Using ClientWORKS™ with DIGITAL PCs

A Guide for Network Administrators

Digital Equipment Corporation

The information in this document is subject to change without notice and should not be construed as a commitment by DIGITAL Equipment Corporation.

Digital Equipment Corporation assumes no responsibility for any errors that might appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license. No responsibility is assumed for the use or reliability of software or equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

Restricted Rights: Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Using ClientWORKS™ with DIGITAL PCs: A Guide for Network Administrators

Contents

1 Introduction 11

2 ClientWORKS, DMI, and SNMP 13

2.1 The Desktop Management Interface 13

2.2 DMI Architecture 14

2.3 SNMP Architecture 16

2.3.1 SNMP System Components 16

2.3.2 The DIGITAL SNMP Extension Agent 18

2.4 DMI and SNMP Working Together 18

3 Using ClientWORKS 21

3.1 Starting ClientWORKS Utilities 21

3.2 Starting the DMI Browsers 22

3.3 Installing the SNMP Extension Agents 23

3.3.1 For Windows 95 24

3.3.2 For Windows NT 4.0 24

3.4 Uninstalling ClientWORKS 25

3.5 Reinstalling ClientWORKS 26

4 Using ClientWORKS Alarms 27

4.1 Sending ClientWORKS Alarms to ServerWORKS Manager .. 27

4.1.1 How ClientWORKS Seeds Traps 28

4.1.2 Receiving ClientWORKS Traps in ServerWORKS Manager 29

4.1.3 Configuring SNMP for Trap Forwarding 29

4.1.3.1 Configuring SNMP Security 30

4.1.3.2 Configuring SNMP Traps 30
4.1.3.3 Configuring the SNMP Agent on Windows 95 31
4.1.3.4 Configuring the SNMP Agent on Windows NT 4.0 32

5 Working with MIFs 35
5.1 The System MIF 35
5.2 The Monitor MIF 36
5.3 Checking SecureBOX Status 37
5.4 Reading Environmental Information 37
5.4.1 Voltage Probe 38
5.4.2 Temperature Probe 38
5.5 The Registry MIF 38
5.5.1 Adding the Registry MIF to ClientWORKS 39
5.5.2 Modifying the Registry MIF 39
5.6 Supplying MIF Information to Microsoft Systems Management Server (SMS) 43
5.7 User-Specified Information 44

6 Using DIGITAL SMARTMonitor 45
6.1 Enabling Monitoring 45
6.2 The SMARTMonitor Display 47
6.2.1 Hard Drives 47
6.2.2 Temperature Probes 48
6.2.3 Voltage Probes 48
6.3 S.M.A.R.T. Event Logging 49

7 Using SecureON for Remote Wake-up 51
7.1 Introduction 51
7.1.1 Features and Benefits 51
7.1.2 Client Application 52
7.1.3 Server Application (Management Console) 52
7.1.4 BIOS Settings 52
7.1.5 Modifying the BIOS Settings 53
7.2 Using Remote Network Wake-Up 53
7.2.1 Installation 53
7.2.2 Client 53
7.2.3 Server (Console Management) 54
7.3 System Administrator User Interface 55

7.3.1 To add a Magic Packet client to the current view 56
7.3.2 To remove a client from the current view 57
7.3.3 To wake up a client 57
7.3.4 To refresh the view 57
7.3.5 Setting Options 57
7.3.5.1 Event Viewer/Logging Options 58
7.3.5.2 Network Options 59

8 Using ClientWORKS with Other System and Network Management Solutions 61
8.1 DIGITAL ServerWORKS Manager 61
8.2 Microsoft Systems Management Server (SMS) 62
8.3 Integration with Enterprise-Level Network Management Tools 63
8.3.1 Integrating DMI Browsing 63
8.3.2 Integrating SNMP Browsing and Alarms 63

9 Using ClientWORKS with Mobile Systems 65
9.1 Using ClientWORKS with Mobile PCs 65
9.2 Using ClientWORKS to Troubleshoot Mobile Clients 67
9.2.1 Considerations for Asset Management 67
9.2.2 Enhancing Security of the Mobile PC 68
9.2.3 Setting Triggers for Remote Dial-Ins 68

Index 69

Preface

This document introduces and explains how to use DIGITAL's ClientWORKS management product to manage DIGITAL desktop systems. It also provides detailed procedures for installing and using the ClientWORKS product.

Audience

This guide is intended for system and network administrators.

Prerequisites

To effectively use all ClientWORKS features, you must be familiar with the operational requirements for managing a system using the Desktop Management Interface (DMI), the Simple Network Management Protocol (SNMP), and Microsoft's Systems Management Server (SMS).

Terminology

The terms "Select" and "Choose" are used frequently in the procedures presented in this guide to perform operations. Both terms refer to specific mouse pointer or keyboard operations:

- Select — Move the mouse pointer to an item (icon, command, name, and so on) and single-click the mouse button, or use the specified set of keyboard keys.

- Choose — Move the mouse pointer to an item (icon, command, name, and so on) and double-click the operational mouse button, or use the specified set of keyboard keys.

Keyboard Conventions

You can use the following standard keyboard conventions with the ClientWORKS Management Suite.

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 focus 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

ClientWORKS Documentation

This manual

Using ClientWORKS with DIGITAL PCs: A Guide for the Network Administrator (this manual) provides information about using ClientWORKS in a network environment.

Online help

ClientWORKS, the SecureON console, and the DIGITAL SMARTMonitor provide online help to assist you while you are using them.

README.TXT

The ClientWORKS README.TXT file is shipped online with the ClientWORKS product. The README.TXT file contains the most recent information about the product, including corrections and additions to the manual and help files. Refer to the README.TXT for the latest detailed information about ClientWORKS and its components.

Latest Product Information and Updates

For any last minute information and directions for how to download the latest version of ClientWORKS, please refer to the README.TXT file located in the ClientWORKS directory on your DIGITAL PC or on the accompanying CD-ROM. The README.TXT file contains up-to-date pointers to the DIGITAL web site and other information sources.

1

Introduction

ClientWORKS is the family of client management and networking tools that Digital Equipment Corporation supports on its entire line of X86 processor-based desktop, personal workstation, and mobile computers and servers. ClientWORKS extends DIGITAL's networking expertise by providing a powerful set of utilities and Desktop Management Interface (DMI) and Simple Network Management Protocol (SNMP) software designed to help you get the most out of your networking environments. ClientWORKS features are also integrated in the DIGITAL ServerWORKS Manager Suite. You can access DMI-based management capabilities of your DIGITAL X86 processor-based systems, as well as enable SQL queries via Microsoft SMS.

ClientWORKS comes bundled in at no additional cost and makes DIGITAL X86 processor-based desktop, personal workstation, and mobile systems manageability-ready. You can start managing your systems right away, without purchasing costly additional software.

Combined with DIGITAL's ServerWORKS Manager™, and other industry-standard network management tools, ClientWORKS provides comprehensive desktop-to-enterprise management solutions.

The ClientWORKS Management Suite helps reduce the total cost of owning and managing a computer network. The ClientWORKS management suite consists of several software tools that help you keep track of the computer systems that make up a network. It provides:

- System information that is updated automatically from various resources -- operating system, system BIOS, vendor-supplied instrumentation
- Local or remote alarming when in response to a warning or error condition that can be integrated into any SNMP manager, including ServerWORKS Manager

- Reports about the status and condition of equipment (support for Secure Features, the DIGITAL SMARTMonitor)
- Asset and inventory management and upgrade planning through the DMI Local and Remote Browsers
- Troubleshooting information
- Integration with ServerWORKS Manager to offer not only powerful server management but workgroup management as well. ClientWORKS client management combined with ServerWORKS Manager provides a comprehensive network management solution
- Compatibility with Microsoft's Systems Management Server (SMS) for report building and other advanced network management functions

Together, these features and components allow you to solve problems such as these:

- Diagnose a problem without ever going to the PC at a remote location
- Reduce travel costs by querying PC configurations over the WAN
- Determine information such as how many SIMM slots a particular system has or what kind of memory it needs without relying on a user's guess or visiting the machine yourself
- Use Microsoft SMS and ClientWORKS MIFMaker to run queries on your network such as "show me all my PCs with 8MB of RAM," or any other popular system variable
- Automate asset management tasks such as end-of-year asset tagging
- Improve response time, accuracy, and end-user satisfaction
- Realize significant savings in cost of ownership

The following chapters discuss these tasks and features in more detail.

2

ClientWORKS, DMI, and SNMP

This chapter discusses the Desktop Management Interface(DMI), the Simple Network Management Protocol (SNMP), and how ClientWORKS uses each.

2.1 The Desktop Management Interface

Supporting today's networks requires increasing amounts of time and money. While the cost of buying individual computer systems has gone down, the cost of managing and supporting those systems has risen as network management expertise has become scarce and environments have become more complex. New tools, better and faster hardware components, new operating environments, and conflicting standards deluge the network administrator.

In response to these needs, the Desktop Management Task Force, (DMTF™), of which Digital Equipment Corporation is a founding member, developed the Desktop Management Interface (DMI) to specify a standard method of collecting and communicating information about individual systems and their components.

DMI allows PC hardware, software, and peripheral components — whether configured as standalone systems or systems linked into a network — to coexist in a manageable PC system. DMI also provides OS-independent management functions for the network devices it supports.

The following sections explain the architecture and components of the Desktop Management Interface and highlight the DIGITAL implementation of DMI in ClientWORKS.

2.2 DMI Architecture

The DMI consists of the standard system Management Information Format (MIF) file, a Service Layer, the Management Interface, and the Component Interface. The MIF defines the standard manageable attributes of PC products in categories including PC systems, servers, printers, LAN adapters, modems, and software applications. DMI manages the information in the standard system MIF file, and passes that information to an application as requested.

A DMI implementation includes a number of components:

- ***Manageable products,*** also called ***components,*** are hardware, software, peripherals, or firmware that are part of a computer system or network server. Components include disk drives, word processors, CD-ROMs, printers, main logic (mother) boards, operating systems, spreadsheets, graphics cards, sound cards, and modems. Each manageable product provides a MIF file that contains the pertinent management information for that product. ClientWORKS gathers the information in all the MIFs on the system and stores them in the MIF database. Once installed, these manageable products communicate with the Service Layer through the Component Interface (CI).
- A product's ***manageable attributes*** are its characteristics that can be viewed or changed. These attributes are described in Management Information Format, or MIF format.
- A ***MIF file*** is a simple ASCII text file describing a product's manageable attributes, grouped in ways that make sense. Attributes are described in MIF or Management Information Format, which has a defined grammar and syntax. Each product has its own MIF file. When a manageable product is installed, the information in its MIF file is added to the MIF database. This information is then made available to the Service Layer and thus to the management applications.
- The ***MIF database*** is the database of system information managed by the Service Layer. The MIF database contains the information about the manageable products on the system. The information is described in MIF files provided with each product. The MIF file may contain the data, and often describes how the data is obtained at run time.

- The ***Service Layer*** is a set of Windows services that collects and manages information from the manageable products on each system. The Service Layer implements the Desktop Management Interface. The Service Layer collects information from manageable products into the MIF database and passes the information to management applications as requested. It controls communication between itself and management applications via the Management Interface (MI) and between itself and manageable products via the Component Interface (CI). The Service Layer starts at boot time, whether a user is logged in or not. Unless the services are stopped manually, they continue to run until the system shuts down.

- The ***Component Interface*** (CI) handles communications between manageable products and the Service Layer. The Component Interface allows for communication with manageable products for get and set operations, receives indications from manageable products, and passes those to the Management Interface.

- The ***Management Interface*** (MI) allows a management application to query for lists of manageable products, access specific components, and get and set individual items of interest. The Management Interface also allows a management application to tell the Service Layer to send information about indications from manageable products.

- An ***indication*** is an unsolicited message sent from the Service Layer to a management application to notify the application that a particular situation has taken place. It is the DMI equivalent of an SNMP trap.

- A ***management application*** is a program for changing, interrogating, controlling, tracking, and listing the elements of a computer system. A management application can be a diagnostic program, an installation program, or other program. The DMI Browser is a management application that can be used to browse machines both locally and remotely. Other management applications include Microsoft SMS and MIFMaker.

2.3 SNMP Architecture

The Simple Network Management Protocol, commonly referred to as SNMP, is an Internet-based protocol commonly used to manage PC networks. The following sections explain the SNMP system components and the DIGITAL extension agents.

2.3.1 SNMP System Components

SNMP stores its data in one or many *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.

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

- An object identifier 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 a complex data type
- The read or write access that is allowed on the object

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 as identified by its object identifier.

The *agent* is the program that receives management requests and processes them by accessing information from the MIBs on the computer. The agent then sends the requested information back to the SNMP management program that initiated the request.

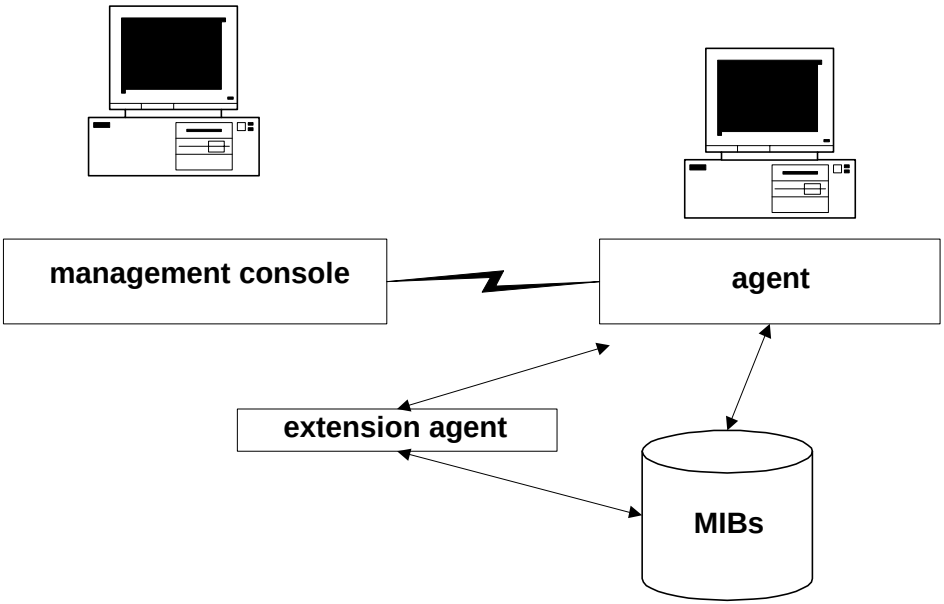
The agent performs four operations:

- **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,* also called a subagent, is software that extends the functionality of the system agent. When the SNMP 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 1.

Figure 1: SNMP Components



2.3.2 The DIGITAL SNMP Extension Agent

SNMP agents are usually provided by the operating system vendor. Microsoft Windows 95 and Windows NT have SNMP agent subsystems that allow you to construct extension modules for specific hardware and software. The DIGITAL Server Agent is exactly this. It 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 can be configured to send its traps directly to any SNMP management console, including ServerWORKS Manager console, or to enterprise management systems, such as HP OpenView or Tivoli TME-10, that use SNMP as their trap and alarming mechanism.

2.4 DMI and SNMP Working Together

ClientWORKS is the family of client management and networking tools that DIGITAL supports across its entire line of desktop, personal workstation, and mobile computers. ClientWORKS extends the Desktop Management Interface (DMI) by providing an enhanced and powerful set of utilities and software to help the Network Administrators keep track of the installed hardware and software, either locally or on a network. ClientWORKS follows the DMI specifications.

DMI and SNMP work together as an integrated, cohesive solution to enhance system management of your networked environment.

The SNMP subsystem reports those data items from both the Host Resources MIB and the DIGITAL private Server System and Server Management MIBs. These MIBs are provided on all DIGITAL desktops, personal workstations, mobile computers, and servers to allow the Network Administrator to read monitored data on both DMI and SNMP on client systems. This is part of DIGITAL's flexible and interoperable management strategy and offers the Network Administrator the power to choose.

DIGITAL's ServerWORKS Manager and ClientWORKS both function in this way, exhibiting both SNMP and DMI information about servers, network components, and DIGITAL PCs on the same console.

ClientWORKS seeds the SNMP traps on Windows 95 and Windows NT systems to include the values for the temperature, voltage, SecureBOX alarms, SecureON unauthorized wake-up attempts, and more. By simply adding the IP address of the network machine that is the SNMP console, you have instantly enabled remote alerts should an error condition or security violation occur. See Section 4.1.1 for more information about alarm seeding.

3

Using ClientWORKS

ClientWORKS Management Suite provides an enhanced and powerful set of utilities and software that follows the Desktop Management Interface (DMI) specifications. These tools help network administrators keep track of the installed hardware and software, either locally or on a network.

This chapter explains the basics of starting the DMI Local and Remote Browsers and other tools in the ClientWORKS management suite. The chapters that follow detail aspects of the product.

3.1 Starting ClientWORKS Utilities

You access the ClientWORKS Management Suite from the Start menu in Windows 95 or Windows NT. The ClientWORKS Management Suite includes a number of components:

- ***DMI Local Browser*** and ***DMI Remote Browser*** start ClientWORKS for local or remote browsing.
- ***Help*** opens the online help file.
- ***Readme*** opens the README.TXT file, where you find late-breaking information about the product, as well as changeable information such as web pointers and BBS telephone numbers.
- ***MIFMaker*** converts standard MIFs to a form that can be used by Microsoft SMS. See Section 5.6.

- ***SecureON Console*** (Windows NT only) opens the SecureON Console, also known as Remote Network Wake-up, if it has been installed on this system. Chapter 7 describes the SecureON Console.
- ***Registry Instrumentation Initializer*** lets you initialize the instrumentation for the registry MIF after you have installed it. See Section 5.5.
- ***Set ClientWORKS Information*** lets you set asset and contact information for the system. You can change the data at any time by opening the Set ClientWORKS Information window again.
- If your system includes any S.M.A.R.T.-enabled devices, you will also have the ***DIGITAL SMARTMonitor*** installed. See Chapter 6.

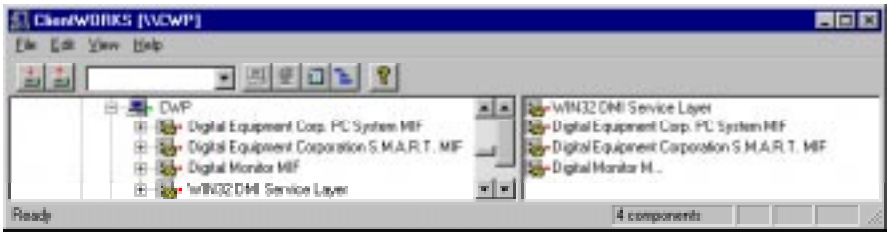
Refer to the ClientWORKS online help for details of how to use the DMI Local and Remote Browsers, the DIGITAL SMARTMonitor, and SecureON Console.

3.2 Starting the DMI Browsers

ClientWORKS provides access to the DMI interface through the DMI Browser, which has two variations:

- The DMI Local Browser accesses only the DMI on your local machine. It supports an interface similar to Microsoft Explorer, allowing you to select the MIF, group, and underlying attributes you want to display.
- The DMI Remote Browser lets you browse DMI components throughout the network. It allows you to select a system to browse, then behaves similarly to the DMI Local Browser.

To view the MIFs on any machine, remote or local, click on the () icon in the tree view to expand it, or use the Expand/Collapse command. The resulting display looks something like this:



The contents of the window vary according to the components available on the machine you are viewing. A typical client has at least two selections:

- System MIF, which lists all devices and MIFs on the system. If manageable components have installed MIFs, they will appear here.
- Service Layer, which lists the manufacturer, product, version, serial number, installation date, and a verify column. The verify column lets you know whether the component exists and is functioning correctly.

Newer PCs from DIGITAL will include additional MIFs:

- DIGITAL Equipment Corporation SMART MIF
- DIGITAL Monitor MIF

You may also install the Registry MIF and other MIFs on your system. See Chapter 4.

As you browse the MIFs, the red box near the line item changes to yellow when browsing, then to green when the selected item is located. Use the Refresh command or click on the Refresh button to update the status.

3.3 Installing the SNMP Extension Agents

The ClientWORKS installation procedure expects, but does not require, the Microsoft SNMP agents to be installed before you install ClientWORKS. You may choose not to install the ClientWORKS SNMP extension agents, or you may install them later.

To install the SNMP extension agents after you have installed ClientWORKS, perform the steps shown in the following sections.

3.3.1 For Windows 95

First, install the Microsoft SNMP agents from the Windows 95 CD:

- Open the Control Panel and click on the "Network" icon.
- Click on "Add."
- Choose "Service" as the type of network component to be installed.
- Click on "Add."
- Click on "Have Disk."
- Install from the "ADMIN\NETTOOLS\SNMP" folder on the Windows 95 CD.

For more information, see the SNMP Agent topic in the Windows 95 Resource Kit (WIN95RK.HLP)

To now install the ClientWORKS SNMP agents, run the ClientWORKS setup program located on the DIGITAL System Software CD in the directory \apps\cw\disk1\setup.exe

- When prompted select "Install ClientWORKS SNMP subagents."
  - If you have previously installed ClientWORKS without installing the extension agents, select only "Install ClientWORKS SNMP subagents." Deselect all other options.
  - If you have not previously installed ClientWORKS components, select the appropriate options.
- Continue with setup.

3.3.2 For Windows NT 4.0

First, install the Microsoft SNMP agents from the Windows NT 4.0 CD:

- Open the Control Panel and click on the "Network" icon.
- Choose "Services" and click "Add."
- Select "SNMP Service" from the list and click "OK."
- Insert the Windows NT 4.0 CD and (if required) update the directory path.

- Click "Continue" and complete SNMP service installation.

To now install the ClientWORKS SNMP agents, run the ClientWORKS setup program located on the DIGITAL System Software CD in the directory \apps\cw\disk1\setup.exe

- When prompted select "Install ClientWORKS SNMP subagents."
  - If you have previously installed ClientWORKS without installing the extension agents, select only "Install ClientWORKS SNMP subagents." Deselect all other options.
  - If you have not previously installed ClientWORKS components, select the appropriate options.
- Continue with setup

NOTE
Remember that if you have installed Microsoft Service Pack 3 for Windows NT V4, you will need to reinstall the Service Pack after you install SNMP and the ClientWORKS SNMP extension agents. If you do not, you will receive SNMP entry point errors.

3.4 Uninstalling ClientWORKS

If you are upgrading from a release of ClientWORKS before Version 2.91, you must uninstall the previous version of ClientWORKS and reboot your system before you install ClientWORKS 2.91. See the README.TXT file for details.

The ClientWORKS components must be installed in a specific order, detailed in the README.TXT file. You must reboot your system after uninstalling.

If you are using ServerWORKS Manager, you should not install ClientWORKS 2.91. ServerWORKS Manager requires ClientWORKS 2.9. If you reinstall ClientWORKS, you may need to reinstall ServerWORKS Manager. See the README.TXT file for details.

3.5 Reinstalling ClientWORKS

If you need to reinstall ClientWORKS, it is important that you get the most recent version. You can conveniently download it from the DIGITAL web site. Consult the README.TXT file in the ClientWORKS folder on your system for the latest directions for downloading.

If you are upgrading from a release of ClientWORKS before Version 2.91, you must uninstall the previous version of ClientWORKS and reboot your system before you install ClientWORKS 2.91. See the README.TXT file for details.

If you are using ServerWORKS Manager, do not install ClientWORKS 2.91. ServerWORKS Manager requires ClientWORKS 2.9.

4

Using ClientWORKS Alarms

4.1 Sending ClientWORKS Alarms to ServerWORKS Manager

ServerWORKS Manager uses the SNMP protocol for its primary communication with servers running a variety of operating systems. ServerWORKS Manager implements SNMP-based MIBs and an SNMP agent extension component to provide the necessary framework for SNMP network management. It allows:

- Remote control of systems through SNMP **Set** and **Get** operations.
- Setting of SNMP agent traps and alarms for the objects being managed.
- Polling of SNMP variables for the creation of console-based threshold alarms. Alarms generated by polling are set on host resource MIB variables; they do not define any SNMP traps.

ClientWORKS includes SNMP extension agents that provide DMI-based environmental and security alarms to SNMP for forwarding to ServerWORKS Manager. The following sections describe SNMP and how to configure it for use with ServerWORKS Manager.

4.1.1 How ClientWORKS Seeds Traps

The first time the system boots after ClientWORKS is installed, ClientWORKS populates the system registry with threshold information specifying conditions for firing alarms by the ServerWORKS agent. These conditions are partly obtained from the BIOS, and partly from corresponding MIBs. You can set alarms for the following sensors:

- Temperature sensor
- 3.3 Volt sensor
- 5 Volt sensor
- 12 Volt sensor
- CPU Core Voltage sensor
- CPU I/O Voltage sensor
- Secure Box status (whether system box has been opened)
- Secure On break-in count (unauthorized wake-up attempts)

For each temperature or voltage sensor, ClientWORKS sets four thresholds values:

- Low warning threshold
- High warning threshold
- Low critical threshold
- High critical threshold

The SecureBOX state defaults to closed. The SecureON break-in count is always set to zero.

ClientWORKS reads the existing threshold values set in the system registry. If the registry does not contain a value for a particular threshold, ClientWORKS reads the threshold value from the system BIOS. It stores that value in the registry and reads the value into memory.

You can overwrite the threshold values for an alarm, but it is not a good idea to do so. The hardware thresholds are set at appropriate values in the factory and you should not change them. ClientWORKS will not change an alarm registry entry that you set.

By default, alarms are not sent. You must enable the alarms first. See Section 6.1.

4.1.2 Receiving ClientWORKS Traps in ServerWORKS Manager

ServerWORKS Manager Console functions as a management console without the SNMP service. Because it uses its own SNMP stack for decoding SNMP traps, it does not require that SNMP be installed on the console machine. 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 SNMP trap entry can be found in the Services file, which is usually located in the \system32\drivers\etc\ folder of the directory where the Windows system is installed. 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
```

4.1.3 Configuring SNMP for Trap Forwarding

SNMP is a connectionless protocol. If the agent system and the management console system do not agree on the trap port number, community name, and so forth, no messages will pass between the two systems. No error will be detected and no exception message will be generated.

A system running Windows NT does not have the SNMP service installed by default. You must add the SNMP service explicitly from the control panel, then configure the SNMP agent with the correct security and access. You need to do this for both the management console and the system that will be generating the traps.

You find the SNMP setup in the NT control panel, under the network applet. You need to configure both the SNMP security and the traps. See Section 4.1.3.3.for Windows 95 directions and Section 4.1.3.4 for Windows NT directions. Before you start configuration, you need to know:

- 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

4.1.3.1 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 such an authentication failure occurs.

The default community name when the SNMP service is installed on a Windows NT-based computer is "public". You can add or remove community names as necessary. Note that 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 relation between community names and domain or workgroup names. Community names function as a shared password for groups of hosts and should be selected and changed 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 console does not recognize the community name contained in the SNMP messages from the management console, it will not accept any messages from the management console. Likewise, if the management console is not configured to recognize the community name the agent's system is using, it will not receive traps from the agent.

4.1.3.2 Configuring SNMP Traps

The SNMP agent generates trap messages, which are sent to an SNMP management console – 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 management console must accept traps from the agent system, using the same community name as the agent system

- The agent system must specify the IP address of the management console system as a trap destination, using a community name the management console system recognizes

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 defines what conditions cause a trap message to be generated, but the user controls where the message is sent.

You can identify the trap destination by name or by IP address. The trap destination must be a host that is running an SNMP manager program, such as ServerWORKS Manager or an enterprise manager.

4.1.3.3 Configuring the SNMP Agent on Windows 95

You must configure the SNMP agent with the location of the system that will receive traps. To do this, follow the instructions below.

You can use either the System Policy Editor, if it is installed on your system, or the Registry Editor.

To configure traps with the Policy Editor, follow these steps:

- Open the policies for Local Computer/Network/SNMP
- Select "Traps for Public community"
- Press the "Show..." button
- From the "Show Contents" dialog, select the "Add..." button
- From the "Add Item" dialog, type in the IP or IPX address of the system that will receive the SNMP traps
- Select OK

If you do not have the Policy Editor installed on your system, you can configure traps using the Registry Editor. Follow these steps:

- Select the following key:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SNMP\Parameters\TrapConfiguration\Public

  This key contains the list of IP or IPX addresses that will receive SNMP traps for the public community. The addresses will be specified in string variables that are labeled 1, 2, 3, and so on.
- Create a new string value:
  - Click the Public key
  - Click the Edit menu
  - Select New, and then click New String
  - Type the value name (if this is the first variable under the key, the name should be "1")
  - Press Enter
- Specify the value data:
  - Click the value name
  - Click the Edit menu, then click Modify
  - In the Value Data box, enter the value data (the IP or IPX address)
  - Click OK

4.1.3.4 Configuring the SNMP Agent on Windows NT 4.0

You must configure the SNMP agent with the location of the system that will receive traps. To do this, follow the instructions below.

- Using the Windows NT Control Panel, select the Network item
- Select the "Services" tab of the Network property page
- Select the "SNMP Service" item from the list of services
- Click the "Properties..." button
- Select the "Traps" tab
- Select the community name that you want to modify
- Click the "Add..." button under the Trap Destinations list box

- Type in the IP or IPX address of the host that will receive traps for this community
- Click the "Add" button on the Service Configuration dialog

5

Working with MIFs

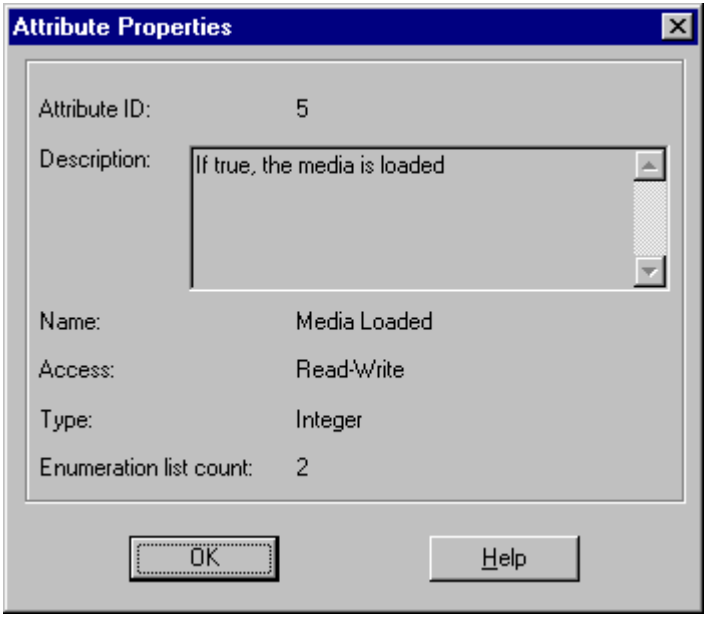
The ClientWORKS DMI Local and Remote Browsers allow you to look at the MIFs installed on a local or remote system. This chapter describes the most useful MIFs supplied by DIGITAL.

5.1 The System MIF

The System MIF file describes the basic system, listing all the components that have MIFs loaded on the system. A portion of the DIGITAL system MIF looks something like this in tree view:

Note that the information listed varies for each system, depending on what hardware and other manageable components have been installed.

To view the attributes for a particular component, click on that component. For instance, if you click on Disks, you see a list that includes information about the storage type, its total physical size and how much space is used, whether the media is loaded, and other information about the disk. To see the properties of an attribute in the list, click the right mouse button. The figure below shows the properties for the "Media Loaded" column in the previous figure.



5.2 The Monitor MIF

The Monitor MIF provides asset and other information about the monitor connected to the Windows 95 system you are browsing. This information can include the name and phone number of the monitor's primary user as well as information about the monitor's features.

To view a system's Monitor MIF through the DMI Local or Remote Browser, click on "DIGITAL Monitor MIF" in the tree view. You will see three groups:

- The ComponentID group lists information about the monitor manufacturer, part number, version of EDID supported by this monitor, serial number, and installation date.
- The Monitor Additional Informations group lists asset information such as the monitor asset tag, location, primary user, and primary user phone number.
- The Monitor Resolutions group lists the horizontal and vertical resolution, refresh rate, and vertical scan mode for each resolution that the monitor supports.

5.3 Checking SecureBOX Status

You can use the DMI Browser to view the status of the SecureBOX cover switch on DIGITAL systems which support this feature. (The system on which you invoke the DMI Browser does not need to support SecureBOX.) Start either the DMI Local Browser to view the local machine or the DMI Remote Browser to view a remote machine. Locate and expand the system you want to view, then click on "Digital Equipment Corp. PC System MIF." Choose the "Digital System Board" MIF group in the system MIF. The following information is displayed in this group:

- Motherboard Serial Number
- SecureBOX state, indicating whether the cover has been opened.

5.4 Reading Environmental Information

Newer DIGITAL systems feature temperature and voltage probes for increased security and fault protection and prevention. The temperature and voltage data is part of the System MIF, so you can view information from these probes through the DMI Browsers even from older machines that do not support these probes. (The system on which you invoke the DMI Browser does not need to support environmental probes.)

To view the environmental information, start either the DMI Local Browser to view the local machine or the DMI Remote Browser to view a remote machine. Select the system you want to view, then click on "Digital Equipment Corp. PC System MIF." From the MIF groups displayed, select either Temperature Probe or Voltage Probe.

5.4.1 Voltage Probe

The System MIF displays information for five voltage probes: one probe for each different voltage provided by the power supply and two CPU probes. Voltage levels are given in millivolts. An exact description of each field in the voltage MIF group can be obtained by right-clicking any value.

A large negative integer value (0x80000000 in decimal) in any field represents "unknown."

5.4.2 Temperature Probe

Data is retrieved from the thermal sensor on the motherboard itself. The temperature is given in 1/10th degrees Celsius. An exact description of each field in the voltage MIF group can be obtained by right clicking any value. A large negative integer value (0x80000000 in decimal) in any field represents "unknown."

5.5 The Registry MIF

ClientWORKS makes the Registry MIF available but does not install it by default. If you want to view a system's registry information, you need to install the MIF on that system. You can tailor the information display to your own needs by modifying the Registry MIF.

The following sections explain these steps in more detail.

5.5.1 Adding the Registry MIF to ClientWORKS

The Registry Instrumentation Initializer lets you initialize the instrumentation for the Registry MIF, allowing you to view registry information from the DMI Local and Remote Browsers. Follow these steps:

- Install the Registry MIF by selecting the icon  or choosing Install MIF from the File menu. Select the Registry MIF from the BACKUP folder of the folder where ClientWORKS was installed and proceed to install the MIF.
- Run the Registry Instrumentation Initializer by double-clicking the icon  . This application will run very briefly to set some context information required by the instrumentation and then exit.
- Press the Refresh button on the DMI Browser toolbar or use the Refresh command to view the newly installed keys.

If you modify the Registry MIF to add new keys, you need to reinstall the MIF and run the Registry Instrumentation Initializer again. See the next section for information about modifying the Registry MIF.

Once you have installed the MIF and run the Registry MIF initialization, you can view the data with the DMI Browser. Note that only registry entries that contain values are displayed. For example, if an entry contains only keys, and terminates without entering a value, that registry path is not displayed.

5.5.2 Modifying the Registry MIF

Figure 2 shows the Registry MIF supplied with ClientWORKS. The Registry MIF currently includes two entries:

```
\SYSTEM\CurrentControlSet\Control\ComputerName
\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
```

Both these entries are in the HKEY_LOCAL_MACHINE hive.

Other information of interest to both system administrators and users can be found under these keys:

\Hardware\Description\System

\SOFTWARE

Both of these keys are in the Registry MIF, but are commented out. You can add these keys or others of your choice simply by typing the correct registry path into the MIF. Make sure that you use a double slash for each normal slash because it is required by MIF grammar. See Figure 2 if you are unsure of the syntax.

NOTE: Please be aware that if the keys you add to the MIF contain many subkeys, it may take some time for ClientWORKS to display them.

After you finish the changes, install the MIF and run the Registry Instrumentation Initializer according to the directions in Section 5.5.1.

Figure 2: Registry MIF

```
Start Component
    Name = "Registry Instrumentation"

   Start Path
        Name = "Registry"
        Win32 = "REGCIDLL.DLL"
    End Path

    Start Group
      Name = "ComponentID Group"
      Class = "DMTF|ComponentID|1.0"
      ID = 1
      Start Attribute
            Name = "Manufacturer"
            ID = 1
            Type = String
            Value = "DIGITAL Equipment Corporation"
      End Attribute
      Start Attribute
            Name = "Product"
            ID = 2
            Type = String
            Value = "Windows NT/95 Registry Reader"
      End Attribute
      Start Attribute
            Name = "Version"
            ID = 3
            Type = String
            Value = "1.0"
      End Attribute
    End Group
```

```
    Start Group
      Name = "Key List Template"
      Class = "DIGITAL|Registry Key List|1.0"
      Key = 1
      Start Attribute
      Name = "Key Name"
      ID = 1
      Description = "The name of a key to be found within the \n"
         " Registry\n"
         "*Note* A key value near the top of the Registry tree \n"
         "    will cause the instrumentation to produce a \n"
         "    very large table of values."
      Access = Read-Write
      Type = DisplayString(256)
      Value = "HKEY_LOCAL_MACHINE"
      End Attribute
    End Group

    // The list of registry keys that is of interest to this
    // component is supplied here.
    // This allows multiple instances of this component to be
    // installed that refer to
    // different sub-trees in the registry.
    //
    // Make any changes/modifications here.

    Start Table
       Name = "Key List"
       Class = "DIGITAL|Registry Key List|1.0"
       ID = 2
       {
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\ComputerNam
e" }
       {
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Session
Manager\\Environment" }
       //{ "HKEY_LOCAL_MACHINE\\hardware" }
       // Be careful when adding the Enum subkey below it will
       // result in a HUGH amount of data being returned!
       //{ "HKEY_LOCAL_MACHINE\\Enum" }
       //{ "HKEY_LOCAL_MACHINE\\SOFTWARE" }

    End Table
```

```
    Start Group
       Name = "Key/Value Table"
       Class = "DIGITAL|Registry Key Value Table|1.0"
       ID = 3
       Key = 1,2,4

       Start Attribute
             Name = "Registry Key"
             ID = 1
             Description = "The fully qualified Key name for this
registry entry"
             Access = Read-Only
             Type = DisplayString(256)
             Value = * "Registry"
       End Attribute

       Start Attribute
             Name = "Value Name"
             ID = 2
             Description = "The name of this attribute"
             Access = Read-Only
             Type = DisplayString(256)
             Value = * "Registry"
       End Attribute

       Start Attribute
             Name = "Value type"
             ID = 3
             Description = "The registry data type string"
             Access = Read-Only
             Type = DisplayString(256)
             Value = * "Registry"
         Storage = Common
       End Attribute

       Start Attribute
             Name = "Multi Instance index"
             ID = 4
             Description = "An index for multi-valued data types"
             Access = Read-Only
             Type = Counter
             Value = * "Registry"
       End Attribute

       Start Attribute
             Name = "Value data"
             ID = 5
             Description = "The value assigned to the key"
             Access = Read-Only
             Type = DisplayString(256)
             Value = * "Registry"
       End Attribute

    End Group

End Component
```

5.6 Supplying MIF Information to Microsoft Systems Management Server (SMS)

Microsoft Systems Management Server (SMS) is system and network management software that centralizes management of computers in an enterprise network. Extending the capabilities built into Windows NT, SMS provides network administrators with a flexible method for centrally managing software and hardware on their corporate networks. Since SMS can manage a few computers or tens of thousands of computers, it is flexible and designed to meet current and future MIS requirements.

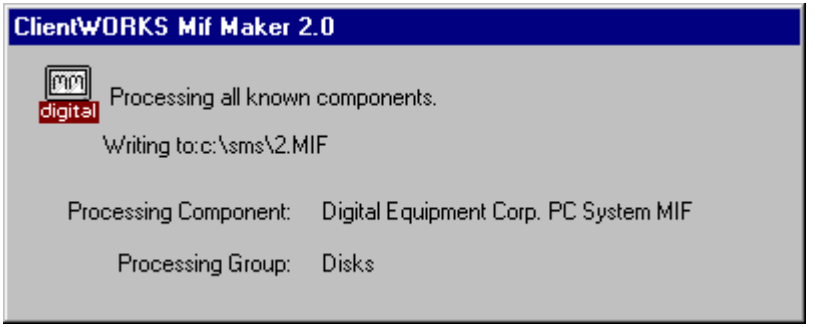
Microsoft SMS offers network administrators many powerful features in managing client PCs. It is the ideal solution for computer professionals who are concerned with the cost and complexity of building, maintaining and managing a business critical network. Many companies today are trying to implement client/server solutions but lack an expert management solution, and this is costing them money. Often companies have several locations around a single country or around the world, making centralized management even more critical. These enterprises need to take control of their distributed systems from one central location and provide proactive management solutions for their users, and SMS can help them do it.

SMS obtains information for its database by reading a Windows system's MIF file. The MIF information is pushed to the SMS server when the SMS script is executed, generally when the user logs in. The ClientWORKS MIFMaker component can automatically generate MIF snapshot files at set intervals that you, the administrator, define. In this way you can have SMS monitor changing information on the client. Your SMS administrator can use tools in SMS to control MIFMaker and collect the MIF snapshot files in its database.

The ClientWORKS MIFMaker utility writes DIGITAL MIFs to a form that can be used by Microsoft SMS. To run MIFMaker, select ClientWORKS MIFMaker from the ClientWORKS group under Windows 95 or from the Administrative Tools group under Windows NT. The MIFMaker icon appears as: 

The MIFMaker utility produces one SMS-compatible file for each installed MIF. It writes these files to the SMS directory, which SMS searches automatically.

While the MIFMaker utility is running, it displays a status window like the following:



MIFMaker updates the window as it processes each installed MIF component and each group within the MIF. It also indicates which SMS-compatible file it is presently writing.

You can use SMS to run MIFMaker automatically at a specified interval.

5.7 User-Specified Information

ClientWORKS provides a utility that allows you to specify the contents of certain fields, such as user name, user phone number, location, or system asset tag. The Set ClientWORKS Information icon in the ClientWORKS group under Windows 95 or in the Administrative Tools menu under Windows NT lets you enter this information.

In addition, since the DMI is extensible, network administrators can add other useful information into fields in the system MIF to aid in tracking client assets, including cost center or department. As long as the administrator is consistent when deploying a large number of DIGITAL systems, DIGITAL clients offer this extra level of manageability. Management tools can then search for these attributes across the LAN, WAN, or remotely-connected mobile machines.

6

Using DIGITAL SMARTMonitor

S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology) is an acronym used to describe devices that implement the S.M.A.R.T. specification. These devices provide the ability to monitor their current state and report an imminent failure. Many vendors and software developers are developing S.M.A.R.T. applications to take advantage of this technology.

The DIGITAL SMARTMonitor:

- Determines whether the host machine is S.M.A.R.T. aware
- Detects and displays information about all relevant S.M.A.R.T. components
- Monitors S.M.A.R.T. device status
- Displays visual indications of errors and alarm conditions

The user may turn the SMARTMonitor on and off, but devices remain S.M.A.R.T. enabled.

If your system includes any S.M.A.R.T.-enabled devices, the SMARTMonitor will start automatically when the system starts.

6.1 Enabling Monitoring

S.M.A.R.T. alarming allows the user to be notified about certain hardware-related conditions that indicate a potential problem:

- A S.M.A.R.T. hard drive signals an error condition

- A S.M.A.R.T. hard drive is running low on disk space
- Voltage probe values exceed thresholds
- Temperature probe values exceed thresholds
- The cover of a system with a SecureBOX switch is opened

When any of these conditions is met, the SMARTMonitor displays a dialog box to notify the user. The notification policy determines how often this warning is displayed.

For each device and event that SMARTMonitor can report on, you can configure the following settings:

- **Turn monitoring on and off.**
- **Set the notification policy**. The notification policy determines how often the user is notified when an event is triggered. Valid values are:
  - **Once per event** per day, meaning the user is notified as soon as the condition is detected. The user is not notified of the same event again until 24 hours have passed.
  - **Once per poll**, meaning the user is notified every time SMARTMonitor detects the condition. You specify the frequency of notification by setting the polling interval.
  - **Once per start**, meaning the user will be notified if SMARTMonitor detects the condition when it starts.
- **Set the polling interval for notification display.** The polling interval determines how often the SMARTMonitor displays the status of the monitored event if the notification policy for that event specifies "once per poll." The polling interval is specified in hours and minutes. Valid values are from 00:10 to 99:99; the default interval is 10 minutes.

  To have the user be notified as soon as an event takes place, select "once per event" as the notification policy.

  The polling interval setting affects only how often the notification is displayed on the user's screen. It does not change how often the ClientWORKS agent checks the value or when an SNMP alarm, if enabled, will be sent. The ClientWORKS agent monitors the hardware at a fixed 30-second interval regardless of the polling

interval. You cannot change the frequency of hardware monitoring.

- Choose whether to **display the SMARTMonitor icon**  in the system tray on the task bar.

You can specify a different notification policy for each event. For example, you can set the temperature threshold notification to "once per event," so the user is notified at once if the temperature started to rise, while setting the disk threshold notification to "once per polling interval" with a polling interval of 12:00 to check disk space usage twice a day.

6.2 The SMARTMonitor Display

6.2.1 Hard Drives

The Hard Drives page displays information for each S.M.A.R.T.-enabled disk on the system.

Note that the minimum resolution for displaying the SMARTMonitor window is 800x600. At lower resolutions, part of the screen is lost.

Drive Space Threshold specifies when the user should receive notification that the disk is getting full. The drive space threshold is specified in terms of percentage full; the minimum setting is 50% full.

All S.M.A.R.T.-enabled drives on the system are displayed in the drop-down list box. Select the number of the drive you want to view. Note that these are physical drives identified by number, not logical drives. The logical drive letter currently assigned to each physical disk is listed in the Disk Information section.

The Disk Information section also lists information about the size and physical characteristics of the selected drive. The manufacturer information section displays the manufacturer's name and the device's model number, serial number, and firmware revision.

The Drive status area displays the drive's S.M.A.R.T. status and indicates whether S.M.A.R.T. monitoring is enabled for the drive.

6.2.2 Temperature Probes

The S.M.A.R.T. Temperature Probe is a thermal sensor mounted on the system motherboard to monitor the current temperature. The system also contains a range of temperature values that determine the validity of the current temperature reading.

The Temperature Probe Page displays information for each temperature probe on the system. Temperature Probe information is retrieved from the DMI. Note that the minimum resolution for displaying the SMARTMonitor window is 800x600. At lower resolutions, part of the screen is lost.

You can view the following information:

- Temperature Scale. You can change the display between degrees Celsius and degrees Fahrenheit.
- Probe number. If a system has more than one temperature probe, you can select the probe for which you want to see information from the drop-down list box.
- Probe Information displays each probe's location, description, tolerance, granularity, accuracy, and normal, maximum, and minimum operating temperatures.
- Temperature Levels displays a gauge indicating the normal range (green), warning range (yellow), and fatal range (red) for the temperature probe. The current reading is displayed below the gauge.

6.2.3 Voltage Probes

The S.M.A.R.T. Voltage Probes are voltage sensors mounted on a system motherboard to monitor the various voltage levels. The system also contains a range of voltage values that determine the validity of the current voltage reading.

The S.M.A.R.T. Voltage Probe information is retrieved from the DMI. Five voltage probes are monitored: one for each different voltage provided by the power supply and two for the CPU. Voltage levels are given in millivolts. A large negative integer value (0x80000000 in decimal) in any field represents "unknown."

Note that the minimum resolution for displaying the SMARTMonitor window is 800x600. At lower resolutions, part of the screen is lost.

The Voltage Levels section displays a gauge indicating the normal range (green), warning range (yellow), and fatal range (red) for the voltage probe. The current reading is displayed below the gauge.

The Probe Information section displays each probe's location, description, tolerance, granularity, accuracy, and normal, maximum, and minimum levels.

The Secure Features page displays information about the system's secure features, if any. This page includes two areas, one for SecureBOX and one for SecureON.

Note that the minimum resolution for displaying the SMARTMonitor window is 800x600. At lower resolutions, part of the screen is lost.

SecureBOX is a physical switch inside the system box that is triggered when the system has been opened. The switch value is maintained in NVRAM and can be reset only via the software. The SecureBOX element displays the switch's current value. It can have one of two possible values: Open or Closed. The Clear button clears the current SecureBOX setting. You can also enable or disable monitoring and set the notification and polling intervals.

SecureON is a mechanism by which a system can be physically turned on by a remote wake-up server. The SecureON element displays the number of times an unauthorized system has attempted to wake up this system. See Chapter 7 for more information on SecureON.

6.3 S.M.A.R.T. Event Logging

The SMARTMonitor logs a range of events to log files. These files are in ASCII format and are placed in the same directory as the executable file. The following information will be logged for all events:

- Date
- Time
- User name (where possible)

The following events and information will be logged by device:

- S.M.A.R.T. drive error monitoring enabled
- S.M.A.R.T. drive error monitoring disabled

- S.M.A.R.T. error detected
- Disk space monitoring enabled
- Disk space monitoring disabled
- Disk space threshold modified
- Disk space threshold exceeded
- Notification dialog acknowledged
- Event log cleared

7

Using SecureON for Remote Wake-up

Remote Wake-up improves client manageability by allowing management applications to power up network-connected PCs from a remote site on the local segment. DIGITAL Remote Network Wake-up supports Magic Packet™ technology which is used to remotely wake up a "sleeping" PC on a network by sending a specific packet of information. To address the security risks inherent in this type of action, DIGITAL also provides SecureON, an enhancement to this wake-up technology.

DIGITAL's SecureON application generates a password which is stored in the Network Interface Chip and required to start a PC remotely. If an unauthorized wake-up is attempted, it is logged in the Remote Network Wake-up hardware.

7.1 Introduction

7.1.1 Features and Benefits

DIGITAL's Remote Network Wake-up application includes the following capabilities:

- ***SecureON feature*** offers flexibility to wake up remote clients while maintaining a secure network on standard operating systems.
- ***Magic Packet™*** technology improves client manageability, allowing remote wake-up even if a client system is powered off.

- ***Break-in count*** keeps track of unauthorized logon attempts, allowing the system administrator to be aware of repeated break-in attempts and to monitor activity to take action against further attempts.
- ***Self-synchronizing password generation*** increases security because the password is known only to the management application and is changed on each power-up cycle.

7.1.2 Client Application

On the client system, DIGITAL's Remote Network Wake-up software is invisible to the user. This application accomplishes the following:

- Identifies the client to the Remote Network Wake-up application on the server.
- Generates the new password.
- Updates the NIC with each new password.

7.1.3 Server Application (Management Console)

The management application, SecureON Management Console, typically installed on a server, provides the controlling portion of the functionality.

- Provides a user interface to wake up client systems on the local segment.
- Supports multiple clients in the wake-up database.
- Stores system information, such as wake-up times and break-in attempts, in a database.
- Manages both Magic Packet and SecureON network clients.

7.1.4 BIOS Settings

First, enable the on-board network adapter.

The wake-up mode allowing a console to remotely wake up the client is controlled by a BIOS setting in the client system. Setting this mode to one of three settings in the BIOS Setup determines if and how the console is able to wake up the client system remotely. The three possible settings are described below:

- **SecureON** - The console wakes up a client by sending a SecureON packet that the client can verify. If the packet is incorrect, or is correctly addressed and formatted but cannot be verified, the client does not wake up and logs a break-in attempt in the hardware.
- **Magic Packet** - The console wakes up a client by sending a Magic Packet to the client. This is not a secure method of remote wake-up.
- **Disabled** - The remote wake-up capability is disabled and the console cannot wake this client remotely.

Using the BIOS to set the wake-up mode prevents any other application software product from changing it.

NOTE
This BIOS setup option defaults to "Disabled."

7.1.5 Modifying the BIOS Settings

To modify the BIOS settings on the client system, follow the steps below:

1. Reboot the computer and enter Setup.
2. Highlight the "Advanced" menu.
3. Highlight "Remote Network Wake-up."
4. Press the [+] key to select one of the available options.
5. Press [Esc] once, then [Enter] twice to exit the BIOS Setup utility and to reboot the computer so changes immediately take effect.

7.2 Using Remote Network Wake-Up

7.2.1 Installation

Installation is quick and simple. Follow the instructions below to install Remote Network software on either a client or server system.

7.2.2 Client

The client application is factory-installed on every DIGITAL X86 processor-based PC system that has the appropriate hardware. If you need to reinstall the client, simply reinstall ClientWORKS.

At the end of the ClientWORKS installation, type the IP name of the system from which this client will be remotely wakened into the "SecureON Server" field. When the client reboots, it automatically contacts the SecureON server and adds itself to the client database.

7.2.3 Server (Console Management)

The server management application, SecureON Management Console, may be obtained from the DIGITAL Web site or BBS.

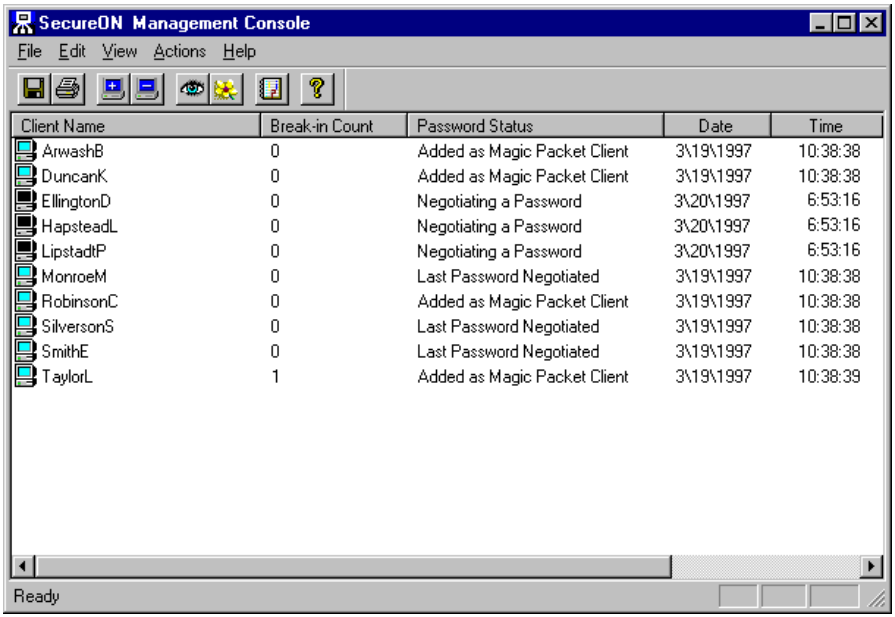
The SecureON Management Console is supported only on Windows NT systems. Follow these steps to install it on your hard drive. (The directions assume you have already downloaded the appropriate file from the Web site or BBS.)

1. Create a new, temporary directory on your hard drive. Copy the downloaded file into that directory.
2. From Windows Start, select Run.
3. Type in the name of the file (designated upon download) or use the Browse button to locate the file and click OK.
4. The installation extracts the necessary files into “Disk1” and “Disk2” directories.
5. From Windows Control Panel, double-click Add/Remove Programs.
6. Following the Windows installation steps, select SETUP.EXE in the directory you have created.
7. The installation of the Remote Network Wake-up Console Management application will begin. You’ll be prompted for a destination directory. Click OK to accept the default, C:\CLIENTWORKS\SECUREON, or use the browse button to specify a different destination.
8. When the installation is complete, a Remote Network Wake-up icon will be added to the Windows NT Administrative Tools program group.

When the SecureON Management Console is launched for the first time, the SecureON Options screen will display, with the Network tab showing. The SecureON Server name defaults to the name of the local PC. The server name is necessary to enable the console application to wake up clients on the network. For additional information about this function, see the Network Options section later in this manual.

7.3 System Administrator User Interface

The remote wake-up capability is controlled from the management console as shown below. Both Magic Packet and SecureON clients are supported from this screen.



The columns in the management console main screen present client information selected for the current view. The data displayed is as follows:

- **Computer Icon** - a black screen indicates that the client PC is Off; a blue screen indicates it is On.
- **Client Name** - the name assigned to the client PC on the network.
- **Break-in Count** - the number of break-in attempts which have been logged for this client.
- **Password Status** - the status of this client at the last Refresh or Wake-up action. This status can be one of the following:

  - Added as Magic Packet Client - This system has been added to the current view as a client which will be wakened using the Magic Packet password.
  - Last Password Negotiated - The password between client and console was last negotiated on the date and time shown.
  - Last Wakeup Packet Sent - The last wake-up packet was transferred on the date and time shown.
  - Negotiating a Password- This client is in the process of negotiating a new wake-up password and should display "Last Password Negotiated" soon.
  - Password Negotiation Failed - The last password negotiation failed for some reason (network error, remote system powered down, etc.).

- **Date** - the date of the last action listed in the password status column.
- **Time** - the time of the last action listed in the password status column.

The information shown in this screen changes each time the current view is refreshed, a wake-up command is sent, or a new client is added.

7.3.1 To add a Magic Packet client to the current view

If you need to add a Magic Packet client to the server, you can do so. Note that the SecureON clients are automatically registered when the client is installed, so you do not need to add them manually.

1. Click  (or select Add from the Edit menu).
2. Fill in the Magic Packet Client Name and MAC Address and click OK. To obtain this address, go to the command line prompt. For Windows NT, enter the command IPCONF/ALL; the physical address is the MAC address. For Windows 95, enter the command WINIPCFG; the Adapter Address is the MAC address. Enter the MAC address as a consecutive string, without spaces.
3. The client system will now be listed in the current view.

7.3.2 To remove a client from the current view

1. Select the client you wish to remove.
2. Click  (or select Delete from the Edit menu).
3. The client will be removed from the current view.

7.3.3 To wake up a client

1. From the current view, select a client by clicking the mouse on it. Multiple clients may be selected by holding down the [Ctrl] key while clicking on all the clients to be chosen.
2. Click  (or select Wakeup from the Actions menu).
3. The management application verifies that the client system is off and attempts to turn it on, if necessary. Password negotiation is attempted and if successful, the client is powered on. The computer icon to the left of the client name displays a blue screen after a successful power-on.
4. If you cannot activate a client, you should research the problem to determine the cause.

7.3.4 To refresh the view

1. From the current view, click on  (or select Refresh from the Actions menu).
2. The management application checks the clients in the current view and update their status if it has changed since the last refresh.

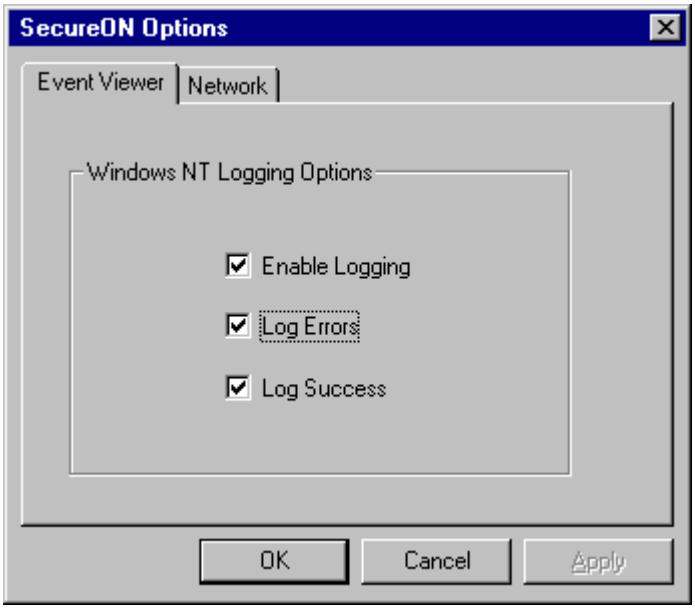
7.3.5 Setting Options

There are two options that can be set from the Options menu choice: Event Viewer/Logging options and Network options. These settings can be modified as shown below.

7.3.5.1 Event Viewer/Logging Options

The SecureON Management Console allows the system administrator to choose whether or not logging should be enabled and what information to log.

1. From the menu, select View, then Options. The following screen will display.



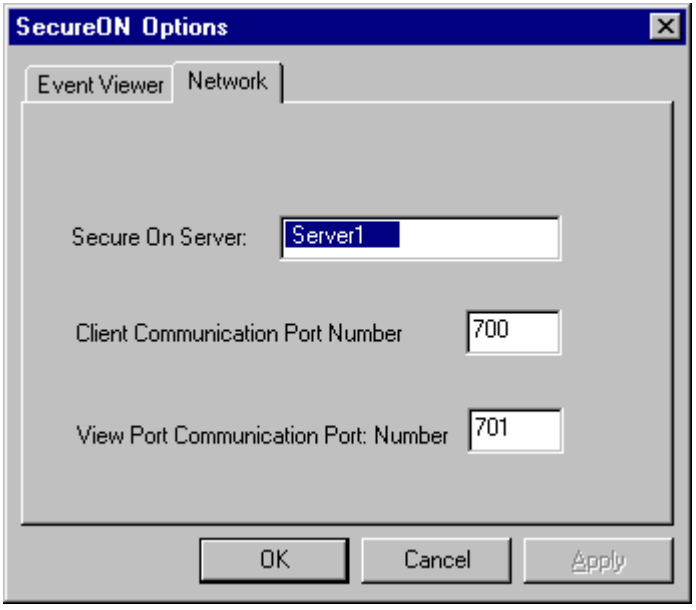
2. By default, Enable Logging and Log Errors are checked while Log Success is not.
   - If you want to disable logging of data, clear the selection box to the left of “Enable Logging.”
   - If you want to log errors, click in the box to the left of “Log Errors.”
   - If you want to log successful wake-ups, click in the box to the left of “Log Success.”
3. When the options are set as you wish, click on OK to save the changes.

Events will be logged to the system event logger. You view the events through the Event Viewer under Administrative Tools (Common) in the Start menu.

7.3.5.2 Network Options

The network options must be set to enable communication between the client and the SecureON Management Console.

1. From the main menu, select View and then Options. The following screen will display.



2. Fill in the server name in the first field.
3. Fill in the Client Communication Port Number in the second field.
4. Fill in the View Port Communication Port Number in the third field.
5. When the options are set as you wish, click on OK to save the changes.

8

Using ClientWORKS with Other System and Network Management Solutions

A variety of powerful system and network management tools, such as DIGITAL's ServerWORKS Manager, Microsoft Systems Management Server (SMS), HP OpenView, and Tivoli TME-10, can read ClientWORKS DMI management code on the client system, or receive alarms from error conditions or security breaches.

8.1 DIGITAL ServerWORKS Manager

ServerWORKS Manager, management software included with all DIGITAL servers, provides a comprehensive PC server and network management solution. With an easy-to-use graphical user interface, ServerWORKS Manager enables network administrators to manage PC servers, print and file servers, and user accounts; and configure LAN manager domains and directories. ServerWORKS Manager also enables network administrators to support distributed SNMP devices such as bridges, routers, hubs and switches from anywhere on the LAN using a Windows-based system manager station.

In addition, ServerWORKS Manager can launch the DMI Remote Browser with context to display DMI information about clients. Using the System Browser in ServerWORKS Manager, you can display SNMP information as well.

You can configure your ClientWORKS client to forward alarm and trap information to ServerWORKS Manager, as described in Chapter 4.

8.2 Microsoft Systems Management Server (SMS)

Microsoft Systems Management Server (SMS) is system and network management software that centralizes management of computers in an enterprise network. Extending the capabilities built into Windows NT, SMS provides network administrators with a flexible method for centrally managing software and hardware on their corporate networks. Since SMS can manage a few computers or tens of thousands of computers, it is flexible and designed to meet current and future MIS requirements.

Microsoft SMS offers network administrators many powerful features in managing client PCs. It is the ideal solution for computer professionals who are concerned with the cost and complexity of building, maintaining and managing a business critical network. Many companies today are trying to implement client/server solutions but lack an expert management solution, and this is costing them money. Often companies have several locations around the country or the world, making centralized management even more critical. These enterprises need to take control of their distributed systems from one central location and provide proactive management solutions for their users, and SMS can help them do it.

SMS obtains information for its database by reading a Windows system's MIF file. The MIF information is pushed to the SMS server when the SMS script is executed, generally when the user logs in. The ClientWORKS MIFMaker component can automatically generate MIF snapshot files at set intervals that you, the administrator, define. Your SMS administrator can use tools in SMS to control MIFMaker and collect the MIF snapshot files in its database.

Section 5.6 explains how to make ClientWORKS information available to SMS using the MIFMaker utility.

8.3 Integration with Enterprise-Level Network Management Tools

ClientWORKS integrates into enterprise managers several ways:

- DMI browsing only on enterprise managers that are based on Windows NT
- SNMP browsing on any enterprise manager
- Sending alarms via SNMP traps to any manager

8.3.1 Integrating DMI Browsing

Most enterprise managers, such as HP OpenView or Tivoli TME-10, allow you to add user-defined applications. By adding ClientWORKS as a user-defined application, you can launch ClientWORKS from within an enterprise manager running on Windows NT or Windows 95. See the DIGITAL web page for information. (The README.TXT file contains up-to-date web page pointers.)

8.3.2 Integrating SNMP Browsing and Alarms

The ServerWORKS Manager System Browser is integrated with Tivoli TME-10. You can then look at client data via the browser. See the ServerWORKS Manager documentation for more information.

The ServerWORKS Manager System Browser can also be integrated into HP OpenView. See the white papers on the DIGITAL web page for more information.

ClientWORKS SNMP data can be viewed by the enterprise manager's MIB browser. You will need to compile the SNMP MIB into the enterprise manager. See the ServerWORKS documentation and the DIGITAL web page for more information.

Because ClientWORKS sends traps using the SNMP protocol, it can work with enterprise network tools that use this protocol. The network tool can receive SNMP traps from alarms generated by ClientWORKS SNMP extension agents.

To send SNMP traps to an enterprise manager, see Chapter 4, and set the IP address to be that of the machine running the enterprise manager's console.

9

Using ClientWORKS with Mobile Systems

Mobile PCs present specific challenges to network administrators and LAN managers. Mobile PCs are difficult to track for several reasons:

- They are deployed across the entire enterprise
- They are only intermittently connected to the network
- They are usually distributed to salespeople, marketing or training staff, and others who travel or work in remote locations
- They often connect to the network from any of several sites, or only through dial-up connections

This chapter tells how to:

- Put together a remote management solution for mobile PC asset management
- Deploy its ClientWORKS client management software, using industry-standard DMI, in mobile environments

9.1 Using ClientWORKS with Mobile PCs

When managing mobile clients, you can take advantage of both local and remote features of ClientWORKS.

You can identify individual mobile clients for the purpose of troubleshooting, remote configuration, analysis, and support. Using ClientWORKS, MIS personnel can locally or remotely view a client's configuration parameters, check S.M.A.R.T. statuses, and solve problems more efficiently.

For more advanced system and network management applications, you can use an enterprise management application that runs reports and queries across the network, allowing you to generate graphs and usage statistics or search for specific PCs by the values stored in the MIF—for example, serial number, memory installed, or a host of other attributes.

ServerWORKS Manager enables you to view SNMP information about your network on the same console as your DMI client data, and to manage your servers as well.

Step 1: Install a connection protocol on the mobile system to allow network communication.

If you use a remote solution such as Microsoft Remote Access Services (RAS) or Dial-Up Networking that can be configured to receive incoming calls as well as initiate outbound connections, it is possible for MIS personnel to dial into remote machines and query them without user intervention. This is useful when mobile machines will be unused for any length of time, and it enables MIS personnel to make the best use of their time, and that of their users. Other popular connection protocols include Point-to-Point Protocol (PPP), Novell NetWare Connect, or Serial Line Internet Protocol (SLIP).

All methods give the user full-functioned access to the host computer, including assignment of their modem connection as a virtual drive, drag and drop file transfers using Explorer or File Manager to these drives, and simplified access to critical files used in the mobile workers' day to day tasks such as transferring price files, inventory reports, and other files from the host computer(s).

Step 2: Install hardware and software to allow your mobile system to access a local-area network.

One of the most frequently-used ways of connecting a mobile machine to remote resources and accessing corporate data is through the local area network while you are in the office, just as stationary machines are connected. Through an Ethernet/PCMCIA connection or a built-in Ethernet port replicator, mobile clients can be full peers with stationary clients.

Step 3: Install ClientWORKS.

See Section 3.4 for directions on obtaining the most recent ClientWORKS version, uninstalling prior versions, and installing the new software.

9.2 Using ClientWORKS to Troubleshoot Mobile Clients

Whether you are connecting via LAN, WAN, or remote access protocol, the procedure for using ClientWORKS is the same. With any of the connectivity options listed above, ClientWORKS can display information about the mobile client. Once the mobile client is connected via the network or modem, you can manage it and query DMI information by simply clicking on the network node assigned by the connection protocol.

ClientWORKS can also help determine why software procedures, such as an automatic download, fail. The administrator can query the machine to make sure it has enough disk space or memory. The administrator can also check the status of S.M.A.R.T.-enabled devices.

Note that although you can set alarms and configure trap forwarding on a mobile PC as you would any other PC, only alarms that are triggered while the mobile PC is connected to the network will be received by the SNMP system to which they have been directed. Because SNMP is a connectionless protocol, alarms that take place while the mobile PC is off line will not be sent, and no error will be sent to either the mobile PC or the system that is supposed to receive the trap.

9.2.1 Considerations for Asset Management

With the proliferation of mobile PCs, network administrators have had to consider new methods of software license tracking. Unlike stationary systems, mobile PCs are intermittently connected, so you typically do not know how the license is used when the mobile PC is taken on the road. Therefore, their asset management solution has to be different.

With Microsoft SMS, you can put an asset management strategy in place for these hard-to-track systems by determining how their licenses are used when they are on the road. Since these products allow you to communicate usage data in batch when next connected to the network, you can realize significant cost of ownership savings even when systems are not connected to the network.

Corporations don't want to buy more mobile computing technology than they will use, but at the same time want their sales force to have a competitive advantage – whether it be communicating with the host office, faxing quotes to customers, or obtaining the vital information they need to do their jobs. Finding the right mix of resources for your organization—how much disk space, which applications, and how much memory—becomes a critical concern when sizing mobile deployment.

9.2.2 Enhancing Security of the Mobile PC

There are a number of ways to enhance security of DIGITAL mobile computers using ClientWORKS and popular management tools. ClientWORKS DMI information includes the system serial number, which can be used to track the location of specific mobile PCs. This unique identifier can be used to track individual systems connected anywhere on the WAN, and those that are only occasionally connected. Therefore, your administrators can set 'traps' for mobile clients that have been reported lost or stolen, for instance.

9.2.3 Setting Triggers for Remote Dial-Ins

With Microsoft SMS, it is possible to set triggers for remote dial-ins. For instance, if a machine has not logged on to the network in two weeks, this fact can trigger a report automatically. Similarly, if clients have been reported missing, you can include these missing serial numbers in an SQL database, set up a notification log, or run reports later to determine if any of these machines have logged on to the network.

Index

Agent
  definition of, 16
  extension. *See* Extension agent
  operations, 16
Asset Management for mobile PCs, 67
Audience
  Preface, vii
BIOS setting
  for SecureON, 52
ClientWORKS
  documentation, ix
  seeding SNMP traps, 28
Community names
  default, 30
  definition of, 30
  in SNMP messages, 30
Component Interface
  definition of, 15
  function of, 15
Configuring SNMP
  agents, 29
    on Windows 95, 31
    on Windows NT, 32
  for Trap Forwarding, 29
  security, 30
  traps, 30
Desktop Management Interface. *See* DMI
Desktop Management Task Force, 13
DIGITAL Monitor MIF, 36
DIGITAL Server Agent, 18
  trap forwarding from, 18
DIGITAL SMARTMonitor
  displaying icon for, 46
  event logging in, 49
  features, 45
  SecureBOX status, 49
  SecureON status, 49
  setting notification policy, 46
  setting polling interval, 46
DIGITAL SNMP Agent Extension, 18
DMI
  components, 14
  features of, 13
  implementation, 14
DMI Browsers, 15, 22, 37, 39
  viewing environmental probes, 37
  viewing Registry MIF, 39
  viewing SECUREBOX status, 37
DMI components
  Component Interface, 15
  definition of, 14
  in MIF displays, 23
  in Monitor MIF, 37
  indications, 15
  management application, 15
  Management Interface, 15
  Service Layer, 15
DMI Local Browser
  starting, 22
  using, 22
  viewing environmental information, 38
  viewing Monitor MIF, 36
  viewing SecureBOX status, 37
DMI Remote Browser
  from ServerWORKS Manager, 61
  starting, 22
  using, 22
  viewing environmental information, 38
  viewing Monitor MIF, 36

viewing SecureBOX status, 37
Environmental data
viewing from DIGITAL SMARTMonitor, 48
viewing from DMI Browsers, 37
Event logging
for SecureON Management Console, 58
Extension agent, 17
Get Next operation, 16
Get operation, 16
HP OpenView, 18, 61, 63
Indication
definition of, 15
Installing the Registry MIF, 39
IP port number
for SNMP traps, 29
Keyboard Conventions
Preface, viii
table, viii
Magic Packet™ technology, 51
Magic Packet™ technology, 52, 53, 55, 56
adding clients to SecureON Management Console, 56
Manageable attributes
definition of, 14
Manageable products
definition of, 14
Management application
definition of, 15
Management console
definition of, 16
ServerWORKS Manager, 29
trap destination, 30
Management information bases. *See* MIBs
Management Interface
definition of, 15
function of, 15
MIBs
definition of, 16
information contained in, 16
vendor-supplied, 16
Microsoft SMS, 11, 12, 15, 21, 43, 62
managing mobile clients with, 68
setting triggers for remote dial-ins, 68
using with ClientWORKS, 62
Microsoft Systems Management Server. *See* Microsoft SMS
MIF database
definition of, 14
MIF file
definition of, 14
MIF information
for Microsoft SMS, 36, 43
MIFMaker utility, 12, 15, 43
running, 43
status window, 44
Mobile PCs
enhancing security of, 68
using ClientWORKS with, 65
Modifying the Registry MIF, 39
Monitor MIF, 23, 36
Network options for SecureON Management Console, 59
Prerequisites
Preface, vii
Registry Instrumentation Initializer, 39
for modified registry MIF, 40
Registry MIF, 38
figure, 40
installing, 39
modifying, 39
Remote dial-ins
setting triggers for, 68
Remote Network Wake-up
installing, 53
Remote Network Wake-up application, 22, 51, 52, 54
S.M.A.R.T. status, 47
S.M.A.R.T. technology
definition of, 45
S.M.A.R.T. Temperature Probe, 48
S.M.A.R.T. Voltage Probes, 48
S.M.A.R.T.-enabled devices, 22, 45, 67
Secure Features, 12, 49
SecureBOX status
in SMARTMonitor display, 49

viewing from system MIF, 37
SecureON, 51
BIOS settings, 52
clients, 55, 56
enabling network adapter, 52
packet, 53
SecureON Management Console, 52, 54, 55
adding Magic Packet clients, 56
event and logging options, 58
main screen, 55
network options, 59
refreshing the view, 57
removing client, 57
waking up client, 57
SecureON status
viewing in SMARTMonitor, 49
ServerWORKS Manager
alarming, 11
as trap destination, 31
ClientWORKS in, 11
DMI and SNMP, 18
integration with ClientWORKS, 12
integration with HP OpenView, 63
integration with Tivoli TME-10, 63
launching DMI Remote Browser from, 61
receiving ClientWORKS traps, 61
required ClientWORKS version, 25
sending ClientWORKS alarms to, 27
using with ClientWORKS, 61
with mobile clients, 66
ServerWORKS Manager Console, 18
Service Layer
definition of, 15
function of, 15
Set ClientWORKS Information tool, 44
Set operation, 17
SNMP agents
configuring, 29
configuring on Windows 95, 31
configuring on Windows NT, 32
role in trap forwarding, 31
SNMP management console. *See* Management console
SNMP messages
community names in, 30
Send Authentication Trap, 30
SNMP operations
Get, 16
Get Next, 16
Set, 17
Trap. *See* SNMP traps
SNMP service, 25, 29, 30
SNMP setup, 29
SNMP stack
ServerWORKS Manager, 29
SNMP system components, 16
SNMP traps
configuring, 30
destination, 31
forwarding, 30
IP port numbers, 29
seeding, 28
Specifying field contents, 44
Subagent. *See* Extension agent
System MIF, 23, 35, 37, 38
viewing environmental data, 37
Temperature Probe, 38, 48
display, 48
threshold values, 46
Temperature Probe information, 48
Terminology
Preface, vii
Thermal sensor. *See* Temperature probe
Tivoli TME-10, 18, 61, 63
Trap forwarding, 30
Trap messages, 30
trap destination, 30
Trap operation, 17
Voltage probes, 37, 38, 48