVC23.INI

Figure 36. System Partition Access Service

Copy from Partition

You can use the Copy from Partition option to copy a specific file from within your System Partition to a selected directory on a local drive. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select the System Partition directory you want to copy a file from by selecting the appropriate directory in the System Partition **Directory** field. When you have selected the directory, all files contained in that directory will be displayed in the System Partition **File name** field.
3. Select from the System Partition **File name** field the file that you want to copy.
4. Select a destination drive for the file. Select the arrow at the right side of the **Logical drive** field to display a list of all available drives. Select one of these drives as the file destination.
5. Select a destination directory for the file. All directories present on the selected logical drive are displayed in the Logical Drive **Directory** field. Select one of these directories. All files located in this directory will then be displayed in the Logical Drive **File name** field.
6. Select **Copy from Partition** to copy the selected System Partition file to the selected destination.

Copy to Partition

You can use the Copy to Partition option to copy a specific file from a local drive to your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select the System Partition directory you want to copy a file to by selecting the appropriate directory in the System Partition **Directory** field. When you have selected the directory, all files

contained in that directory will be displayed in System Partition **File name** field.

3. Select the source drive for the file. Select the arrow at the right side of the **Logical drive** field to display a list of all available drives. Select one of these drives as the source drive.
4. Select the source directory for the file. All directories present on the selected logical drive are displayed in the Logical Drive **Directory** field. Select one of these directories. All files located in this directory will then be displayed in the Logical Drive **File name** field.
5. Select from the Logical Drive **File** field the file that you want to copy.
6. Select **Copy to Partition** to copy the selected file to the System Partition.

Delete Directory

You can use the Delete Directory option to delete a directory from your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select from the System Partition **Directory** field the System Partition directory you want to delete. Double-click on the directory name to open the directory.
3. Select **Delete Directory** to delete the selected directory from your system. To prevent accidental directory deletion, you must confirm this choice.

Note: The directory that you are deleting *must be empty* before the Netfinity System Partition Access will allow you to delete it. For information on deleting System Partition files, see “Delete File” on page 143.

Rename Directory

You can use the Rename Directory option to select a new name for a directory within your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select the System Partition directory you want to rename. Double-click on the directory name to open the directory.
3. Select **Rename Directory**. The System Partition Access will ask you to enter the new name for the selected directory.
4. Enter the new directory name and press **Enter**. System Partition Access will rename the directory.

Delete File

You can use the Delete File option to delete individual files from within your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select from the System Partition **Directory** field the System Partition directory that contains the file you want to delete. When you have selected the directory, all files contained in that directory will be displayed in the System Partition **File** field.
3. Select from the System Partition **File name** field the file you want to delete.
4. Select **Delete File**. System Partition Access will then delete the selected file.

Rename File

You can use the Rename File option to rename individual files within your System Partition. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select from the System Partition **Directory** field the System Partition directory that contains the file you want to rename. When you have selected the directory, all files contained in that directory will be displayed in the System Partition **File name** field.

3. Select from the System Partition **File name** field the file you want to rename.
4. Select **Rename File**. System Partition Access will then ask you what you want to rename the file. Enter the new name for the file and press **Enter**. The file is now renamed.

Delete Partition

Attention:
Deleting the System Partition on a system that requires a System Partition can render the system inoperative. Do not use the Delete Partition option unless you are certain that your system will function properly after the System Partition has been deleted.

You can use the Delete Partition option to remove a selected System Partition (displayed in the **System Partition** field) from your selected Logical Drive. When you have selected this option, System Partition Access will ask you to confirm that you want to delete the partition. To continue, select **OK** and the selected System Partition (as well as all directories and files within the partition) will be deleted.

Backup Partition

You can use the Backup Partition option to copy the System Partition to a file on any logical drive. To use this function:

1. If you have multiple System Partitions, select from the **System Partition** field the partition you want to access.
2. Select a destination drive for the System Partition backup file to be written to. Select the arrow at the right side of the **Logical drive** field to display all available logical drives, and then select the appropriate drive.
3. Select a destination directory. Directories present on the selected logical drive are displayed in the Logical Drive **Directory** field.
4. Select **Partition Backup** to write a file of the selected System Partition to your specified destination.

Restore Partition

You can use the Restore Partition option to restore your System Partition using backup diskettes or files created with the Backup Partition function. To use this function:

1. Select the source drive where the System Partition backup file is located. Select the arrow at the right side of the **Logical drive** field to display all available logical drives, and then select the appropriate drive..

2. Select the source directory where the backup file is located. All directories present on the selected logical drive are displayed in the Logical Drive **Directory** field. Select one of these directories. All files located in this directory will then be displayed in the Logical Drive **File name** field. Select the backup file that you want to use from the Logical Drive **File name** field.

3. Select **Restore Partition** to copy your backup file to the System Partition.

Make Directory

You can use the **Make Directory** option to add a directory to the selected System Partition (displayed in the **System Partition** field). After you have selected this option, System Partition Access will ask you to provide a name for the new directory.

Quit

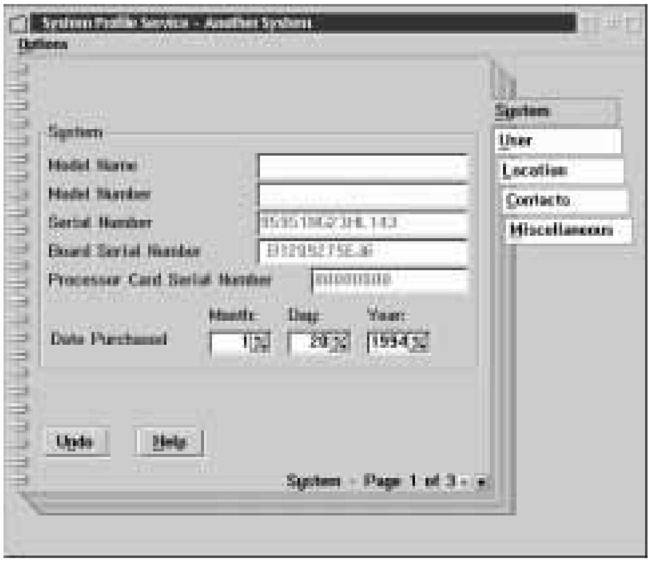
Select **Quit** to exit System Partition Access.

Chapter 15. System Profile

System Profile provides you with an easy-to-organize repository for a variety of system- and user-specific information that might not be readily available otherwise. The System Profile service comes with many predefined fields to help simplify organization and entry of this data. The System Profile service also features many user-definable fields to help you customize the System Profile to meet your individual needs.

System Profile's data can be saved to an ASCII file. The combination of System Information Tool's sophisticated hardware information gathering abilities with System Profile's extensive selection of system- and user-specific data fields results in an extraordinarily flexible and useful system-inventorying and information facility.

Note: System Profile supports export of collected data to a Netfinity database. However, database export can be performed only by the Netfinity Manager. No database export functions are available for local use on systems running Client Services for Netfinity Manager.



System Profile Service - Another System

System

Model Name:
Model Number:
Serial Number: [illegible]
Board Serial Number: [illegible]
Processor Card Serial Number: [illegible]
Date Purchased: Month: 1 Day: 28 Year: 1994

System - Page 1 of 3

Figure 37. The System Profile service window.

The System Profile service window is made up of five sections, each of which consists of two or more pages and is devoted to a specific type of system- or user-specific information. Each section is identified by its own tab. These sections are:

- System

  The System section of the System Profile service contains predefined fields to help you organize the information specific to your computer, display, printer, and modem.

- User

  The User section of the System Profile service contains predefined fields to help you organize the information specific to a system's primary user including name, phone number, home address, and emergency contact.

- Location

  The Location section of the System Profile service contains predefined fields to help you organize the information specific to the system's physical location, including office number, building number, site name, city, and country.

- Contacts

  The Contacts section of the System Profile service contains predefined fields to help you organize the information regarding various ways of contacting the system's primary user (telephone number, fax number, Email address, and so on) and other personnel associated with the primary user (for example, manager, secretary, and so on).

- Miscellaneous

  The Miscellaneous section of the System Profile service contains undefined fields that you can use to store additional information, such as nicknames and birthdays.

To enter and save data in the System Profile service:

1. Enter the data you want to save in the appropriate fields.

   Select a field and type in the appropriate data. To change pages, select one of the small arrows at the lower right corner of the page (select the right-pointing arrow to advance one page, and the left-pointing arrow to go back one page). To change sections, select the section's tab from the right side of the service window. You do not need to fill in all of the available fields.

2. Close the System Profile service.

   When you have finished entering information, double-click on the upper-left corner of the System Profile service to save your information and close the service window.

Select **Undo** to reset the current page's fields to their last saved values. Selecting Undo will not have any affect on the other pages in the service window.

To close the service window without saving any changes, select **Close Without Saving** from the Options pull-down menu.

Other actions available from the Options pull-down menu are:

- Refresh

  Select **Refresh** to update the information that is displayed in the System Profile service window. Changes can be made to the service window's contents by other users while you are viewing it; selecting **Refresh** will update the data displayed in the System Profile service window's fields.

- Save to File

  Select **Save To File** to save all information contained in the System Profile service to an ASCII text file.

Appendix A. Installation Configurations

When installing the Client Services for Netfinity Manager, you can choose one of three installation configurations. Each of these configurations installs a specific group of Netfinity services on your system.

Stand-Alone Operation

This installation configuration installs base programs and interfaces for:

- Netfinity Service Manager
- System Information Tool
- System Profile
- System Monitor
- Alert Manager
- Critical File Monitor
- Software Inventory

Also, the following services are installed if they are supported by your system:

- ECC Memory Setup (requires ECC memory)
- System Partition Access (requires a System Partition)
- Predictive Failure Analysis (requires a PFA-enabled hard disk drive)
- RAID Manager (requires a RAID adapter)
- DMI Browser (requires DMI Service Layer)

Passive Client Operation

This installation configuration installs:

- Netfinity Service Manager
- Network Communications drivers
- Alert Manager
- Security Manager
- Serial Connection Control
- All base programs for Netfinity services supported by your system

Note: Passive Client Operation is designed specifically for the remote management and access of Passive Client systems by a Netfinity Remote System Manager. Aside from the Alert Manager, Security Manager, and Serial Connection Control, local access to the Client Services for Netfinity Manager is not available.

Active Client Operation

This installation configuration installs the following for remote system management:

- Netfinity Service Manager
- Network Communications drivers
- Alert Manager base program and user interface
- All base programs for Netfinity services supported by your system

The following programs are installed to support local system management:

- Netfinity Service Manager
- System Information Tool
- System Profile
- System Monitor
- Alert Manager
- Security Manager
- Serial Connection Control
- Critical File Monitor

The following services are also installed if they are supported by your system:

- ECC Memory Setup (requires ECC memory)
- System Partition Access (requires a System Partition)
- Predictive Failure Analysis (requires a PFA-enabled hard disk drive)
- RAID Manager (requires a RAID adapter)
- DMI Browser (requires DMI Service Layer)

Appendix B. Supported PFA Hard Disk Drives

The following PFA-enabled hard disk drives are supported by Predictive Failure Analysis. Only the listed hard disk drives can be monitored or managed by the Predictive Failure Analysis service. If one of these drives is not present in your system when Netfinity is installed, the service will not be installed.

- IBM Type 0664 Hard Disk Drive
- IBM Type 0663 Hard Disk Drive
- IBM Type 0662 Hard Disk Drive
- IBM Type DPES-31080 Hard Disk Drive (product revision 531Q only)
- IBM Type DFHS Hard Disk Drive
- IBM Type DFMS Hard Disk Drive
- IBM Type XP31 Hard Disk Drive
- IBM Type XP32 Hard Disk Drive
- IBM Type XP34 Hard Disk Drive
- IBM Type DORS-3216DW Hard Disk Drive
- IBM Type FIREBALL12805 Hard Disk Drive (product revision 630N or later)

In addition to these hard disk drives, Netfinity Manager and Client Services for Netfinity Manager for OS/2 or Windows NT support PFA-enabled hard disk drives that conform to the self-monitoring analysis and reporting technology (SMART) standard. Support for SMART hard disk drives is available only on systems running Netfinity Manager or Client Services for Netfinity for OS/2 or Windows NT.

Appendix C. Supported RAID Adapters

The following RAID adapters are supported:

- IBM RAID Adapter
- IBM SCSI-2 Fast/Wide-Streaming RAID Adapter/A
- IBM SCSI-2 Fast PCI-Bus RAID Adapter
- IBM PC ServeRAID Adapter
- IBM PC ServeRAID PCI Adapter
- IBM PC ServeRAID PCI II Adapter

Appendix D. RAID Alerts

A RAID adapter (RAID means *redundant array of independent disks*) attaches to multiple physical disk drives, and enables you to treat these drives as up to eight system (or logical) drives. Although the System Monitor service does not display a monitor if a RAID system is present, it does monitor the status of all disk drives that are attached to the RAID adapter to ensure that they are online and functioning correctly.

The RAID adapter will detect when physical drives or system drive become active or inactive. This is called a drive's *state*.

System drives report one of three states. These states are:

- Online
- Critical
- Offline

Note: The Critical state can only be reported by RAID level 1, 2, 3, or 4 system disk drives. RAID level 0 system disk drives cannot report a Critical state. All RAID level 0 disk drives are either Online or Offline. For more information on RAID levels, see your RAID adapter documentation.

Physical drives report one of three states. These states are:

- Online
- Standby
- Defunct

RAID alerts are generated *only* when the RAID disk drive changes state. It the state remains unchanged, additional alerts will not be generated.

The alert text of all RAID alerts generated by System Monitor follow this format:

```
Alert: RAID Device state  Attribute typeandlocation
in subsystem set to state
```

where *state* is the state reported by the drive., *typeandlocation* is the type of RAID disk drive (Physical or System) and its designated location (System Drive number or Physical Bay number), and *subsystem* is the name of the RAID subsystem reporting the state change.

The alert-specific information for each RAID alert follows.

RAID Physical Disk Drive State is Online

Description	Generated when a physical drive changes state from Standby or Defunct to Online.
Alert Type	Information
Severity	3
Application ID	MonitorB
Application Alert Type	130

RAID Physical Disk Drive State is Standby

Description	Generated when a physical drive changes state from Online or Defunct to Standby.
Alert Type	Error
Severity	2
Application ID	MonitorB
Application Alert Type	130

RAID Physical Disk Drive State is Defunct

Description	Generated when a physical drive changes state from Online or Standby to Defunct.
Alert Type	Failure
Severity	0
Application ID	MonitorB
Application Alert Type	130

RAID System Disk Drive State is Online

Description	Generated when a system drive changes state from Critical or Offline to Online.
Alert Type	Information
Severity	3
Application ID	MonitorB
Application Alert Type	131

RAID System Disk Drive State is Critical

Description	Generated when a system drive changes state from Online or Offline to Critical.
Alert Type	Warning
Severity	2
Application ID	MonitorB
Application Alert Type	131

RAID System Disk Drive State is Offline

Description	Generated when a system drive changes state from Critical or Online to Offline.
Alert Type	Failure
Severity	0
Application ID	MonitorB
Application Alert Type	131

Note: If a RAID physical disk drive generates an alert message, you will generally receive alert messages from all system drives that are associated with that physical drive.

Several of Netfinity's services can be accessed from your system's command line. The following sections describe how these services can be accessed from a command line, as well as the various parameters associated with their use.

Alert Manager Command Line Operations

The Alert Manager service does not have any command line operations. However, GENALERT.EXE is a program that causes an alert to be generated within your system. This alert may have a number of user-specified parameters, described below.

Note: If you want alerts generated using GENALERT to be forwarded to a host system using the "Send alert to host via APPC" alert action, see "Adding GENALERT Alert Descriptions to the NMVT.INI File" on page 157.

The command-line format for GENALERT.EXE is:

```
GENALERT /T:"text" /APP:id_name
/SEV:0..7 /TYPE:sssttt /ATYPE:hexnum
```

where:

/T:"*text*" Defines the text message describing the alert. The quotation marks are required.

/APP:*id_name* Defines the application ID for the alert (1—8 characters)

/SEV:*0...7* Defines the priority or severity of the alert (0=highest priority, 7=lowest priority).

/TYPE:*sssttt* Defines the standard type of alert.

The *sss* field describes the ID of the alert:

UNK - Unknown
SYS - System
DSK - Disk or DASD
NET - Network
OS_ - Operating System
APP - Application
DEV - Device
SEC - Security

The *ttt* field describes the class of the alert:

UNK - Unknown
FLT - Fault or Failure
ERR - Error
WRN - Warning
INF - Information

/ATYPE:*hexnum* Defines the application-specific alert type as a hexadecimal value. Values range from 0000 to FFFF.

Adding GENALERT Alert Descriptions to the NMVT.INI File

The NMVT.INI file, found in the Netfinity directory, contains alert descriptions that map standard Netfinity alerts to NMVT-style alerts that can then be properly passed to a host system using advanced program-to-program communications (APPC) and the “Send alert to host via APPC” alert action. However, because alerts generated using the GENALERT command are configured and defined by the user, they are not included in this file. As a result, if you do not add entries to the NMVT.INI file for GENALERT alerts, the “Send alert to host via APPC” alert action will not have the data it needs to build the NMVT (including alert description, failure causes, recommended actions, and so forth) and will be unable to pass this information to the host.

To enable a system to pass GENALERT-created alert information to the host, you must add an entry to the NMVT.INI file located in the Netfinity directory of the system generating the alert. This entry, like all other entries in the NMVT.INI file, must consist of information about the Netfinity alert (including application name, alert type, and alert severity) followed by configuration data for the NMVT that will be sent to the host.

For example, generate an alert using the following GENALERT command:

```
GENALERT /T:"Virus Detected" /APP:ANTVIR /SEV:0
/TYPE:SECWRN /ATYPE:000C
```

In order for this alert to be properly forwarded to the host, you must edit the NMVT.INI file and include an entry specifically created to translate the Netfinity alert information into NMVT-specific information. For example:

```
APP:ANTVIR TYPE:SECWRN SEV:0 ATYPE:000C GTYPE:01
DESC:C007 CAUSE:6700 USER:7199:1026 FAIL:0501:18003103
```

Once this entry is added to the NMVT.INI file, the Alert Manager will be able to use the "Send alert to host via APPC" alert action to convert this alert into an NMVT and forward it to the host system.

System Information Tool Command Line Operations

The System Information Tool can be started from a command line, and supports five command line parameters. The command line format for System Information Tool is:

```
SINFG30 /P:filename /H:filename
/F:history filename /NOLOGO /B
```

The command line parameters are as follows:

/P: *filename* This parameter is used to generate a report of all the information collected by the program. A logical printer name like LPT1 can be substituted for a file name, which will send the report to a printer. The program logo screen will be displayed while the information is being gathered, and the program will terminate after the report has been generated.

/H: *filename* This parameter is used to generate a binary history file that contains all of the information detected by the program, as well as the time and date that the report was generated. This file can then be used as an input source using the **/F** command-line parameter. The program logo screen will be displayed while the information is being gathered, and the program will terminate after the file is generated.

/F: *history filename*

This parameter causes the program to use a previously generated history file as the source for information gathering, rather use than the physical system the program is being executed on. You can use this option to view a history file from another system.

/NOLOGO When this parameter is used, the program logo will not be displayed. This parameter can be used in conjunction with any of the other parameters.

/B This parameter causes the program to bypass all warning and informational messages while the program is starting. This could be used for unattended system startups. This parameter can be used in conjunction with any of the other parameters.

ECC Memory Setup Command Line Operations

All functions of the ECC Memory Setup can also be accessed from your OS/2 command line, using ECCMEM.EXE.

Note: ECCMEM.EXE is available for use only on systems running OS/2.

The command line format for ECCMEM.EXE is:

```
ECCMEM /INIT /SCRUB:ON or OFF /THRESH:ON or OFF
/COUNT:ON or OFF /QUIET  /COUNTVAL:number
/THRESHVAL:number
```

where:

/INIT Causes the ECC memory to be initialized to the saved settings

/SCRUB*ON or OFF*[1] Enables or disables single-bit error scrubbing

/THRESH:*ON or OFF*[1] Enables or disables single-bit error threshold nonmaskable interrupt (NMI)

/COUNT:*ON or OFF*[1] Enables or disables single-bit error counting

/QUIET Causes ECCMEM.EXE to generate no textual output

/COUNTVAL:*number* Sets the single-bit error count to a given value

/THRESHVAL:*number*[1] Sets the single-bit error threshold to a given value

[1] These options update the saved settings to the value provided. When the system is restarted, the saved settings will configure the ECC memory.

Starting and Stopping Service Base Programs Remotely

You can use the Netfinity STRTBASE.EXE and STOPBASE.EXE command-line programs to remotely start or stop the base program of most Netfinity services.

Note: STRTBASE.EXE and STOPBASE.EXE can start and stop the base programs only for individual Netfinity services. These programs cannot be used to remotely start or stop the Netfinity Network Interface, the Netfinity Support Program, or any base program that is started by the Netfinity Network Interface or the Netfinity Support Program (these include the base programs for Alert Manager, Power-On Error Detect, System Monitor, and Serial Connection Control). One of these programs **must** be running on the remote system for STRTBASE.EXE or STOPBASE.EXE to function properly.

Starting Service Base Programs Remotely

From your system, use STRTBASE.EXE to start a Netfinity service's base program on a remote system. The command line format for STRTBASE.EXE is:

```
STRTBASE \N:networktype::networkaddress
\BASE:servicebase [\BATCH] [\?]
```

Variable	**Definition**
networktype	Name of the protocol to be used to send the message (for example, TCPIP)
networkaddress	Protocol-specific address of the remote system on which the base program will be started (for example, user.network.com)
servicebase	The service connection name of the program base to be started on the remote system. For a list of the service connection names that must be used with this command, see "Service Connection Names" on page 163.
BATCH	Program runs with no output. When STRTBASE.EXE is run in BATCH mode, a file named SYSNAME.OUT that contains

	the remote system’s name is created in the same directory as STRTBASE.EXE
?	Displays command line help.

Stopping Service Base Programs Remotely

From your system, use STOPBASE.EXE to stop a Netfinity service’s base program on a remote system. The command line format for STOPBASE.EXE is:

```
STOPBASE \N:networktype::networkaddress
\BASE:servicebase [\BATCH] [\?]
```

Variable	**Definition**
networktype	Name of the protocol to be used to send the message (for example, TCPIP)
networkaddress	Protocol-specific address of the remote system on which the base program will be stopped (for example, user.network.com)
servicebase	The service connection name of the program base to be stopped on the remote system. For a list of the service connection names that must be used with this command, see “Service Connection Names” on page 163.
BATCH	Program runs with no output. When STOPBASE.EXE is run in BATCH mode, a file named SYSNAME.OUT that contains the remote system’s name is created in the same directory as STOPBASE.EXE
?	Displays command line help.

Service Connection Names

A list of the service connection names that must be used with the STRTBASE.EXE and STOPBASE.EXE programs follows.

Service Connection Name	Service Name
CFMBase	Critical File Monitor
ProcMgr	Process Manager
ECCMemory	ECC Memory Setup
Gatherer3.0	System Information Tool (Version 3.0 or later)
Gatherer	System Information Tool (all other versions)
PFAServiceBase	Predictive Failure Analysis
ScreenID	Screen View
DMIBrowserBase	DMI Browser
RAID_BASE	RAID Manager
RCSHD	Remote Session
SoftInvB	Software Inventory
FileBase	File Transfer
PartionBase	System Partition Access
SCH_BASE_NODE	Event Scheduler
ProfileBase	System Profile
CAPMGT	Capacity Management
RWCService	Remote Workstation Control
DiagMgr	System Diagnostic Manager
SCFMgr	Service Configuration Manager
ServiceProcessorBase	Service Processor Manager
UpdateConnector	Update Connector Manager (interface)

UpdateConnectorClient	Update Connector Manager (interface or client)

Appendix F. Netfinity Alerts

All Netfinity Alerts include the time and date at which the Alert was generated. The other information depends on which service generated the Alert and the circumstances that caused the Alert to be generated.

Some Alerts have values that can be assigned by the user. This often applies to Severity values, although there are some exceptions. In this case, the Alert information will be signified with a variable, and a note below the alert data will provide any clarification necessary.

Some alerts support macro parameter strings. These strings (%P1–%P9) can be passed through to and used by other programs.

Each alert and its alert-specific information are listed beneath the heading of the service that generates the alert.

Power On Error Detect

Explanation	Generated by the Power-On Error Detect service when a Power-On Error is detected on a remote system. The Power-On Error Detect will generate this alert only if the service's **Generate Alert on Error** option is enabled.
Alert Text	Netfinity Power-On Error Detect Alert
Type of Alert	Failure
Severity	4
Application ID	Power-On Error Detect
Application Alert Type	0201

This alert does not support additional parameter strings.

Predictive Failure Analysis

Explanation
Generated by the Predictive Failure Analysis service when the service receives notification from a PFA-enabled hard disk drive that a drive failure will occur within 24 hours. The Predictive Failure Analysis service will generate this alert only if the service's **Generate Alert** option is enabled.

Alert Text
Predictive Failure Analysis has detected an imminent failure on PUN *w*, LUN *x* hard drive. Back up physical drive *y* and call your service provider for a replacement.

Type of Alert
Disk Failure

Severity
z

Application ID
PFA

Application Alert Type
0000

This alert does not support additional parameter strings.

Notes:

1. The Alert Text variables *w*, *x*, and *y* are determined by the Predictive Failure Analysis service, and represent the PUN, LUN, and drive letter assigned to the failing PFA-enabled hard disk drive, respectively.
2. You can add additional text to this alert. For more information, see "The PFA Options for Drive Window" on page 63.
3. You can specify the Severity variable *z*. For more information, see "The PFA Options for Drive Window" on page 63.

Critical File Monitor

Alerts generated by the Critical File Monitor follow.

File Changed Alert

Explanation	Generated by Critical File Monitor when a monitored file changes size, date, or time.
Alert Text	The following file has changed: '*filename*'.
Type of Alert	Application Warning
Severity	*x*
Application ID	MonCritF
Application Alert Type	0

This alert does not support additional parameter strings.

Notes:

1. The Alert Text variable *filename* is the name of the file that has changed.
2. You can set the Severity variable *x*. The default Severity value for this alert is 3.

File Deleted Alert

Explanation	Generated by Critical File Monitor when a monitored file is deleted.
Alert Text	The following file has been deleted: '*filename*'.
Type of Alert	Warning
Severity	*x*
Application ID	MonCritF
Application Alert Type	1

This alert does not support additional parameter strings.

Notes:

1. The Alert Text variable *filename* is the name of the file that has been deleted.
2. You can set the Severity variable *x*. The default Severity value for this alert is 3.

File Created Alert

Explanation	Generated by Critical File Monitor when a monitored file is created.
Alert Text	The following file has been created: '*filename*'.
Type of Alert	Warning
Severity	*x*
Application ID	MonCritF
Application Alert Type	2

This alert does not support additional parameter strings.

Notes:

1. The Alert Text variable *filename* is the name of the file that has been created.
2. You can set the Severity variable *x*. The default Severity value for this alert is 3.

Process Manager

Alerts generated by Process Manager follow.

Process Terminated Alert

Explanation	Generated by Process Manager when a monitored process is stopped.
Alert Text	Process '*%P1*' has terminated.
Type of Alert	Application Information
Severity	*x*
Application ID	ProcMgr
Application Alert Type	0901

Notes:

1. This alert supports the following macro parameter string:

   %P1 Name of the process that has been terminated.
2. You can set the Severity variable *x*.

Process Started Alert

Explanation	Generated by Process Manager when a monitored process is started.
Alert Text	Process '*%P1*' has started.
Type of Alert	Application Information
Severity	*x*
Application ID	ProcMgr
Application Alert Type	0900

Notes:

1. This alert supports the following macro parameter string:

   %P1 Name of the process that has been started.

2. You can set the Severity variable *x*.

Process Failed to Start Alert

Explanation	Generated by Process Manager when a monitored process fails to start within a specified time of system startup.
Alert Text	Process '*%P1*' has failed to start.
Type of Alert	Application Information
Severity	*x*
Application ID	ProcMgr
Application Alert Type	0902

Notes:

1. This alert supports the following macro parameter string:

   %P1 Name of the process that has failed to start.

2. You can set the Severity variable *x*.

Remote System Manager

Alerts generated by the Remote System Manager follow.

System Online Notification Alert

Explanation
Generated when the Remote System Manager receives notification from a remote system that the system is online and reachable. The Remote System Manager service will generate this alert only if the service's System Notifications: Notify When Online option has been enabled for a system within a system group.

Alert Text
Alert Text: System '*%P1*' (Address '*%P2*' on Network '*%P3*') is active and online.

Type of Alert
System Information

Severity
x

Application ID
NetMgr

Application Alert Type
000A

Notes:

1. This alert supports the following macro parameter strings:

   %P1 System Name of active system. This is set to indicate the system that has come online.

   %P2 Network Address of active system. This is set to indicate the system that has come online.

   %P3 Network Type of active system.

2. You can set the Severity variable *x*.

System Offline Notification Alert

Explanation	Generated when the Remote System Manager is incapable of reaching a remote system. The Remote System Manager service will generate this alert only if the service's System Notifications: Notify When Offline option has been enabled for a system within a system group.
Alert Text	Alert Text: System '*%P1*' (Address '*%P2*' on Network '*%P3*') is offline or unreachable.
Type of Alert	System Information
Severity	*x*
Application ID	NetMgr
Application Alert Type	000B

Notes:

1. This alert supports the following macro parameter strings:

   %P1 System Name of inactive system. This is set to indicate the system that has gone offline.

   %P2 Network Address of inactive system. This is set to indicate the system that has gone offline.

   %P3 Network Type of inactive system.

2. You can set the Severity variable *x*.

Security Manager

Access Granted Alert

Explanation	Generated by the Security Manager service when access to one or more services is granted to a remote user who has used a UserID / Password combination to gain access.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been granted system access.
Type of Alert	Security Information
Severity	7
Application ID	SecMgr
Application Alert Type	14

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

Public Access Granted Alert

Explanation	Generated by the Security Manager service when Public access to one or more services is granted to a remote user.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been granted public system access.
Type of Alert	Security Information
Severity	6
Application ID	SecMgr
Application Alert Type	15

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

System Access Denied Alert

Explanation	Generated by the Security Manager service when access to the system is denied to a remote user.
Alert Text	Logon attempt by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' has been rejected.
Type of Alert	Security Warning
Severity	5
Application ID	SecMgr
Application Alert Type	16

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system access
%P2	Network Address of system requesting access
%P3	Network Type of system requesting access

System Restart Initiated Alert

Explanation Generated by the Security Manager service when a remote Netfinity Manager uses the Remote System Manager's Restart System option to restart your system.

Alert Text System Restart initiated by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*'.

Type of Alert Security Information

Severity 5

Application ID SecMgr

Application Alert Type 41

Note: This alert supports the following macro parameter strings:

%P1 User ID requesting system restart

%P2 Network Address of system requesting restart

%P3 Network Type of system requesting restart

System Restart Request Rejected Alert

Explanation Generated by the Security Manager service when a remote Netfinity Manager attempts to use the Remote System Manager's Restart System option to restart your system, but does not have adequate security access to do so.

Alert Text System Restart request by User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' rejected.

Type of Alert Security Error

Severity 3

Application ID SecMgr

Application Alert Type 40

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting system restart
%P2	Network Address of system requesting restart
%P3	Network Type of system requesting restart

Service Manager

Alerts generated by the Service Manager follow.

Service Start Request Alert

Explanation	Generated by the Service Manager when a remote Netfinity Manager attempts to use one of your Netfinity services.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' requested start of '*%P4*' service.
Type of Alert	Security Information
Severity	7
Application ID	SvcMgr
Application Alert Type	0900

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting service start
%P2	Network Address of system requesting service start
%P3	Network Type of system requesting service start
%P4	Name of service requested to be started

Service Start Request Rejected Alert

Explanation	Generated by the Service Manager when a remote Netfinity Manager's request to use one of your Netfinity services is rejected.
Alert Text	User ID '*%P1*' from Address '*%P2*' on Network '*%P3*' request to start '*%P4* rejected.'
Type of Alert	Security Warning
Severity	5
Application ID	SvcMgr
Application Alert Type	0901

Note: This alert supports the following macro parameter strings:

%P1	User ID requesting service start
%P2	Network Address of system requesting service start
%P3	Network Type of system requesting service start
%P4	Name of service requested to be started

System Monitor

Alerts generated by System Monitor follow.

Upper-Range Threshold Error Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component exceeds the upper-range Error value for greater than the specified time.
Alert Text	Error Alert *%P1*: Monitor '*%P2*' has been above or equal to *%P3* for *%P4*.
Type of Alert	Error
Severity	*x*
Application ID	MonitorB
Application Alert Type	0000

Notes:

1. This alert supports the following macro parameter strings:

%P1	Name of the threshold
%P2	Name of the monitor
%P3	Threshold value
%P4	Duration of threshold violation

2. You can set the Severity variable *x*. The default value for this variable is 3.

Upper-Range Threshold Warning Alert

Explanation Generated by the System Monitor service when the value of a monitored system component exceeds the upper-range Warning value for greater than the specified time.

Alert Text Warning Alert *%P1*: Monitor '*%P2*' has been above or equal to *%P3* for *%P4*.

Type of Alert Warning

Severity *x*

Application ID MonitorB

Application Alert Type 0000

Notes:

1. This alert supports the following macro parameter strings:

   %P1 Name of the threshold

   %P2 Name of the monitor

   %P3 Threshold value

   %P4 Duration of threshold violation

2. You can set the Severity variable *x*. The default value for this variable is 4.

Lower-Range Threshold Warning Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component falls below the lower-range Warning value for greater than the specified time.
Alert Text	Warning Alert *%P1*: Monitor '*%P2*' has been below or equal to *%P3* for *%P4*.
Type of Alert	Warning
Severity	*x*
Application ID	MonitorB
Application Alert Type	0000

Notes:

1. This alert supports the following macro parameter strings:

%P1	Name of the threshold
%P2	Name of the monitor
%P3	Threshold value
%P4	Duration of threshold violation

2. You can set the Severity variable *x*. The default value for this variable is 4.

Lower-Range Threshold Error Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component falls below the lower-range Error value for greater than the specified time.
Alert Text	Error Alert *%P1*: Monitor '*%P2*' has been below or equal to *%P3* for *%P4*.
Type of Alert	Error
Severity	*x*
Application ID	MonitorB
Application Alert Type	0000

Notes:

1. This alert supports the following macro parameter strings:

%P1	Name of the threshold
%P2	Name of the monitor
%P3	Threshold value
%P4	Duration of threshold violation

2. You can set the Severity variable *x*. The default value for this variable is 2.

Threshold Return To Normal Alert

Explanation	Generated by the System Monitor service when the value of a monitored system component returns from a threshold exception state to a specified “normal” state or range.
Alert Text	Informational Alert *%P1*: Monitor '*%P2*' has returned to normal.
Type of Alert	Error
Severity	*x*
Application ID	MonitorB
Application Alert Type	10

Notes:

1. This alert supports the following macro parameter strings:

%P1	Name of the threshold
%P2	Name of the monitor

2. You can set the Severity variable *x*. The default value for this variable is 6.

Physical RAID Device Online Alert

Explanation	Generated by the System Monitor service when a physical RAID drive changes state to Online.
Alert Text	RAID Device Online: Attribute Physical Drive *x* in *y* set to online.
Type of Alert	Information
Severity	3
Application ID	MonitorB
Application Alert Type	130

Notes:

1. Alert Text variable *x* is the physical drive's designated location (Physical Bay number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix C, "Supported RAID Adapters" on page 152).

Physical RAID Device Standby Alert

Explanation	Generated by the System Monitor service when a physical RAID drive changes state to Standby.
Alert Text	RAID Device Standby: Attribute Physical Drive *x* in *y* set to standby.
Type of Alert	Information
Severity	2
Application ID	MonitorB
Application Alert Type	130

Notes:

1. Alert Text variable *x* is the physical drive's designated location (Physical Bay number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix C, "Supported RAID Adapters" on page 152).

Physical RAID Device Dead Alert

Explanation	Generated by the System Monitor service when a physical RAID drive changes state to Dead.
Alert Text	RAID Device Dead: Attribute Physical Drive *x* in *y* set to dead.
Type of Alert	Failure
Severity	0
Application ID	MonitorB
Application Alert Type	130

Notes:

1. Alert Text variable *x* is the physical drive's designated location (Physical Bay number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix C, "Supported RAID Adapters" on page 152).

Logical RAID Device Online Alert

Explanation	Generated by the System Monitor service when a logical RAID system drive changes state to Online.
Alert Text	RAID Device Online: Attribute System Drive *x* in *y* set to online.
Type of Alert	Information
Severity	3
Application ID	MonitorB
Application Alert Type	131

Notes:

1. Alert Text variable *x* is the system drive's designated location (System Drive number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix C, "Supported RAID Adapters" on page 152).

Logical RAID Device Critical Alert

Explanation	Generated by the System Monitor service when a logical RAID system drive changes state to Critical.
Alert Text	RAID Device Critical: Attribute System Drive *x* in *y* set to critical.
Type of Alert	Warning
Severity	2
Application ID	MonitorB
Application Alert Type	131

Notes:

1. Alert Text variable *x* is the system drive's designated location (System Drive number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix C, "Supported RAID Adapters" on page 152).

Logical RAID Device Offline Alert

Explanation	Generated by the System Monitor service when a logical RAID system drive changes state to Offline.
Alert Text	RAID Device Offline: Attribute System Drive *x* in *y* set to offline.
Type of Alert	Failure
Severity	0
Application ID	MonitorB
Application Alert Type	131

Notes:

1. Alert Text variable *x* is the system drive's designated location (System Drive number), and *y* is the name of the RAID subsystem reporting the state change.
2. This alert will be generated only by systems that have a supported RAID adapter (see Appendix C, "Supported RAID Adapters" on page 152).

Appendix G. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

IBM	Netfinity
Micro Channel	NetView
OS/2	Predictive Failure Analysis
PS/2	SystemView

The following terms are trademarks of other companies:

cc:Mail	cc:Mail, Inc. division of Lotus Development Corporation
DMI	Desktop Management Task Force
IPX	Novell, Incorporated
Lotus Notes	Lotus Development Corporation
NetWare	Novell, Incorporated
Novell	Novell, Incorporated
Sportster	U. S. Robotics

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Pentium is a registered trademark of Intel Corporation.

Tivoli is a trademark of Tivoli Systems.

Other company, product, and service names may be trademarks or service marks of others.

Appendix H. Index

Part Number: 10L9268

Printed in U.S.A.

10L9268