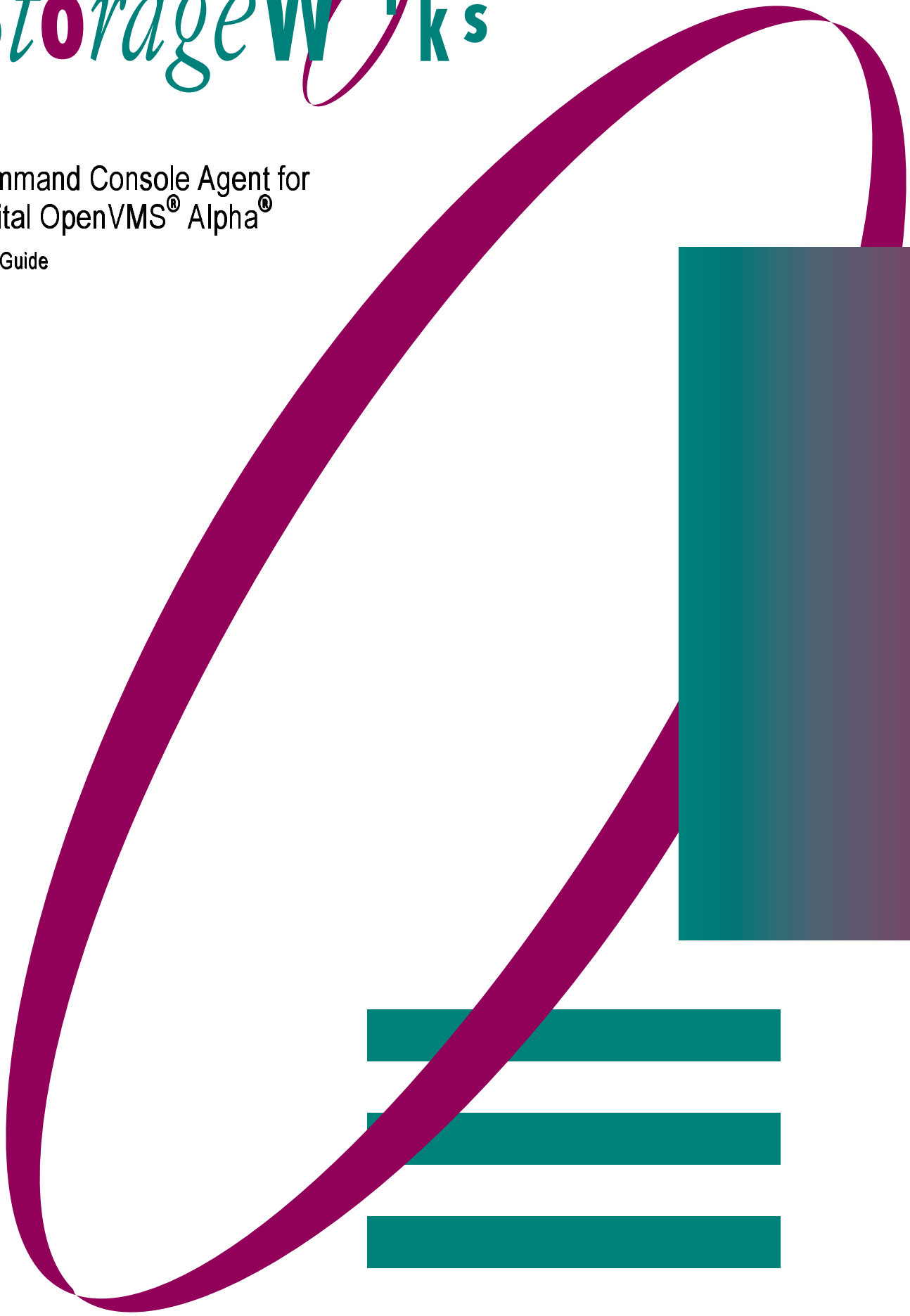
StorageWorks™

Command Console Agent for Digital OpenVMS® Alpha®

User Guide



Part Number: AA–C11DV–UB

digital™

November, 1996

While Digital Equipment Corporation believes the information included in this manual is correct as of the date of publication, it is subject to change without notice. Digital makes no representations that the interconnection of its products in the manner described in this document will not infringe existing or future patent rights, nor do the descriptions contained in this document imply the granting of licenses to make, use, or sell equipment or software in accordance with the description. No responsibility is assumed for the use or reliability of firmware on equipment not supplied by Digital or its affiliated companies. Possession, use, or copying of the software or firmware described in this documentation is authorized only pursuant to a valid written license from Digital, an authorized sublicensor, or the identified licensor.

Commercial Computer Software, Computer Software Documentation and Technical Data for Commercial Items are licensed to the U.S. Government with Digital's standard commercial license and, when applicable, the rights in DFAR 252.227-7015, "Technical Data—Commercial Items."

© Digital Equipment Corporation, 1996.

Printed in U.S.A.
All rights reserved.

StorageWorks, Alpha, OpenVMS, and the Digital logo are trademarks of Digital Equipment Corporation. All other trademarks and registered trademarks are the property of their respective holders.

Revision History		
Revision	**Date**	**Content**
A	10/96	Version 1.1a release
B	11/96	Version 1.1c release

Contents

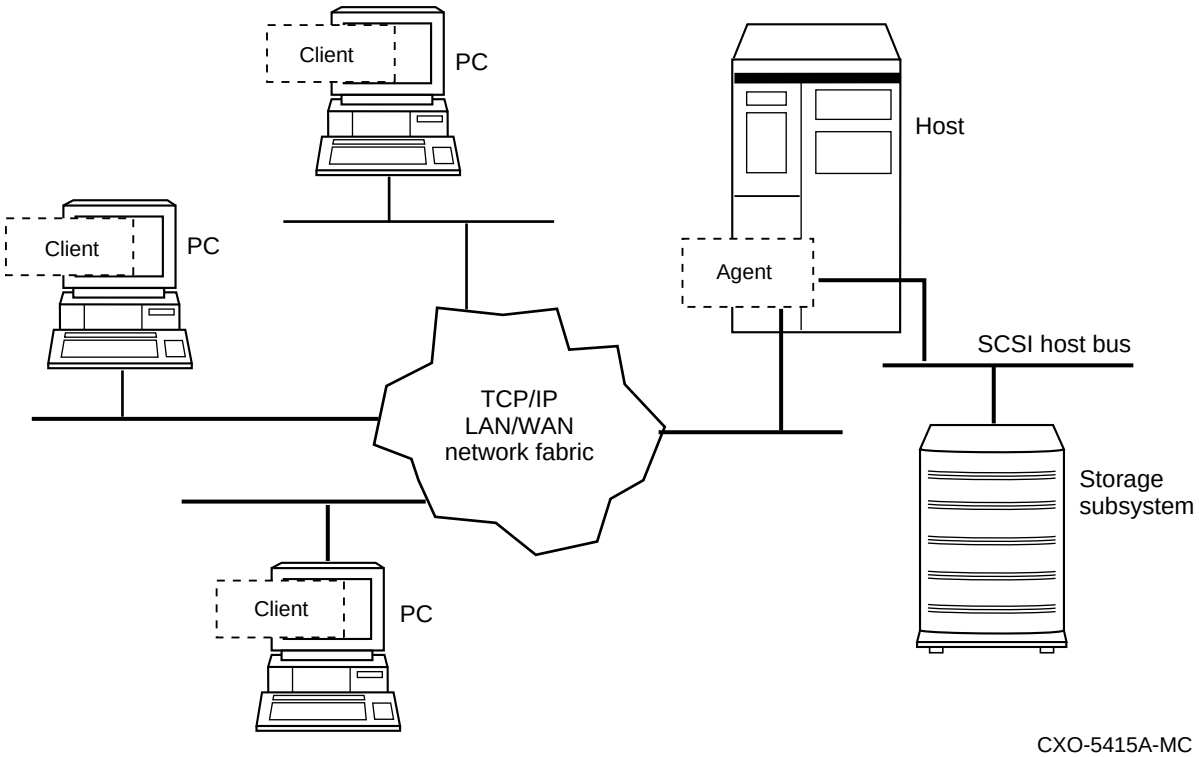
Command Console Agent for Digital OpenVMS® Alpha®

This guide describes Command Console Agent for Digital OpenVMS Alpha. It includes a product description, minimum system requirements, and installation and configuration instructions.

Product Description

Command Console Agent for Digital OpenVMS Alpha is a companion application to the Command Console Client graphical user interface (GUI) program. Agent serves as Client's assistant in configuring, operating, and monitoring your host's storage subsystems. Agent runs on your host system as a server application. It connects to Command Console Client sessions via the TCP/IP network protocol, as shown in Figure 1.

Figure 1 Command Console Client/Agent Connection



Command Console Agent provides a network connection between a host storage subsystem and any number of Command Console Client sessions running on either the host or other remote systems. Agent provides access protection on a network address-by-network address basis. You can configure Agent to

allow, for instance, one Client session complete configuration access to the storage subsystem, while another Client session might only be allowed monitoring capability.

You can also use Agent for asynchronous fault notification. The program monitors your host’s storage subsystems and sends notification messages to all Client sessions connected to it the moment a fault occurs. You can configure Agent to use TCP notification to Client and SNMP notification to an SNMP-compatible monitoring application.

Minimum System Requirements

Agent requires the minimum host system resources shown in Table 1. The program is designed to operate with Command Console Client Version 1.1 for Windows NT® and Windows 95®.

Table 1 Minimum System Requirements

Host Feature	Requirement
Architecture	Digital Equipment Corporation Alpha® platform, 1000 blocks free space on system disk
Operating System	Digital OpenVMS Alpha version 6.2, 7.0, or 7.1
Controller Compatibility	StorageWorks 2 or 6-port controller running operating firmware Version 3.0 or higher.
Support software	Digital TCP/IP Services, version 4.0 (or later) for OpenVMS.

Installing Command Console Agent

Agent is Client's network assistant. You'll need one Agent program running on each host system you wish to connect to Client over the network. The Agent installation program installs the Agent program of your choice at the host system of your choice.

NOTES

You can install an Agent for Digital OpenVMS only from a Windows NT system with a CD-ROM. Further, you can only install this Agent over a network connection to a remote host.

You can run the Agent installation program on either Intel® or Digital Equipment Corporation Alpha® Windows NT platforms.

Installing an Agent

Here's how to install an Agent in one of your host systems:

1. Your host's system resources must meet the minimum requirements to run the Agent program you wish to install. The minimum system requirements for each Agent type are listed in its user guide on the accompanying CD–ROM. Before going on, verify that your host system will support the Agent you wish to install.
2. Before you can install an Agent, at least one logical volume must exist on each storage subsystem you wish to connect to. If your subsystems do not each contain at least one volume, use your operating system utilities to connect to your controller's command line interpreter (CLI) interface to create one. Subsystems without at least one logical volume are invisible to Agent and the host operating system.
3. Place the Command Console CD–ROM in your local system's CD–ROM drive.
4. Open the \AGENTS subdirectory in File Manager.
5. Double click the INSTALL.BAT file.

   The installation program begins, displaying a series of windows in which you must enter configuration information for your Agent.
6. Enter the appropriate information in each window, until you have completed the installation of your Agent.

   Click the *Info* button on any window for helpful information on its use.

   Be sure to read the special instructions included in some *Info* windows. In addition, see "Special Digital OpenVMS Alpha Agent Installation Instructions" below for more information.

Special Digital OpenVMS Alpha Agent Installation Instructions

When you run the Agent installation program from Windows NT, and you select the OpenVMS Agent type, the program performs the first part of the installation process over the network. You must have access to the system account on the remote host, your local system must have network access to the remote system, and the remote host must have Digital TCP/IP Services for OpenVMS installed and configured for FTP and Telnet service.

The installation program prompts you for the remote host's name, along with your personal user name and password. It then uses the file transfer protocol (FTP) to transfer a compressed set of installation files named "DEC-AXPVMS-SWCC-V*xxxx-xx*.PCSI" to the remote host's SYS$MANAGER: directory.

When this file is transferred, the program opens a separate Telnet window on your local system. You must use the Telnet window to complete the remaining steps of the Agent installation.

Using the Telnet Window to Complete Your Installation

Perform the following actions in the Telnet window to complete your Agent installation. Use the special instructions included with the text-based prompts for assistance as you go along.

1. Log on to the remote host system using the *system* user name and password.
2. Run the Agent installation program at the host. At a DCL prompt, enter "PRODUCT INSTALL SWCC /SOURCE=[]".
3. Follow the text-based prompts. Use the default value for each option.
4. Agent is now installed on your host.

Configuring Agent Using the Telnet Window

Once Agent is installed on your host, you must configure it. Using the Telnet window, run the configuration program by entering "@SYS$MANAGER:SWCC_CONFIG" at the DCL prompt.

When you run the configuration program on a newly installed system, the program prompts you for the following information:

- The names of Clients authorized to access the Agent, the Clients' access privileges, and the type of notification to be used in the event of a change in storage subsystem status.
- The names and OpenVMS device specifications of the storage subsystems you wish to connect to the Agent, along with a time interval to be used by the Agent when monitoring each subsystem.
  Note that subsystem names are arbitrary and are only used by the Client as a way to reference specific subsystems. The OpenVMS device specification, however, must refer to a valid "DK" device on a directly attached 2 or 6-port controller. (As mentioned previously, at least one such device (that is, logical volume) must exist on each system before you can operate your Agent.)
- A 4–16 character password to be used by Clients to access this Agent and its associated subsystems.
- The method by which your Agent is to be started. You can choose to immediately start your Agent from the configuration program, to activate it automatically each time the host is

booted, or to run it as an auxiliary service of UCX. The UCX Service option is the default, and it starts the Agent on demand when any Client accesses the Agent.

Note that your Agent is available on all the nodes in your cluster. After installation, however, you must individually configure the Agent on each node on which it is to run. Storage subsystems to be accessed by an Agent on any particular node must be directly attached to that node. Subsystems that are directly attached to two nodes can be accessed by either node, but not simultaneously. Time sharing is enforced automatically by OpenVMS cluster locking.

Installing Additional Agents

You may want to install Agents on your host systems in other clusters. To install more Agent programs, simply repeat the procedure above, using the appropriate host system name and Agent type for each session.

Agent Documentation for Alpha® Platforms

If you're running the Agent installation programs on a Digital Equipment Corporation Alpha® Windows NT platform, you cannot install the Acrobat Reader. The *\DOCS* subdirectory on the CD–ROM contains Agent user guides in Word for Windows format for use in this situation.

Running Command Console Agent

Your Agent runs as an OpenVMS process called “SWCC$AGENT”. You can use the Agent configuration program to control the execution of this process. The program offers the following options for running Agent:

- You can choose to immediately start or stop your Agent.
- You can choose to start your Agent automatically each time the host is booted.
- You can choose to run your Agent as an auxiliary service of UCX. The UCX Service option is the default, and it starts the Agent on demand on any Client access.

For information on using the configuration program, see “Reconfiguring Command Console Agent”, on the next page.

Reconfiguring Command Console Agent

You can reconfigure previously installed Agents using the Agent configuration program. To run the configuration program, enter “@SYS$MANAGER:SWCC_CONFIG” at a DCL prompt and use the menus to choose the options you wish to modify.

You can also use the Agent configuration program to control the execution of your Agent. See “Running Command Console Agent”, on the previous page, for more information.

Note that configuration changes do not immediately take effect as long as Agent is running. To place configuration changes in effect, you must stop Agent and restart it, using the menu options provided.

Uninstalling Command Console Agent

You can remove an Agent using the Agent configuration program. To remove an Agent, enter "@SYS$MANAGER:SWCC_CONFIG" at a DCL prompt and choose the Agent uninstall menu option.

Note that this option stops all instances of the Agent on all cluster nodes. It also deletes all Agent files, except for the .PCSI file that was transferred to your host over the network when the Agent was originally installed.

If you must reinstall Agent for some reason, use the configuration utility to first uninstall any existing copies of the program. Then proceed with your installation, as described in "Installing Command Console Agent".

For Advanced Users

The fastest and most user-friendly method of configuring an Agent is to use the configuration program. Use of the program is the recommended method for Agent configuration.

If you wish, however, you can manually configure any Agent by editing the Agent's configuration files with a text editor on the Agent's host system. To configure Command Console Agent for access protection and proper connection with your subsystems, you must edit four, ASCII files.

- Services file
- Agent Configuration file
- Client Access file
- Subsystem Identification file

The following sections describe the function of each file, along with the process of editing it.

Editing the Services File

Agent uses ports (sometimes called “sockets”) to communicate with its Clients. Agent uses an even/odd number pair for the port numbers. Further, the port numbers at the Client and Agent ends must match for network communication to occur.

The default port numbers for Command Console are 4998 and 4999. If you are installing Agent and these numbers are already taken by another application, you must find an unused pair of numbers for Agent’s use.

In OpenVMS systems, port numbers are assigned in Digital TCP/IP Services for OpenVMS. You can use UCX to view these assignments by entering “UCX SHOW SERVICE” at the DCL command prompt. Pick two consecutive numbers above 1023 *that are not already shown as used*.

To assign the port numbers you have chosen, modify the numbers in the following two lines in the SWCC_CONFIG.COM file in SYS$MANAGER:

```
$spgui  =4998
$spagent=4999
```

Note that the port numbers that you select must match the port numbers used by all of the Clients to which you wish to connect your Agent.

Editing the Agent Configuration File

The agent configuration file, STEAM.CFG, configures Command Console Agent within its operating system. The file is located in SYS$SYSDEVICE:[SWCC$AGENT] and contains five lines of ASCII text, formatted as follows:

device_special_file_path

In OpenVMS, this line must be identical to the *agent_executable_file_path* in the next line.

agent_executable_file_path

The full path to the CLIENT.INI, and STORAGE.INI files.

encrypted_password

The encrypted password from the password generation program.

manufacturer_name

Your manufacturer name. The default is "Digital Equipment Corporation" You can use up to 80 characters.

snmp_enterprise_assignment

Your SNMP enterprise assignment number. The default is "36.2.15.21.". (Note that this parameter is *not* your numerical TCP/IP address.) If you are unsure about this parameter, use the default or contact your network administrator.

Editing the File

Edit the SYS$SYSDEVICE:[SWCC$AGENT]STEAM.CFG file by performing the following actions:

1. Run the password generation program by changing to the SYS$SYSTEM directory and entering the following at a DCL command prompt:

   ```
   $SPSW:==$SP_PASSWD
   $SPSW "yourpassword"
   ```

   where "*yourpassword*" is a 4 to 16-character text string of your choosing.

   The program generates an encrypted password string and displays it on the screen.

2. Use an ASCII editor to modify the STEAM.CFG file you copied during the installation process. Use the encrypted password from Step 1 as line 3 in the file.

Following is a sample STEAM.CFG file:

```
SWCCGUI_LOCAL
SWCCGUI_LOCAL
Q1</Sn_k
Digital Equipment Corporation
36.2.15.21.
```

Editing the Client Access File

The client access file, CLIENT.INI, configures Command Console Agent for proper operation with its Command Console Client companions. The file is located in the SYS$SPECIFIC:[SWCC$AGENT] directory on each cluster node on which the Agent is configured.

Use an ASCII editor to modify the CLIENT.INI file you copied during the installation process. Add a separate line in the file for each system that you wish to grant access to this host system. Use vertical bars (sometimes called the “pipe” character) to delimit the three fields. You may add comment lines as long as they start in very first position and begin with the exclamation point character, "!".

NOTE

Blank lines are not allowed in the CLIENT.INI file. A blank line may interfere with Agent execution.

The line for each client system must be in the following format:

system_network_name|notification _method|access_allowed

where:

system_network_name
The network name, including the domain information if appropriate, of the remote system to which you wish to grant access. The address must be alphanumeric and not a numeric IP address. The address can be up to 128 characters long, including periods. If you are unsure of this address, consult your network administrator.

notification_method
The mechanism you wish Agent to use to notify Client sessions of a fault, where:

0 = no notification
1 = notify via TCP
2 = notify via SNMP
3 = notify via both TCP and SNMP
If you are unsure of which mechanism to use, use "1" for this parameter.

access_allowed
You can configure Agent for three levels of subsystem access:

- High-level monitoring—Good/Bad indication at the host and storage subsystem levels. Good/Bad indication of Client/Agent communication link. Client notified of subsystem faults as they occur.
- Low-level monitoring—All detailed information about the status of the storage subsystem available, in addition to high-level monitoring capabilities.
- Configuration—Capability of changing the configuration of the storage subsystem, in addition to high and low-level monitoring capability.

The *access_allowed* parameter sets the level of access you are granting to this remote system, where:

0 = High-level monitoring only. No low-level monitoring or configuration changes allowed.
1 = High and low-level monitoring. No storage subsystem configuration changes allowed.
2 = High and low level storage subsystem monitoring and configuration access.

Following is a sample CLIENT.INI file. This file enables full access for the remote Client system at network address DREAMON.YOUR.COMPANY.COM, and sends fault notifications to Client using the TCP mechanism. It also disables any monitoring or configuration access by Client running on the system at network address WANDERLUST.YOUR.COMPANY.COM, but still enables asynchronous fault notification via the TCP mechanism.

```
!  Access list for system HOST123:
dreamon.your.company.com|1|2
wanderlust.your.company.com|1|1
```

Editing the Subsystem Identification File

The subsystem identification file, STORAGE.INI, configures Agent to communicate with the storage subsystems on the host on which Agent is running. The file is located in the SYS$SPECIFIC:[SWCC$AGENT] directory on each cluster node in which the Agent is configured.

Use an ASCII editor to modify the STORAGE.INI file you copied during the installation process. Add a separate line in the file for each system that you wish to grant access to this host system. Use vertical bars (sometimes called the “pipe” character) to delimit the three fields. You may add comment lines as long as they start in very first position and begin with the exclamation point character, "!".

NOTE

Blank lines are not allowed in the CLIENT.INI file. A blank line may interfere with Agent execution.

The line for each system must have the following format:

subsystem_name|*driveID*|*monitor_interval*

where:

subsystem_name
The name you wish to refer to the subsystem by when using the Client GUI. The name must be alphanumeric and can consist of up to 32 characters.

driveID
The name that identifies this storage subsystem in OpenVMS. The name has the format dk*xy0z*, where:
“dk” is a fixed string that identifies the subsystem as a Digital OpenVMS, SCSI device.
x is the alphabetic identifier of the SCSI adapter to which the subsystem is connected.
y is the SCSI target ID of the subsystem on the adapter
z is the LUN number of the subsystem on the adapter

(Note that *driveID* may or may not include an OpenVMS allocation class prefix such as “1”.)

monitor_interval
The time interval, in seconds, between Agent’s periodic status checks on this subsystem. The range of intervals is from 1 to 99,999 seconds. If you set this parameter to 0, Agent does not perform periodic status checks on the subsystem.

Following is a sample STORAGE.INI file. This file configures Agent to communicate with and to periodically monitor subsystems SW300 on drive DKC100, and MINI_B on drive DKA500 (specified with allocation class.) Agent will check SW300 at 20-second intervals, and MINI_B at 300-second intervals (that is, every 5 minutes).

```
! Storage subsystems for HOST123
sw300|dkc100|20
mini_b|$1$dka500|300
```

Miscellaneous Support Files

Agent uses several files in cooperation with the operating system. Do not delete these files. Most are in the SYS$SYSDEVICE:[SWCC$AGENT] directory.

In particular, do not delete these files:

- SWCC_STARTUP.LOG—This file is used to capture an audit trail of significant Agent events, for use in debugging Agent problems.
- CHANGE_REGISTER.COM and CHANGE_REGISTER.LOG—These files are used to track configuration changes across the cluster.
- LOGIN.COM—This file is used for UCX logins.

SNMP Trap Information

Agent sends out an SNMP trap (that is, an asynchronous event notification) to any hosts that are listed in the CLIENT.INI file with this option enabled. (See “Editing the Client Access File” in this document for more information.) This section describes the format of the SNMP trap.

Information Fields

An Agent SNMP trap consists of the following information fields:

- Source IP address
- GENERIC = 6 (6 = ENTERPRISE SPECIFIC VALUE TO FOLLOW)
- SPECIFIC = 0 or 1, where:
  - “0” indicates that the field-replacable unit (FRU) transitioned from a bad to a good state
  - “1” indicates that the FRU transitioned from a good to a bad state
- OID Variable of the offending FRU
- OCTET STRING Value returning the name of the storage subsystem containing the FRU specified by the OID Variable

OID Variables

Each object ID (OID) is prefixed by a base enterprise number (BEN) for the Command Console product. The default BEN for Command Console Agents is as follows:

1.3.6.1.4.1.36.2.15.21
(iso.org.dod.internet.private.enterprises.dec.ema.sysobjects.raidmanager)

Following are the OID values used by Command Console:

- Disk Status = BEN + .3.2.1.4
  (BEN + .subsys.ssStatusTable.ssEntry.ssDiskStatus)
- Power Supply Status = BEN + .3.2.1.5
  (BEN + .subsys.ssStatusTable.ssEntry.ssPowerStatus)
- Cooling Status = BEN + .3.2.1.6
  (BEN + .subsys.ssStatusTable.ssEntry.ssFanStatus)
- Cache Battery Charge Status = BEN + .3.2.1.7
  (BEN + .subsys.ssStatusTable.ssEntry.ssCacheBatteryStatus)
- OverTemperature Status = BEN + .3.2.1.8
  (BEN + .subsys.ssStatusTable.ssEntry.ssTemperatureStatus)
- Communication Status = BEN + .3.2.1.9
  (BEN + .subsys.ssStatusTable.ssEntry.ssCommStatus)

- Controller 1 Status = BEN + .3.2.1.12
  (BEN + .subsys.ssStatusTable.ssEntry.ssController1Status)
- Controller 2 Status = BEN + .3.2.1.19
  (BEN + .subsys.ssStatusTable.ssEntry.ssController2Status)

If your SNMP Management Utility has the Agent MIB compiled, the utility should display the character string values in parentheses above.

Trap Example

An example SNMP trap for storage subsystem “subsys1” with a failing power supply on an Agent at IP address “16.82.16.01”, would contain the following information:

Source address = 16.82.16.01
GENERIC = 6
SPECIFIC = 1
OID Value = 1.3.6.1.4.1.36.2.15.21.3.2.1.5
(iso.org.dod.internet.private.enterprises.dec.ema.sysobjects.raidmanager.subsys.ssStatusTable.ssEntry.ssPowerStatus)
OCTET STRING = subsys1