ClientWORKS 2.91 Readme
for DIGITAL PCs
3-September-1997

README.TXT file for ClientWORKS Manager Version 2.91

This README.TXT is intended for the ClientWORKS user.
Its purpose is to provide additional product information and
corrections to the user documentation.

IMPORTANT

If you need to reinstall ClientWORKS, it is important that you get the most recent version. You can conveniently download the most recent version from:

- The DIGITAL web site at http://www.pc.digital.com or http://www.pc.digital.com/~ftp

  Click on "Products"

  Locate the pointer to the ClientWORKS page under "Software Products, Client and Server Management Tools"

- DIGITAL Bulletin Board Services (BBS):

  In the United States, call 1-978-496-8800

  In Europe, call (33) 92 960312

Note that before you upgrade to Version 2.91 of ClientWORKS, you must deinstall
previous versions. It is critical that you deinstall previously installed
versions in the order shown:

1. DMI Browser
2. SMARTMonitor
3. SNMP

When you deinstall the last ClientWORKS component (DMI Browser, SMARTMonitor,
or SNMP), you must select "YES" for all the dialogs that display the message,
"Are you sure you want to delete all files and components?"

After you deinstall, you must reboot before proceeding with the installation
of ClientWORKS Version 2.91.

What Is New in ClientWORKS 2.91

The following features were updated or improved in Version 2.91 of ClientWORKS
Management Suite. These features are available on all systems running

Windows 95.
For Windows NT, these features apply only to the DIGITAL PC 5100:

-- DIGITAL SMARTMonitor

The DIGITAL SMARTMonitor has been updated to monitor temperature and voltage probes in computers so equipped. The SMARTMonitor now also displays the number of attempted breakins. In addition, support for SecureBOX has been added. SecureBOX supports monitoring when the computer enclosure has been tampered with.

The SMARTMonitor runs on any platform with Microsoft Windows 95 or Windows NT, but on platforms that have no SMART functionality, the SMARTMonitor exits immediately.

-- DIGITAL SNMP Agents

Two new SNMP agents have been added to the ClientWORKS Management Suite. These agents provide the same monitoring support as the DIGITAL SMARTMonitor, only through SNMP. Network administrators can now monitor the current temperature, voltage, and SecureBOX state of a ClientWORKS computer remotely, using the SNMP protocol. These SNMP agents are tightly integrated with the DIGITAL ServerWORKS Manager package, which provides world-class support for managing your network.

What Is New in ClientWORKS 2.9

Version 2.9 of the ClientWORKS Management Suite includes several new features.

The following features apply to IDE hard disks on Windows 95 systems:

-- DIGITAL SMARTMonitor

DIGITAL SMARTMonitor is an application designed to display SMART data from the IDE hard disks. In case of a disk failure, SMARTMonitor provides visual alarming and suggests actions to prevent data loss.

-- SMART MIF

Hard disk SMART information can be viewed from the ClientWORKS Browser using the SMART MIF. Users do not need to activate the SMARTMonitor each time they want to view drive information.

The following feature applies to Windows 95 systems:

-- Monitor MIF

The Monitor MIF provides asset data and other information about the monitor connected to a browsed system. Information such as the monitor's primary user, the user's phone number, and the monitor asset tag can be viewed.

The following features apply to the DIGITAL PC 5100 only:

-- SecureBOX information

Information about the status of the SecureBOX cover switch on DIGITAL PC 5100 systems can be viewed in the ClientWORKS DMI Browser on Windows 95 and Windows NT systems.

-- Environmental information

The user can view temperature and voltage information from the environmental sensors of the DIGITAL PC 5100 system on Windows 95 and Windows NT systems.

-- SecureON (Secure remote wake-up)

The system administrator can remotely wake up clients in a secure fashion.

DIGITAL SMARTMonitor

The DIGITAL SMARTMonitor provides information about the SMART IDE hard disks, information about the SMART status of the disks, and the ability to set up and configure the drive space threshold. It also visually alarms the user when a drive failure is predicted.

During the ClientWORKS installation, the DIGITAL SMARTMonitor is optionally installed and set up to start automatically at boot time.

The DIGITAL SMARTMonitor can be configured to display an active icon in the system tray to represent the current status of system SMART devices.

Note that if you set one or more polling intervals to a value less than 10 minutes, you may negatively impact the performance of other applications you are running.

The SMARTMonitor must be run at a minimum resolution of 800 x 600. If you run the monitor at 640 x 480, the display occupies the entire screen.

SMART MIF

The SMART MIF supports the Windows 95 operating system and the IDE hard disk

interface.

The SMART MIF can be viewed using the ClientWORKS DMI Browser. Start either
the ClientWORKS DMI Local or ClientWORKS DMI Remote Browser, select a machine
and/or click on "Digital Equipment Corporation S.M.A.R.T MIF."

The following information is provided:

-- ComponentID Group

This is information about the SMART instrumentation itself.

-- Drive Attributes

For each SMART drive, the manufacturer information, model number,
serial number, Firmware Revision, and SMART status is provided.

Monitor MIF

The Monitor MIF can be viewed using the ClientWORKS DMI Browser. Start either the DMI Remote Browser for remote viewing, or the DMI Local Browser
for local browsing, and click on "DIGITAL Monitor MIF." The following information is provided:

-- ComponentID

This is information about monitor manufacturer, part number, the version of EDID supported by this monitor, serial number, and installation date.

-- Monitor Additional Information (asset information)

This information includes monitor asset tag, location, primary user, and primary user phone number.

-- Monitor Resolutions

For each resolution the following information is given:

horizontal and vertical resolution
refresh rate
vertical scan mode

SecureBOX Information

The status of the SecureBOX cover switch of the DIGITAL PC 5100 desktop systems can be viewed by the ClientWORKS DMI Browser in the System MIF by doing the following:

-- Invoke the ClientWORKS DMI Local Browser
-- Click on "Digital Equipment Corp. PC System MIF"
-- Click on the "Digital System Board" MIF group.

The following information is displayed in this group:

Motherboard Serial Number
SecureBOX State (status of the cover switch)

Note that each time a box is opened, you must reset SecureBOX before you can set alarms.

Environmental Information

The DIGITAL PC 5100 system features temperature and voltage probes for increased security and fault protection/prevention. Information from these probes can be viewed by ClientWORKS. The temperature and voltage data is part of the System MIF. To view this information, do the following:

-- Start up either the DMI Local Browser for local viewing or the DMI Remote Browser for remote viewing.
-- Click on "Digital Equipment Corp. PC System MIF"
-- From the MIF groups displayed, select either "Temperature Probe" or "Voltage Probe"

The following information is displayed:

Voltage Probe

Five voltage probes are monitored: one 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. The following information is retrieved for each probe:

Location
Description
Status
Current voltage
Voltage nominal level
Normal maximum and minimum according to specification
Maximum and minimum measurable in a correctly functioning system
Non-critical lower and upper threshold
Critical lower and upper threshold
Non-recoverable lower and upper threshold
Voltage probe resolution, tolerance, and accuracy

For Voltage Probe Status, the following values can occur:

-- OK

The voltage level is within specified maximum and minimum.

-- Non-critical

The voltage level is outside specified maximum and minimum,
but still within the non-critical region.

-- Critical

The voltage level is outside the noncritical region. Action needs to be taken to prevent system failure: turn the system off. The automatic power-off feature is invoked
if the user does not switch off the system.

-- Non-recoverable

The voltage level is beyond critical. Severe damage to the
system components will occur due to too high voltage.

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

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. The following data is displayed:

Location
Description
Status
Current temperature
Temperature nominal level
Normal maximum and minimum according to specification
Maximum and minimum measurable in a correctly functioning system
Non-critical lower and upper threshold
Critical lower and upper threshold
Non-recoverable lower and upper threshold
Temperature probe resolution, tolerance, and accuracy
FRU group index and operational group index

For Temperature Probe Status, the following values can occur:

-- OK

The temperature level is within specified maximum and minimum.

-- Non-critical

The temperature level is outside specified maximum and minimum,
but still within the non-critical region.

-- Critical

The temperature level is outside the noncritical region.

Action
needs to be taken to prevent system failure: turn the system
off. The automatic power-off feature is invoked if the user
does not switch off the system.

-- Non-recoverable

The temperature level is beyond critical. Severe damage to
the system, that is, CPU component damage, will occur.

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

SecureON (Secure remote wake-up)

The DIGITAL PC 5100 desktop systems come with the SecureON Client software
factory installed. The system administrator can remotely wake up the desktops
in a secure fashion.

At the end of the ClientWORKS installation, the SecureON Client software asks for the location of the SecureON Management Server. The system name
of the server needs to be entered.

The SecureON console application, which supports remote wake-up of clients,
is available on the DIGITAL web site. The SecureON documentation describes
how to enable the client for remote wake-up.

Note that SecureON works only on the local segment.

Updating User Information Reported by the ClientWORKS Suite

An applet is provided with the ClientWORKS DMI Browser to allow the user to update some information reported by the ClientWORKS application to both
local and remote users. You start the applet by double-clicking the "Set ClientWORKS Information" icon. You then can enter your user name, phone
number, location, asset tag, chassis serial number, and the SecureON Management
Server name. The information is stored for later remote or local retrieval.

SNMP Subagent Support under Windows 95 and Windows NT

A host resource subagent is now included with the ClientWORKS DMI Browser
which reports those data items common to both the Host Resource MIB and

the System MIF.

The installation now expects the Microsoft SNMP agents to be installed prior
to installing ClientWORKS. The installer may choose not to install the ClientWORKS SNMP subagents, or may install them at a later date.

ClientWORKS requires SNMP. If the installer has chosen to install the ClientWORKS SNMP subagent but has not installed the Microsoft SNMP master
agent, a message is displayed to indicate that SNMP is required.

To Install SNMP on Windows 95:

-- Open the Control Panel and click on the "Network" icon

-- Click on "Add"

-- Choose "Select Service" as the type of network component to be installed

-- Click on "Add"

-- Click on "Have Disk"

-- Install from the "ADMIN\NETTOOLS\SNMP" subdirectory on the Windows 95 CD.

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

To Install SNMP on Windows NT 4.0:

-- 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 install the ClientWORKS SNMP agents, run the ClientWORKS setup program
located on the DIGITAL System Software CD in the following directory:

\apps\cw\disk1\setup.exe

-- When prompted, select "Install ClientWORKS SNMP subagents"

-- Deselect "Install ClientWORKS DMI Browser" (and "SMARTMonitor" when
applicable)

-- Deselect "SMART"

-- Continue with setup, installing ClientWORKS SNMP sub agents only

Enabling SNMP Trap Support under Windows 95 and Windows NT

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

For Windows 95:

Use either the System Policy Editor, or the Registry Editor.

Using the System Policy Editor:

-- 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'

Using the Registry Editor:

-- 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 by clicking the Public key, click the Edit menu, point to New, and then click New String, type the value name, and press Enter. (If this is the first variable under the key, the name should be "1".)

-- To 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), then click OK.

For Windows NT 4.0

-- Using the Windows/NT Control Panel, select the Network item

-- Select the "Services" tab of the Network property page

-- Click the "SNMP Service" item from the list of services

-- Hit the "Properties..." button

-- Select the "Traps" tab

-- Select the community name that you want to modify

-- Hit 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

-- Hit the "Add" button on the Service Configuration dialog

Installing the Registry MIF

In the BACKUP MIFs subdirectory where the ClientWORKS DMI Browser was installed, you will find the Registry MIF. This MIF allows the ClientWORKS DMI Browser to report information found in either the Windows 95 or Windows NT registry.

To install the Registry MIF, you must first decide which keys you want to report on. Any changes to the keys you want to view should be made in the "Key List" table found at about the midpoint of the MIF. Currently the table contains two entries, although it can contain as many as you want.

The current entries are:

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

Both of these are in the HKEY_LOCAL_MACHINE hive.

Other information of interest to both system administrators and users can be found in:

\Hardware\Description\System
and in
\SOFTWARE

Both of these keys are in the Registry MIF, but they 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;
this is required by MIF grammar. See the samples if you are unsure of the
syntax.

NOTE: Please be aware that if you add keys to the MIF that contain many subkeys,
it may take some time for the Browser to display them. Don't be alarmed by this.
The delay is normal.

Once you have made modifications and/or added any keys, install the MIF by
selecting the "Install MIF" icon (a computer with a red down arrow above it)
and enter the path to the modified MIF. Review the displayed MIF and hit the
install button if the MIF is correct.

After you have modified the registry MIF and installed it, run the registry
MIF initialization application. Double click the icon marked "Registry
Instrumentation Initializer." This application will run very briefly to set
some context information required by the instrumentation and then exit. If you
modify the Registry MIF to add new keys and reinstall it, you need to rerun
the "Registry Instrumentation Initializer."

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

The Registry MIF is now installed and available.

Uninstall and Pentium(P5) Based Legacy Celebris GL Systems

On legacy Celebris systems, Celebris GL adds one line to your CONFIG.SYS
under Windows 95. This driver sets up state information for the system
instrumentation. You need to remove this driver manually after uninstalling
the ClientWORKS application.

Using your favorite editor, simply delete the "DEVICE=...\DECDMI.SYS" from your
config.sys file. You should also delete the state information file which
is created by this driver at boot time from your root directory. This file is
saved as c:\decdmi.dat.

Deleting "Unused" DLLs

If you receive notification that a DLL is unused and are asked whether you want to delete the DLL, answer "No to All."

Notes on the ClientWORKS Browser (Either Local or Remote)

When you access a remote node using the Remote Browser, selecting a node may take much longer then expected. This is normally due to processing that is taking place at the remote end. Eventually the remote node will respond.

When you view a group that contains attributes which are listed as unsupported, the editor will not display the unsupported column, causing the attribute data to align under the wrong heading. This problem does not exist in any of the supplied MIFs, but it may occur if you install externally provided MIFs.

In certain situations, ill-behaved instrumentation can hang the service layer, causing the ClientWORKS Browser to return an error, and afterwards, each time you access the service layer, the Browser appears to browse forever. In this case, simply shut down the Browser and service layer manually by either rebooting (under Windows 95) or stopping and restarting the DMI SL service (under Windows NT), and normal functionality will be restored. Make sure to note the group and attribute you were accessing when the error occurred and report it to the appropriate vendor.

Notes on Communicating with a Remote Machine Running ClientWORKS

In order for two machines to communicate, they must be running at least one communications protocol in common. If you experience a problem connecting two machines together, make sure that they are running a protocol in common.

To determine which protocols are in use on a given machine, run the XDMIEPT application. This is a command-line application which should be run at a DOS prompt. It displays the currently registered endpoints. Make sure that one or more endpoints are shared. Also note that LRPC stands for local RPC (remote procedure call) and is used only from one application to another on the same machine.

For best interoperability, DIGITAL strongly recommends that you always install
TCP/IP in addition to any other protocol stacks.

Trademarks