DIGITAL ServerWORKS™ Manager

Installation and User Guide

Part number: ER-4QXAA-UA. H01

Digital Equipment Corporation

September 1998

Contents

3 Installation

4 Discovering Networks and Objects

5 Setting Alarms

7 Getting the Data You Want

8 Managing Windows NT and NetWare

A Additional Procedures and Information

B Troubleshooting

C Reference sources

Figures

Tables

Preface P

This document explains how to use the DIGITAL ServerWORKS Manager® product to manage DIGITAL servers and other devices. It also provides detailed procedures for installing, configuring, and using the ServerWORKS Manager Console.

Audience

This guide is intended for the network administrator or server administrator who is installing and configuring ServerWORKS Manager Console and agents. This guide assumes that you are familiar with networking fundamentals and the SNMP protocol.

Related Information

Refer to the following sources for more information:

- Appendix C, which contains a bibliography and glossary
- *DIGITAL ServerWORKS Manager Enterprise Management Integration Guide*
- *Using the ClientWORKS® Management Suite with DIGITAL PCs: A Guide for Network Administrators*

Conventions Used in This Guide

The terms “Select” and “Choose” are used frequently in the procedures. Both terms refer to specific mouse pointer or keyboard operations:

- Select—Move the mouse pointer to an item (icon, command, name) and single-click the mouse button, or use the specified set of keyboard keys to indicate a choice.
- Choose—Move the mouse pointer to an item and double-click the mouse button, or use the specified set of keyboard keys to start an action on the selected item.

The following icons are used in the manual:

Note: Indicates helpful information. The note can be a tip, special technique, shortcut or other information to help you use the product. A note is not a warning or caution of serious consequences.

Caution: Indicates important information. Failure to use the information can result in problems.

Warning: Indicates significant information or instructions to be observed. Failure to use the information can result in loss of data or other catastrophic failure.

Keyboard Conventions

To Do This	Press These Keys:
Scroll one window up or down	PAGE UP or PAGE DOWN
Go to the beginning of the list	CTRL+HOME
Go to the end of the list	CTRL+END
Move focus left or right	LEFT or RIGHT ARROW
Move one line up or down	UP or DOWN ARROW
Move to next window	CTRL+TAB
Move to previous window	CTRL+SHIFT+TAB
Go to the next field	DOWN ARROW or TAB
Go to the previous field	UP ARROW or SHIFT+TAB
Go to the next group	CTRL+DOWN+ARROW
Go to the previous group	CTRL+UP+ARROW
Move the focus up or down without affecting the state of the previous line (to add or remove lines from a selected set)	SHIFT+UP ARROW or SHIFT+DOWN ARROW
Toggle the state of the focus item	SPACEBAR
Display Help	F1
Display Help (from a console window)	CTRL+ALT+F1

Introduction 1

DIGITAL ServerWORKS Manager is a management tool for network and server administrators. You can monitor and manage the following objects using ServerWORKS agents and the Console:

- DIGITAL and non-DIGITAL servers and clusters running a wide range of operating systems
- Multi-vendor network components and non-server objects
- DIGITAL desktop systems

The Advantages of ServerWORKS Manager

ServerWORKS Manager is a comprehensive network management tool that facilitates network monitoring and diagnosis. ServerWORKS uses SNMP (Simple Network Management Protocol) as its primary mechanism for communication with servers and managed objects. Using ServerWORKS you can find, monitor, and manage devices that support SNMP from a single management console.

ServerWORKS Manager agents running on DIGITAL systems provide the communication channel to the management console over a network. The agents provide real-time system and performance data in addition to information about alarms.

ServerWORKS uses the Desktop Management Interface (DMI) for its communication with desktop and mobile systems. The DIGITAL DMI agents provide configuration data on DIGITAL desktop or mobile systems.

ServerWORKS Manager uses Discovery, a process that first finds network objects and then returns information about the objects to a management station, the Console. ServerWORKS Manager Console is an easy-to-use Windows-based management station from which you can access your entire network and view your current network configuration in its actual or logical view in a hierarchical list or graphical map.

The Objects That ServerWORKS Discovers

ServerWORKS discovers:

- Servers, including all DIGITAL servers and non-DIGITAL servers whose MIBs are compiled into ServerWORKS. For example, Compaq® server MIBs are already compiled into ServerWORKS.
- Clusters, including DIGITAL NT and Microsoft NT clusters. A cluster icon appears in the hierarchy or map views. Expanding the icon reveals the servers and resources in the cluster.
- Network components like routers, bridges, hubs, and concentrators.

- Non-server nodes like desktop systems, printers, RAID controllers, and uninterruptible power supplies (UPS).

Integration with Enterprise-Level Management Tools

Because ServerWORKS Manager uses SNMP, ServerWORKS integrates with industry-standard enterprise management products so you can effectively monitor and manage DIGITAL servers from an enterprise manager. Conversely, you can compile non-DIGITAL MIBs into ServerWORKS Manager, which allows you to monitor other vendors' servers and network objects from the ServerWORKS Manager Console.

The DIGITAL server agents use the operating system's native SNMP protocol stack and extensible SNMP agent. You can set up the DIGITAL server SNMP agents to send traps to a network management system like ServerWORKS Manager Console. ServerWORKS can then forward traps to an enterprise manager.

ServerWORKS is integrated with:

- Compaq Insight Manager®
- Hewlett-Packard OpenView®
- Tivoli TME 10 NetView®
- Computer Associates Unicenter TNG®
- NetWare ManageWise®

You can find complete details for integrating DIGITAL MIBs into enterprise managers in the *DIGITAL ServerWORKS Manager Integration Guide*.

Minimal Health

ServerWORKS Minimal Health establishes an early warning system at installation time with default settings for your platform and components. ServerWORKS agents provide out-of-the-box configuration of alarms for common hardware components such as the fans and disks on DIGITAL servers. The Minimal Health agent sets alarms for environmental conditions—power supplies, voltage, fans, and temperature—and for status on processors, disks, and memory components.

Intelligent Monitoring

ServerWORKS agents gather server and component information intelligently. Instead of relying on constant polling from the management console, ServerWORKS agents that are installed on managed systems interrogate themselves and notify the console when a unit reaches an alarm threshold, saving considerable network bandwidth.

Detailed Component Usage

ServerWORKS gathers current vital statistics like the name and IP address of a device, which ServerWORKS displays on an IP Discovery map or in the ServerWORKS Explorer hierarchical view. ServerWORKS also collects details about network devices, such as network adapter statistics, disk storage, and CPU use, which you can view from the System Browser.

You can set alarms on network objects. When the value of an alarm parameter exceeds the threshold you have defined, you are notified. Then you can make adjustments before minor concerns become major problems.

You can record real-time activity using graphs, view the data on a dynamic graph, and accumulate the data for later analysis. The analyzed historical data can help you troubleshoot problems. If you suspect a problem on a component, you can run the graph for several hours or days and recall the data when you are ready to analyze it.

Notification Options

ServerWORKS lets you define the precise action to take when the Console receives a trap or alarm. You can send electronic mail, page an administrator using an alphanumeric or numeric pager, or launch an application that initiates a solution for the problem on the alarmed device.

NT and NetWare Management

ServerWORKS monitors and manages Windows NT® from the Console, eliminating the need to use multiple NT administration tools. ServerWORKS automatically discovers your NT domains and lets you display the contents and properties of objects in the Explorer as part of a custom collection or view.

In the map view, you can drag and drop objects between domains or servers and perform group operations easily. For example, you can select several groups and modify their privileges or manage printer queues.

If you run Novell NetWare on the Console, you can view the NetWare servers in your network the using ServerWORKS Explorer. You can also manage those servers, using the NetWare utilities whose icons appear on the ServerWORKS toolbar.

When you select a NetWare server, icons for the following NetWare utilities are displayed on the ServerWORKS Manager toolbar: Filer, Pconsole, Printcon, Rconsole, Syscon, Userdef, and NWAdmin. A click on the button starts the utility.

DIGITAL and Third-Party Application Integration

ServerWORKS integrates third-party applications so you can manage the devices on which their agents are installed. Integration with ServerWORKS accomplishes the following tasks:

- Enables ServerWORKS Manager to associate the application with objects on which the third-party agents are installed
- Adds a menu option on the Console menu that launches the third-party application from the Console menu
- Adds an icon to the Console toolbar that launches the application
- Adds an icon to the toolbar when a third-party object is discovered in a view

You can integrate the following applications:

ClientWORKS — ClientWORKS is the DIGITAL desktop system management tool that is based on DMI (Desktop Management Interface). ClientWORKS finds PCs that support DMI and retrieves information both locally and remotely. ClientWORKS also creates system snapshots (MIF files) for use with SMS (Microsoft Systems Management Server).

StorageWorks Command Console — Monitors, manages and troubleshoots large storage subsystems attached to a DIGITAL StorageWorks RAID controller.

Remote Server Manager (RSM) — Provides management by modem for DIGITAL servers with RSM installed.

Remote Management Console (RMC) — Monitors and manages Alpha systems configured with RMC functionality or KCRCM option hardware.

Global Array Manager — Monitors and manages the disk array subsystems that are attached to a MYLEX RAID controller.

APC PowerNet — PowerNet is the device manager for American Power Conversion uninterruptible power supplies. PowerNet provides information on APC UPS devices. Integration with ServerWORKS places an icon on the toolbar and a menu command to launch PowerNet from the Console.

Exide OnliNet® — OnliNet is power management software for uninterruptible power supplies from Exide Electronics Corporation. Exide UPS devices are available for DIGITAL Alpha systems. The OnliNet plug-in for ServerWORKS allows you to start OnliNet from the ServerWORKS toolbar.

Using SNMP with ServerWORKS Manager 2

ServerWORKS Manager uses SNMP, SNMP agents and MIBs to monitor and manage a network. Some background knowledge of SNMP is useful before you begin using ServerWORKS Manager.

This chapter describes the Simple Network Management Protocol (SNMP V1.0) that ServerWORKS Manager uses and explains how SNMP works with DIGITAL agents to extend the information you need for predictive management.

About SNMP

SNMP is an application layer protocol for exchanging management information between network devices. SNMP is the most commonly used protocol for managing diverse networks running a variety of operating systems. ServerWORKS Manager uses the SNMP V1.0 protocol for its primary communication with servers.

SNMP System Components

SNMP retrieves data from one or more *Management Information Bases (MIBs)* that describe the manageable objects on that host. In addition to system-supplied MIBs, vendors can define additional MIBs that allow vendor-developed devices to be monitored and managed by SNMP management consoles. ServerWORKS Manager compiles the Host Resources MIB (RFC1514), DIGITAL MIBs, and the MIBs of numerous vendors into its database to provide a collection of information about network objects.

ServerWORKS Manager implements SNMP-based MIBs and an SNMP extension agent component that allow:

- Remote control of systems through SNMP operations
- Setting of SNMP agent traps and alarms using ServerWORKS agents on the objects being managed
- Polling of SNMP variables to create Console-based threshold alarms

MIBs

A MIB includes the following information about every object it describes:

- An object identifier, known as an OID, that uniquely identifies the managed object on the network
- A definition of the data type used to define the object
- A textual description of the object
- An index method used for objects that are of a complex data type

The read or write access that is allowed on the object MIBs have been defined for TCP/IP routers and hosts, interface types such as token ring and FDDI, and devices such as servers and bridges.

Network Manager Programs

A *manager* is a program that requests data from other computers on the network. An *SNMP management console* is any computer running SNMP management software. When an administrator at the management console requests information about a managed object, the SNMP management program requests information about the object using its object identifier.

Agents

The *agent* is the program that receives management requests and then sends the requested information back to the SNMP management program that initiated the request.

Network objects that are monitored must have an agent residing on them or interacting with them. The agent performs four operations:

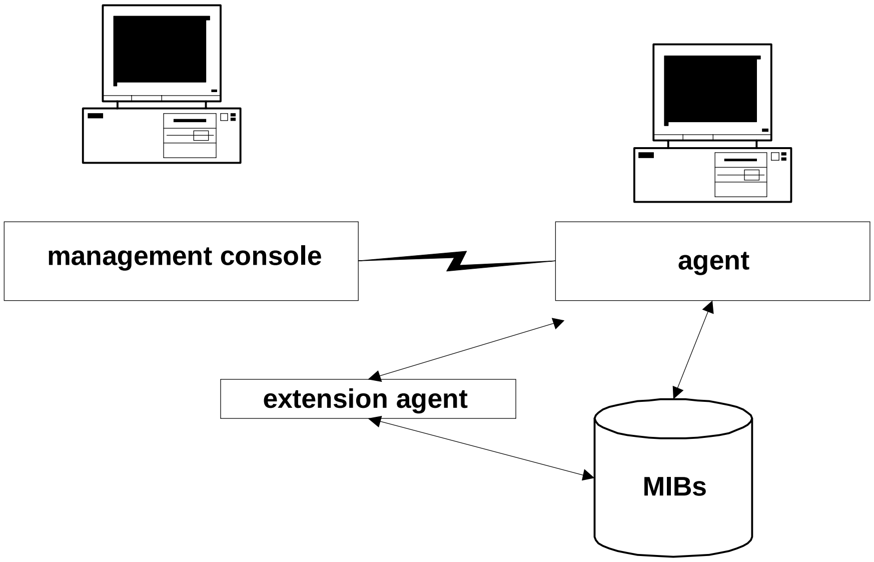
GET and **GET NEXT—** Retrieve information about the managed object and return it to the management console.

SET — Changes the value of a managed object variable. Only variables whose object definitions allow read/write access can be set.

TRAP — Sends messages to the SNMP management console when a change or error occurs in a managed object. The trap is the only operation initiated by the agent without a specific request from a management program.

An extension agent is software that extends the functionality of the system SNMP master agent. When the agent receives a request for information about one of the objects handled by an extension agent, it passes the request to the extension agent for processing. The extension agent returns the information to the SNMP agent, which returns it to the management console that requested the information, as shown in Figure 2-1.

Figure 2-1 Extension Agents in SNMP



The DIGITAL SNMP Extension Agent

Most operating systems provide SNMP agent subsystems that allow you to construct extension modules for specific hardware and software. The DIGITAL server agent uses the operating system's native SNMP protocol stack and distribution mechanisms to return information about DIGITAL hardware and software and to export traps to other systems.

An SNMP agent must be configured to send its traps directly to any SNMP management console such as ServerWORKS Manager Console, or to enterprise management systems, such as HP OpenView or Tivoli TME 10, that use SNMP as their trap and alarm mechanism.

How the Console Uses SNMP to Communicate

ServerWORKS Manager Console functions as a management console without the SNMP trap service. Because it uses its own SNMP stack for decoding SNMP traps, it does not require that SNMP be installed on the console system.

However, systems that are to be viewed by the management console *must* have SNMP agents installed and configured. If the management console will be used to view the system on which it is installed, then SNMP must be installed and configured on the management console as well.

ServerWORKS Manager Console relies on the operating system SNMP components to provide the IP port number of the SNMP trap (usually 162). This entry can be found in the services file. On a Windows NT system, this file is usually at c:\winnt\system32\drivers\etc\services. On a UNIX system, this file is at /etc/services.

Note: ServerWORKS Manager attempts to use the trap port if it is not already in use. The ServerWORKS Manager Event Dispatcher receives traps from the SNMP trap port. In order to run an enterprise manager on the same system as ServerWORKS Manager, you must close the Event Dispatcher process.

Some Windows 95 and Windows NT systems may have the SNMP trap entry removed. Make sure the following line is in the services file:

```
snmp-trap  162/udp     snmp
```

Changing this entry tells the Event Dispatcher to use another port number for listening to traps.

Configuring SNMP for Trap Forwarding

SNMP is a connectionless protocol, which means there is no mechanism in SNMP for requesting and acknowledging a formal connection session. If the agent system and the management console system do not agree on the trap port number and other details about the exchange, no messages will pass between the two systems. No error will be detected and no exception messages will be generated.

A system running Windows operating systems does not have the SNMP service installed by default. You must add the SNMP service explicitly from the Control Panel and then configure the SNMP agent with the correct security and access. You will not receive traps at the destination console if you do not configure the SNMP services correctly.

The SNMP setup is in the Control Panel under the Network icon. You need to configure the SNMP service and specify a trap destination on the managed server. Refer to the section *“Configuring SNMP and Trap Destinations”* in Chapter 7 for instructions on configuring SNMP for Windows NT and Windows 95. The procedures differ in the two versions, but both require the same information:

- The community name or names you will be using
- The network name or the IP address of each SNMP management console that will be the destination for trap messages generated within a specific community

The following sections explain these items in more detail.

Configuring SNMP Security

The SNMP security service uses *community names* to authenticate messages. All SNMP messages must contain a community name. The SNMP agent that receives the message checks the community name against the list of names with which the SNMP service is configured. If the message contains a known community name, the message is processed. If no known community name matches the one in the message, the message is rejected. The “Send Authentication Trap" check box in the setup window determines whether the SNMP service sends a trap message to the requesting server when an authentication failure occurs.

The default community name is Public when the SNMP service is installed on a Windows NT-based computer. You can add or remove community names as necessary.

Note: If you remove all community names, including the default name, the SNMP service on that computer will authenticate and process SNMP messages containing any community name.

There is no relationship between community names and domain or workgroup names. Community names are a shared password for groups of hosts and you should select and change them as you would any other password.

Only agents and managers that are configured with the same community name can communicate with each other. If the agent does not recognize the community name contained in the SNMP messages from the management console, the console will not receive traps from the agent.

Configuring SNMP Traps

The SNMP agent generates trap messages, which are sent to an SNMP management console called the *trap destination.* If you want a system to forward SNMP traps to a management console, you must make sure both systems are properly configured:

- The community name on the management console must be the same as the community name set on the agent system.
- The agent system must specify the management console system as a trap destination.

If you set up an alarm without having configured the SNMP services, you are prompted to configure SNMP and an SNMP trap destination on the managed system before proceeding.

When an agent trap condition occurs on the sending system, the agent sends the appropriate SNMP trap message to the management console system. If you do not configure both systems properly, no traps are passed.

Traps typically notify the management console about events such as a service starting or stopping, the existence of a serious error condition, or other event that is important to the agent. The SNMP agent or extension agent and its associated MIB define what conditions cause a trap message to be generated, but the user controls where the message is sent.

The trap destination must be a host that is running an SNMP manager program, such as ServerWORKS Manager or an enterprise manager.

Although you can identify the trap destination by its unique name, using the numeric IP address is most efficient. DHCP (Dynamic Host Configuration Protocol) is not recommended due to the uncertainty of DHCP address translation. Do not use a subnet address for the trap destination.

Installation 3

ServerWORKS Manager facilitates network management, a complex process with network, software, and hardware configuration requirements. This chapter describes the environment you need to operate ServerWORKS Manager, including

- Network configuration requirements
- List of supported platforms for operating system SNMP and DMI agents that come with ServerWORKS Manager
- Hardware and software requirements to run ServerWORKS Manager Console
- Hardware and software requirements to run agents on managed devices
- Requirements for cluster management
- Installation instructions

Network Configuration Requirements

Each network device has a unique numeric IP address and Media Access Control (MAC) address. ServerWORKS Manager uses the IP address to find objects on the network. SNMP uses the MAC address to communicate information about the network object.

To resolve names and address conflicts, install a Domain Name Service (DNS) server. The DNS binds a name to an address. Because a Console that moves has a dynamically allocated IP address and is not able to maintain a trap destination easily, it is recommended that you do not use DHCP for the Console.

For network objects to communicate with the ServerWORKS Manager Console using SNMP:

- Install an SNMP agent on each managed server
- Make sure that SNMP service is installed and running on all network objects to be monitored.
- Specify the IP address of the management console as the trap destination when you configure SNMP on the managed device

As an administrator of an NT network, you need two types of administrator privileges:

- Administrator privileges in your domain
- Trust relationships that allow domain administration in other domains you plan to manage from the Console

Become familiar with the NT operating system. NT imposes little-known restrictions on user accounts. Typically the Administrator has full administrative capabilities, but others who are designated as Account Operators must be explicitly assigned rights to perform tasks on user accounts. Among the user rights that are explicitly assigned are the rights to access a local system from the network, back up files and directories, log on locally to a system, shut down the system, and take ownership of files or other objects.

Finally, understand network fundamentals and protocols. To learn more about these, refer to the bibliography in Appendix C.

SNMP Supported Platforms

The following table lists the SNMP and DMI agents that are provided with ServerWORKS Manager or as part of the operating system.

Table 3-1 SNMP and DMI Agents

Minimum OS Version Supported	Host Resource SNMP Agent	X86 processor-based DIGITAL Server SNMP Agent	Alpha processor-based DIGITAL Server SNMP Agent	DIGITAL DMI Agent
NetWare® V3.12, V4.11 (X86 processor-based DIGITAL servers only)	Yes	Yes	N/A	N/A
Windows NT® V4.0 server and workstation (for all DIGITAL servers)	Yes	Yes	Yes	Yes
Windows 95[1](X86 processor-based DIGITAL servers only)	Yes	Yes	N/A	Yes
SCO® UNIX OpenServer V5.02, V5.04	Yes	Yes	N/A	N/A
DIGITAL UNIX V4.0	Yes	N/A	Yes	N/A
DIGITAL OpenVMS 6.2[2] or greater (Alpha processor-based servers only)	Yes	N/A	Future	N/A
OS/2 Warp 3.0 provided with the operating system [3](X86 processor-based DIGITAL servers only)	Yes	N/A	N/A	N/A

[1] Provided with ClientWORKS on DIGITAL mobile computers.

[2] Available with DIGITAL TCP/IP Services for Open VMS V4.2 (formerly known as UCX).

[3] Provided as part of the OS/2 operating system.

Management Console Hardware

You need the following hardware to run ServerWORKS Manager.

Table 3-2 Minimum Hardware Requirements for ServerWORKS Manager Console

Component	Minimum Requirements
Processor	Pentium 133 MHz
Storage Devices	1 GB hard drive CD-ROM drive 3.5-inch diskette drive
Network Interface Card	Network adapter with TCP/IP support installed
Monitor	SVGA 800 x 600 (1024x768 resolution recommended on an 18” monitor)
Memory	32 MB

Management Console Software

You need the following software to run ServerWORKS Manager Console.

Table 3-3 Software Requirements for ServerWORKS Manager Console

Component	Minimum Requirements
Operating System	One of the following on X86 processors • Window NT V4.0 • Windows 95
Management Protocol	SNMP service provided with the operating system (ServerWORKS Manager requires SNMP service only if a DIGITAL system SNMP agent is being installed on the management console system.)
Transport and Network Protocols	One of the following: • TCP/IP service provided with the operating system • IPX service provided by Novell

Agent Hardware

You need the following minimum hardware to support ServerWORKS agents. Some options in the system parameter area (assets or FRU information, for example), remain hardware dependent.

Table 3-4 Minimum Hardware Requirements for Agents

Component	Minimum Requirements
X86 processor-based DIGITAL servers	LX, MX, XL, HX and ZX Servers DIGITAL 500, 1000, 3000, 5000, 7000, and 9000 family of servers
Alpha-based systems	AlphaServer 300, 400, 800, 1000, 1000A, 1200, 2000, 2100, 2100A, 4000, 4100, 8200, and 8400 DIGITAL Server 3000, 5000, 7000 (Windows NT)
Desktop computers[4]	Venturis FX, Venturis GL-6xxx,[5] Venturis 486, Venturis 486 LP, Venturis Pentium, Venturis Pentium LP, Celebris XL 6xxx, DIGITAL PC 5500, and DIGITAL PC 5400
Notebook computers[6]	HiNote Ultra 2000
Network Interface Card	X86 processor-based DIGITAL servers — TCP/IP adapter (Ethernet, Token Ring, or RAS) NetBEUI Alpha-based systems — All TCP/IP network adapters

Agent Software

You need the following software to run ServerWORKS Manager agents.

[4] Desktop computers may not support environmental parameters, RSM, or RMC.

[5] Venturis GL 6xxx is equivalent to the DIGITAL PC 3400. The DIGITAL PC 3400 is not available in all areas.

[6] Notebook computers do not support environmental parameters, RSM, or RMC.

Table 3-5 Software Requirements for Agents

Component	Requirement
Network Operating System	
For X86 processor-based DIGITAL servers	One operating system: • Novell NetWare V3.12 or V4.11 • SCO UNIX OpenServer V5.02, V5.04 (not on clusters) • Windows NT V4.0 • OS/2 V3.0
For Alpha-based systems	One operating system: • DIGITAL UNIX V4.0 • OpenVMS 6.2 or greater • Windows NT V4.0 for Alpha (agents only)
Network Protocols	SNMP TCP/IP or IPX (NetWare servers only)

Network Cluster Support

You need the following items configured on cluster members to manage clusters.

Table 3-6 Requirements for Network Cluster Support

Cluster Type	Requirements
DIGITAL Clusters V1.1	Windows NT Enterprise, V4.0 with Service Pack 3 running on DIGITAL servers Common Cluster MIB agent Cluster Extension MIB agent
Microsoft NT Clusters	Windows NT Enterprise, V4.0 with Service Pack 3 running on DIGITAL servers Common Cluster MIB agent Cluster Extension MIB agent Microsoft Cluster Server (MSCS)

Pre-Installation Considerations for ServerWORKS

Read the following sections for background information about ServerWORKS Manager components before you install ServerWORKS Manager.

Order of Installation

You can install the following software from the ServerWORKS CD-ROM. Install them in the order they appear:

- Agents
- ServerWORKS Manager Console
- ServerWORKS Console Integration
- ClientWORKS
- Remote Server Manager (RSM)

- Remote Management Console (RMC)
- StorageWorks Command Console (SWCC)

Always uninstall previous versions of ServerWORKS, ClientWORKS, or ManageWORKS before you install ServerWORKS V4.0. Refer to Appendix B, "*Troubleshootin*g" for details.

DIGITAL recommends that you install the components in the default directories as suggested in the installation. Avoid running two versions in different directories.

Choose one language under which to install and uninstall. Only one copy of the uninstall program is kept in your Windows directory. Therefore, it is always in the language selected during the last installation on that system.

Make sure you have local and domain administrator privileges if you are installing and configuring ServerWORKS with Windows NT. Remember that Windows NT administration rules and restrictions for Groups and Users continue to apply when you work from ServerWORKS Manager NT Server Management.

You need 100 MB of temporary disk space to install. The installation uses the directory set by your TEMP variable, or if TEMP is not defined, the Windows directory. For the environment variable 'TEMP,' specify a directory with a minimum 100 MB of storage to hold the temporary files used during installation. In addition, specify a TEMP directory that is not in your PATH. Otherwise, unpredictable results may occur. On Windows NT, use the Control Panel applet System Properties→Environment to modify the TEMP variable.

Incomplete Installations

If you stop an installation before it is complete, close the installation program completely and start over. For best results, use the Control Panel→Add/Remove Programs applet to remove any files from the incomplete installation before you attempt another installation. The uninstall program removes only files that were changed the last time an installation was run. Changed files from previous installations are not removed.

The system files copied to your system's Windows system directory are not deleted when ServerWORKS Manager Console is uninstalled. They are retained to avoid a problem with the InstallShield uninstall program, which removes Windows system files no longer used by any other running program without asking for confirmation. If the ServerWORKS uninstall program deleted the system files, some required DLLs would be removed, causing problems later when other programs are started.

Closing Other Programs Before Installation

Shut down all programs that are running, including mail programs and the Microsoft Office shortcut bar.

If you are upgrading ServerWORKS, shut down all ServerWORKS Manager background processes (Event Logger, Event Dispatcher, Poller, Ping Server, Data Collector) before you install or integrate any third-party applications.

To install ServerWORKS Manager on a system that has Tivoli TME 10 NetView installed, first shut down the NetView daemons. Daemons continue to run in the background after you exit NetView. To stop the daemons, select the menu item Server Management from the NetView program group. Then select Stop Server to stop the daemons.

Keeping a Previous ServerWORKS Database

The installation program checks to see whether a version of ServerWORKS Manager Console already exists on the system. If so, you have the following options:

Preserve the database — Merges an existing V3.2 or greater database into a new Microsoft Access database, retaining all the information from the old version, including historical data files.

Remove the previous version — Deletes databases created from ServerWORKS V3.0 or earlier.

You can upgrade a Version 3.0 database if you first install Version 3.2. Then install Version 4.0.

Manipulating the Database

If you create your own Access reports or messages, upgrade Microsoft Access 95 or earlier to Access 97 before the ServerWORKS Manager Console is installed.

Integrating ServerWORKS with Insight Manager

ServerWORKS Console integration merges ServerWORKS with Insight Manager. You can choose the integration option when you install. Integration enables you to view Compaq or Digital servers from Insight Manager V4.01 or from WBEM, the Web-based Insight Manager. Integration makes WBEM the default application for Compaq objects on a map. Before you integrate, Insight Manager V4.01 and Internet Explorer V4.01 must be installed.

Integrating ServerWORKS with Enterprise Managers

ServerWORKS Console integration merges ServerWORKS agents into enterprise managers. DIGITAL agents can provide the enterprise managers with precise details about DIGITAL servers. Before you integrate ServerWORKS Manager, the enterprise manager should be correctly installed.

Using ManageWORKS

ServerWORKS Manager Console and OpenVMS Management Station can be installed and run *separately* on the same system. Continue to use ManageWORKS as the interface for the OpenVMS Management Station.

SNMP Service and Agents

Install SNMP on the managed systems and configure a trap destination if you want to receive trap messages generated by the SNMP agents. Refer to the section “Configuring SNMP and Trap Destinations” in Chapter 7.

SNMP agents may be supplied with the operating system or with the installation. Install the SNMP agents on the ServerWORKS Manager CD-ROM even if the operating system comes with SNMP agents.

Agents Supplied with ServerWORKS

Agents for the following systems are supplied and installed on the ServerWORKS Manager:

- Windows NT 4.0 or greater

Agents for the following operating systems are supplied on the ServerWORKS Manager CD-ROM. Install them using instructions provided with the ServerWORKS installation kit.

- NetWare V3.12, V4.11
- SCO UNIX Open Server 5.02, 5.04

Agents for the following options for X86-based processors running Windows NT are supplied with ServerWORKS Manager:

- DIGITAL Server Management agents, including the ServerWORKS V4.0 Minimal Health agent for X86-based processors running NT. This option is recommended.
- DIGITAL Server Agents for Insight Manager. These agents allow you to view information about DIGITAL servers using ServerWORKS Manager utilities from Compaq Insight Manager.

Agents Supplied with an Operating System

Agents are supplied and installed with the following operating systems:

- DIGITAL UNIX 4.0
- OpenVMS SNMP agent for Alpha-based systems is included in the DIGITAL TCP/IP Services for OpenVMS product V4.2 or greater and is a component of the NAS Client/Server Package. The SNMP agent is installed when TCP/IP is installed.
- IBM OS/2 SNMP agents are included with the operating system. Refer to the OS/2 documentation for details.

Refer to the operating system documentation and to Appendix A *"Additional Procedures and Information"* for more information about installing SNMP agents on these operating systems.

Installing an Agent on the Console Device

If you are installing ServerWORKS Manager Console software on an X86 processor-based server running NT 4.0 on which you also want to install an agent for local monitoring, install the agent software first, then install ServerWORKS Manager Console.

Pre-Installation Considerations for ClientWORKS

For more information about ClientWORKS, refer to *"Using the ClientWORKS® Management Suite with DIGITAL PCs: A Guide for Network Administrators"* and the ClientWORKS V3.0 README.TXT.

Pre-Installation Considerations for RSM

RSM consists of hardware and software components. They are installed on X86 processor-based DIGITAL servers running Window NT or nodes running Windows 95. In order to integrate RSM with ServerWORKS Manager console, the RSM software must be installed on the same system as the ServerWORKS Manager Console software.

RSM software should be installed on an X86 processor-based DIGITAL server into its default directory:

```
        <windows drive>:\rs_mgr
```

A separate integration procedure is provided to integrate RSM into ServerWORKS Manager Console. The integration is automatic if RSM was installed into its default directory. If RSM was installed elsewhere, the RSM integration tool will ask for the destination directory where RSM was installed.

Pre-Installation Considerations for RMC

This section describes how to access the Remote Management Console (RMC) on an Alpha processor-based system. After configuring the RMC, you can start it from ServerWORKS Manager.

The RMC is a hardware/firmware feature of Alpha processor-based servers. The RMC allows you to control and monitor an AlphaServer system from a remote location. RMC commands are used to reset, halt, and power the monitored system on or off.

The control logic for the RMC is part of the system hardware in AlphaServer 800, 1200, 4000, and 4100 systems. Refer to the user documentation for these systems for instructions on configuring and using RMC. The AlphaServer 1000 and 1000A systems provide RMC capabilities through a hardware option, the KCRCM AlphaServer Remote Console Module, which can be ordered separately. The KCRCM module is connected to an EISA/ISA slot on the AlphaServer 1000 or 1000A system. Refer to the documentation provided with the module for installation and configuration instructions.

To invoke RMC from ServerWORKS, install HyperTerminal (HYPERTRM.EXE) on Windows NT V4.0 and Windows 95. To integrate RMC into ServerWORKS Manager Console, HyperTerminal must be installed in the default directory selected by the operating system installation. Install as directed for Windows 95 and Windows NT.

Invoke RMC from ServerWORKS Manager as follows:

1. If you are using HyperTerminal, configure it as desired, using the menus displayed on the screen. If you are using another terminal program, install and configure it according to the documentation.

2. Run Discovery to identify the servers on the network.

3. Select an AlphaServer object in the Discovery map or the Explorer.

4. Select the RMC menu item from the Tools menu or click on the RMC integration icon in the toolbar to launch the terminal program.

The terminal program connects through your COM1 port to a modem, terminal switch, or PBX, depending on how you have configured it. If your connection is by modem, dial the telephone number configured for the modem. From the COM1 port, enter the escape sequence to invoke RMC.

When the RMC integration is complete, the installation program confirms that the links between RMC and ServerWORKS Manager Console were successful.

First Steps for Installing All Components

Every component installation begins from the main screen after you select an installation language. The following steps open the main screen.

1. Insert the CD-ROM into the CD-ROM drive. For example, insert it into the CD-ROM drive of a managed system if you are installing agents. (You cannot install from a network drive.)
2. On Windows NT or Windows 95 systems, as soon as the CD-ROM is engaged the main screen appears. If it does not start automatically do the following:
   - From the desktop, click the Start menu.
   - Choose Run. Enter the path as follows and click OK:

     On Windows systems:`<cd-rom drive>:\Autoplay.exe`

     On Alpha systems:`<cd-rom drive>:\Alpha\Autoplay.exe`
3. Choose your preferred language. The selected language remains the default the next time you install or uninstall any component from the CD-ROM. The main screen opens with the following options:
   - **Insight Manager Options.** Explains your options regarding ServerWORKS and Insight Manager.
   - **Install.** Displays the components you can install.
   - **Tutorial.** Runs the online tutorial. You can install the tutorial or view it at any time from the CD-ROM.
   - **Documentation.** Displays the manuals and other hardcopy documentation using the Adobe® Acrobat™ reader located on the CD-ROM. (You do not need to install Adobe Acrobat on your system.) You can open the manual from the CD-ROM. Online help is installed with the applications.
   - **Finish.** Closes the installation and offers to start ServerWORKS Manager Console (if it was installed) or to exit.

4. Do one of the following:

   – Click on Install to open the component screen. From this screen you can choose other components to install.

   – Click on any of the other options and follow the prompts to navigate through the option. For example, click on the Tutorial to open the tutorial and view it. When you exit from the tutorial, you are returned to the main screen where you can choose to install a component or exit.

Component Installation Instructions

Use the step-by-step instructions in the following sections to install specific components. Begin by installing the ServerWORKS agents on all systems you want to manage. Then install ServerWORKS Manager Console on the management station.

Installing ServerWORKS Manager Agents

Install the agents before you install any other component. Install the agents on the remote systems that you will manage from the ServerWORKS Manager Console. The installation program provides only the agents that are appropriate for the operating system and platform on which you are running the ServerWORKS Manager CD-ROM.

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.
3. From the component screen, click ServerWORKS Manager Agents.
4. Choose one option:

   – Click Install to install the agents for DIGITAL x86 server platforms. Then proceed to Step 5.

   – Click the Read button to learn more about installing an agent on other operating systems. Follow the instructions for the operating system and exit from the instructions following any prompts.

5. Acknowledge prompts as they appear.
   - Click Next on the licensing screen.
   - If SNMP service is running, click Yes to turn it off.
6. On the Digital Agents Setup - Operation screen, select one option and click Next.
   - **Install the Server SNMP Agents V4.0**. Choose this option to install or upgrade. Then click Next.
   - **Remove the Server SNMP agents.** Choose this option to remove installed agents.
7. On the Select Optional Agent Components screen, you can select the following:
   - **Digital Server Management Agent.** Installs the ServerWORKS V4.0 Server Management agent, including Minimal Health. This agent replaces all alarms previously defined with ServerWORKS V3.x or earlier.
8. Acknowledge the prompt to restart SNMP service now or later or other prompts to continue.

On the component screen, choose the next component to install. If you are not installing other components, click Close and then click Finish on the main screen.

Do You Plan to Monitor Your Management Console?

You can install an agent and the console software on a management console running Windows NT 4.0. Use the preceding instructions for the agent installation.

Installing ServerWORKS Manager Console

The ServerWORKS Manager Console installation process consists of the following segments, which contain multiple steps:

- Starting the installation, by choosing either the Windows NT 4.0 or Windows 95 installation
- Installing the Console
- Completing the Installation

Starting the Installation for Windows NT 4.0

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.
3. From the component screen, choose ServerWORKS Manager Console.
4. Choose from the following options on the intermediate installation screen:
   - **Step 1 Install.** Installs the NT agents on systems running Windows NT 4.0. Skip this option unless you are installing an agent on the Console system.
   - **Step 2 Read.** Displays information about Microsoft Data Access (MDAC) Components. Choose this step to ensure you are using the correct version of Microsoft drivers. Choose File→Exit to return to the intermediate installation screen.
   - **Step 3 Install.** Installs the required Microsoft Data Access Pack. To install:
     a. Follow the prompts for the MDAC installation.
     b. When prompted, choose Typical installation. (For a Custom installation, you must choose the Data Sources and MDAC Core Files).
     c. Reboot your system, as per Microsoft recommendations.
     d. Return to the intermediate installation screen.
5. Choose Step 4 Install to begin the ServerWORKS Manager Console installation.

Continue the installation with the procedure in the section *“Installing the Console.”*

Starting the Installation for Windows 95

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.

3. From the component screen, choose ServerWORKS Manager Console.

4. Choose from the following options on the intermediate installation screen:

   – **Step 1 Install.** Displays information about Microsoft Data Access Components, including ODBC. Choose this step to ensure you are using ODBC 3.5 or greater. Choose File→Exit to return to the intermediate installation screen.

   – **Step 2 Read.** Displays information about Microsoft Data Access Components. Choose this step to ensure you are using the correct version of Microsoft drivers. Choose File→Exit to return to the intermediate installation screen.

   – **Step 3 Install.** Installs the required Microsoft Data Access Pack. To install:

     a. Follow the prompts for the MDAC installation.

     b. When prompted, choose Typical installation. (For a Custom installation, you must choose the Data Sources and MDAC Core Files).

     c. Reboot your system, as per Microsoft recommendations.

     d. Return to the intermediate installation screen.

5. Choose Step 4 Install to begin the ServerWORKS Manager Console installation.

Continue the installation with the procedure in the section *“Installing the Console.”*

Installing the Console

You can upgrade from ServerWORKS Manager Console V3.2 or V3.3. Upgrades from earlier versions are not supported.

1. On the Welcome screen, click Next to accept the license terms and conditions.

2. For a new installation, register your name and organization on the ServerWORKS Manager Console screen, follow any prompts, and click Next.

3. On the Choose Destination Location screen, click Next to place the files in the specified default directory. On a subsequent installation, you may have problems sharing files between the two versions if one version resides in another directory. If you want to change the directory, use the Browse command to select the location and return to the Choose Destination Location screen. Then click Next to proceed.

4. If this is the first installation, skip to Step 5. If you are reinstalling, do one or both of the following:

   – Select "Use the existing database." This option preserves the current database and merges it into a new database. If you do not select this option, the old database is saved in:
   \Program Files\Digital\SWMgr\database\old

   – Select "Remove the installed ServerWORKS." Follow any messages in the prompts regarding uninstalling previous versions of the software.

   Then click Next.

5. Choose one of the following options:

   – **Automatically startup the background tasks.** Background tasks start running immediately after installation. If your console is dedicated to ServerWORKS and administration, you may want to run them automatically.

   – **Manually start them up each time.** Background tasks run only when ServerWORKS is opened.

   Then click Next and follow any prompts to continue.

Completing the Installation

1. Choose to accept or reject the option “View README.TXT now.” If you select the option, read the file and exit using File→Exit.

2. Click Finish. Close the program group if necessary. Follow the messages to close any remaining dialog boxes. The intermediate installation screen appears.

3. Click Close.

4. On the component screen, click Close again to return to the main screen.
5. On the main screen, click Finish.
6. On the next prompt, select "Start ServerWORKS Manager immediately" or click Exit.
7. On exiting you are returned to the component screen. If you do not plan to install any other components, click Close.
8. On the main screen, click Finish.

Installing ServerWORKS Console Integration

The ServerWORKS installation begins the process of integrating with the enterprise manager. Instructions vary for different platforms and enterprise managers.

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.
3. From the component screen, choose ServerWORKS Console Integration.
4. Choose from the following options on the intermediate installation screen:
   - HP OpenView/ServerWORKS
   - HP OpenView/HPUX
   - Tivoli TME 10 NetView for Windows NT/ServerWORKS
   - Tivoli TME 10/NetView for Digital UNIX
   - CA Unicenter TNG/ServerWORKS
   - Compaq Insight Manager /ServerWORKS
5. Follow the instructions for the specific platform and enterprise manager. When the installation is complete, click Close to return to the ServerWORKS component screen.

Installing ClientWORKS

For complete details about upgrading ClientWORKS, refer to the ClientWORKS readme.txt.

1. Open the main screen by following the procedure in "First Steps for Installing All Components."
2. Click Install to open the component screen.
3. Click ClientWORKS Components. You can install two ClientWORKS components. Both are optional.
   - From the component screen, choose ClientWORKS DMI Explorer to install the explorer for your local system. Follow the prompts to complete the installation.
   - From the component screen choose ClientWORKS DMI Explorer and Agents to install the components for network browsing and management. Follow the prompts to complete the installation.
4. Proceed with the ClientWORKS portion of the installation. Continue to follow any prompts. Then click Next.
5. On the first licensing acknowledgment screen, click Next. On the second licensing screen, click Yes.
6. On the ClientWORKS components screen, select the option(s) and then click Next.
7. On the language option screen, choose the same language that you used to install ServerWORKS Manager and click Next to proceed.
8. Choose the destination for ClientWORKS and click Next.
9. Choose the default folder name or enter your own folder name. Then click Next. Follow any prompts regarding SNMP service.

Installing RAID Storage Management

If you are not installing a RAID controller management application, disregard the sections “*Installing StorageWorks*” and “*Installing MYLEX GAM.”*

Installing StorageWorks

StorageWorks Command Console consists of a client for the management console and agents for the managed servers. The StorageWorks Command Console client is installed on a Windows NT or Windows 95 node. The StorageWorks agents are installed on servers that are connected to a StorageWorks RAID controller running Windows NT, NetWare, or SCO UNIX.

StorageWorks is installed from the CD-ROM. The StorageWorks client can be installed on a management system. The StorageWorks agents can be installed on managed servers to which a RAID controller is connected. If StorageWorks cannot be automatically installed on the system, more information is displayed. StorageWorks must be reinstalled with the version provided on the ServerWORKS Manager CD-ROM (or a more recent version).

1. Open the main screen by following the procedure in *"First Steps for Installing All Components."*
2. Click Install to open the component screen.
3. From the component screen, click RAID Storage Management.
4. Choose StorageWORKS Command Console.
5. On the next screen, click on Agent or Client and follow the prompts to return to the main screen.
6. On the main screen, choose the next component to install. If you are not installing other components, click Finish.

Installing Mylex GAM

Mylex GAM consists of a client that is installed on the management console running Windows NT or Windows 95 and agents that are installed on servers that are connected to Mylex GAM RAID controllers.

GAM is installed from the CD-ROM. If GAM cannot be automatically installed on the system, information on how to install it is displayed. Mylex GAM must be reinstalled with the version provided on the ServerWORKS Manager CD-ROM or a more recent version.

1. Open the main screen by following the procedure in *"First Steps for Installing All Components."*
2. Click Install to open the component screen.
3. From the components screen, choose RAID Storage Management.
4. Choose Mylex GAM.
5. On the next screen, click Install and follow the prompts to return to the main screen.
6. On the main screen, choose the next component to install. If you are not installing other components, click Finish.

Installing Remote Management Integration

If you are not installing remote management integration, disregard this section.

Your selection for remote management depends on the operating system of the management console where you are installing the component. Install RSM software before you install the RSM integration. Refer to RSM documentation for details.

1. Open the main screen by following the procedure in *"First Steps for Installing All Components."*
2. Click Install to open the component screen.
3. From the components screen, choose a remote management service for your system.
4. Follow the prompts and click Finish when the integration is successful.
5. On the main screen, choose the next component to install. If you are not installing other components, click Finish.

Tutorial

The ServerWORKS Manager Tutorial is installed as part of the ServerWORKS Manager Console software. This tutorial contains basic information about ServerWORKS Manager. You can complete the tutorial in about 20 minutes. If you are a first-time user, DIGITAL recommends that you use the tutorial to get started.

Documentation

During the ServerWORKS Manager Console installation, the readme.txt and install.txt files are copied to the root of the installation directory. Online help is installed with the products. You can view or print these documents from the CD-ROM using Adobe Acrobat.

Post-Installation Options

Several features of ServerWORKS may be manually installed or configured after ServerWORKS is installed.

WatchDog Timer on Multiple Platforms

WatchDog Timer is an option you can install on X86-processor based servers after ServerWORKS Manager is installed. The Watchdog Timer is a utility that automatically recovers a hung operating system by rebooting the server. The Watchdog Timer is disabled by default at installation. For security reasons ServerWORKS V4.0 supports enabling or disabling this feature at the agent system from the system prompt.

On the NT, NetWare, and SCO UNIX operating systems, ServerWORKS Manager offers Watchdog Timer support for Prioris ZX6000, HX6000, MX6000 and XL6000 servers and the DIGITAL Server 3000, 5000, and 7000 series.

To enable WatchDog Timer:

1. Open the system prompt.
2. Enter the program name followed by a space and the number of minutes to wait before rebooting of the system occurs. For example:

   – On an NT system:

   ```
   sw_wdt 4
   ```

   – On a NetWare system:

   ```
   load ServerWORKS_wdt 4
   ```

   The system displays a message describing the result. For example, an NT system displays the message “WatchDog enabled for a one to four minute wait before reset after system hang.”

To disable WatchDog Timer:

1. Enter the program name at the system prompt
2. Omit the number of minutes.

Using sw_wdt sets the Watchdog Timer permanently on a server. If the Watchdog Timer causes a system to be reset, the message screen confirms the reset and also displays the reason for the last shutdown.

WatchDog Timer on SCO UNIX

You can enable WatchDog Timer at installation time when you install ServerWORKS agents on SCO UNIX systems. In response to the prompt, enter the number of minutes to wait before rebooting occurs. You must be logged in as /root or as an administrator to enable WatchDog Timer on SCO UNIX. For ManageWORKS V2.2, edit the line to:

```
INI file=<path of previous installation>\MWORKS.INI
```

Discovering Networks and Objects 4

An IP Discovery with ServerWORKS Manager collects volumes of information on all network objects. You can view the information from displays of network nodes in the ServerWORKS Explorer window list view or in the IP Discovery Map graphical view.

This chapter

- Describes the elements on the Explorer and Map Viewer windows
- Explains how to manipulate objects in the windows
- Explains how to discover your network
- Describes the Alarm Viewer and how you can use it to check the status of network objects

The Network Views

IP Discovery finds TCP/IP and SNMP objects on the network and places the information in the ServerWORKS Manager database. The database information is used to construct the ServerWORKS Explorer and IP Discovery map views that represent the network. Figure 4-1 illustrates the two views.

ServerWORKS Explorer View

The ServerWORKS Explorer is the main entry to ServerWORKS Manager and is the default view. The Explorer opens as a list or tree view that consists of root objects for each of the object types in your network. From this hierarchical view, you can see:

NT Server Management — Includes all servers running Windows NT. This category appears only when the management console is running Window NT Server or NT Workstation.

NetWare Objects — Includes Novell NetWare file servers. This category appears only when the management console is running Novell NetWare Client for Windows NT.

Server Objects — Includes all DIGITAL (X86 processor-based and Alpha) servers running Windows NT, Novell NetWare, SCO UNIX, OS/2, DIGITAL UNIX, and OpenVMS. The appropriate agents must be installed. (See Table 3-1).

SNMP and IP Objects — Includes bridges, routers, hubs, servers (including non-DIGITAL servers whose MIBs are enrolled in the ServerWORKS database), desktop systems, printers, token rings, FDDI rings, and Ethernet networks.

Cluster Objects — Includes Microsoft NT clusters and DIGITAL NT clusters. A cluster is represented by a cluster object on a map or list. Expanding the cluster object reveals the cluster members and the resources—storage, applications, etc.—associated with each cluster member. See Figure 4-1.

The ServerWORKS Explorer view is a permanent read-only viewer that you cannot modify, delete, or rename. The Explorer contents are temporary and are updated when you open it. However, you can create and save other list views.

The Explorer view may include collections, which contain multiple objects of one type. Use the Explorer view to see individual nodes and their status. The Explorer view is an appropriate window from which to manage daily operations because it is always current.

IP Discovery Map Views

The Map Viewer is a graphical representation of the network layout. ServerWORKS performs a discovery and builds the map.

You have the following options for working with map views:

- Run multiple discoveries that are filtered to discover specified object types
- Save updated views in existing maps
- Save newly discovered objects in new maps
- Rename or delete map views
- Manually add objects into map views

On either the Explorer or Map Viewer, SNMP and IP objects are color-coded to represent their current status. Alarms that were triggered are indicated by an alarm icon attached to the object. Cluster objects on a map show a bell icon if one of the members or resources has triggered an alarm. Figure 4-1 illustrates objects tagged with alarm bell icons.

The Explorer view on the left shows the root objects of the default object types. The plus (+) sign indicates there are objects under the root object. Double-click to expand the root object. The (-) indicates that the root has been expanded. On this illustration the Cluster, Printer, and Server objects are expanded.

This map view shows servers, clusters, and a printer on one subnet. One server has triggered an alarm, which is indicated by the small bell icon.

An object can appear under several root objects. For example, a DIGITAL server running Microsoft Windows NT appears under Server Objects, SNMP Objects, and NT Server Management Objects because it fulfills the requirements of each one.

Below the viewing window is the Alarm status bar. You can see the number and type of alarms at a glance. When you click on a status button, you open the Alarm Viewer.

Elements on the Viewer Windows

When either the Explorer window or the Map Viewer window is opened, the Console displays:

- The Menu Bar
- The Tool Bar
- Alarm Status bar

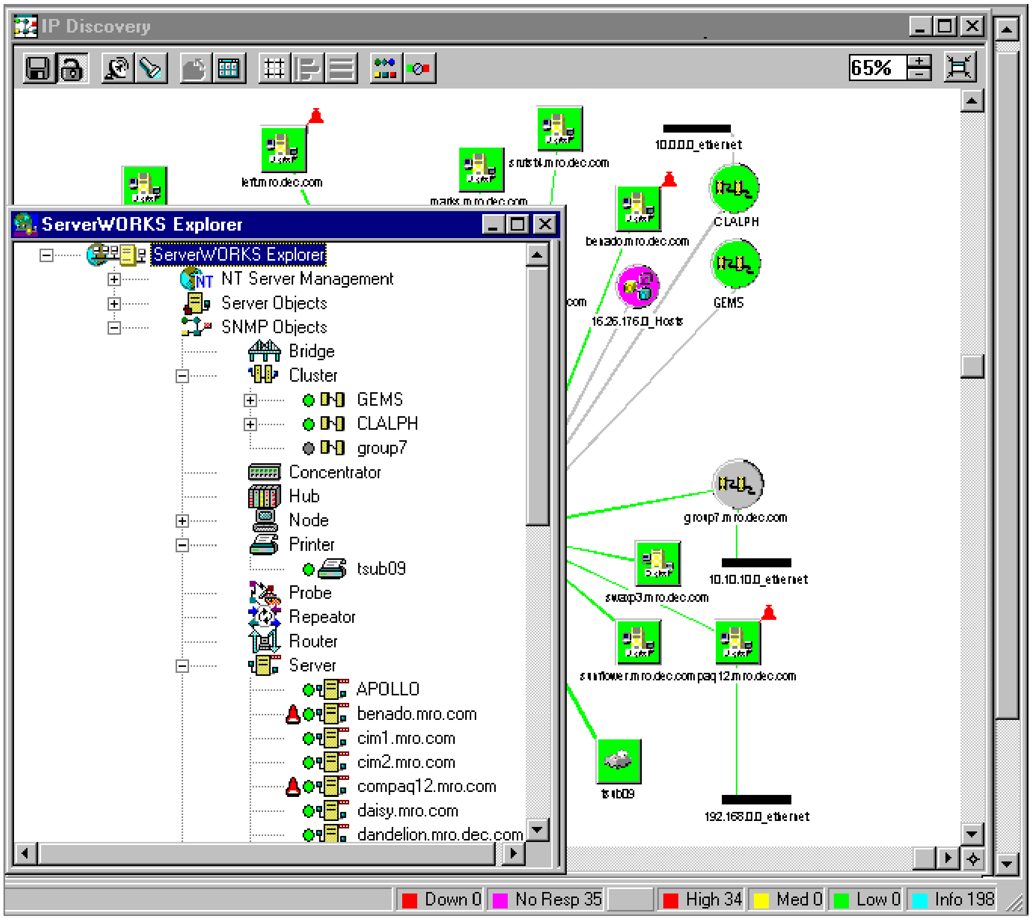
The Menu Bar

The menu bar contains the menu options for operating the Console. A brief description of a menu option appears in the menu status bar at the bottom of the window. As you move the cursor across the menu options, the description changes for each command. You can read complete descriptions of the menu commands in the ServerWORKS Manager Console online help.

To open the menu bar help topic

1. Choose Help→Help Topics→Contents.
2. Double-click on the topic ServerWORKS Menu Bar topic.

Figure 4-1 Map and Explorer Views of a Network



The Command Toolbar

ServerWORKS contains a command tool bar that appears in both the Explorer and the Map Viewer windows. The toolbars change dynamically according to the network objects that appear in the list or map. For example, toolbar buttons for NetWare and NT do not appear if your network does not have servers that are running these operating systems. For a complete description of the toolbars, refer to the online help.

To open the Explorer and Map Viewer Toolbar help topic

1. Choose Help→Help Topics→Contents.
2. Double-click on the topic ServerWORKS Toolbar.

To change the size of the toolbar buttons on the command toolbar

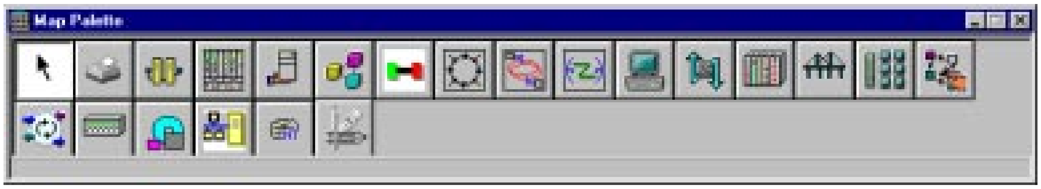
- Choose View→Small Icons or View→Large Icons.

The Map Viewer Palette

The Map Viewer also contains an object palette for inserting objects onto a map. The Palette contains the generic object types and any object types you have created. As you move the cursor over the Palette buttons, the object type name appears in the status bar.

The Palette is useful when you are creating a specialized map view because you can associate an icon with an object type. For example, all servers in the Engineering department may be DIGITAL servers, but for a specialized map, you can assign the Engineering department logo, a set of tools. Figure 4-2 illustrates the Map Palette with the extra icon.

Figure 4-2 The Map Palette



Opening and Exiting From ServerWORKS

To open ServerWORKS Manager Console

- From the desktop, choose Start→Programs→ServerWORKS Manager Console→ ServerWORKS Manager.

You can close a view or map and keep ServerWORKS Manager Console open or you can exit from ServerWORKS Manager Console. Exiting closes all views and maps.

To close a map or view

1. Click on the map or view to select it.
2. Choose File→Close Viewer.

To exit from ServerWORKS Manager Console

- From the Explorer or Map Viewer window choose File→Exit.

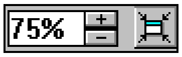
To exit from ServerWORKS and close all processes

1. Choose Tools→Options→Default Actions.
2. Select Close All Applications on Exit and click OK.

Navigating Through Maps And Explorer Views

You can manipulate the objects on a map for better viewing or logical grouping and move between map and list views in several ways.

You can resize a map because a large subnet viewed at 100% may be too large for your monitor.



To fit a map to the current window

- Click on the scale button.

To scale a map to a specific size

- Click on the (+) or (-) sign or enter a number in the % field and press Enter.

On the other hand, to keep the view as is, you can bring other parts of the map into view.

To view regions of the map that extend beyond the current window

- Click and drag the horizontal or vertical scroll bar handles until the hidden portion of the map is in view.

To select a portion of the map for viewing

1. Choose View→Navigator.
2. Click on the section of the map you want. That section then appears in the Map view.

A busy subnet may have hundreds of connections and objects. Once you have established that connections are valid and you want to focus on specific objects, you can hide the connections.

To alternate between showing and hiding connections

- Choose View→Show Connections or View→Hide Connections.

The Explorer view is read-only. However, you can recreate the list view in other list views or transfer objects between map views.

To copy an object to another view

- Click and drag the object from one map to another map or from one list view to another list view. (You cannot drag and drop between a list view and a map view.)

To move an object to another map

1. Select the object.
2. Press CTRL+X.
3. Click on the destination map.
4. Press CTRL+V.

Viewing Options on Individual Maps

You have several layout and alignment options for better viewing. Gridlines provide horizontal and vertical orientation.

To show or hide grid lines

1. Choose File→Viewer Properties.
2. On the Map Viewer Properties dialog box, click Snap to Grid or Display Grid and choose the dimensions for the cell.

Auto-placement determines the best arrangement for a specific map.

To auto place objects

- Choose Edit→Auto Placement.

Tiling aligns all objects horizontally and vertically.

To tile the objects

- Choose View→Tile View.

Alignment arranges selected objects in the orientation you choose (by the top, bottom, right, or left sides of the objects).

To align selected objects

1. Choose Edit→Align Objects.
2. On the Align Objects dialog box, click the alignment option.
3. Click OK.

Removing and Deleting Objects

You can also remove or delete objects. Removing an object removes the object from the view, but leaves it on the network. Deleting *permanently* removes Windows NT objects, such as domains, users, groups, and directories from the network. Be sure you want to delete the object.

To remove any object from a view

1. Select the object.
2. Choose Edit→Remove.

To delete an NT object from the network

1. Select the object.
2. Choose Edit→Cut or CTRL +X.

How Discovery Finds Objects

Discovery identifies objects using a specific sequence. Discovery first uses IP, followed by querying the SNMP MIB II System Descriptor (the sysDesc). Discovery also checks to see whether a DIGITAL agent is running on the object. If the agent is running, Discovery looks for the DIGITAL base agent system descriptor string (svrSystemDescr). On finding this string, Discovery identifies the object as a Server.Digital.

Discovery continues to query the object and learns

- If the object is a server, Discovery determines whether the object is a cluster server.
- If the object is a cluster server, Discovery determines whether the object is a Microsoft NT cluster or a DIGITAL NT cluster.

- If Discovery does not find any of the preceding information, the object is identified as a Node.Generic. (Most objects appear as generic nodes because SNMP is not configured on the managed devices). Objects are also classified as Node.Generic if they have an SNMP layer, but it is not identifiable from the list of known SNMP object types.
- If an object has multiple adapters, and is not running the DIGITAL agent, the object is identified as a Router.

Discovering Networks

Discovery begins with a search of the subnet of the system on which the Console is installed using the default community of Public. The Discovery wizard detects the local subnet based on the local system IP address. On subsequent discoveries, you can specify other subnets and save each as a separate map view. Discovering by subnets is an orderly way to discover an entire network.

For the first discovery, start with the default subnet and network mask.

1. From ServerWORKS Manager, choose Actions→Discover IP Objects. The dialog box Networks to discover opens.
2. If this is the first discovery, click Next. If this is a subsequent discovery, enter a subnet IP address or a unique IP address (to discover a known object and place it in a view) in the Network field.
3. In the Netmask field, enter the subnet mask.
4. Click Add to place the new network or system on the list.
5. Click on the subnet to select it for discovery.
6. Click Next.
7. On the Discovery Security dialog box, do one of the following:
   - Click Next to accept Public, the default community.
   - Enter a community name. Discovery then finds only those objects that belong to the same community as the management console system.

8. On the Types to discover dialog box, do one of the following:
   - Click on Next to discover All Types of objects.
   - Select the specific types of objects you want to discover. Then click Next.
9. On the Discovery options dialog box, choose the discovery method. Unless you are familiar with your subnet and can specify a Start Host for beginning the discovery, choose Ping Spray. If you have created hierarchical views or maps, select one for the discovery results from the list in the “Select a map viewer for discovery results:” list.
10. Click Finish.
11. Choose Yes or No to indicate whether you want to view the discovery report.
12. Choose Yes or No to add new objects to the current view.

Note: Discovery time varies from 15 seconds for a single node to more than 30 minutes for a large subnet. Watch the TCP/IP Discovery in progress dialog box. The status bar displays current activity. When the Finish time appears, the Discovery is complete.

What Have You Discovered?

After the first discovery you have a graphical or list view of your subnet. The map contains icons for the default object types on your network.

Subsequent Discoveries

The Discovery process is incremental. You can run a discovery each time you open ServerWORKS Explorer to update the information in the database and on a map. When you open the Explorer and do a subsequent discovery on a view:

- New connections and nodes are added to the map
- Configuration information is updated for previously discovered nodes
- Customized maps are preserved

To perform a subsequent discovery from the Explorer

- Click on an object type on the Explorer tree or click on a (+) sign next to an object type. The IP Discovery dialog box opens. Do one of the following:
  - Click Discover to rerun a discovery on the subnet in the view.
  - Click View Objects Already Discovered to open the view without refreshing it.

Discovering Clusters

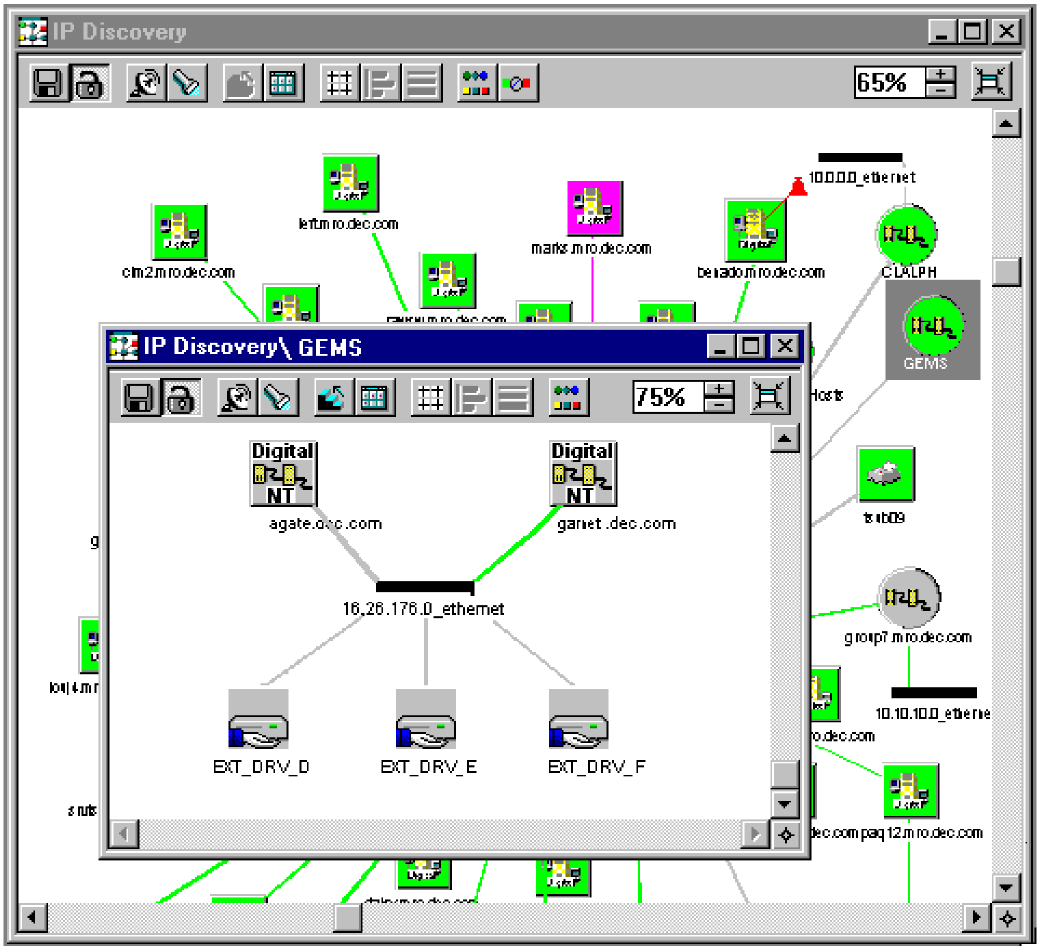
ServerWORKS finds clusters on a network and displays them with a cluster icon in the Explorer or map view. Figure 4-3 shows a map of an expanded cluster domain in the map and hierarchical views.

To display the cluster members and resources

Do one of the following:

- Double-click on the cluster object on the map. The temporary windows lists the servers and resources.
- Double click on the cluster object type on the Explorer view, which expands the cluster object to show its servers and resources.

Figure 4-3 Expanded Cluster Map



Printing Reports of Discovery Information

IP Discovery is updated each time you open a view in ServerWORKS. You can save the information in a report. The reports are text files that you can view and print in an editor such as Notepad. You can choose a Discovery Report or an IP Address Report. The reports provide different information.

Discovery Reports

Discovery Reports are generated by IP Discovery and contain information about the discovered objects. When a Discovery is complete, the report lists newly discovered IP hosts, configuration changes, duplicate IP address, and misconfigured devices. You can print

- From Discovery as the discovery concludes. Follow the prompts to print the report.
- From the saved text file, which you can open in Notepad. The saved files are found in the following directory:

  ```
  Program Files\DIGITAL\SWMGR\database\IPREPORT
  ```

  With the file name format of

  ```
  <month><date><hour>minutes>.txt
  ```

  For example, the report for March 31, 1998, appears as

  ```
  03311998.txt
  ```

To set specific output for the report

1. Proceed through a Discovery (see the section *"Discovering Networks"* in this chapter) to the Discovery Options dialog box.
2. Choose the Advanced button.
3. On the TCP/IP Advanced Options dialog, choose the Output tab.
4. Specify the output file name and click on the information types you want in a report and click OK.
5. Finish the discovery.

To print an IP Discovery Report

1. From the Console, choose Tools→IP Discovery Report.
2. Double-click on the file you want to print.
3. In Notepad, choose File→Print.

IP Address Reports

IP Address Reports are created from the database after a discovery is completed. The information in the report includes the IP address, name, and MAC address of each discovered object. The is report is useful for resolving conflicts between IP addresses and MAC addresses.

To print an IP Address Report

1. From the Console, choose Tools→IP Address Report.
2. From the Dump Object window, choose File→Save. The file is saved as Report.txt.
3. To print the file, locate the file in

```
Program Files\DIGITAL\SWMGR\database\report.txt
```

4. Double-click on the file.
5. In Notepad choose File→Print.

How Is Your Network Operating?

After a discovery and from either view, ServerWORKS displays the overall system status at a glance. You can use any of the following methods for quick status checks.

- Color-coded status and alarm icons on the Map and Explorer views
- Alarm Status Bar
- Alarm Viewer

Color-Coded Status Checks

You can monitor status changes on objects on the view by color. On a hierarchical view, status is indicated by a circle to the left of the object. On a map view, status is indicated by the background color of the object icon. For cluster objects, a status of Down or No response on a resource or member is indicated at the cluster group level. Expanding the cluster icon reveals the source of the problem.

Table 4-1 Status Color Indicators on Map and Hierarchical Views

Color	Meaning
Green	The object is operating.
Red	The object has gone down (but this may be an intentional action by an administrator).
Yellow	An SNMP poll indicates that the device is abnormal is some way; for example, one interface may be down.
Magenta	The system is not responding.

You can change the default colors. Refer to the section in Chapter 7, "*Customizable Options for a View or Map*."

Quick Checks from the Status Bar

Use a daily updated Explorer or Map view for daily alarm checks using the Alarm Viewer status bar (Figure 4-1). The Down and No Resp (Response) buttons on the left side tell you at a glance if any object is off line or not communicating. On the right side, the Alarm counter buttons display the number of alarms that were triggered at each severity level.

Learning From the Alarm Viewer

The Alarm Viewer lists all current alarms. Use the Alarm Viewer to view the alarm details. Use the Alarm Filter to customize the view.

To open the Alarm Viewer and check the messages

- Click on an alarm severity button or Choose Actions→View Alarms.

On the Alarm Viewer (see Figure 4-4), you can analyze the alarm messages in several ways:

- Choose All Acknowledged Alarms to see every alarm of any type on all systems.
- Sort the viewer columns alphabetically by device or by severity, date, in ascending or descending order. To sort a column, click on the column label. Information in the adjacent row changes as the column sorts. You may want to sort by severity and show all High alarms first.
- Click on a single alarm to read the alarm message in the Detail window.
- Drag diagonally from the window corner to expand or contract the Alarm Viewer window. The first three columns contain the most significant information (object name, severity, and date and time). If you need the remaining details about the alarm, you can either scroll or expand the window. The Alarm Viewer in Figure 4-4 is expanded to show more columns.
- Filter the alarms for more precise listings.

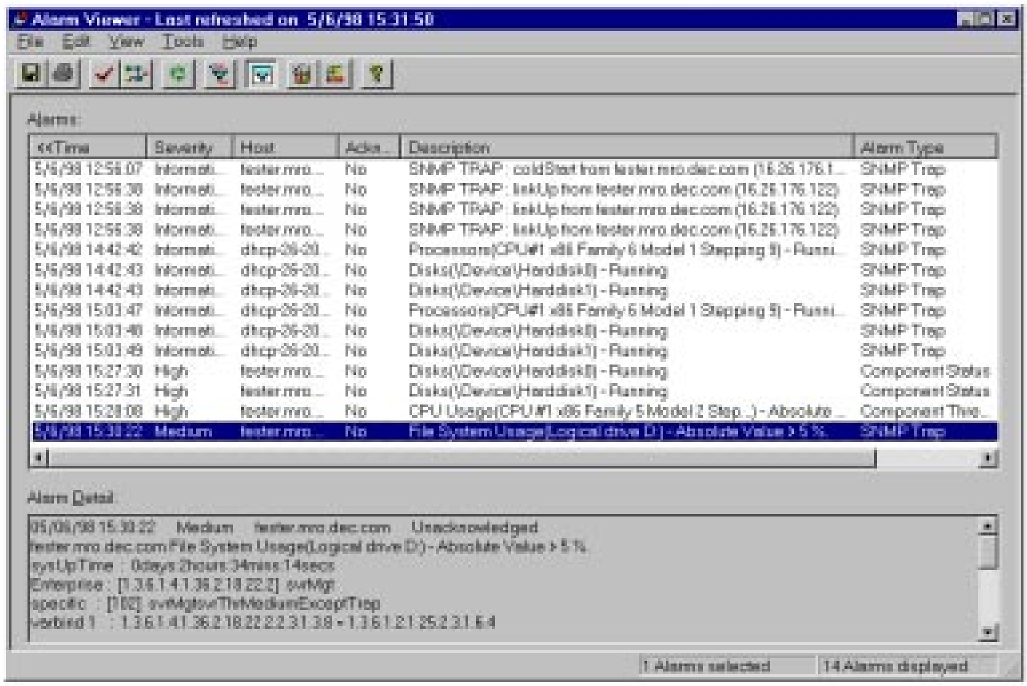
Saving and Printing the Alarm List

You can save the alarms as they have been sorted in the Alarm Viewer window. Then you can import the file into Microsoft Excel.

To save the alarm list

1. Choose File→Save As.
2. Enter a file name and click Save. The file is saved in a tabular format for importing into spreadsheet programs.

Figure 4-4 Alarm Viewer



<<Time	Severity	Host	Ackn...	Description	Alarm Type
5/6/98 12:56:07	Informati...	tester.mro....	No	SNMP TRAP : coldStart from tester.mro.dec.com (16.26.176.1...	SNMP Trap
5/6/98 12:56:38	Informati...	tester.mro....	No	SNMP TRAP : linkUp from tester.mro.dec.com (16.26.176.122)	SNMP Trap
5/6/98 12:56:38	Informati...	tester.mro....	No	SNMP TRAP : linkUp from tester.mro.dec.com (16.26.176.122)	SNMP Trap
5/6/98 12:56:38	Informati...	tester.mro....	No	SNMP TRAP : linkUp from tester.mro.dec.com (16.26.176.122)	SNMP Trap
5/6/98 14:42:42	Informati...	dhcp-26-20...	No	Processors(CPU#1 x86 Family 6 Model 1 Stepping 9) - Runni...	SNMP Trap
5/6/98 14:42:43	Informati...	dhcp-26-20...	No	Disks(\Device\Harddisk0) - Running	SNMP Trap
5/6/98 14:42:43	Informati...	dhcp-26-20...	No	Disks(\Device\Harddisk1) - Running	SNMP Trap
5/6/98 15:03:47	Informati...	dhcp-26-20...	No	Processors(CPU#1 x86 Family 6 Model 1 Stepping 9) - Runni...	SNMP Trap
5/6/98 15:03:48	Informati...	dhcp-26-20...	No	Disks(\Device\Harddisk0) - Running	SNMP Trap
5/6/98 15:03:49	Informati...	dhcp-26-20...	No	Disks(\Device\Harddisk1) - Running	SNMP Trap
5/6/98 15:27:30	High	tester.mro....	No	Disks(\Device\Harddisk0) - Running	Component Status
5/6/98 15:27:31	High	tester.mro....	No	Disks(\Device\Harddisk1) - Running	Component Status
5/6/98 15:28:08	High	tester.mro....	No	CPU Usage(CPU#1 x86 Family 5 Model 2 Step...) - Absolute ...	Component Thre...
5/6/98 15:30:22	Medium	tester.mro....	No	File System Usage(Logical drive D:) - Absolute Value > 5 %.	SNMP Trap

```
05/06/98 15:30:22     Medium     tester.mro.dec.com     Unacknowledged
tester.mro.dec.com File System Usage(Logical drive D:) - Absolute Value > 5 %
sysUpTime  :  0days 2hours 34mins 14secs
Enterprise :  [1.3.6.1.4.1.36.2.18.22.2]  svrMgt
specific   :  [102]  svrMgtcwThMediumExceptTrap
varbind 1   :  1.3.6.1.4.1.36.2.18.22.2.2.3.1.3.8 = 1.3.6.1.2.1.25.2.3.1.6.4
```

1 Alarms selected | 14 Alarms displayed

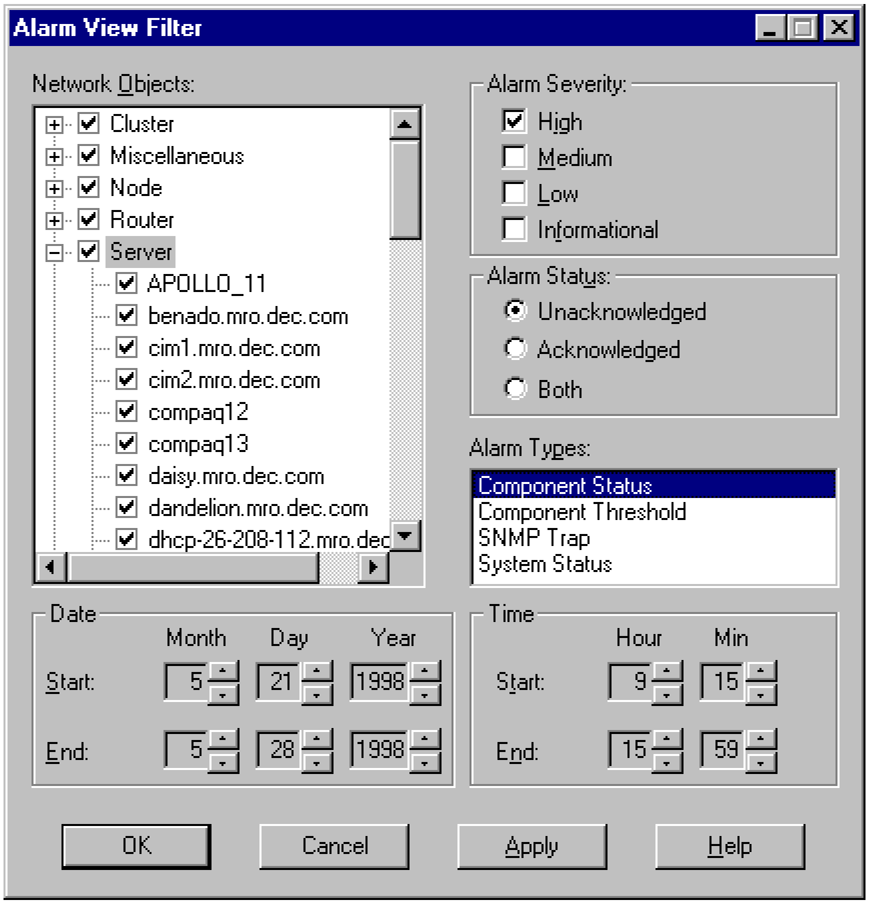
To import the alarm list to Microsoft Excel

- In Windows Explorer, click and drag the saved file to an Excel shortcut on the desktop. Excel opens and inserts the text files into a spreadsheet.

Filtering Alarms for Viewing

The Alarm Filter lets you choose which alarms will appear in the Alarm Viewer window. The Alarm Viewer Filter in Figure 4-5 is set to show all unacknowledged component status alarms of high severity on all network object types. For analysis of a certain period, times and dates were set. Only alarms that occurred during the time period appear.

Figure 4-5 Alarm Filter Dialog Box



Alarm View Filter

Network Objects:

- ☑ Cluster
- ☑ Miscellaneous
- ☑ Node
- ☑ Router
- ☑ Server
  - ☑ APOLLO_11
  - ☑ benado.mro.dec.com
  - ☑ cim1.mro.dec.com
  - ☑ cim2.mro.dec.com
  - ☑ compaq12
  - ☑ compaq13
  - ☑ daisy.mro.dec.com
  - ☑ dandelion.mro.dec.com
  - ☑ dhcp-26-208-112.mro.dec

Alarm Severity:

- ☑ High
- □ Medium
- □ Low
- □ Informational

Alarm Status:

- ● Unacknowledged
- ○ Acknowledged
- ○ Both

Alarm Types:

- Component Status
- Component Threshold
- SNMP Trap
- System Status

Date

	Month	Day	Year
Start:	5	21	1998
End:	5	28	1998

Time

	Hour	Min
Start:	9	15
End:	15	59

Setting Alarms 5

Checking the status of network objects is useful, but current status is not an indicator of future performance. For example, an UP status indicates only that operation is adequate for now. To be forewarned of developing problems, use ServerWORKS Alarm Configuration. This chapter explains:

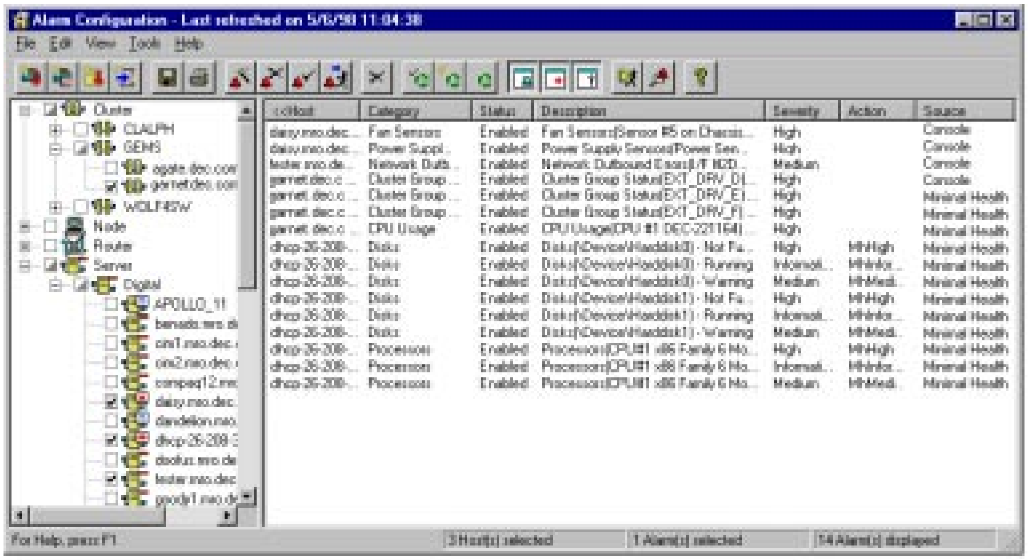
- The Alarm Configuration window and toolbar
- Minimal Health default alarms
- Console (user-defined) alarms
- Alarm notification actions

The Alarm Configuration Window and Toolbar

This section explains Alarm Configuration, which is used to create and view details about the alarms set on network hosts. (Use the Alarm Viewer to view all alarms that were triggered.)

The Alarm Configuration window displays the network host names in the left pane. The right pane contains the alarm description and details, such as the host name, IP address, object type, a description, the alarm severity, the source of the alarm, the category, and its enabled status. Figure 5-1 illustrates the Alarm Configuration window.

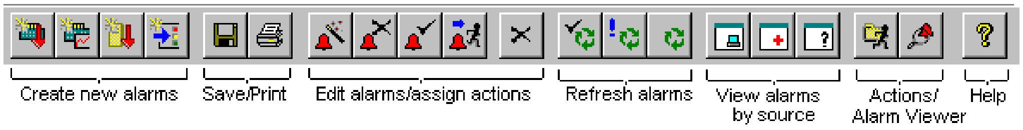
Figure 5-1 Alarm Configuration Window



<<Host	Category	Status	Description	Severity	Action	Source
daisy.mro.dec...	Fan Sensors	Enabled	Fan Sensors(Sensor #5 on Chassis...	High		Console
daisy.mro.dec...	Power Suppl...	Enabled	Power Supply Sensors(Power Sen...	High		Console
lester.mro.de...	Network Outb...	Enabled	Network Outbound Errors(I/F 82D...	Medium		Console
garnet.dec.c...	Cluster Group...	Enabled	Cluster Group Status(EXT_DRV_D)...	High		Console
garnet.dec.c...	Cluster Group...	Enabled	Cluster Group Status(EXT_DRV_E)...	High		Minimal Health
garnet.dec.c...	Cluster Group...	Enabled	Cluster Group Status(EXT_DRV_F)...	High		Minimal Health
garnet.dec.c...	CPU Usage	Enabled	CPU Usage(CPU #1 DEC-21164)...	High		Minimal Health
dhcp-26-208-...	Disks	Enabled	Disks(\Device\Harddisk0) - Not Fu...	High	MhHigh	Minimal Health
dhcp-26-208-...	Disks	Enabled	Disks(\Device\Harddisk0) - Running	Informati...	MhInfor...	Minimal Health
dhcp-26-208-...	Disks	Enabled	Disks(\Device\Harddisk0) - Warning	Medium	MhMedi...	Minimal Health
dhcp-26-208-...	Disks	Enabled	Disks(\Device\Harddisk1) - Not Fu...	High	MhHigh	Minimal Health
dhcp-26-208-...	Disks	Enabled	Disks(\Device\Harddisk1) - Running	Informati...	MhInfor...	Minimal Health
dhcp-26-208-...	Disks	Enabled	Disks(\Device\Harddisk1) - Warning	Medium	MhMedi...	Minimal Health
dhcp-26-208-...	Processors	Enabled	Processors(CPU#1 x86 Family 6 Mo...	High	MhHigh	Minimal Health
dhcp-26-208-...	Processors	Enabled	Processors(CPU#1 x86 Family 6 Mo...	Informati...	MhInfor...	Minimal Health
dhcp-26-208-...	Processors	Enabled	Processors(CPU#1 x86 Family 6 Mo...	Medium	MhMedi...	Minimal Health

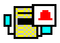
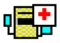
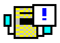
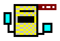
You can use the menu options or the companion toolbar to work with alarms. (See Figure 5-2).

Figure 5-2 Alarm Configuration Toolbar



Any one of several icons next to the host name in the left pane indicate whether alarms are configured on the host.

Table 5-1 Alarm Configuration Host Icons

This Icon	Indicates
	One or more Console or Other Source alarms are configured for this host.
	One or more Minimal Health alarms are configured for this host. Console or Other Source alarms may also be configured.
	One of the following conditions: • The host is newly discovered. There has never been communication with the host to determine if alarms are configured. • SNMP communication with the host was unsuccessful for this session (for example, due to time-outs) so the list may not be current. Alarms that appear in the list are alarms reported from the last successful communication with the host.
	No alarms of any type are configured on this host.

You can choose which data is displayed and the order in which it appears in the right pane and sort the column data alphabetically.

To sort column data

- Click on the column label at the top of the column.

To set up the column data and save the display scheme

1. Choose View→Column Display. The Column Display dialog box opens.
2. To select a data column for the display, click on the check box of the data column.
3. To change the order of the columns, select the data column name and click Up or Down to reposition the column.
4. To save the display, click Save As. Then enter a name in the Save As Display Name dialog box and click OK.
5. Click OK to close the Column Display dialog box.

To view alarms set on selected hosts

- Select the host and one of the following menu commands:
  - Choose View→Show Console to view user-defined alarms.
  - Choose View→Show Minimal Health to view Version 2.x Minimal Health alarms.
  - Choose View→Show Other Sources to view alarms generated by enterprise management programs (for example, HP OpenView.)

You can save the alarm list as a text file. The file, which contains the list of currently configured alarms, is saved in the SWMGR directory.

To save an alarm list

1. Choose File→Save As.
2. Enter a file name click Save. The file is saved in a tabular format for importing into spreadsheet programs.

To import the alarm list to Microsoft Excel

- Locate the file in Windows Explorer and drag it to an Excel shortcut on the desktop.

Refreshing the List of Configured Alarms

Refreshing the list of configured alarms is recommended so the list includes nodes whose alarms were set, deleted, or modified from other management stations and nodes that are new discoveries.

To update the list of configured alarms

Do one of the following:

- Choose View→Refresh All Nodes to update alarms on all nodes. This action may take awhile.
- Refresh View→Selected Nodes to update alarms set on selected nodes. The time needed to update increases with he number of hosts selected.
- Refresh View→Newly Discovered Nodes to update alarms set on nodes that were never included in an alarm Configuration view. This update includes nodes that were manually inserted and is faster than updating all nodes. These nodes are indicated by an exclamation point (as shown in Figure 5-1) so node selection is unnecessary.

Printing the Alarm List

You can print the current Alarms list, sorted by the contents of a selected column. Only the information that is displayed appears in the report. For example, if you are displaying the columns in Figure 5-1, and sort on the IP address, the report contains the host and alarm information on the hosts beginning with the host with the lowest IP address.

To print an alarm list

1. Set up the Alarm list.
2. Click on a sort column.
3. Choose File→Print.

Configuring Alarms

Alarm Configuration is used to set alarms on servers, desktop computers, and mobile systems. The Console receives the alarms and trap messages. You can configure the same alarm for more than one host object as long as the system parameter that is being alarmed (for example, a disk) is present on all the hosts that were selected.

Minimal Health

Minimal Health is the first line of defense for servers. Minimal health provides a set of hardware-specific thresholds on the following X86 processor-based platforms on which it is installed:

- Environmental conditions on power supplies, fans, voltage, and temperature, and operating conditions on hard disks, processors, and memory components for platforms running Windows NT
- Environmental conditions of power supplies, fans, voltage, and temperature on platforms running Novell NetWare

Hosts with Minimal Health are indicated by the red cross icon next to the host name in the Alarm configuration window. (See Figure 5-1.)

Understanding Minimal Health Alarms

Minimal health is an installation option on a host. The following guidelines describe how to use Minimal Health alarms.

- If you choose Minimal Health when you install ServerWORKS agents, a template that defines the alarms and thresholds is applied when the ServerWORKS Version 2.x Minimal Health agents are installed. If you do not install Minimal Health with the ServerWORKS installation kit, you can install it at a later time using the kit. You cannot enable minimal health conditions until you install Minimal Health.
- Minimal Health replaces all thresholds that were set by the Version 1.x. agents in previous versions of ServerWORKS.

- Minimal Health alarms and Console alarms can co-exist. You can have multiple alarms on one component or environmental condition.
- Once installed, you can turn Minimal Health on and off from the menu. When turned off, all Minimal Health thresholds are removed. Turning on Minimal Health reactivates the thresholds.
- Minimal Health stays off until you reactivate it in one of the following ways:
  - Choose the menu option Alarm Configuration→File→Minimal Health On.
  - Reinstall Minimal Health on the host.
  - Change the variable enabling Minimal Health is from the MIB Browser. (To do this you must be familiar with the MIB).
- When you select multiple hosts on which to turn on Minimal Health alarms, check that Minimal Health agents were previously installed on the selected hosts. If the selected hosts contain Version 1.x and Version 2.x agents, Minimal Health is only applied to the hosts with Version 2.x agents.
- You can specify actions for predefined action names that are associated with Minimal Health alarms. Refer to the section "*Associating an Action with a Minimal Health Trap*" in this chapter.
- Modifying Minimal Health alarms is not allowed in Alarm Configuration. However, you can delete individual minimal health alarms and then restore them by turning on Minimal Health from the Console.

User-Defined Console Alarms

ServerWORKS lets you create four kinds of user-defined alarms:

Component Status alarms — Report the operational status of a DIGITAL server or node object.

Component Threshold alarms — Report when a characteristic of a DIGITAL server meets a specified condition. For example, the temperature exceeds a value or a disk exceeds its capacity.

System (interface) Status alarms — Report when a system or interface, such as an adapter, changes its status. For example, a system goes down.

SNMP Traps — Send SNMP messages that are triggered by the SNMP agent.

Setting Up SNMP and the Trap Destination

If you have not done so, you must configure SNMP service on each system where a ServerWORKS agent is installed and specify the trap destination IP address. The Console does not receive any traps from a managed device if a the Console destination is not specified.

You can have multiple trap destinations specified in the SNMP configuration and you can forward traps from the destination Console to other Consoles or to enterprise managers. Refer to the section Chapter 7 for details about configuring SNMP and setting trap destinations.

Component Status Alarms

Status alarms are sent when a device fails, issues a warning, or comes back online. You can set status alarms on the following components:

- Processors
- Disks
- Fan Sensors
- Voltage Sensors
- Power Supply Sensors
- Temperature Sensors
- Memory Status
- Cluster Group Status

Component Threshold Alarms

In a threshold alarm you specify a value for a measurable condition or characteristic. When the alarm condition reaches the specified value, the alarm is triggered. You can set threshold alarms on the following conditions or characteristics:

- CPU utilization, file system utilization, and disk storage usage
- Voltage, temperature, and fan status
- Total Packets, inbound errors, outbound errors, inbound packets, inbound packet discards, unknown protocol errors

When you set up the threshold you also specify a value that resets the alarm when the condition returns to a reasonable value. The reset value should be out of the alarm range. Depending on the relational operator (greater than, less than, etc.) that you use, the reset can be higher or lower than the threshold.

For example, if you are alarming a device for excessive temperature, you can set the threshold for temperatures greater than 60° and reset the alarm at 50°. You will avoid alarms on momentary spikes near the 60° level as the unit is returning to normal. On the other hand, if you are watching for low temperatures, you might set the threshold less than 32° with a reset value of 40°.

You can also set the threshold alarm to send multiple traps on the same alarm by applying a repeat mode, which sends the trap until the condition is reaches the reset value.

Responding to Prompts During Alarm Configuration

Alarm Configuration displays several message boxes if you are sending multiple traps. These are explained in the sections that follow. As you become familiar with the messages and know how you plan to respond to them, you can turn off the prompts. You can restore them at anytime.

To manage the prompts

- On the message box, click the selection “Do not prompt again.”

To restore the prompts

- Choose Edit→Re-enable all prompt messages to display the prompts again.

Setting up Multiple Traps for Threshold Alarms

You may be running Version 1.x agents and Version 2.x server management agents on devices on your network. The agent versions behave differently when you are setting thresholds and repeat modes for multiple traps. A message appears that explains your options.

- You can send multiple traps from devices on which Version 1.x agents are installed. To do this, the agents allow a reset value that is within the alarm range, which in turn will send multiple traps to a trap destination per one alarm event. The frequency of the traps sent is the polling interval.
- You can send multiple traps from devices on which Version 2.x agents are installed by entering a repeat mode when you set the alarm. Version 2.x agents do not allow an invalid reset number for a threshold. If you enter an invalid number, you are prompted to change it.

Setting Multiple Traps With Multiple Agent Versions

In general, avoid setting alarms simultaneously on multiple devices running Version 1.x and Version 2.x alarms. However, if you select multiple devices, a message appears that explains your options:

- Continue setting the alarms. To do this, choose Yes on the message prompt. The threshold reset value on the Version 1.x devices will be used as the repeat mode and the reset value for Version 2.x devices will be equal to the alarm triggering value.
- Stop setting the alarms. To do this, choose No. Then begin the process again, setting alarms separately for different agent versions.

Setting Traps for Network Inbound and Outbound Packets

Network Inbound and Outbound Packets are not affected by the agent version. Whether the agents are Version 1.x or Version 2.x, the threshold reset value is equal to the polling interval. When prompted, choose Yes to continue setting the alarms.

System Status Alarms

System Status alarms report an Up, Down, No Response or Test status on a server. (Test status may appear if you are using SNMP instead of ICMP for polling. A Testmessage is returned as a status on an interface, for example, in loopback testing of an interface.)

SNMP Trap Alarms

SNMP Trap alarms are sent when the SNMP agent detects a status change. Alarm Configuration provides a list of valid SNMP traps to set on components

To learn more about the SNMP variables that are monitored for traps, read the vendor MIB for the particular device.

Creating Alarms and Notification Actions

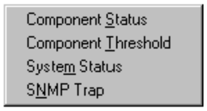
When you create an alarm, complete the following tasks. Each of these tasks is composed of several smaller steps.

- Select the hosts.
- Choose the type of alarm and specify the settings for the alarm.
- Refresh the alarm list when you add or modify an alarm.

In addition, if you are creating an optional notification for the alarm, associate an action with the alarm. You can create notifications using the actions as follows:

- You can reuse the action for different types of objects or for different types of alarms.
- You can assign multiple actions to one action name.
- You can assign multiple action names to one alarm.

Creating Component Status Alarms



1. From the ServerWORKS Manager Console menu, choose Tools→Alarm Configuration.
2. Select the hosts from the list of network objects.
3. From Alarm Configuration, choose File→New Alarm→Component Status.
   On the Category tab of the Add New Component Status Alarm dialog box, select an Alarm Category and the items to be monitored. The elements you can alarm are based on the object type. In turn, the sub-elements you can alarm change with the category. The Alarm at a Glance pane displays a summary of the alarm.
4. On the States tab from the list of Possible States, select the states you want in the alarm definition (for example Not Functional) and click the right arrow button to add the state to the Alarm States list.
5. On the Severity tab choose the importance of the alarm being set.
6. On the Polling tab select the polling interval for the object. A high severity alarm should have frequent polling, for example, one minute.

7. If you are specifying an action, do one of the following:

   – On the Actions tab choose an existing action from the Action Directory and click OK to finish setting the alarm.

   – Click on Add New and refer to the section "*Adding the Notification Action on an Alarm*" and the subsection that describes the action you want:

Paging action	*Setting up a Pager Notification Action*
Email action	*Setting up an Email Notification Action*
Application launch	*Setting up an Application Launch*

8. Choose OK.

Creating Component Alarms

1. From the ServerWORKS Manager Console menu, choose Tools→Alarm Configuration.

2. Select the host(s) for alarming from the list of network objects.

3. From Alarm Configuration, choose File→New Alarm→Component Status.

4. On the Category tab of the Add New Component threshold Alarm dialog box, select an Alarm Category and the Items to be Monitored. The alarm category lists the elements you can alarm based on the object type. In turn, the sub-elements you can alarm change with the category. The Alarm at a Glance pane displays a summary of the alarm.

5. On the Threshold tab select an absolute or relative value from the list of Alarm Computation Methods. Then set the threshold computation choosing an operator (for example, greater than), and a baseline. Click the Current Value button to see current usage. At Re-enable Alarm, choose an optional repeat trigger. Enter the value at which to trigger. the states you want in the alarm definition (for example Not Functional) and click the right arrow button to add the state to the Alarm States list.

6. On the Severity tab choose the importance of the alarm being set.

7. On the Polling tab select the polling interval for the object. A high severity alarm should have frequent polling, for example, one minute.
8. If you are associating an action with this alarm, on the Actions tab, do one of the following:
   - Choose an existing action from the Action Directory and click OK to finish setting the alarm.
   - Or click on Add New and refer to the section "Adding the Notification Action on an Alarm” and the subsection that describes the action you want.
9. Choose OK.

Creating System Status Alarms

1. From the ServerWORKS Manager Console menu, choose Tools→Alarm Configuration.
2. Select the object (host) for alarming from the list of network objects.
3. From Alarm Configuration, choose File→New Alarm→System Status.
4. On the Add New System Status Alarm dialog box specify the following:
   - System Status: Choose one from Up, Down, No Response, and Test.
   - Choose a severity from High, Low, Medium, or Informational.
   - Choose an action from the Actions Directory or choose Add New to create a new action and proceed to the section *“Adding the Notification Action on an Alarm.”*
5. Choose OK.

Creating SNMP Trap Alarms

1. From the ServerWORKS Manager Console menu, choose Tools→Alarm Configuration.

2. Select an object (host) for alarming from the list of network objects.
3. From Alarm Configuration, choose File→New Alarm→Component Status→SNMP Trap.
4. From the Add New SNMP Trap Alarms dialog box, specify the following items:
   - SNMP Traps: Choose each item for which you want a trap message sent.
   - Choose a severity from High, Low, Medium, or Informational.
   - Choose an action from the Actions Directory or choose Add New to create a new action and proceed to the section “Adding the Notification Action on an Alarm.”
5. Choose OK.

Modifying an Alarm

You may need to change a setting, an action, or the severity of an alarm.

1. From the Alarm list pane, select the alarm, and choose Edit→Modify Alarm or double-click on an alarm in the list.
2. On the dialog box that opens, edit the alarm settings and click Apply after each change to an alarm tab page, or click OK when all changes are made.

Adding a Notification Action on an Alarm

You can choose among several actions when an alarm condition occurs—pager notification via alphanumeric or numeric pagers, electronic mail (email) notification, and an application launch. For any action, you also set the frequency of the action from the following choices on the Policy property page:

- Always, for any alarm, for any action, whenever the alarm condition is met
- Once for the first alarm only
- At specified intervals for all alarms, regardless of how often the alarm condition occurs
- At specified intervals for some individual alarms, up to a maximum number of times regardless of how often the alarm occurs

For high severity alarms, you might choose always. For less severe alarms, choose an interval to avoid overloading your email account or pager with repeat messages. For minor alarms, once is sufficient (assuming you act on the notification before the problem becomes severe).

Setting Up a Pager Notification Action

ServerWORKS Manager V4.0 supports alphanumeric and numeric paging.

The message that you receive on a numeric page is the pager message.

To send a numeric page, you need:

- The Pager number, which is the telephone number to dial the pager
- The Pager Message, a numeric code that represents the message you are sending

The message that you receive from an alphanumeric page is received from the network and contains the date, time, node name, and a description of the condition that triggered the alarm. To send an alphanumeric page, you need:

- The dial-up terminal number, which is the paging vendor’s dispatch telephone number
- A PIN (personal identification number), which is your pager number
- The message you want to send
- The maximum message length your pager supports. Consult your pager documentation

Before you can use the pager for notification, check that you have a modem and comm port configured on the Console to dial the telephone number correctly. Refer to Appendix B for more information.

1. In the Add New Actions dialog box, choose the Pager tab and click New.
2. On the New User dialog box General tab, enter the User Name, which is required and an optional email address and comments.

3. Click on the Paging tab.
4. Choose one paging mode and complete the information:
   - Numeric Paging**.** Enter the Pager Number and the Pager Message." Refer to the section "Changing the Default Pager Wait Time for details about using commas with numeric pagers.
   - Alphanumeric Paging. Enter the Dial-up Terminal Number and the PIN. Then select the message length from the Max Message Length list.
5. On the Paging tab, specify the Modem information. Select the Comm Port and baud rate for your modem configuration.
6. Click OK. The user name appears in the All Users With Pager list. Click Add to place the name in the Action Assigned Page Users list.
7. Click on the Policy tab and choose the interval (as described previously in this section) if you want to specify an interval for the pager notification only. Then click OK.
8. Enter the action name, for example Page Me. Click OK. The new action Page Me appears in the Action Directory Contents list. Click OK.

When an alarm condition is detected on an alarm with an associated paging action, the modem dials the pager and sends the message to the pager.

Changing the Default Pager Wait Time for Numeric Paging

Numeric pagers allow you to include a wait time to adjust for timing between dialing a phone number and sending the numeric message. The standard symbol is a comma. ServerWORKS Manager Console paging alarm has a default wait time of five commas. You can change the wait time if you need more or less wait time between dialing the phone number and sending the numeric message.

To change the wait time

1. Open the swmgr.ini file and find the section [Setup].
2. Add the following statement to the section:

   ```
   PagerWaitTime=
   ```

3. Enter a number for the page wait time. The page wait time is the number of commas. You may have to try several numbers until you find the right wait interval for your paging system.

Setting Up an Email Notification Action

Before you can use email for notification, you must check that you have a valid profile for Microsoft Exchange mail so the recipient gets the notification and that Exchange is running. First check that the profile for your mail is ‘MS Exchange Settings.’ If not, you must specify it as the default profile. Refer to the section *“Setting Up the ‘MS Exchange Settings’ Default Profile.”* Restart MS Exchange before setting up the email notification action.

1. On the Add New Actions dialog box, choose the Email tab and click New.
2. On the New User dialog box General tab enter the user information. The email address is the Internet mail address for the recipient (for example support@company.com). The message to the recipient contains the date and time, node name of the object that triggered the alarm, and a description of the triggering condition. SNMP traps may include additional information.
3. Click OK. The user name appears in the All Users With Email list.
4. Click on the Policy tab and choose the interval (as described previously in this chapter) if you want to specify an interval for the email notification only.
5. Click Add to place the name in the Action Assigned Email Users list.
6. Enter the action name, for example Email Me and click OK. The new action Email Me appears in the Action Directory Contents list.

When an alarm condition is detected on an alarm with an associated email action, the mail protocol sends a message to the named recipient.

Setting Up the ‘MS Exchange Settings’ Default Profile

To configure Exchange for email notifications, first install your favorite mail protocol on the same system where ServerWORKS Manager Console is installed. (Refer to the mail protocol installation documentation for details. Instructions for specific mail applications are beyond the scope of this manual). When you run ServerWORKS Manager, also run Microsoft Exchange to receive the notification at the Console.

The ‘MS Exchange Settings’ default profile contains your mail protocol and logon information. The profile is required for the email notification action.

1. From the Windows desktop, right click on the Exchange Inbox icon and choose Properties.
2. Choose the Show Profiles button. If ‘MS Exchange Settings’ appears in the list of profiles and in the “When starting MS Exchange, use this profile” field, choose Close. If the profile is not listed, create the profile.
3. Before you proceed, consult your system administrator for the mail protocol name and logon information (such as the user name or mailbox and whether you are using Exchange Server, Internet mail, or other information services).
4. Click the Add button. On the Inbox Setup Wizard dialog box, select the option “Use the following information services” and choose your protocol from the list of information services.
5. Click the Next button. In the Profile Name dialog box, select ‘MS Exchange Settings’ (or enter the name ‘MS Exchange Settings’ exactly, if it does not appear. You must use this name). Then click Next again.
6. Continue to follow the prompts on the remaining dialog boxes. These vary according to the information service you selected but will include protocol and user information.

7. Continue to follow the prompts and choose Finish on the last Wizard dialog box.

The ‘MS Exchange Settings’ profile is added to the list of profiles. Select the profile and choose Close.

Setting Up an Application Launch Action

The application launch action can call a simple executable or a complex batch file. For example, you can create a BAT file with multiple commands. You will have to determine the command line for any procedure.The following is a simple example.

1. On the Add New Actions dialog box, choose the Application Launch tab.
2. Enter the file name. You need the full path name and the file extension (for example, c:\netscape.exe to open a browser window).
3. Select the alarm information (parameters) that you want passed to the application to be launched. Your application must be programmed to use the parameters (for example, to display an animated alert and the passed parameters on an HTML page).
4. Click on the Policy tab and choose the interval (as described previously in this chapter) if you want to specify an interval only for the application launch notification. Then click OK.
5. On the Action Name dialog box, enter a name for the action (for example, Alert Me.) The name appears in the Actions Directory list.

When an alarm condition is detected on an alarm with an associated application launch, the activity specified in the command line is performed.

Setting Up Notification for Minimal Health Traps

The Minimal Health template associates action names for Minimal Health traps. The default is that no actions are assigned to the names. If you want notification of a Minimal Health message, you can modify the properties of the action name by assigning your choice of action(s) for the following Minimal Health alarms.

- MhHigh
- MhMedium
- MhInformational
- MhLow

To modify a Minimal Health action name with an action

1. Choose Tools→Action Directory Setup.
2. Select a Minimal Health action name and click Properties.
3. Select from the Pager, Email, Application Launch, or Policy dialog box pages and define the action. (Refer to procedures earlier in this chapter for details.)
4. When all actions are defined, choose OK to close the dialog box.

Setting Alarms on Clusters and Cluster Resources

You can set alarms on a cluster server or resource in the same way that you set alarms on other objects. One condition of a cluster server or resource that administrators find useful is a message indicating failover from one server to another. The DIGITAL agent that monitors clusters can send the following trap messages, which indicate transition of control from one server to another:

- Not Current Controller. The server sending this trap has lost control of a resource.
- Current Controller. The server sending this trap has gained control of a resource.

On a cluster of two servers, A and B, you can set alarms in the following ways:

- Set a trap for Not Current Controller on Server A to indicate that Server A’s control of a resource has failed over to Server B.
- Set a trap for Current Controller on Server B to indicate that Server B is in control of a resource.Set Not Current Controller and Current Controller trap alarms on the same resource to receive both messages. By using this scheme, you can determine if failover has occurred from a server that is not running. (A server that goes down cannot send a Not Current Controller trap, but the server that has assumed control can send a Current Controller trap.)

To set an alarm on a cluster server or resource

1. From ServerWORKS Manager Console, choose Tools→Alarm Configuration.
2. Select the server on which you are setting the alarm.
3. Choose File→New→Component Status.
4. On the Add New Component Alarm dialog box, click the Category tab.
5. From the Alarm Category drop-down list, choose the Cluster Group Status.
6. On the Items to be Monitored list, select the cluster resources on which you are setting the alarms. Choose from:
   - All Cluster Groups (all resources that were defined when you created the cluster).
   - Any or all of the remaining resource groups. Different clusters will have different selections.
7. Click the States tab and set an alarm on the selected resources. To show failover from the primary server to the secondary server, select Not Current Controller. Then click the Right arrow to add the state to the Alarms states list.

8. Click the Severity tab and select a severity.
9. Click the Polling tab and set polling parameters.
10. Click the Actions tab to set up a notification for the alarm. This is optional. Refer to the previous section for details about setting notification actions.
11. Choose OK.

Monitoring for Transitions

Use the Alarm Viewer to watch for transition activity on a cluster. From the ServerWORKS Manager Console, click on the Alarm Viewer status button for the severity that you chose for the Not Current Controller and Current Controller alarm. If a transition of control has occurred, the alarm appears in the Alarm Viewer.

Managing from the Console 6

ServerWORKS Manager uses the following components for network management:

- The System Browser for viewing comprehensive data about DIGITAL servers, including historical data
- The MIB Browser for viewing SNMP information and performing SNMP operations on an object
- The MIB Profiler, MIB Compiler, and the MIB Enroller, which work together to integrate MIBs into ServerWORKS
- Other background tools that complete ServerWORKS Manager capability

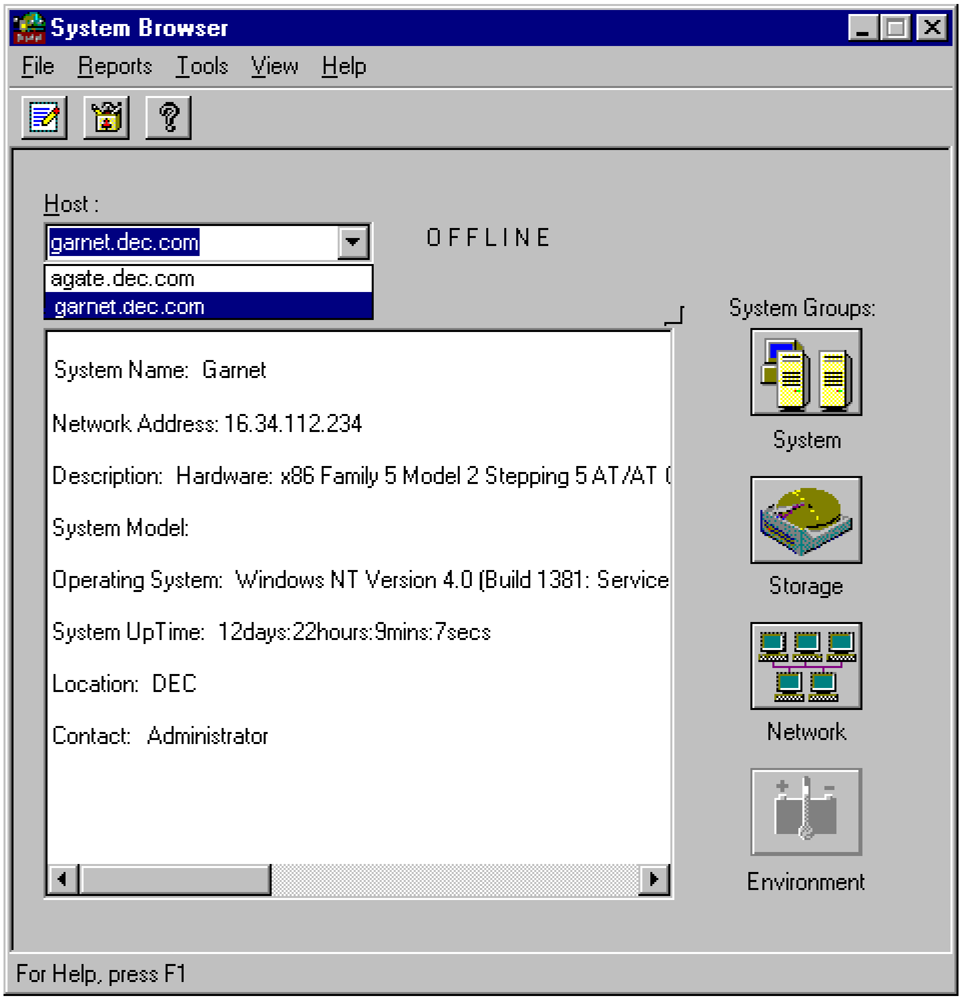
The System Browser for DIGITAL Hosts

The System Browser provides information on both static and dynamic parameters found in DIGITAL objects such as servers, clusters, desktop systems, and mobile devices. The System Browser uses information provided by DIGITAL SNMP agents loaded on the server, desktop, or mobile system.

The System Browser displays:

- System configuration information that generally does not change.
- Current information that is refreshed each time you examine an object from the System Browser. Table 6-1 shows the type of information found in each of the System Browser windows.
- Historical information that is displayed when current information is not available due to network or system problems. This information was previously collected and saved using the System Browser.
- Information about cluster members and cluster resources.
- Dynamic or historical graphed data that show usage patterns on disks and processors, pinpoint environmental spikes, and monitor network transmission statistics.

Figure 6-1 System Browser Window



garnet.dec.com

agate.dec.com

garnet.dec.com

System Name: Garnet

Network Address: 16.34.112.234

Description: Hardware: x86 Family 5 Model 2 Stepping 5 AT/AT (

System Model:

Operating System: Windows NT Version 4.0 (Build 1381: Service

System UpTime: 12days:22hours:9mins:7secs

Location: DEC

Contact: Administrator

For Help, press F1

Table 6-1 System Browser Information

This Window	Displays This Information
System Browser	Host name Network (IP) address Description Physical location and contact Model and operating system* Length of system has been running (Up Time)
System	General information I/O devices Processor FRU* Cluster (when the server is a cluster member)*
Storage	Disks Disk Partitions File System Storage Memory* Memory Component Slots (SIMMs and DIMMs)*
Network	Interface Statistics
Environment*	Thermal Sensors Voltage Sensors Cooling System (fans)* Power (supply)

*Not always present on all systems

Viewing Node Data with System Browser

You can open System Browser to view current or historical data. If you open System Browser from a map or hierarchical view, System Browser displays current information. If the node cannot be reached over the network, System Browser reverts to historical information if it is available. In Figure 6-1, the node is unavailable and is labeled OFFLINE.

Each time you view a node, the node name is added to the drop-down list and data is collected on the node for each system group you view.

To launch System Browser from a map or view

- Double-click a DIGITAL host on a map or hierarchical view or choose Actions→System Browser. Data collection begins on each node you examine.

  If the node or network is inaccessible, and you previously viewed the node, you can select the node from the Host drop-down list and view its historical data.

To view details about the server or host

- Click on one of the System Groups buttons. (See Figure 6-1).

To view details about additional servers or hosts that you can reach over the network

Do one of the following:

- Enter the host name or IP address or select a node from the drop-down list in the Host field. Then press Enter. In Figure 6-1, garnet.dec.com was selected from the drop-down list. You could also enter 16.34.112.234 or garnet. But always use the same node name when you access data on a system because a new file is created for each name.
- Select multiple objects from the map or view and click on the System Browser toolbar icon. System Browser opens with information about the first object selected. The remaining objects appear in the drop-down list.

To view information about a cluster

1. Double-click on a cluster server from a view.
2. Click the Clusters tab.

Comparing Systems and Components

You can use System Browser to view multiple sources of data.

- Select a system. Then open all System Browser groups to view all aspects of the system simultaneously.
- Select multiple systems. Open the same group for each system to compare them by category of information.

Setting FRU Asset Numbers

You can change the FRU (field replaceable unit) asset number on the current board of a node that displays FRU information.

To change the asset number

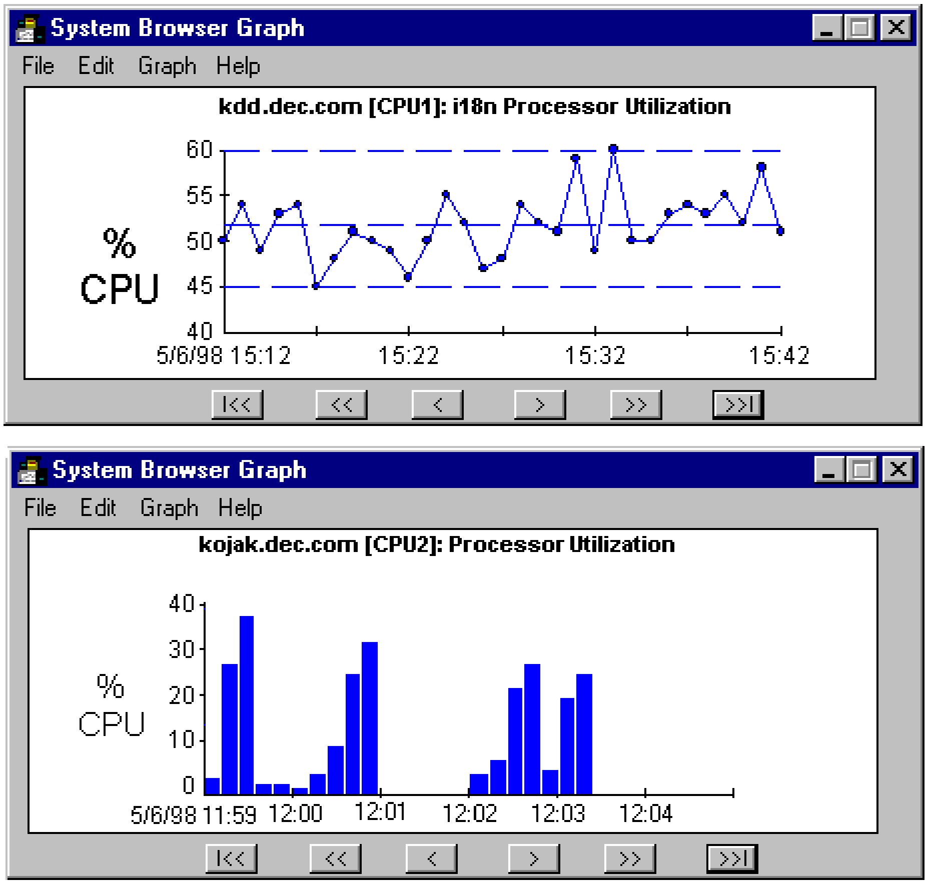
1. From the System Browser, click on the FRU page.
2. Select a current board from the components in the Types list.
3. In the highlighted row, click on the Asset No column and enter the asset number.
4. Click on Set Asset No.
5. Click Refresh.

Graphing Real-Time Activity

You can record activity as a real-time graph for CPU utilization, file system utilization, statistics of network variables, and thermal and voltage sensor readings and save the information as historical data. (Not all systems support all graph types.) You can view graphed data when the node is off line if you have previously graphed and saved data for the selected variable.

You can choose between line or bar graphs and set a sampling interval. Graphing begins to save data after the first sample. The graph shows the start and end times and has gaps for times when graphed data was not saved. Figure 6-2 shows a line and a bar graph.

Figure 6-2 ServerWORKS Graphs



To graph information

1. Choose Actions→System Browser or double-click on a server.
2. From the System Browser window, choose one of the buttons:
   - For CPU processor utilization that record patterns of use
     a. Choose System→Processors.
     b. Select a CPU and click Graph.
   - For file system utilization (disk space usage) that can help you predict potential disk space problems
     a. Storage→File System.
     b. Select a file system from the list and click Graph.
   - For network interface statistics that show traffic patterns or disparities in transmission
     a. Choose Network→Statistics.
     b. Select an interface.
     c. Select a transmission parameter and click Graph.
   - For thermal and voltage readings that reveal random spikes or long term increases
     a. Choose Environment→Thermal Sensors or Voltage Sensors.
     b. Select the component (chassis, power supply) and click Graph.
3. Do one of the following:
   - Choose File→Close and Save to save the graph data.
   - Choose File→Close to discard the current graph data.
   - Choose File→Delete and Close to permanently discard an unnecessary or obsolete graph file.

To change the graph style

1. Choose Edit→Style.
2. Select either Bar Graph or Line and the attributes for each style.

To change the sampling and time interval

1. Choose Edit→Parameters.
2. Enter sampling interval and number of sample points.

Collecting a Node History

System Browser creates historical data folders for each node you examine. Each folder contains an INI file that keeps a list of the data recorded from each of the System Browser groups you view. For example, garnet.com.ini is the file for the node garnet.com. The INI file is a complete record for a node. MIBs that correspond to the node provide this information.

At subsequent sessions, data that was previously recorded is updated and new data is added to the historical data. If you also graph data for a node variable, a graph file with the saved graphed data is kept for that parameter and node. You can import the graph files, which are in tabular format that uses the TAB as a delimiting character, into Microsoft Excel.

You can see historical data whenever a node is off line using the History Viewer if you have previously viewed the node online from System Browser. If you are viewing historical data, the label OFFLINE appears next to the system name, as in Figure 6-1.

When the node is online and the network is responding, new data is appended to the graph. The graph shows breaks between collections of data with null (empty) samples for the unrecorded time period.

To start collecting historical data

1. Choose Actions→System Browser.
2. Enter or select the node name.
3. Click on the System Group pages for the data you want to collect.

To view historical data on a node

1. From the desktop choose Start→Programs→ServerWORKS→ History Viewer. System Browser opens and displays a list of nodes for which historical data has been collected.
2. Select a node.

To collect graph data or view historical graph data

1. Choose Actions→System Browser. System Browser opens and displays a list of nodes for which historical data has been collected.
2. Enter or select a node and click on a System Group page from which you have collected graphs.
3. Select the item and click on a the Graph button. Then choose a directional arrow.

To View Graph Data	Click This Button
Backward to the graph start time	|<<
Backward by one screen	<<
Backward by the sampling parameter	<
Forward from the most recent time and date	>>|
Forward by one screen	>>
Forward by the sampling parameter	>

The MIB Browser for SNMP Objects

The Management Information Base (MIB) Browser is used to query (GET) and modify (SET) MIB variables on SNMP-compliant objects on the network. The MIB Browser lists all of the MIB groups that apply to the object and the MIB variables in each group. For example, if you select a bridge, the MIB Browser displays bridge MIB variables.

Use the MIB Browser to perform the following operations:

- Query SNMP agents to perform a GET or retrieval of Management Information Base (MIB) variables, such as the system name, system ID, and up time for a router, hub, or bridge from the standard MIB II groups or any other MIB enrolled with the MIB database.
- Perform SNMP SET operations against one or more SNMP agents.

- View the properties of any MIB variable (for example, the variable's data type or object identifier, read/write access, and description).
- Open the MIB Profiler to modify or create MIB profiles. See "*Enrolling MIBs in the ServerWORKS Database*" in Chapter 7.
- Open the MIB Enroller and the MIB Compiler to compile and enroll new MIB groups into the ServerWORKS database or modify existing groups. See "*Additional Tools*" in this chapter.

For SNMP objects other than DIGITAL hosts, the MIB Browser is the default management action for viewing the object.

To start the MIB Browser

- Select an object from a view and choose Action→Browse MIB.

Managing an Object From the MIB Browser

The MIB Browser lets you view information by MIB group and variable. Figure 6-3 illustrates the MIB Browser window. Each of the command buttons displays information about the MIB group in MIB II (RFC1213). The MIB variables contained in the group appear in the Variable list.

Modifying Variables

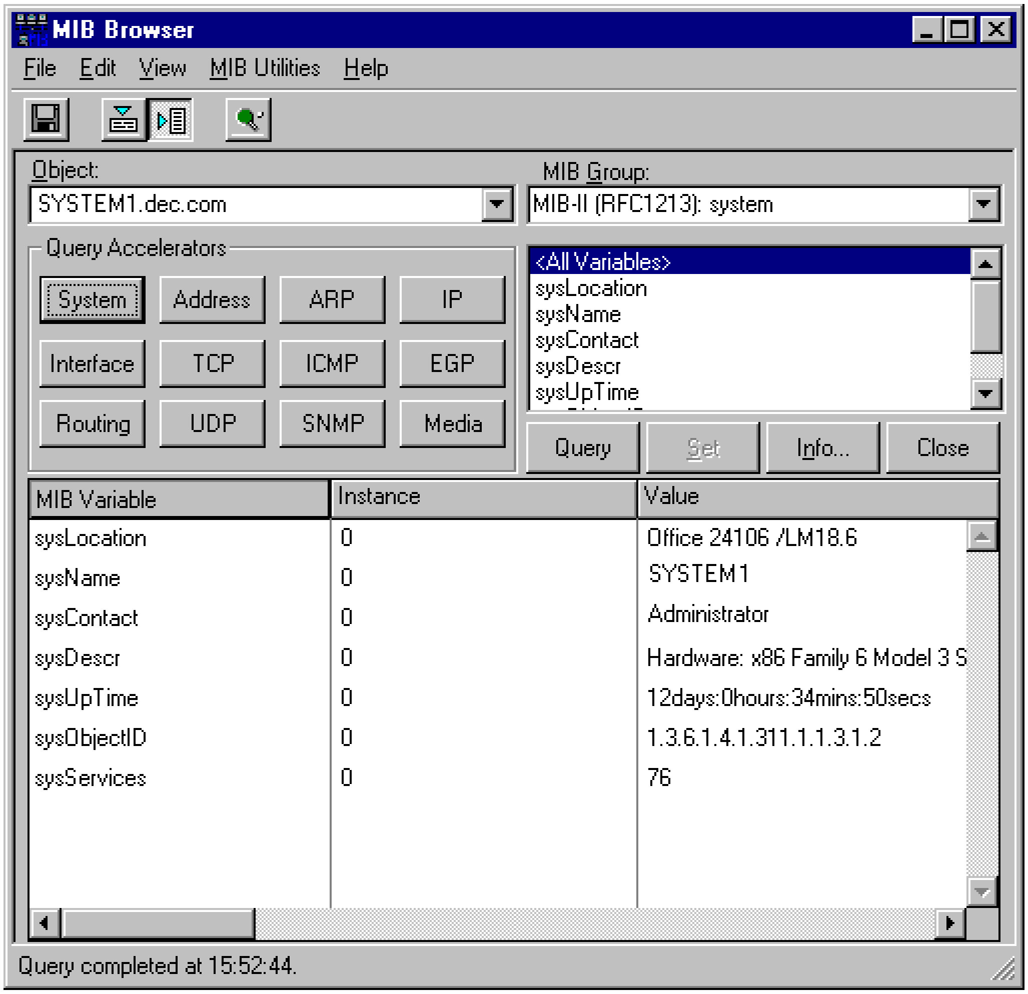
You can use the MIB Browser to modify variables. Some of the MIB variables are Read/Write. A Read/Write variable is one that you can modify because you can write or a new value, as well as read the value. For example, sysLocation is a Read/Write variable, which means that you can a enter new location whenever the system is moved. The change is made in the MIB. Other individuals using another network management system can also change Read/Write variables. You can see which variables are Read/Write using the MIB Enroller.

To change a variable value from MIB Browser

1. Select the variable. If the Set button is active when a variable is selected, you can change the value.

2. Edit the variable and choose OK.

Figure 6-3 MIB Browser Window



Object: SYSTEM1.dec.com

MIB Group: MIB-II (RFC1213): system

<All Variables>
sysLocation
sysName
sysContact
sysDescr
sysUpTime

MIB Variable	Instance	Value
sysLocation	0	Office 24106 /LM18.6
sysName	0	SYSTEM1
sysContact	0	Administrator
sysDescr	0	Hardware: x86 Family 6 Model 3 S
sysUpTime	0	12days:0hours:34mins:50secs
sysObjectID	0	1.3.6.1.4.1.311.1.1.3.1.2
sysServices	0	76

Query completed at 15:52:44.

To view a description of a variable

- Select the variable from the MIB group variable list and click the Info button.

To read a MIB

1. Select the object from a view.
2. Choose Tools→MIB Enroller→MIB Compiler.
3. In the MIB Compiler, choose File→Open.
4. Select the MIB and click OK. The MIB appears in the window.

Using the Query Button Accelerators

The query buttons on the MIB Browser correspond to MIB groups for the MIB II agent. When you click a query button you are performing an SNMP GET operation, on the group of variables.

If you use another MIB on an object, you can change a button to query a variable group from a different MIB.

To change a Query button

1. Choose Edit→Customize Query Accelerators.
2. Select the button you want to change.
3. In the Query Accelerator Label field, enter a label for the button.
4. In the Associated MIB Group, select a MIB group that is appropriate for the object types you monitor, for example, Compaq servers.
5. Click OK.
6. Click Close on the Customize Query Accelerator dialog box.

To see all variables in the Query group at once

- Choose All Variables in the MIB Group list and choose View→Vertical Output and scroll through the list.

To see all the instances of one variable

- Choose View→Horizontal. Select the variable. For example, if you are checking the number of interfaces, horizontal orientation will show all of them.

To sort the variable information alphabetically

- Choose View→Sort Output.

Viewing Cluster Information from the MIB Browser

The MIB Browser displays information about servers and resources that are part of a cluster, which may include the cluster types, vendor, software version, status, NT cluster group members and resources, IP addresses of cluster members, aliases for the cluster, system OID, and vendor and version. The information comes from the variables in the cluster MIBs.

To use the MIB Browser to view cluster data

1. Choose Actions→MIB Browser.
2. Select a MIB Group or variable in the group. The cluster MIBs have prefixes of SrvClu, SrvNTC, and ntcmtg.
3. Enter the cluster name or a cluster server name and press RETURN.

The MIF Browser

The Management Information Format (MIF) Browser is used in a similar fashion to the MIB Browser to examine the system-supplied MIFs. It is used on desktop and mobile systems and may also be used on systems running Windows NT or Windows 95. With the DMI service layer running on the system to be browsed, you can see an inventory of various system software, hardware, settings, and configurations. This information can be passed on to Microsoft System Management Server (SMS) through the MIF Maker program that is supplied with ClientWORKS.

The MIF Browser is available as an icon on the tool bar and from the menu. For complete details, refer to the *ClientWORKS Network Administrator's Guide* and the ClientWORKS online help.

The MIB Compiler

Before an object type can be used in ServerWORKS Manager Console, MIB groups associated with the object must be enrolled in the ServerWORKS database. The MIB Compiler is used to load new MIB group and MIB variable definitions into the database. Refer to section *"Creating Custom Object Types and Profiles"* in Chapter 7 for details about compiling and enrolling MIBs.

You can also read a compiled MIB in the MIB Compiler.

To read a MIB

1. Choose Actions→MIB Enroller.
2. Choose Compile→MIB Compiler.
3. Choose File→Open and select the MIB from the Choose MIB Input File dialog box.
4. Click OK.

The MIB Profiler

The MIB Profiler is used to associate MIBs with an object type. For example, a DIGITAL server object type has certain MIBs that have been defined to be associated with that object type.

If the MIBs associated with an object need to be modified, this is done using the MIB Profiler. The MIB profiler:

- Assigns MIB groups to an object type.
- Deletes (disassociates) MIB groups from an object type.

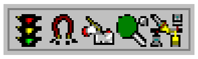
The MIB Profiler saves the MIB group assignments in the database so they can be referenced by the MIB Browser. For example, after a particular SNMP object is selected, the MIB Browser obtains the object type and uses this information to display all the associated MIB groups from the database. Only the applicable MIB groups are listed in the MIB Groups field of the MIB Browser window. Then either a group or one or more variables from that group can be chosen to perform GET and SET operations against the specified object.

Refer to Chapter 7, *“Getting the Data You Want”* to learn about using the MIB Profiler.

The MIB Enroller

The MIB Enroller is a source of MIB information. The MIB Enroller displays a group and its variables, the object identifier for the variable, data type, and read/write access. Knowledgeable administrators can modify a MIB variable from the Enroller.

Background Tasks



ServerWORKS Manager operates background tasks to collect and distribute network information. The background tasks appear on the system tray when they are running. Right-click on an icon to display a menu.

The Ping Server

ServerWORKS Manager Console has the capability to contact or “ping” devices on the network. The Ping server examines the network to see if a device is up, down, or not responding using an ICMP request and waiting for a reply. Select a device and ping it using the toolbar button. The ping server notes this activity and the time it takes for a round-trip from Console to device and back.

The Poller

The Poller periodically requests status information (up, down, or no response) from specified network objects and their interfaces. The objects that may be polled are all interfaces belonging to network objects that have an SNMP agent or that have IP support (for example, routers and end nodes).

By default, the Poller is automatically started after an IP discovery is done. Using the default settings, all objects that are listed in the database are polled at the same interval.

You can also poll on a user-defined group. A group can consist of a collection of similar objects that would be polled at the same intervals.

The Data Collector, Event Logger, and Event Dispatcher

The Data Collector, Event Dispatcher and Event Logger must be running for the Console to receive alarms.

The Event Dispatcher and Event Logger must be running to receive alarms notifications or to automatically run a script when an alarm threshold is reached.

If these three utilities are not placed in the Windows NT or Windows 95 Startup Group, the Event Dispatcher and Event Logger are automatically started when ServerWORKS Manager Console is started.

Check the system tray in the lower right corner of the window to see if the ServerWORKS tasks are running.

Getting the Data You Want 7

An IP Discovery with ServerWORKS presents volumes of information on all the network objects. ServerWORKS lets you manipulate data and customize views. This chapter explains how to customize ServerWORKS to perform the following tasks:

- Acquire data based on your network requirements
- Present the data the way you want

Customizable Options for a View or Map

You can customize list and map views to meet specific requirements. Several different viewers can be created to serve different purposes. For example, one view might contain all the servers in an organization, while another can display files and applications on multiple servers, and a third can display the TCP/IP topology. Any type of information can be grouped in a view, regardless of the source or content. ServerWORKS Explorer is a good starting point for customizing viewers because it is a source of objects to copy into other viewers.

Once you create a map or hierarchical view, you can modify it manually or run a subsequent discovery to update it.

To change the appearance and window behavior

1. Click on a map to select it.
2. Choose File→Viewer Properties.
3. Select your preferences for the following settings on the Map Viewer Properties dialog box:
   - Choose an optional background file. For example, select a country map and drag servers onto their geographic locations.
   - Chose a default scale for opening a map.
   - Click Configure. Then select defaults to minimize, close, or auto-save maps and to hide node bitmaps when the map scales below a specified percent.
   - On the Configure dialog box, click Colors. Then change the colors on map elements.

To get basic information quickly

- Double-click on a network object to display the associated browser. ServerWORKS Manager has associated servers and network objects with System Browser, MIB Browser, and the MIF Browser.

To create a logical network map

You may want to manage particular network objects on a map as a group because they have similar usage or for organizational purposes. You can isolate them easily. Simply drag the network objects from map to map.

To view vital statistics on a map

You can add a label to a network object to display specific information on the map. For example, you may want to see the IP address, name and netmask of an object.

1. From the Tools menu, choose Options→Object Display.
2. From the Hidden list, select the information you want to display in a label.
3. Click Show. If you want to put the labels in a specific order, select each label and choose Before or After until the labels are positioned.
4. Click Close.

To modify the menus for the work you do

You can edit the Tools menu to add or delete programs. For example, you can create a menu command that runs a batch file or starts an application

1. From the Tools menu, choose Options→Tools.
2. Do one of the following:
   - Click Add to add another application to the Tools list. Enter the tool name (for example, Notepad) and the Path (for example, c:\windows\notepad.exe) and click OK.
   - Select an application and click Remove to delete the application.
   - Select an application and click Change to modify the display name or path of the tool.
3. Click Close.

To manage network objects as a group

A group is a collection of server or SNMP objects on which you can perform SNMP operations. You can select a logical group of network objects and apply the same alarms and options to them. First, create the group.

1. From a map view, select the object(s) by doing one of the following:
   - Hold down the CTRL key and click on each object you want to add to the group.
   - Click and drag across the map to draw a selection rectangle around the objects you want to add to the group.
2. From the Tools menu, choose Group Management.
3. Do one of the following:
4. Click Add Group to create a new group containing the selected objects. Enter a group name, polling properties and the community name for SNMP Get and Set operations in the Group Properties group.
5. Select one of the existing groups. Copy its polling properties and community name into the new group and modify them as needed.
6. Select from Objects not in group and click Add to place them on the Objects in group list. To remove objects from the group, select them and click Remove.
7. Click OK.

Launching With Context

Individual vendors of SNMP-compliant objects may offer tools that are fine-tuned for viewing their own object's properties and information. For example, Compaq offers Insight Manager for viewing Compaq servers.

A better way to use these applications is to launch them from the Console *with context*. For example, when you launch Insight Manager with context, it opens with the data for a Compaq object that you have selected in ServerWORKS.

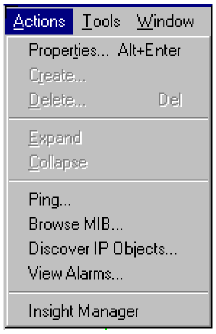
To set up an application to launch with context, you must perform the following steps:

- Configure the application to associate it with the object type.
- Specify the application as the default action for the object type.

In the following procedures, Insight Manager and the Server.Compaq object type are used as examples.

To configure the application

1. From the Console, choose Tools→Application Launch.
2. On the Configure Application Launch dialog box, select or enter the following information:
   - In the Object field, select the object type (for example Server.Compaq).
   - In the Menu Item Name field, enter the name for the menu option (for example, Insight Manager).
   - In the Application Path field, click on the browse button and search for the application. Be sure to use the full path and exact spacing (for example: "c:\Program Files\Compaq\Insight Manager\cim.exe").
   - In the Toolbar button field, choose any 16x16 pixel bitmap.



3. On the Application Command Line Setup group of the dialog box, enter the command that will launch the application. Always use exact spacing and match case sensitivity.
   To launch Insight Manager, use the following command line:

   ```
   cim.exe -ObjIPAddress=<Internet Address>
   ```

   You have the option of selecting statements for the command line. The Command Line Parameters selection list lets you choose from commonly used parameters, which are added to the Parameters and switches field. If your command line includes several commands, select Allow multiple objects and enter a delimiter type.

4. Choose Add to place the menu name on the Actions menu and add the bitmap as a toolbar button.
5. Choose Close.

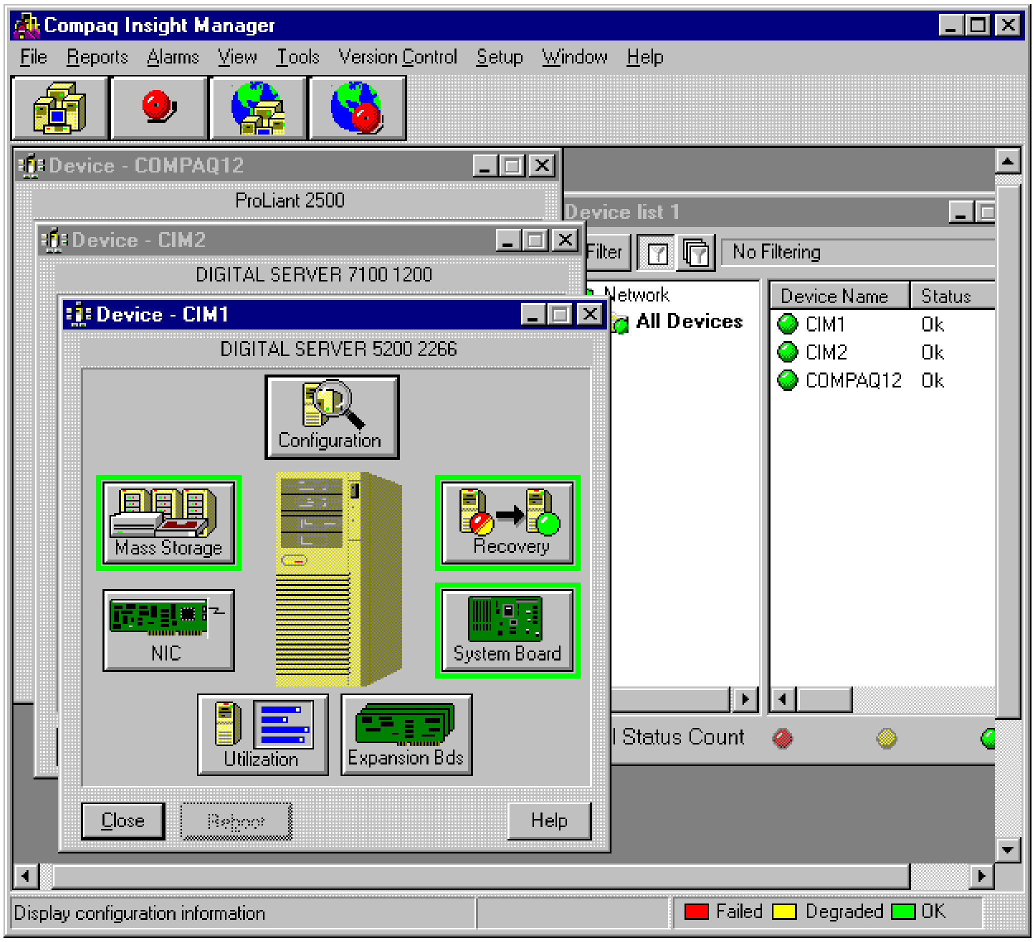
To specify the application as the default action

1. Choose Tools→Options.
2. On the Options dialog box, click on the Default Actions page.
3. From the object list, select the object type.
4. From the Action list, select the application, in this case, Insight Manager.
5. Choose Close.

To open the application with context

From a Discovery map or hierarchical view, double-click on a Compaq server. Figure 7-1 illustrates a Compaq server as seen through Insight Manager and launched from a ServerWORKS Discovery map.

Figure 7-1 Insight Manager launched from ServerWORKS Manager Console



Device Name	Status
CIM1	Ok
CIM2	Ok
COMPAQ12	Ok

Display configuration information

Discovering and Managing Printers

You can create maps or tree views of one type of object. For example, you may want to monitor printers, which are prone to maintenance problems. ServerWORKS recognizes the system object identifiers for DIGITAL, Hewlett-Packard, and Lexmark printers.

To create a map of printers

1. From the Console window, choose File→New Viewer and the map or hierarchical view.
2. Enter a map name in the New Viewer dialog box. An empty map opens with the Palette.
3. Choose Actions→Discover IP Objects.
4. Specify the network and netmask and choose Next.
5. Specify the community to discover.
6. On the Types to discover dialog box, select the printer types and choose Next.
7. On the Discovery Options dialog box, choose the view and click Finish.
8. Choose Yes or No to indicate whether you want to view the discovery report.
9. Choose Yes or No to add new objects to the current view.

Using Netmasks to Refine Discoveries

If you are knowledgeable about networks, IP addressing, and the use of netmasks, you can use other netmasks to limit a Discovery. In a Discovery the Console queries IP-addressed subnets for a list of its nodes. An IP address consists of four numerals, from 1 to 255, separated by decimals (dots). The address 16.151.24.36 is an example. The address corresponds to four octets in binary format. A netmask identifies which parts of an IP address specify the network and which specify the host portions. Discovery uses the combination of the IP address and the netmask to look for the nodes that are attached to the specified network.

The default netmask is 255.255.255.0 for a Discovery. For example, if you use the network address 16.151.24.0, using the netmask 255.255.255.0, the netmask masks the first three numerals of the address and attempts to discover all nodes in the host part, up to 254 nodes.

Use a single node netmask to limit a Discovery to a single network object (for example, one that you manually inserted). For the node with the address 16.151.24.36, use the exact node address with the netmask 255.255.255.254. This netmask finds up to two nodes—16.151.24.36 and 16.151.124.37, the consecutively addressed node—due to the interpretation of the address by Discovery.

Using Collections and Domains for Status Checks

In a Discovery, ServerWORKS finds hosts and cluster domains. ServerWORKS displays host domains and clusters so you can drill down to see the nodes or cluster members. You can apply the same concept if you want and assemble multiple objects into a subset called a collection.

Note: A collection or a domain is not an SNMP group, although objects in either a collection or a domain can also be found in an SNMP group. A domain in a view has no relationship with a Windows NT domain.

To create a collection

1. Choose Edit→Insert.
2. Click Collection and enter a name for the collection.
3. Open a list view and drag objects from the view into the collection.

To create a domain

1. Choose Edit→Insert.
2. Click Domain from the Insert dialog box.
3. Enter a display name and choose the object type in the domain. For example, to create a cluster domain, choose Cluster.
4. Open a view and drag the objects into the domain. For a cluster, include the members and resources of the cluster.

To view the contents of a collection or host domain

- Double-click on the domain icon. The contents open in a separate, temporary, tiled map.

Polling Effectively

Polling consumes network resources if the polling frequency is too high or the object base being polled is too broad. Customizing the poller lets you focus on as few or as many objects as you want by polling the objects as a group. The default is to poll all discovered and inserted objects.

To poll by groups, perform the following tasks:

- Set up a polling group. You can start with either of two groups named Critical and Non-Critical that are established by ServerWORKS or you can create your own group. Each group has its own timeout period, number of retries, and polling interval. Each group belongs to a community for authentication.
- Fine-tune the polling parameters.

Creating a Polling Group

1. Choose Tools→Group Management.
2. On the SNMP Group Management dialog box, choose Add Group.
3. On the Add Polling Group dialog box
   - In the Group Name field, enter a new name.
   - In the Group Properties field, enter a Retry, Timeout, and Interval. The Timeout and Interval are measured in seconds. As an example, the Critical group interval is 60 seconds (one minute) and the Non-Critical is 300 seconds (five minutes).
   - Enter the community name or use Public.
   - Choose OK.
4. On the SNMP Group Management dialog box, select the new group from the Group Name list.
   - The Group Properties were specified when you created the group. To change a property, select it and enter a new value.
   - Use Public as the Set Community and Get Community unless you have created other community names.
   - On the Objects not in Group list, use CTRL+Click to select group members. Then click Add.
5. When all members are selected, click OK.

Setting Group Polling Parameters

Stop the poller to reset a group's parameters or to enable polling of a new group. Stop the Poller after you open the Poller window.

To open the Poller

- Click on the Poller taskbar button or choose Tools→Poller.

To stop polling

- On the Poller window, click Stop Polling.

To enable a group and set group parameters

1. On the Poller window in the Enable column, click on the box in the group row. A check appears in the box and the background color changes to green. (The polling frequency parameters were set when you created or modified the group).
2. Choose Options→Set Polling Parameters. Set values for the following items:
   - Maximum interfaces to poll outstanding: Enter the number of interfaces the poller can queue for polling at any one time.
   - Maximum number of events: The number of SNMP Get and Set operations, pings, Event Logger messages, and status alarms that can be sent per second.
3. Choose OK.
4. On the Poller window, choose Options→Poller Output. (If the Poller is off, no output appears in the field). Choose the Options button and click on the types of information you want from the polling. Click OK to close the Poller Output dialog box.
5. On the Poller window, click Start Polling to poll the selected groups.

Viewing Polled Information

You can view small segments of polled information from the opened Poller Output dialog box (as described in the previous section).Use the poller log to view polling activity over time and print the poller.log file.

To use the poller.log file

- From Windows Explorer or My Computer, double-click on the poller log, found at

```
\Program Files\Digital\SWMgr\Database\poller.log
```

Changing Variables from Object Properties

Properties combines several activities in one dialog box. Properties gives you a quick glance at the object and lets you modify the object, which is an SNMP Set operation on the object.

Use Properties to view details:

- Object name, IP address, MAC address, and object type. If you know either the name or the IP address, ServerWORKS finds the other. Click Get Addr to find the IP address or click Get Name to find the device name.
- The contact person responsible for the object and comments (for example, the location) in the description of the object.
- The trap destination if one is configured.
- Groups to which the object belongs.
- Third-party applications associated with the object (for example, RSM or StorageWorks Command Console).

Use Properties to modify the network configuration:

- Change the global name that is used for name resolution
- Modify the polling information or polling protocol
- Change the object type

To view and modify the properties

1. Click an object on a map or list view.
2. From the menu, choose Actions→Properties.
3. Modify editable fields.
4. Click OK to close the Properties dialog box.

Working with the ServerWORKS Manager Database

The ServerWORKS Manager database is PCMGR.mdb. It is a Microsoft Access 97 database that you can view in Access. The database is installed in the subdirectory named `database` of the ServerWORKS Manager Console kit. If you chose the default directory at installation the location is:

/Program Files/DIGITAL/SWMgr/database/PCMGR.mdb

The database contains all the information about objects discovered on your network, alarm and alarm configuration information, and event data.

If you are familiar with Access and database structure, you can modify records in the database to create query reports, use scripts, or perform specialized SNMP operations. Information in the tables may be easier to view in the database table records than in the actual MIB files.

The following list describes the most commonly accessed database tables:

Table 7-1 Access Database Table Records

This Table	Contains records about
APPL_GR	All integrated third-party applications. A record exists for each integrated application.
EVT_LOG	The alarm log table. All alarms and events, object IDs, and messages associated with each event are stored here.
MIB_CLAS	MIB class name and the group the MIB belongs to, for all MIBs compiled in the database.
MIB_DESC	A description of each MIB variable.
MIB_NAME	Names of the MIB groups.
MIB_PROF	Object type and subtype profile for each MIB.
MIB_TABL	The internal MIB variable ID for all MIB groups that are compiled in ServerWORKS. The ID is useful for joining this table with other tables.
OBJ_DEF	Actual name and the polling interval of each machine.
OBJ_IP	Global name information (including the IP address, alternate address or subnet, and netmask) of each machine.
OBJ_SNMP	SNMP community names.
TRAP_ENT	Trap definitions and enterprise OID for all MIBs compiled in the database.

Note: The ServerWORKS V4.0 database is an Access 97 database. If you are running Access 95, you can continue to use the database from ServerWORKS V3.x. However, if you plan to use scripts to create Access reports or to modify the database, you must use Access 97 and follow Microsoft directions for converting the database to Access 97 format. Databases from V2.x must be converted after installing ServerWORKS Manager V3.2 and then using Access 97 to convert it to ServerWORKS Manager V4.0 format.

The following table lists the prefixes used to name the database tables.

Table 7-2 Database Table Prefixes

Prefix	Table Information
ALM	Alarm configuration
APPL	Third-party application integration
AUTO	Auto-discovery information
COL	Data Collector information
DB	ServerWORKS database information
EVT	Event log data
GR	Group information
LOG	Event log data
LTBL	Reserved for future use
MIB	MIB II variable information
NMDB	Maximum counters for database fields
NOTF	Notification information
OBJ	Object type information that ServerWORKS uses
POD	Reserved for future use
SUBT	Object subtype information
SYS	Mapping of SYSOID and subtype information for MIB II variables
TRAP	Trap information
TYPE	Object type information
USR	User information
VIEW	Map and hierarchical view information
VWER	Internal viewer information

Using the DB Utility

The DB Utility accomplishes several database maintenance tasks. You use the DB Utility in the following situations:

- If you suspect the database or some portion of it (for example, a table) is corrupted.
- If you want to erase a table and start over. For example, you want to change the levels on all threshold alarms. (The cleanup erases everything in the selected table, so be certain you want to recreate the information in ServerWORKS Manager).
- If you want to modify the alarm log table. For example, you set a "false" alarm that sent numerous messages for a non-alarm condition and you want to clear the log of excess entries. You can also change the size of the log table (the number of lines).

Shut down ServerWORKS Manager Console, including the background tasks, before you start the DB Utility.

To open the DB Utility

1. From the Start menu, choose Programs→ServerWORKS Manager Console→ServerWORKS DB Utility.
2. Do one of the following:
   - In the Database Table to Clean Up group, select one table and click Initialize.
   - In the Alarm Log Table, enter the maximum lines you want in the table (up to 10,000, but note that 10,000 log entries consume disk space and memory).
3. Choose File→Exit.

Creating Custom Object Types and Profiles

ServerWORKS Manager lets you create custom object types and assign MIB groups of variables for non-DIGITAL servers to extend ServerWORKS management to include objects that are not in the default set or to include new objects types that might be added to your network in the future.

To create the object type and assign the variables, you must complete the following tasks. Each of these tasks is composed of several smaller steps. When you have completed the tasks, you can manually add the object to your network map and begin managing it immediately.

- Define the object type so ServerWORKS recognizes objects on your network that match the description
- Enroll the MIB groups
- Assign the MIB groups that focus on information you want about the object type

Use the following procedure as a guide to creating an object type and profile for any network element. This example creates an object type for the Compaq ProLiant 2500 Server, assigns MIB groups, and explains how to add the object type to your network map manually and through Discovery.

Defining the New Object Type

From the ServerWORKS Tools menu, choose Tools→Object Types and click the Add button. The Add SNMP Object Types dialog box opens. This is where you enter the object definition. (See Figure 7-2.)

1. In the Add SNMP dialog box, enter or select:
   - The object type name, for example, Server
   - The object subtype name, for example, Compaq
   - Bitmaps to represent the object icons (see Figure 7-2)
   - The icon's background shape (for example, endnode)
2. Click Apply.

3. Click Close. A message prompts you to exit from ServerWORKS Manager.

4. Choose File→Exit.

About Naming Objects

You can name an object anything you want. For example, if you plan to view the network by organization, you might have object types named Server.Finance or Node.Sales1, Node.Sales2.

About Selecting Bitmaps

You can create your own bitmaps or you can select them from the ServerWORKS bitmaps collection and modify them slightly to represent a new object.

You can find the ServerWORKS bitmaps at:

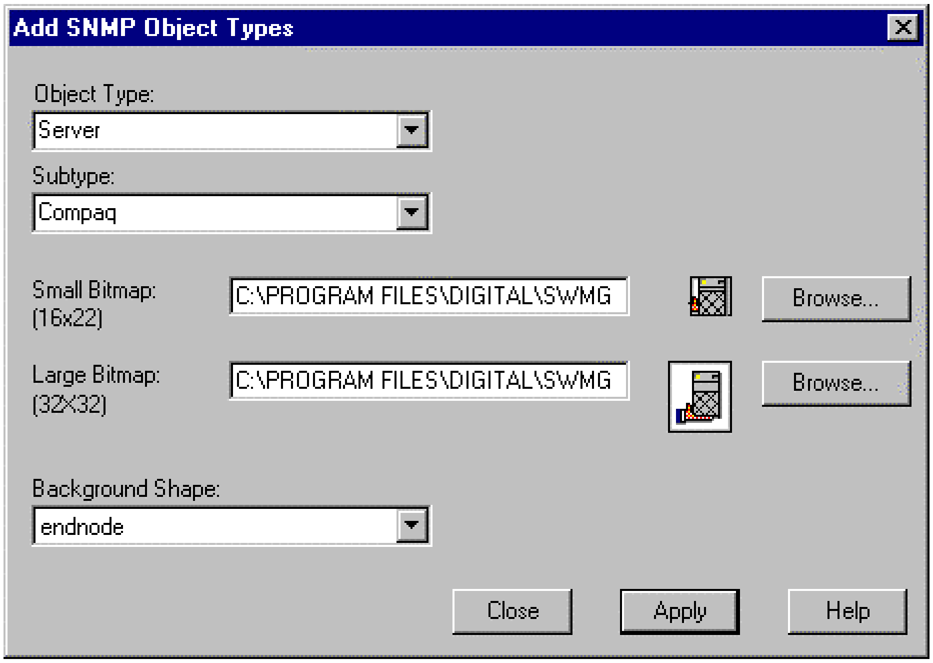
```
<ServerWORKS directory>:\database\bitmaps
```

A color change is a simple change that is accomplished easily using a tool such as Paint. The sample bitmaps `serverg.bmp` and `server32.bmp` provide a good starting point for modifying bitmaps because they are the correct size. Modify and rename the bitmaps in Paint. For example, for a Compaq object, use serverc16.bmp and serverc32.bmp and store them with the ServerWORKS bitmaps.

About the Background Shape

Each network element that appears in the object list (server, node, bridge, and so on) has a default shape for the icon. Use the default.

Figure 7-2 Entries in the Add SNMP Object Types Dialog Box Define an Object Type



Add SNMP Object Types

Object Type: Server

Subtype: Compaq

Small Bitmap: (16x22) C:\PROGRAM FILES\DIGITAL\SWMG

Large Bitmap: (32X32) C:\PROGRAM FILES\DIGITAL\SWMG

Background Shape: endnode

Enrolling MIBs in the ServerWORKS Database

Before an object type can be used in ServerWORKS Manager Console, MIB groups associated with the object must be enrolled in the ServerWORKS database. ServerWORKS Manager has already enrolled hundreds of MIB groups that are ready for assignment to new object types. For example, if the object type Node.Finance is a DIGITAL server, you can assign DIGITAL MIBs already enrolled for the “Server.Digital” object type. (For the convenience of Compaq server administrators, the Compaq MIB variables are already enrolled in the ServerWORKS database.)

However, if you are creating an object type with MIBs you have acquired from a vendor, a Web site, or a bulletin board service, you must enroll (compile) them into the ServerWORKS database first.

1. From the ServerWORKS menu, choose Tools→MIB Enroller. The SNMP MIB Enroller dialog box opens.
2. From the Compile menu, choose MIB Compiler.
3. Choose File→Open to browse for the MIB on your system.
4. Select the MIB. The MIB text appears in the MIB edit box.
5. Click the Enroll button. Enter a name for the MIB and choose OK.
6. Choose OK again at the prompt "Do you want to store this MIB in the permanent database?"

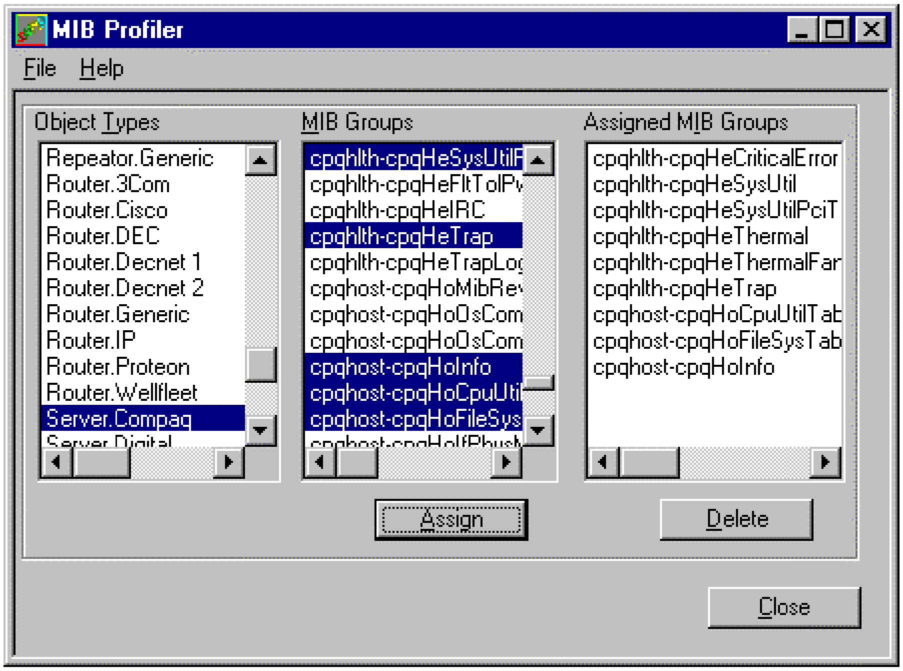
About MIB Group Variables and Their Purpose

How do you know which MIB group to choose? Each group variable is explained for you. To learn more about a group's variables, choose the group from the MIB groups list. Select a MIB variable and click on the MIB Info button to display an explanation of the variable. You can also add to the definition and save your comments.

Assigning MIB Groups to the Object Type

1. From the ServerWORKS menu, choose Actions→Browse MIB→MIB Utilities.
2. From the MIB Browser menu, choose MIB Utilities→MIB Profiler.
3. Select the new object name from the Object Types list, as illustrated in Figure 7-3.
4. Scroll through the MIB Groups list and select the groups of variables to assign to the object type. In this case, Compaq MIBs are identified with the cpq prefix.
5. Choose Assign to add the groups to the Assigned MIB Groups list.
6. Click Close.

Figure 7-3 MIB Groups are Assigned to the New Object Type



Object Types
- Repeator.Generic
- Router.3Com
- Router.Cisco
- Router.DEC
- Router.Decnet 1
- Router.Decnet 2
- Router.Generic
- Router.IP
- Router.Proteon
- Router.Wellfleet
- Server.Compaq
- Server.Digital

MIB Groups
- cpqhlth-cpqHeSysUtilP
- cpqhlth-cpqHeFltTolPv
- cpqhlth-cpqHeIRC
- cpqhlth-cpqHeTrap
- cpqhlth-cpqHeTrapLog
- cpqhost-cpqHoMibRev
- cpqhost-cpqHoOsCom
- cpqhost-cpqHoOsCom
- cpqhost-cpqHoInfo
- cpqhost-cpqHoCpuUti
- cpqhost-cpqHoFileSys
- cpqhost-cpqHoIfPhysM

Assigned MIB Groups
- cpqhlth-cpqHeCriticalError
- cpqhlth-cpqHeSysUtil
- cpqhlth-cpqHeSysUtilPciT
- cpqhlth-cpqHeThermal
- cpqhlth-cpqHeThermalFar
- cpqhlth-cpqHeTrap
- cpqhost-cpqHoCpuUtilTab
- cpqhost-cpqHoFileSysTab
- cpqhost-cpqHoInfo

Quick Scrolling Through ServerWORKS Manager Lists

MIB groups and variables number in the hundreds. To reduce the searching time, click anywhere on the list and then type the first letter or two of a group name to move to the section of the list that contains the variables. For example, type *s* in the Object Types list to display the server objects, type `cp` in the MIB Groups list to find the Compaq groups.

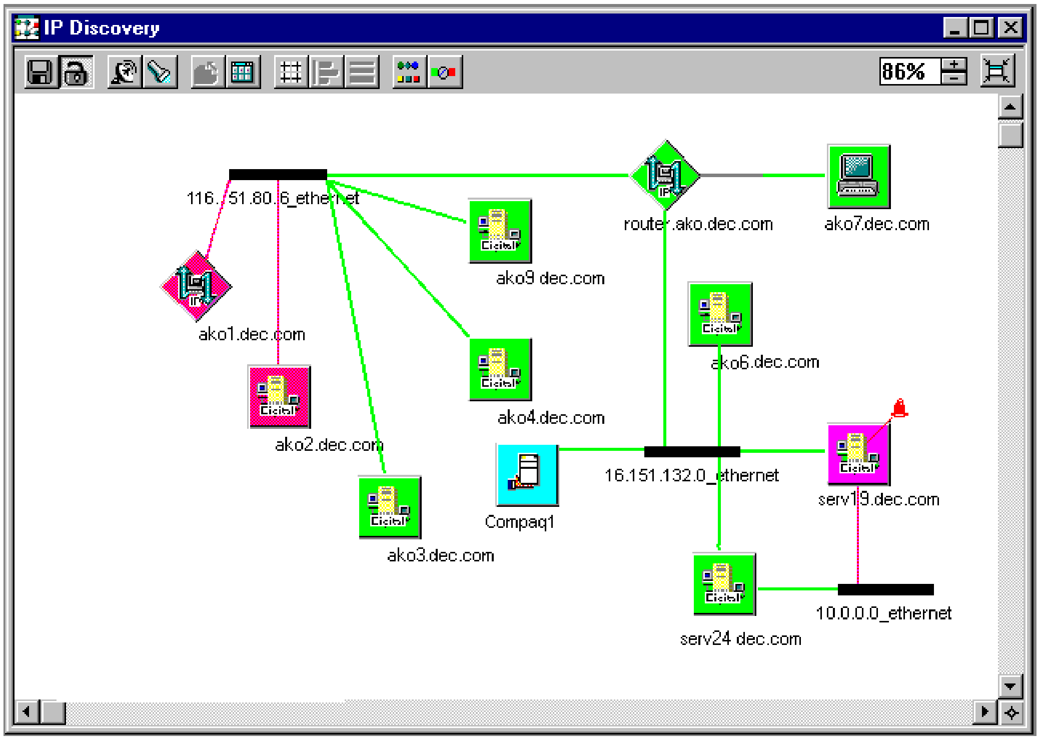
Manually Adding the Object to the Network Map

1. Adding a network element manually is the fastest and least complex way to begin managing the objects.
2. From the ServerWORKS Manager menu, choose File→New Viewer to create a new map or choose File→Open Viewer to open an existing map where you will add objects of the new object type—in this case, the Server.Compaq type.
3. Choose Edit→Insert and select the object type (Server) from the Insert dialog box list.
4. In the Insert: Server dialog box, enter a display name, for example Compaq1. This name is also the default IP Name. You can change the IP name. Choose a network object type from the Type list. For this example, it is Server.Compaq.
5. Click on Get Addr to display the IP Address.
6. Click OK. An auto-discovery is started to insert the new object into the view you selected.

Checking for the Object

From the map, double-click on the object to open the MIB Browser. The new object is identified with the Compaq name as part of the system descriptor. After you run IP Discovery, view the Discovery Report to see the list of new Compaq objects. Figure 7-4 shows the map view of a network with the new object type.

Figure 7-4 A New Object Type Discovered in Map and Hierarchical Views



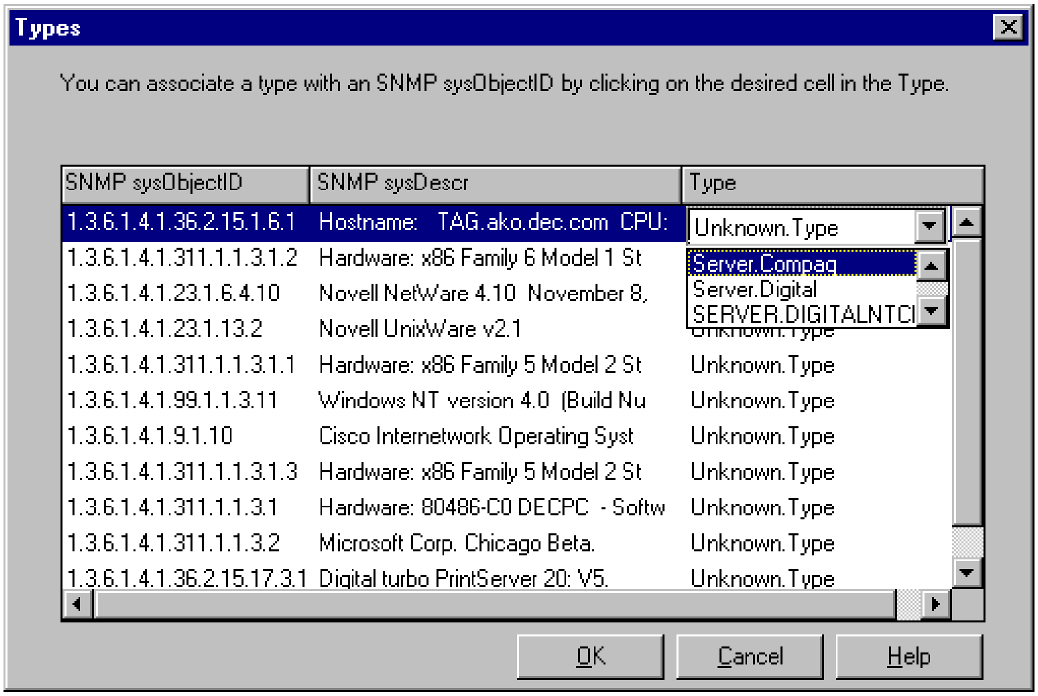
Associating Unknown Objects with Known Object Types

When SNMP is running, Discovery might also find objects that are not associated with a known object type. These objects are named Unknown.Type. The SNMP sysObjectID for the object is not mapped to an existing object type so the appropriate MIBs are not applied to the object.

To create the association, you must map the unknown object type to an existing network object. You can perform the mapping when you run a new Discovery.

1. From the ServerWORKS Manager window, choose Actions→Discover IP Objects.
2. On the Networks to discover dialog box, select the network and netmask. Then click Next.
3. On the Types to discover dialog box, click the Types button.
4. On the Types dialog box, you can view the list of Unknown.Type objects.
5. Select an object to associate with a type. You can identify the object by the sysObjectID or the SNMP sysDescr. (Double-click on the object in a map to open the MIB Browser and find the information.)
6. Click on the Unknown.Type label in the object’s row. A drop-down list appears with the list of existing object types. Select the object type. Because you defined the new object Server.Compaq, the name appears on the list.
7. Click OK. From the Types to discover dialog box, click Next
8. On the Discovery Options dialog box, select the view or map to hold the discovery and click Finish.

Figure 7-5 Types Dialog Box for Associating Unknown Objects with Existing Objects



You can associate a type with an SNMP sysObjectID by clicking on the desired cell in the Type.

SNMP sysObjectID	SNMP sysDescr	Type
1.3.6.1.4.1.36.2.15.1.6.1	Hostname: TAG.ako.dec.com CPU:	Unknown.Type
1.3.6.1.4.1.311.1.1.3.1.2	Hardware: x86 Family 6 Model 1 St	
1.3.6.1.4.1.23.1.6.4.10	Novell NetWare 4.10 November 8,	
1.3.6.1.4.1.23.1.13.2	Novell UnixWare v2.1	Unknown.Type
1.3.6.1.4.1.311.1.1.3.1.1	Hardware: x86 Family 5 Model 2 St	Unknown.Type
1.3.6.1.4.1.99.1.1.3.11	Windows NT version 4.0 (Build Nu	Unknown.Type
1.3.6.1.4.1.9.1.10	Cisco Internetwork Operating Syst	Unknown.Type
1.3.6.1.4.1.311.1.1.3.1.3	Hardware: x86 Family 5 Model 2 St	Unknown.Type
1.3.6.1.4.1.311.1.1.3.1	Hardware: 80486-C0 DECPC - Softw	Unknown.Type
1.3.6.1.4.1.311.1.1.3.2	Microsoft Corp. Chicago Beta.	Unknown.Type
1.3.6.1.4.1.36.2.15.17.3.1	Digital turbo PrintServer 20: V5.	Unknown.Type

When the Discovery is complete, the unknown object appears on the map as the new Server.Compaq object. Double-click on the object to view details in the MIB Browser.

Editing the Registry to Recognize the New Object

Manual insertion is a quick way to insert one or two objects, but if you are adding multiple objects of a type, you might prefer to use IP Discovery. On NT systems, IP Discovery uses a key in the NT Registry to identify objects. You can change the key to reflect a unique characteristic of the object for a particular map view (for example, a hardware-specific identifier or an organizational identifier).

1. Open the Registry editor regedit.exe. (Using Start→Find→Files or Folders is one way to locate the file.)
2. In the Registry, find the entry

```
HKEY_LOCAL_MACHINE\
       HARDWARE\
              DESCRIPTION\
                     System\
                            CentralProcessor\
```

3. Double-click on the Identifier value and prepend the string with Compaq, as follows:

   ```
   REG_SZ: Compaq - x86 Family 6 Model 1 Stepping 7
   ```

   In this example the expression “Compaq” uniquely identifies the server object type.
4. Click OK and exit from the Registry.

Editing the Registry with a Batch File

Creating a new object type temporarily changes the Registry. Because the change is not permanent, you can write a batch file to make this change each time you reboot. Use the Windows NT Resource Kit regcgh.exe to get the key value for the Registry.

The following is an example of a batch file you can use as a guideline:

```
if "%1"=="" goto error
set tmpfile=C:\temp.reg
echo REGEDIT4>%tmpfile%
echo.>>%tmpfile%
echo [HKEY_LOCAL_MACHINE
   \HARDWARE
         \DESCRIPTIONS
            \System
                  \CentralProcessor
                        \0]>>%tmpfile%
echo "Identifier"="Compaq Server">>%tmpfile%
call regedit %tmpfile%
del %tmpfile%
goto exit
echo Set of Compaq MIB II System Descriptor failed
:error
pause
:exit
```

Configuring SNMP and Trap Destinations

In order to receive SNMP traps from managed devices at the Console you must set up SNMP service on the managed device and specify a destination address. You may have configured SNMP when you installed ServerWORKS or an agent on a managed device.

SNMP Security

You can maintain security when you use SNMP as follows:

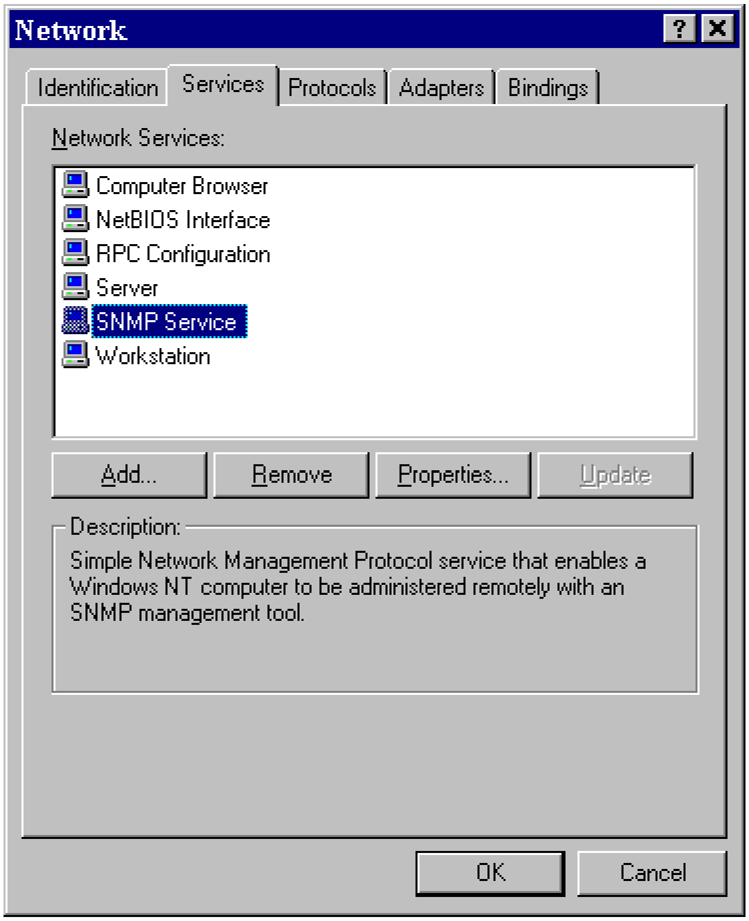
- Specify GET and SET community names for authentication when you set up SNMP service on the managed device. The community name on the managed device must be the same as the community name on the Console for authentication.
- A community name that is associated with a trap destination is used as a filtering device for sending traps only to selected destinations. It does not authenticate. Because ServerWORKS has the capability to view the community names of the trap destinations, use a different community name than the GET and SET community names.
- On operating systems that support access control, specify different GET and SET community names to restrict read and write access to managed devices.
- Lock your Console workstation when you are not present.

Configuring SNMP and the Trap Destination on Windows NT 4.0

You can configure SNMP on managed devices from the Control Panel of the managed device. Install and configure the SNMP agent on the Windows NT 4.0 server with the IP address or name of the client that will receive the traps.

1. Using the Windows NT Control Panel, select the Network item.
2. Select the Services tab of the Network property page.
3. Select the SNMP Service item from the list of services as shown in the next figure. (If the service does not appear on the list, load the SNMP service from the operating system installation disks. Refer to the operating system documentation.)
4. Click the Properties button.
5. Select the Traps tab.
6. Select the community name that you want to modify, or enter a new community name and click the Add button. (Public is the Windows NT default community name).

Figure 7-6 Selecting SNMP Agent from the Network Services Page



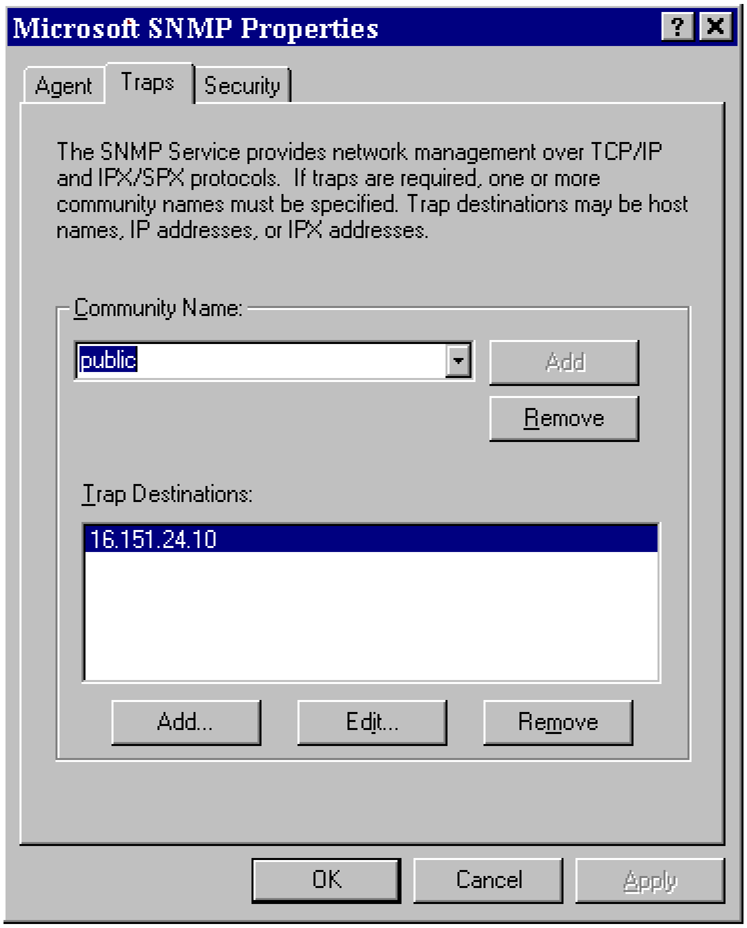
Network Services:

- Computer Browser
- NetBIOS Interface
- RPC Configuration
- Server
- SNMP Service
- Workstation

Description:

Simple Network Management Protocol service that enables a Windows NT computer to be administered remotely with an SNMP management tool.

Figure 7-7 Trap Destination Specified on the Traps Property Page



The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses, or IPX addresses.

Community Name: public

Trap Destinations: 16.151.24.10

7. Click the Add button under the Trap Destinations list box. The trap destination represents a node running an application (such as ServerWORKS Manager) that is listening for traps on a port specified in the /Windows/Services file (typically port 162).

8. Enter the unique IP or IPX address of the host that will receive traps for this community. Do not use a subnet address.

9. Click the Add button on the Service Configuration dialog.
10. According to Microsoft recommendations, reinstall the latest Service Pack.

Check that the SNMP service is running. Use Control Panel→Services on Windows NT or Control Panel→Network→Services on Windows 95. Do not start the SNMP Trap service on the management console.

Refer to Appendix B for details about configuring SNMP and setting a trap destination for Windows 95.

Configuring SNMP on Windows 95

Install and configure the SNMP agent on the Windows 95 node with the IP address or name of the client that will receive the traps.

Installing SNMP Software

1. From the Control Panel, click the Network icon.
2. Click the Add button on the Network option.
3. In the Select Network Component Type dialog box, double-click on Service.
4. In the Select Network Service dialog box, click the Have Disk button.
5. In the Install From Disk dialog box, type the path to the ADMIN\NETTOOLS\SNMP directory on the Windows 95 compact disc, and then click OK.
6. In the Select Network Service dialog box, click Microsoft SNMP Agent in the Models list and click OK. If you are prompted to specify the location of additional files, specify a path to the files on the CD-ROM or shared network drive.
7. Restart the computer.

Configuring the Trap Destination on Windows 95

You can also configure the trap destination on Windows 95 with the System Policy Editor. The Policy Editor is not a standard installed component for Windows 95.

1. From the Start menu, choose Control Panel.
2. Choose Add/Remove Programs and click on the Windows Setup tab.
3. Click on Have Disk and specify the path \ADMIN\APPTOOLS\POLEDIT. Click OK.
4. Select System Policy Editor from the Component list box and click Install and exit from the Add/Remove Programs tool.
5. From the Start menu, click Run and enter the command

   ```
   poledit
   ```

6. Choose OK to start the program.
7. In the System Policy Editor, choose File→Open Registry.
8. Double-click on Local Computer.
9. On the Local Computer Properties dialog box, double-click on the Network icon.
10. Double-click on SNMP to display the properties for the SNMP agent. Then set the community, permitted managers, (the IP or IPX addresses that are allowed to get information from an SNMP agent), and trap destinations for the Public Community (the IP or IPX address of hosts in the Public community to which you want SNMP to send traps).

Note: To send traps to a community other than Public, you must edit the Registry directly. That procedure is explained in detail in your Microsoft Windows 95 documentation and is beyond the scope of this manual.

Configuring the Trap Destination from the Console

You are reminded to set a trap destination when you set an alarm on a managed device. You can specify the destination from the Console using the Trap Control Remote Destination tool if you have not already specified a trap destination on the remote system.

You can have one or more trap destinations on the managed device, but the trap destination must be a system on which ServerWORKS Manager Console or an enterprise network manager is installed.

You must know the GET and SET Community names of the remote machine if you do not accept the default Communities. The GET and SET Community names provide authentication.

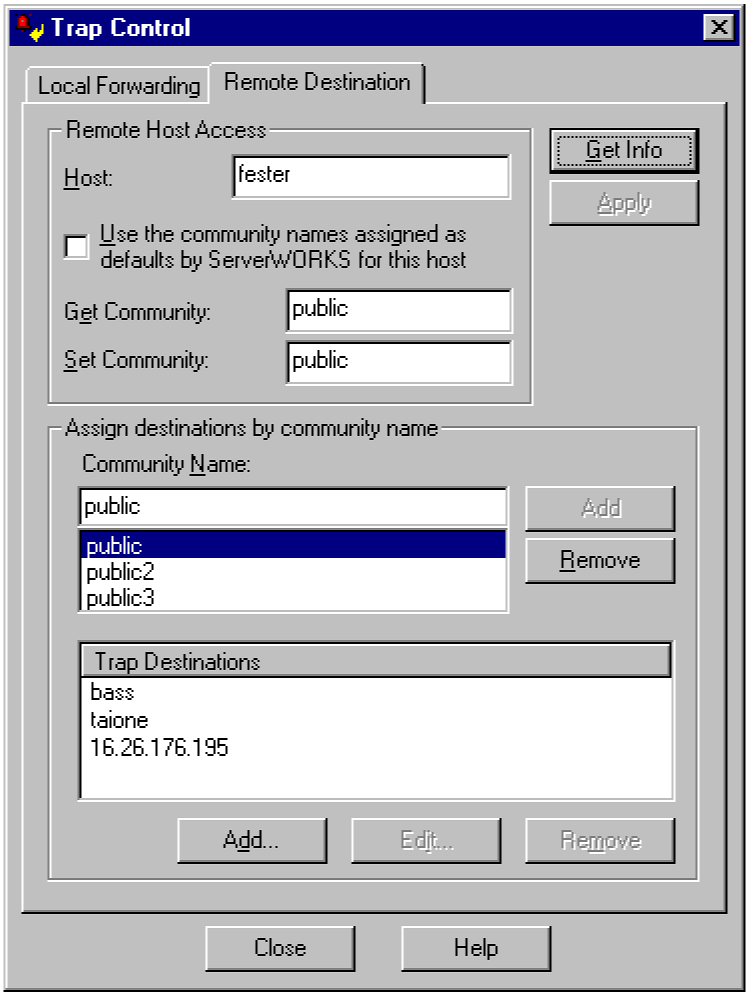
To configure the trap on a managed device

1. Choose Tools→Trap Control from the Console or from Alarm Configuration.
2. Click the Remote Destination tab.
3. Enter the Host name (managed device name). See Figure 7-8.
4. Choose one of the following:
   - Accept the default community (for example, Public for Windows NT)
   - Deselect the default option and enter Get Community and Set Community names.
5. Click Get Info to display the current community name and trap destination information for the host.
6. Specify the assigned destinations by community name. These destination is included in the trap message and are sent only to the destinations in the current community.
7. To add a new community name, enter the name in the community name box and click add.

8. To modify the list, select a community name and a destination. Then click Add, Edit, or Remove. On the Add or Edit dialog box, enter the IP address of the destination and click OK.

9. Click Apply to enable the changes and Close to discard the changes.

Figure 7-8 Trap Control Dialog Box: Remote Destination



Host: fester

□ Use the community names assigned as defaults by ServerWORKS for this host

Get Community: public

Set Community: public

Community Name: public

public
public2
public3

Trap Destinations
bass
taione
16.26.176.195

Forwarding Traps

The ServerWORKS Manager Console that receives traps can in turn *forward* those traps to other systems. This allows workgroup-level managers to run ServerWORKS Manager, while enterprise-level managers run manager programs such as HP OpenView or Tivoli TME 10. Forwarded traps are redirected by the ServerWORKS Event Dispatcher and Event Logger, not by the agent.

To forward traps from the Console, define the forwarding destinations using the Console Trap Control utility.

Trap forwarding takes place only when the Event Dispatcher and Event Logger are running and only if no other application has opened trap port 162. By default, no forwarding takes place. Agent-based traps are always forwarded to the management console. Alarms can be forwarded as traps if you specify this in the Trap Control utility.

Specify a unique address and a port for each destination. If a port number is not specified, then port 162 is assumed to avoid problems with systems that have multiple SNMP trap listeners on them. All traps will be forwarded to each destination you define. ServerWORKS allows up to ten forwarding destination addresses.

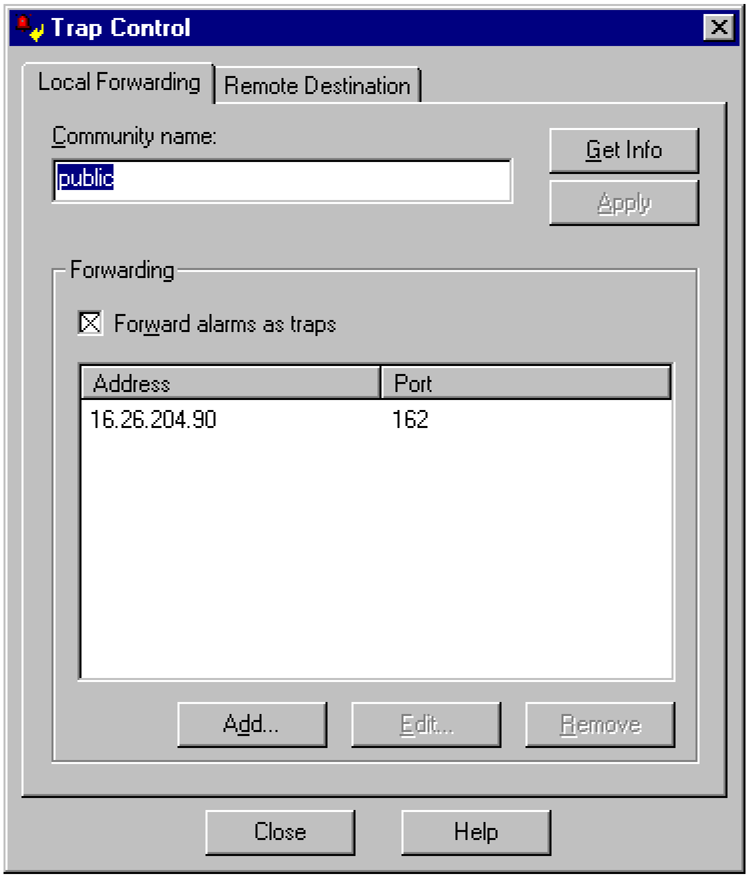
To specify a trap forwarding destination

1. From the Console menu, choose Tools→Trap Control.
2. Click the Local Forwarding tab and perform the following tasks:
   - Enter the community name, if necessary. Public is the NT default community. You can change the community name, but the name you use applies to all forwarding destinations in the list.
   - Select Forward alarms as traps.
   - Click Get Info to see a list of the forwarding addresses for the selected community.
3. To add a forwarding address, click Add. On the Add dialog box, enter the Address and Port number. For example, to forward all traps received at a management console to the IP address of 16.20.204.90, complete the dialog box as shown in Figure 7-9. Then click OK.

- You can also delete or modify a forwarding address. To delete, select an address and click Remove. To modify, select an address and click Edit. Then change the Address and Port information on the Edit dialog box.

4. Click Apply to enable the changes and Close to close the dialog box.

Figure 7-9 Trap Control Dialog Box: Local Forwarding



Community name: public

☒ Forward alarms as traps

Address	Port
16.26.204.90	162

Using NT Event Viewer to Track Alarms

You can send alarms to the Windows NT Event Viewer by modifying the ServerWORKS initialization file.

To use Event Viewer as an alarm viewer

1. From the Start menu, choose Find→Files and Computers.
2. Enter swgmr.ini in the Name field and click Find.
3. When the search is complete, double-click on swgmr.ini.
4. Search the file for the parameter section [Setup].
5. Change the following parameter value

   ```
   WriteTrapMsgToNTEventLog=1
   ```
6. Close the swgmr.ini file.

Managing Windows NT and NetWare Networks 8

You can manage a Windows NT network or a Novell NetWare network using ServerWORKS Manager.

Using the NT Server Management component from the Console, you can perform most NT administrative tasks including setting up new accounts, domains, and groups, managing printer queues and shared directories, and managing trust relationships.

The NetWare administrative tools are available to use from the Console for networks with NetWare servers.

NT Server Management Discovery

NT Server Management Discovery lists the Microsoft Network objects (those running LAN Manager V3.0 protocol). This category includes all DIGITAL servers on a LAN running the Windows NT operating system. This category can also include non-DIGITAL servers whose MIB II variables are enrolled in the ServerWORKS database.

ServerWORKS Explorer displays the root object, which you can expand to show the entire Microsoft Network. Objects found may include more objects than just NT servers (such as OS/2 or Windows 95). The systems that respond may not have the full functionality of Windows NT, and as a result may not have all its capabilities.

In addition, you need the DIGITAL agent installed on an NT system you are monitoring to get complete information on the NT system. NT Server Management tools can be used to administer some tasks on those systems, but not necessarily all.

Before You Manage NT From ServerWORKS

You need administrator privileges in the domain you manage. To modify accounts in other domains, the trust relationship between domains must allow domain administration from other domains.

Using NT Server Management for Windows NT Domains

To manage an NT domain on your network, you can use ServerWORKS Manager NT Server Management instead of using the NT administration utilities. The following procedure explains how to create a Local group and assign rights to the group. It is but one an example of an NT administrative task that you can accomplish from ServerWORKS Manager Console.

To create a group in ServerWORKS Manager NT Server Management

1. From the Explorer, choose NT Server Management.
2. Select the NT domain. The list expands to display the Groups, Servers, and Users objects for the domain.
3. Select Servers. The list expands to display the servers in the domain.
4. Select the server or workstation where you want to create the group.
5. Select Groups.
6. From the Actions menu, choose Create. The Create Group dialog box appears.
7. Enter the group name and a brief comment identifying the group. Then select Global or Local.
8. Click Apply to create the group and remain in the Create Group dialog box to create more new groups, or click OK to create the group and close the dialog box.
9. You are prompted to set other attributes for the new group. Do one of the following:
   - Select No to accept the default attributes.
   - Select Yes to open the Properties of Groups dialog box to change other attributes.

To modify the rights

1. From the NT Server Management, select the domain and machine where you are assigning group rights.
2. Select Groups.
3. Choose Actions→Properties.
4. On the Properties of Server dialog box, click on the User Rights tab.
5. On the User Rights page, select a right from the Right drop-down list. For example, to allow the group members to log on locally to the selected machine, click Log on Locally.
6. Click Add.

7. On the Add Groups and Users to… dialog box, select the group and click Add to include this right for this group. Then click OK.
8. Repeat steps 1 to 7 for each right you are assigning until you are satisfied that the group has the appropriate rights.

Assigning Rights to Multiple Groups at Once

Simply select several groups in the Groups list. Press and hold CTRL and click on the groups you are including. All rights assigned or deleted are applied to all groups selected.

More About NT Administration

To review the administrative procedures you can perform from the Console, read the NT Server Management Help.

To open the help

1. Choose Help→NT Server Management.
2. From the Contents window, double-click on a topic of interest.

Novell NetWare Server Manager

When you are running Novell NetWare on the ServerWORKS Console, you can view the NetWare servers in your network. Novell NetWare discovery is similar to the NT Server Management discovery in that it is started by expanding the root NetWare object in the ServerWORKS Explorer. This results in dynamically finding the NetWare objects on the LAN. Note that NetWare V3.x and V4.x systems have different capabilities.

NetWare discovery information is not stored in the database, but is obtained each time that the Novell NetWare object is expanded.

This category includes all DIGITAL servers that are on a LAN running the Novell NetWare operating system and that can be managed using the NetWare Management tools.

Managing a NetWare Network from ServerWORKS

You can discover and manage all DIGITAL servers that are on a LAN running the Novell NetWare operating systems using the standard NetWare tools:

- Filer
- Pconsole
- Princon,
- Rconcols
- Syscon
- Userdef
- NWAdmin

When you select a NetWare server, the NetWare utilities appear on the ServerWORKS Manager toolbar. For details managing a NetWare network from ServerWORKS, refer to the online help.

Additional Procedures and Information A

This section contains the following information:

- How to install SNMP agents for the following operating systems:
  - DIGITAL UNIX V4.0
  - OpenVMS 7.1-1H1
  - IBM OS/2

  These agents are part of an operating system and not provided with ServerWORKS Manager. In addition to the information in the following sections, refer to the installation instructions and release notes for your operating system for any last minute changes to your operating system by the vendor.
- Running a second version of ServerWORKS in another directory.

Installing DIGITAL UNIX SNMP Agents

ServerWORKS Manager monitors Alpha servers running DIGITAL UNIX V3.2d-1 and greater. DIGITAL UNIX SNMP agents and associated MIBs are included with the operating system and are installed by default on all servers on which you install DIGITAL UNIX. The subagents and the MIBs are a part of the OSFCLINETXX mandatory subset.

The Digital Server System MIB will facilitate the monitoring of the complete state of an Alpha Server System, including hardware, firmware and environmental information. The Digital Server Management MIB will help in managing the attributes of any MIBs. It will monitor the attribute values, invoke actions if they exceed their pre-defined thresholds, and if specified, poll the attributes on every restart of the subagent.

The Digital Server System MIB (svrSystem.mib) and the Digital Server Management MIB (svrMgt.mib) definition MIBs reside at

```
/usr/share/sysman/mibs.
```

The agents reside at

```
/usr/sbin/svrMgt_mib
/usr/sbin/svrSystem_mib
```

Installing OpenVMS SNMP Agents

The OpenVMS SNMP agent for Alpha-based systems is included in the DIGITAL TCP/IP Services for OpenVMS product V4.2 or greater and is a component of the NAS Client/Server Package. The SNMP agent is installed when TCP/IP is installed. Refer to the operating system directions, which also contain installation instructions for TCP/IP.

ServerWORKS Manager monitors Alpha servers running OpenVMS Alpha Version 7.1-1H1 The Extensible Simple Network Management Protocol (eSNMP) makes it possible for network managers to manage many different types of devices across all network and vendor boundaries through the use of databases called MIBs (Management Information Bases). Essentially, information is exchanged between master agents and subagents, which are devices such as routers and servers on the network being managed, and managers, which are the devices on the network through which the management is done.

The DIGITAL Server MIB (DSM) consists of two extensions, or subagents:

- System. Describes a management interface to Alpha system information not defined by standard MIBs.
- Management - Describes instrumentation in the DIGITAL extension agent, including the ability to detect and monitor thresholds on integer variables.

The representation of the DSM within the standard Structure of Managed Information (SMI) framework is:

> iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) 36

OpenVMS Alpha Version 7.1-1H1 implements the DSM subagents on the AlphaServer 800, 1000, 4000, 4100, 8200, and 8400 systems. With the DSM subagents, customers can remotely determine and manage important information like:

- Firmware revision numbers
- Base system descriptions
- FRU (field replaceable unit) information and descriptions
- Processor and cache status
- Interface configurations
- Environmental conditions in the system enclosure that might be detrimental to the hardware

You can access the DSM subagents using the following software:

- The DIGITAL ServerWORKS Manager Version 3.0 or greater or any MIB browser that has access to the DSM definitions.
- DIGITAL TCP/IP Services for OpenVMS Version 4.2 (formerly known as UCX). The DSM subagents use the SNMP agent supplied with UCX to communicate with SNMP clients.

Overview of DSM Subagents

DSM subagents respond to SNMP requests for :

- A DSM object—the data item that the network manager is concerned with
- A trap—information about a change of status. A subagent is responsible for reporting on and maintaining the data pertaining to these objects and traps.

A full description of the MIB and its variables is available in the OpenVMS Alpha Version 7.1-H1 Release Notes.

Setting Up the System to Use the DSM Agents

To configure SNMP on the system and enable the master agent to accept SET commands from SNMP clients, issue the following UCX management command from the UCX> prompt. This operation requires SYSPRV or BYPASS privileges.

```
       UCX> SET CONFIGURATION SNMP /FLAGS=SETS
```

To enable or disable the type of access to your local MIB data, use the following UCX commands, qualifiers, and options:

```
UCX> SET CONFIGURATION SNMP /[NO]COMMUNITY="name" -
_UCX> /[NO]ADDRESS=host address /TYPE=([NO]READ,[NO]TRAP,
_UCX> [NO]WRITE)
```

For example, the following command configures SNMP, specifies the community name and address, specifies that the agent can accept SET commands from members of the community, and enables the master agent to send trap messages to members of the community. (Note that READ access is assumed when specifying TRAP or WRITE.)

```
UCX> SET CONFIGURATION SNMP /COMMUNITY="public"
/ADDRESS=128|45.2.8 - _UCX> /TYPE=(TRAP,WRITE)
```

To start the DSM subagents, the system or network manager must modify two files that are provided on the DIGITAL TCP/IP Services for OpenVMS product kit, as follows:

1. Add the following commands to the end of the SYS$STARTUP:UCX$SNMP_STARTUP.COM file

```
    $ RUN   /DETACHED -
      /PROCESS_NAME="UCX$SERVER_MIB" -
      /OUTPUT=SYS$SYSDEVICE:[UCX$SNMP]UCX$SERVER_MIB.LOG -
      /ERROR=SYS$SYSDEVICE:[UCX$SNMP]UCX$SERVER_MIB.ERR -
      /UIC=UCX$SNMP -
      SYS$SYSTEM:SVRSYSTEM_MIB
$ RUN   /DETACHED -
      /PROCESS_NAME="UCX$SVRMGT_MIB" -
      /OUTPUT=SYS$SYSDEVICE:[UCX$SNMP]UCX$SVRMGT_MIB.LOG -
      /ERROR=SYS$SYSDEVICE:[UCX$SNMP]UCX$SVRMGT_MIB.ERR -
      /UIC=UCX$SNMP -
      SYS$SYSTEM:SVRMGT_MIB
```

2. Modify the SYS$MANAGER:UCX$SNMP_SHUTDOWN.COM file to enable the shutdowns. The following file differences show modifications made to UCX$SNMP_SHUTDOWN.COM;2 to include shutdown of the DSM subagent:

```
File SYS$COMMON:[SYSMGR]UCX$SNMP_SHUTDOWN.COM;2
52   $ SUBAGT2 := ucx$server_mib
53   $ SUBAGT3 := ucx$svrmgt_mib
54   $ CONTEXT = ""
******
```

Installing SNMP Agents for OS/2

Refer to the operating system installation instructions to install native SNMP agents for OS/2.

In ServerWORKS Manager, OS/2 DIGITAL servers are discovered as “server” objects and not as server.Digital. In order to manage OS/2 DIGITAL servers, change the server properties as follows:

1. Select the discovered OS/2 DIGITAL server on the map or Explorer view.
2. Choose Actions→Properties.
3. Click the Properties→General Information tab.
4. In the Type list box, select server.Digital.
5. Choose OK.

```
File SYS$COMMON:[SYSMGR]UCX$SNMP_SHUTDOWN.COM;1
53   $ CONTEXT = ""
 ************
 ************
File SYS$COMMON:[SYSMGR]UCX$SNMP_SHUTDOWN.COM;2
59   $   IF  (PRCNAM .EQS. AGENT)  .OR. -
60           (PRCNAM .EQS. SUBAGT) .OR. -
61           (PRCNAM .EQS. SUBAGT2) .OR. -
62           (PRCNAM .EQS. SUBAGT3) THEN  STOP /ID='P1'
63   $   GOTO _LOOP1
******
File SYS$COMMON:[SYSMGR]UCX$SNMP_SHUTDOWN.COM;1
59   $   IF  (PRCNAM .EQS. AGENT) .OR. (PRCNAM .EQS.
   SUBAGT)  THEN  STOP  /ID='P1'
60   $   GOTO _LOOP1
************
```

Number of difference sections found: 2

Number of difference records found: 4

Environmental Data Restrictions: AlphaServer 8200 and 8400 Systems

The power regulators on AlphaServer 8200 systems do not contain sensors for environmental conditions. Therefore, data cannot be reported in the thermal and power supply MIB groups of the DSM System subagent.

Although the power regulators on AlphaServer 8400 systems contain environmental sensors, some configurations might not report environmental information correctly to the DSM System subagent. This problem affects the thermal and power supply MIB groups and will be resolved in a future release of the software.

Device IIA0: Now Configured on AlphaServer 4100 Systems

OpenVMS Alpha Version 7.1-1H1 automatically configures device IIA0: on AlphaServer 4100 systems.

The IIA0: device, which is controlled by SYS$IIDRIVER.EXE, provides access to fan, temperature, and power supply status information available through the integrated I2C bus. The DIGITAL Server System MIB, described in Section 1, provides the status information to the ServerWORKS console. The interface to the device driver is reserved for DIGITAL use only.

Device OPA1: Now Configured on AlphaServer 8200 and 8400 Systems

OpenVMS Alpha Version 7.1-1H1 automatically configures device OPA1: on AlphaServer 8200 and 8400 systems. The OPA1: device, which is controlled by SYS$OPDRIVER.EXE, provides access to temperature and power supply status information available through the integrated H7263 power regulators. The DIGITAL Server System MIB, described in Section 1, provides the status information to the ServerWORKS console. The interface to the device driver is reserved for DIGITAL use only.

Running a Second Version of ServerWORKS

If you want a second version, first rename the files of the older version in the Start Menu directories. Use the following procedures:

For Windows NT 4.0 or Windows 95:

1. From the Desktop, choose Start→Settings→Taskbar.
2. Select the Start Menu Programs tab and click the Advanced button.
3. Choose Tools→Find→ Files and Folders. Then enter Start in the Named: field.

Browse the directory tree for the ServerWORKS, ClientWORKS or ManageWORKS directories and rename the files.

Do You Have ManageWORKS Installed?

ServerWORKS Manager Console and OpenVMS Management Station can be installed and run *separately* on the same machine. Continue to use ManageWORKS as the interface for the OpenVMS Management Station.

If you do not have ManageWORKS installed, you can skip this section.

Only ManageWORKS V2.2 is supported for upgrading to ServerWORKS Manager 3.x. The installation checks to see whether ManageWORKS is installed. If it is, you can preserve the IP Discovery maps from ManageWORKS V2.2. Only IP objects in the IP Discovery View are preserved. User preferences and custom SVN views from ManageWORKS must be reapplied to new hierarchical views that you create in ServerWORKS Manager. Other ManageWORKS views, alarm and polling information, application launch information, or default actions are not preserved. If you do not remove ManageWORKS after upgrading to ServerWORKS Manager, you can continue to use it *separately* from ServerWORKS Manager.

After Upgrading to ServerWORKS Manager

You can expect the following conditions:

- The first time you run ServerWORKS Manager after upgrading from ManageWORKS V2.2, the message “Database inconsistency detected” appears. Choose the Ignore button. On the next dialog, choose the Ignore Forever button to prevent seeing the message each time you run ServerWORKS Manager.
- When you are discovering a network using the IP Discovery Wizard after upgrading, you are asked to choose a map view for the discovery results. The map views are equivalent, so you can select either one.
- If you preserve the ManageWORKS database, a read-only viewer named Browser is created. You cannot delete the Browser.
- To initialize a ManageWORKS database after upgrading to ServerWORKS Manager V3.x, first close all ServerWORKS Manager components (Event Logger, Event Dispatcher, Poller, Ping Server, and the Data Collector).

Then initialize using the ServerWORKS Manager DB Utility with this procedure:

1. From the Start menu, choose Programs→ServerWORKS DB Utility.
2. Select "Entire Database except MIB."
3. Click Initialize.
4. Choose OK to exit from the utility.

If you preserve the ManageWORKS V2.2 version and execute it without the full command line (including the initialization file SWMGR.INI), you will get incorrect database path pointers from the new version in addition to the following messages:

```
CODEBASE ERROR
Wrong DB version 0.0.0
Expected DB version 2.0.X
```

If you do not remove the ManageWORKS menu items from the Start menu, you may experience similar behavior.

Troubleshooting B

This section describes common occurrences when an installation is unsuccessful and suggests solutions. Review the list for your particular situation if you are dissatisfied with the installation. If you have not yet installed, reviewing the list before you proceed is recommended.

Common Problems and Solutions

Condition ServerWORKS Manager does not launch. The last exit from ServerWORKS Manager or another component that uses the file PCMGR.MDB may have been abnormal or system shutdown may have been improper (for example, a power outage).

Action The .MDB database file may need repair. To do this, follow the instructions:

1. Start the ODBC management utility from the Control panel.
2. Click on the user DSN page.
3. Select SWMgrDB.
4. Click on the Configure button.
5. Click on the Repair button.
6. Choose OK to exit.
7. Reboot and try ServerWORKS Manager again.

Condition The ServerWORKS Manager Event Logger does not record events as expected.

Action This condition may have any of the following causes:

- If the Event Logger terminates abnormally (for example, it is closed from the System Tray), new events are not recorded and existing events are not acknowledged. Rebooting your management console may alleviate this.
- If unacknowledged events fill up the log, the log buffer reaches its limit and new events are added to the log from the top of the buffer, overwriting the existing events. Increase the buffer file size using the ServerWORKS Manager DB Utility.
- The Event Logger recognizes community names from SNMP traps of only up to six characters. Longer names are truncated. Review the documentation for your operating system for information on setting community names.

Condition The SNMP service does not start from the installation program or from the NET START SNMP command.

Action First check the Event Viewer and look for either of the following messages:

On NT 4.0: The SNMP Service is ignoring trap destination <node name> because it is invalid.

If you see this messages, use the following procedure:

1. Remove the offending node from the trap destination list in the SNMP Service Configuration dialog.
2. Start SNMP from the DOS prompt using the NET START SNMP command. Repeat this procedure for every failing node in the list.
3. If there are many Trap Destinations listed, do the following:
4. From a DOS Prompt, type NET STOP SNMP to insure that SNMP service is stopped.
5. Start the service using SNMP command.
6. Check the Event Log for errors and remove from the trap destination list any nodes that timed out.

There are other SNMP errors that cause the service-specific error 1 to be posted to the event log. If the previous procedure does not change the condition, consider the following alternatives:

- Check your DNS and WINS settings. Make sure that LMHOSTS lookup is enabled if you intend to resolve the problem using LMHOSTS.
- A single invalid destination can cause a time-out if the network is running slowly. Waiting for multiple time-outs will cause this problem on a healthy network.

Configuring a Modem and Comm Port for Paging

If you have not already done so, install the modem hardware and software according to the manufacturer's instructions.

Attempt to dial from the modem using any dial-up software. If you cannot connect and reach the phone number of the test location, recheck the computer-to-modem and modem-to-phone physical connections and make sure the modem is turned on. Also check that the phone number, area codes, and country codes are correct. Refer to the dial-up software manufacturer’s directions for details about the dial-up software.

If you cannot install successfully, you can edit the Registry keys for ServerWORKS Manager Console, ClientWORKS, and the agents.

Before you edit the Registry, review the following guidelines.

Editing the Registry

In some instances the new installation may continue to fail if previous versions of ServerWORKS , ManageWORKS, and ClientWORKS were not uninstalled properly. Some earlier versions of these products cannot be completely removed without intervention in the Registry.

You should first remove the software using the Control Panel→ Add/Remove Programs applet. Then you can remove items from the Registry. You can find the Registry in the following locations:

- On Windows NT \Windows\Regedt32.exe
- On Windows 95 \Windows\Regedit.exe

Removing Registry Keys

Follow these guidelines before you edit the Registry.

- Always use the ServerWORKS Manager Console→unInstallShield menu item or the Control Panel→Add/Remove Programs applet first to remove previous versions of ServerWORKS Manager Console, ClientWORKS, and the agents.
- Always back up the Registry before you edit it in case you must restore a damaged Registry. From the Registry editor, use the Registry→Export Registry File menu item to save the file as a .reg file. The Registry online help describes how to complete this procedure and restore the backed up Registry.
- Keys and values may be different for Windows NT and Windows 95 systems.
- Not all keys and values appear on all systems. Keys entered with earlier versions may be obsolete although they remain on your system.
- If your system does not contain a value for a key as listed in the following tables, do not remove the key.
- Keys and values are subject to change between releases.

Warning: Do not edit the Registry unless you are familiar with Windows NT or Windows 95 operating systems. Do not remove the full tree path.

Registry Keys for ServerWORKS

Table B-1 Registry Keys for ServerWORKS HKEY_LOCAL MACHINE Key

HKEY_LOCAL_MACHINE	
	\\SOFTWARE\\ODBC\\ODBC.INI\\ODBC Data Sources
	\\SOFTWARE\\ODBC\\ODBC.INI\\SWMgrDB
	\\SOFTWARE\\ODBC\\ODBC.INI\\SWMgrDBEmpty
HKEY_LOCAL_MACHINE	
	\\SOFTWARE\\DigitalEquipmentCorporation\\ServerWORKS Manager Console\\4.0
	\\SOFTWARE\Microsoft\\Windows\\CurrentVersion\\AppPaths\\pwMgmt.EXE
	\\SOFTWARE\Microsoft\\Windows\\CurrentVersion\\AppPaths\\smb.exe

Registry Keys for Agents

Table B-2 Registry Keys for Agents HEKY_LOCAL_MACHINE Key

HKEY_LOCAL_MACHINE
\\SOFTWARE\\DigitalEquipmentCorporation\\CimHealthAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\CimHostAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\CimScsiAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\CimSinfoAgent
\SOFTWARE\\DigitalEquipmentCorporation\\CimStdeqAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\CimThresAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\DigitalClusterExtensionAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\DigitalCommonClusterAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\HostResourcesAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\ServerManagementAgent
\\SOFTWARE\\DigitalEquipmentCorporation\\ServerSystemAgent
\\System\\CurrentControlSet\\Services\\SNMP\\Parameters\\Extension Agents
\\System\\CurrentControlSet\\Services\\SNMP\\Parameters\\ServerSystemAgent \\SvrCpuPllInterval

Registry Keys for ClientWORKS

Table B-3 Registry Keys for ClientWORKS HKEY_LOCAL_MACHINE Key

```
HKEY_LOCAL_MACHINE
        \\SOFTWARE\\DigitalEquipmentCorporation\\AssetWORKS LiveLINK
        \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS
        \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS\\CW Shared
        \\SOFTWARE\\DigitalEquipmentCorporation\\DMI\2.00
        \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS DMI Browser
        \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS DMIExplorer
        \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS SMART
        \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS SNMP
        \\SOFTWARE\\DigitalEquipmentCorporation\\Host Resources Agent
        \\SOFTWARE\\DigitalEquipmentCorporation\\Server Management Agent
        \\SOFTWARE\\DigitalEquipmentCorporation\\Server System Agent
        \\SOFTWARE\\DigitalEquipmentCorporation\\ClientWORKS Init

HKEY_LOCAL_MACHINE
        \\SYSTEM\\CurrentControlSet\Services\\DIGITAL DMI Instrumentation
        \\SYSTEM\\CurrentControlSet\Services\\tvdddrv
        \\SYSTEM\\CurrentControlSet\Services\\Win32sl
        \\SYSTEM\\CurrentControlSet\\Control\\VirtualDeviceDrivers\\VDD
```

Table B-4 Registry Keys for ClientWORKS HKEY_CURRENT_USER Key

HKEY_CURRENT_USER
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\ClientWORKS
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\CWSNMP1.0
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\LiveLINK1.0
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\SMART1.0
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\DMIPATH
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\ Digital DMI
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Digital SmartMonitor
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Read BIOS
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\SNMP
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\CW SMARTMonitor
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\CW Shared
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\SecureOnClient
\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Win32SL

References C

Familiarity with your operating system and network fundamentals is critical for using ServerWORKS Manager functions to their full potential. The following sources are suggested reading.

Bibliography

Topic	Additional Source of Information
DIGITAL UNIX	Network Administration and Network Programmer’s Guide
Discovering objects on your network	Online help, Chapter 3 of this manual
KCRCM	KCRCM AlphaServer Remote Console Module Installation and User's Guide (EK-KCRCM-IN) included with the KCRCM product
Monitoring Systems	The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994 SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993

continued

Topic	Additional Source of Information
Monitoring Systems (continued)	Internetworking with TCP/IP, Volume 2, Design, Implementation, and Internals by Douglas E. Comer and David L. Stevens published by Prentice Hall 1991 Internetworking with TCP/IP, Volume 1, Principles, Protocols, and Architecture by Douglas E. Comer published by Prentice Hall 1991, Second Edition
Mylex GAM	Mylex Global Array Manager 2 Installation and User's Guide (ER-MYL02-IA) found on the ServerWORKS Manager CD-ROM in the documentation section
Novell NetWare	Novell's Guide to Multiprotocol Internetworking, by Laura A. Chappell and Roger L. Spicer published by the Novell Press NetWare, The Professional Reference, Third Edition, published by News Rider Publishing 1994
OpenVMS	TCP/IP Networking on OpenVMS Systems and OpenVMS System Manager's Manual
RSM	RSM Installation Guide (ER-PCDSC-IA) and RSM Station Software User's Guide (ER-PCDSM-UA) included with the RSM product
SCO UNIX	SCO OpenServer Handbook How to install, configure, and start using an SCO OpenServer system, published by The Santa Cruz Operation 1995

continued

Topic	Additional Source of Information
Sending SNMP Traps	Online help, Chapters 5, 7 of this manual. The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994 SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993
Setting and Receiving Alarms	Online help, Chapter 5 of this manual
SNMP	The Simple Book - An Introduction to Internet Management by Marshall T. Rose, published by Prentice Hall 1991, second edition 1994 SNMP, SNMPV2, and CMIP - The Practical Guide to Network - Management Standards by William Stallings, published by Addison Wesley 1993 Internetworking with TCP/IP Volume 2 Design, Implementation, and Internals by Douglas E. Comer and David L. Stevens published by Prentice Hall 1991
SWCC	StorageWORKS Command Console Installation Guide (AA-R0HJB-TE) found on the ServerWORKS Manager CD-ROM in the documentation section
Windows 95	Microsoft Windows 95 Resource Kit published by Microsoft Press 1995

continued

Table C-1 Bibliography *(continued)*

Topic	Additional Source of Information
Windows 95 SNMP	Microsoft Windows 95 Resource Kit published by Microsoft Press 1995
Windows NT	Windows NT Networking Guide - Windows NT Resource Kit by and published by Microsoft Press
Windows NT SNMP Service	Windows NT Networking Guide - Windows NT Resource Kit published by Microsoft Press

Web Site

The following web site may also provide additional information on ServerWORKS:

```
http://www.digital.com/info/alphaserver/sworks.html
```

Glossary

The following terms are used frequently in any discussion of SNMP and network management.

Term	Definition
Alarm	An SNMP trap generated by an agent or an event and triggered by the results of polling an agent.
Allocation Units	The size in bytes for a particular storage device. For example, the allocation units for a disk are typically 512, 1024, or 2048 bytes and are sometimes referred to as ‘block size.’
CPU Utilization	Average percentage of time that this processor was not idle.

continued

Term	Definition
Data Collector	Process that runs on the management console and polls objects for SNMP data. The collector analyzes the data and either generates alarms or passes the data on to registered applications such as the System Browser.
DMI	Desktop Management Interface.
FAT	File Allocation Table (listed on the System Browser File System property page).
File System Utilization	The percentage of the file system being used (local file systems).
IP	Internet Protocol (see also TCP/IP).
IP Address	An address of an object on a network. The standard address is composed of four numbers each of which is less than 255.
Management Information Base (MIB)	Data Specification for passing information using the SNMP protocol.
MIF	Management Information File - This is a database file that defines a given host's configuration, hardware inventory, storage devices, processors, and memory.
Mount Point	The top level name for a mounted file system.
MTU	Maximum Transmission Unit.
Network Interface	Communication between the management console machine and the network. Usually completed through Network Interface cards.
Network Interface Inbound Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Network Interface Inbound Packet Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

continued

Term	Definition
Network Interface Inbound Packets	The number of packets delivered to a higher-layer protocol.
Network Interface Outbound Errors	The number of outbound packets that could not be transmitted because of errors.
Network Interface Unknown Protocol Errors	The number of packets received through the interface which were discarded because of an unknown or unsupported protocol.
NOS	Network Operating System. The operating system and protocol used to communicate between objects on a network.
NTFS	NT File system. File system used on NT.
Polling Interval	The time between polling queries of a device.
Re-Enable Value	Value that can be set in the Threshold screen to automatically enable an alarm that has previously triggered.
SNMP	Simple Network Management Protocol - The application protocol offering network management service in the Internet.
SNMP Trap	An asynchronous event generated by the agent and sent to the SNMP manager.
Status Alarm	Alarm set on server processors or disks to indicate the status of the device (options are running, non-functional, and warning).
System Name	The name of the object on the IP network as returned by the Naming server or found in the Hosts file on the management console machine.
System Up Time	The time the system has been up since it was booted.
TCP/IP	Transmission Control Protocol/Internet Protocol. A widely used set of software communications protocols. TCP delivers data over a connection between applications on different computers on a network: IP controls how packets (units of data) are transferred between computers on a network.
Threshold Alarm	Alarm triggered when a value entered on the Threshold Alarm screen meets a specified condition.
Threshold Value	Value at which an alarm is triggered (e.g., 10000 packets per second).

Index