
AlterPath Manager E2000 Manual

*A reference guide for users and systems administrators
of Cyclades AlterPath Manager E2000*

Product Version 1.1.0 Revision No. 8

This document contains proprietary information of Cyclades and is not to be disclosed
or used except in accordance with applicable contracts or agreements.

©Cyclades Corporation, 2003

We believe the information in this manual is accurate and reliable. However, we assume no responsibility, financial or otherwise, for any consequences of the use of this product or manual. This manual is published by Cyclades Corporation, which reserves the right to make improvements or changes in the products described in this manual as well as to revise this publication at any time and without notice to any person of such revision or change. All brand and product names mentioned in this publication are trademarks or registered trademarks of their respective holders.

Cyclades, AlterPath ACS, and AlterPath Manager E2000 are registered trademarks of Cyclades Corporation.

Microsoft, Windows 95, 98, XP, ME, NT, and 2K are trademarks of Microsoft Corporation.

UNIX is a trademark of UNIX System Laboratories, Inc.

Linux is a registered trademark of Linus Torvalds.

For latest manual revisions, please refer to Cyclades website on:

<http://www.cyclades.com/support/downloads.php>

All rights reserved. This document may not, in whole or part, be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form without the prior written consent of Cyclades Corporation, 41829 Albrae Street, Fremont, CA 94538, USA. Telephone (510) 771-6100. Fax (510) 771-6200. www.cyclades.com.

Product Version: 1.1.0

Revision Number: 3

Table of Contents

Before You Begin

Audience	i
Document Organization	i
Typographical Conventions	ii
Naming Conventions	ii
Symbols	iii

Chapter 1: Introduction

Connectivity and Capacity	1-1
Key Features	1-2
Single Point Security Gateway	1-2
Centralized Authentication	1-3
Consolidated Views and Console Access	1-3
One-Click Access to Consoles and Devices	1-3
Centralized Data Logging System	1-4
Log File Compression and Rotation	1-4
Prioritized Triggers & Alarms	1-4
Other Alarm Features	1-5
Modem Support for Remote Sites	1-5
Network Health Monitoring	1-5
Console Wizard	1-5
Device Discovery	1-5
Backup, Restore, and Replicate User Data	1-6
Change and Configuration Management	1-6
Exhaustive Reporting	1-6
Simple and Easy Web User Interface	1-6
Command Line Interface (CLI)	1-7
Deploying the E2000	1-7
Private Network Topology	1-7
Single Network Topology	1-7

Private Network Diagram	1-8
Single Network Diagram	1-9

Chapter 2: Installing the E2000

Product Installation Checklist	2-1
Rack Mounting and Connecting the E2000	2-1
Safety Considerations When Rack Mounting	2-2
Configuring the COM Port Connection and Logging In	2-3
Pre-Configuration Requirements	2-4

Chapter 3: Using the E2000

User Interface Overview	3-1
Accessing the E2000 Web Management Interface	3-2
Login Screen	3-3
Logging In	3-3
General Screen Features	3-4
Using the Alarm List Form	3-5
Responding to an alarm	3-5
Alarm List Form	3-6
Options Available from the Alarm List Form	3-7
Ticket Information Form	3-8
Assigning/Re-assigning a Ticket to another User	3-9
Adding Notes to an Alarm	3-9
Using the Console List Form	3-10
Sorting by Fieldname	3-11
Viewing Console Details	3-11
Connecting to a Console	3-11
Multiple Users and Read/Write Access	3-11
Console Detail Form	3-12
Using the Logs Form	3-14

Viewing the Logs	3-15
Access Logs	3-16
Event Logs	3-17
Console Log Buffer	3-18
User Profile	3-19
Working from a Command Line Interface (CLI)	3-20
Logging In	3-20
Shell Commands	3-20
Copying and Pasting Text within the Console Applet Window	3-21
Connecting Directly to Ports	3-21
Sample Command Line Interface	3-22
CLI Commands	3-23
Changing the Escape Sequence	3-23
Re-defining the Interrupt Key	3-24
Chapter 4: Configuring the E2000	
Operational Modes	4-2
Configuration Process Flow	4-3
First Time Configuration	4-4
Using the First Time Configuration Wizard	4-5
Resetting Configuration to Factory Default Settings	4-6
First Time Configuration Wizard: An Example	4-7
Connecting to the E2000 Web Interface	4-9
Disabling HTTP to Use Only HTTPS	4-9
Using the Admin Mode	4-10
Logging Into the E2000 Web Interface	4-11
E2000 Web User Interface	4-12
Device Management	4-13
Device List Form	4-14
Adding a Device	4-15
Uploading Firmware to a Device	4-15

Table of Contents

Deleting a Device	4-16
Device Definition Form	4-16
Configuring Your DHCP Server	4-18
About the Status: OnDemand	4-19
About Auto Upload and Manual Upload	4-20
Modem Dialing Capability for	
Remote Access to Devices	4-20
Configuring the Modem Dialing Capability	4-21
Modem Management via	
Command Line Interface	4-22
Configuring the Health Monitoring System	4-24
Using the Console Wizard	4-24
Device Discovery	4-31
Uploading Firmware into the Console Devices	4-37
Profile List Form	4-38
Profile Definition Form	4-39
Form Fields and Elements	4-39
Adding a New Profile	4-40
Modifying a Profile	4-40
Console Management	4-41
Console List Form	4-42
Sorting by Field Name	4-42
Connecting to a Console	4-43
Defining a Console	4-43
Console Definition Form	4-44
Form Fields and Elements	4-44
Selecting Users to be Notified	4-46
Log Rotate Now	4-46
Setting Log Rotation in Auto Mode	4-46
Where Log Files are Archived	4-47
Backing Up Log Files to a Remote Server	4-47

User Management	4-48
User List Form	4-49
User Definition Form	4-50
Adding a User	4-51
Deleting a User	4-51
Selecting Consoles for a User	4-52
Setting Up the Local Password	4-52
Triggers and Alarms Management	4-53
Forms used to Manage Triggers and Alarms	4-53
Alarm Trigger List Form	4-54
Adding or Deleting an Alarm	4-54
Alarm Trigger Definition Form	4-55
Creating an Alarm Trigger	4-56
Deleting an Alarm Trigger	4-56
Configuring Alarms for	
Device Health Monitoring	4-56
Using the Logical AND in the	
Alarm Trigger Expression	4-58
How Health Monitoring Works	4-59
Info Reporting Main Form	4-61
Info Reporting Detail Form	4-62
Firmware Management	4-63
Firmware List Form	4-64
Adding Firmware	4-64
Deleting Firmware	4-65
Uploading Firmware into the	
Console Devices	4-65
Firmware Detail Form	4-66
Viewing and Accessing Firmware Information	4-67
Upgrading the E2000 Firmware	4-67
Backing Up User Data	4-68
Backup and Restore Scenarios	4-68
Backup and Restore Commands	4-69
System Recovery Procedures	4-69

Table of Contents

Appendix A: <i>Hardware Specifications</i>	A-1
Appendix B: <i>Modem Access in ACS</i>	B-1
Appendix C: <i>Installing SSL Certificates</i>	C-1

Before You Begin

Welcome to the AlterPath Manager E2000 Manual! This manual is designed to guide you in installing, configuring, and operating the E2000, as well as other necessary information to guide you in your day-to-day operations of the product.



For convenience, the AlterPath Manager E2000 will be referred to as simply E2000.

Audience

This document is designed for System administrators and regular users of AlterPath Manager E2000. Users are expected to have a basic knowledge of using a graphical user interface.

Document Organization

The document is organized as follows:

- | | |
|--------------------------|---|
| 1: Introduction | Defines and explains the overall product features and uses. |
| 2: Installing the E2000 | Explains the installation procedure for installing the E2000 |
| 3: Using the E2000 | Explains to regular users how to use the user interface. This chapter is particularly designed for regular users (as distinguished from the system administrator) of the E2000. It highlights such procedures as connecting to a console, dealing with alarms, and other system tracking and management procedures. |
| 4: Configuring the E2000 | Explains how the system administrator can configure the system features and enable users to perform the various fault management procedures such as connecting to a console, |

responding to an alert and the like. Configuration settings include user access, alarm triggers, device management, firmware control, as well as running the configuration wizards.

Typographical Conventions

Form/Window Labels

Words that appear on forms, windows, or any part of the user interface are typed in **boldface**.

Examples:

The **Alarm** definition form; the **Password** field.

Hypertext Links

With the exception of headings and the Table of Contents (which are already linked), all underlined words are hypertext links.

Window Levels

Window levels are indicated by the “greater than” symbol (>), starting from the parent screen to child. Most E2000 screens or windows contain only two levels.

Example:

Consoles List>Console Detail

Naming Conventions

Administrator

The person who is defined in the E2000 as the administrator and has the authority to configure and manage the E2000 in that capacity. This is the only administrator referred to by this manual.

E2000

For convenience, this is the short name for AlterPath Manager E2000. The short name is also commonly used in the Index.

Form

The form is the largest part of the user interface; it contains the user selection or input fields for each selected item in the menu.

Form Names	<p>The form names of the application’s GUI do not necessarily appear on the actual window. Because some forms do not have titles, these names are used to distinguish each form as well as to reflect the form function.</p> <p>The most commonly used form names are “List” forms and “Definition” forms. In fact, the configuration forms of E2000 almost consistently use the two types of forms.</p> <p><i>Examples:</i> Console List form; Console Definition form</p>
Select	<p>To <i>select</i> is the same as to <i>click your mouse</i>.</p>
User(s)	<p><i>User</i> or <i>users</i> refer to those who use the E2000 application as a regular user (i.e., the application is running on Access mode, and not in the Admin mode) even though the user may be system administrator.</p>

Command Line Syntax

While this manual is primarily designed for using the E2000 web interface, some advanced features show you how to configure the E2000 using the Command Line Interface (CLI). The typographical conventions used for showing the syntax for these commands are as follows.

Brackets and Hyphens (dashes)

The brackets ([]) indicate that the parameter inside them is optional, meaning that the command will be accepted if the parameter is not defined. When the text inside the brackets starts with a dash (-) and/or indicates a list of characters, the parameter can be one of the letters listed within the brackets.

Example:

iptables [-ADC] chain rule-specification [options]

Ellipses

Ellipses (...) indicate that the latest parameter can be repeated as many times as needed. Usually this is used to describe a list of subjects.

Example:

```
ls [OPTION]... [FILE]...
```

Pipes

The pipe (|) indicates that one of the words separated by this character should be used in the command.

Example:

```
netstat {--statistics|-s} [--tcp|-t] [--udp|-u] [--raw|-w]
```

When a configuration parameter is defined, the Linux command syntax conventions will be also used, with a difference.

Greater-than and Less-than signs

When the text is encapsulated with the “<>” characters, the meaning of the text will be considered, not the literal text. When the text is not encapsulated, the literal text will be considered.

Spacing and Separators

The list of users in the following example must be separated by semicolons (;); the outlets should be separated by commas (,) to indicate a list or with dashes (-) to indicate range; there should not be any spaces between the values.

sXX.pusers: The user access list. For example: jane:1,2;john:3,4. The format of this field is:

```
[<username>:<outlet list>][;<username>:<outlet list>...]
```

Where <outlet list>'s format is:

```
[<outlet number>|<outlet start>-<outlet end>][,<outlet number>|<outlet start>-<outlet end>]...
```

Symbols

This manual uses three symbols to indicate the following:



This icon indicates a reference to another section, chapter, or document.



This icon indicates a note or comment.



This icon indicates a warning.

This page has been intentionally left blank.

Chapter 1

Introduction

The AlterPath Manager E2000 is a feature-rich, out-of-band (OOB) manager designed to provide OOB users and administrators a centralized and convenient way to remotely access target devices and perform all their system fault management work from a single user interface.

Through an easy and convenient web user interface, you (as a regular E2000 user) can easily view and access consoles, view consolidated logs and reports, and respond to triggers, alarms, and other system issues that may arise.

Likewise, if you are the administrator, you can accomplish all your configuration and management work from a single location without the need to work directly on a target device or server console.



*For clarity, anyone who uses the E2000 application in Access mode is referred to as a **user**, regardless of whether that user is a system administrator or not. An **administrator**, on the other hand, is anyone who has the exclusive authority to configure and to perform various system administrative tasks for the E2000.*

Connectivity and Capacity

The E2000 allows you to configure 2048 console port connections and maintain 256 simultaneous connections to consoles and devices. You can perform firmware upgrades on 256 separate console management devices. The E2000 also supports up to thirty simultaneously connected users, and allow multi-user access to each port.



Figure 1.1 - Front view of E2000

The port connections available from the E2000 box are shown below:

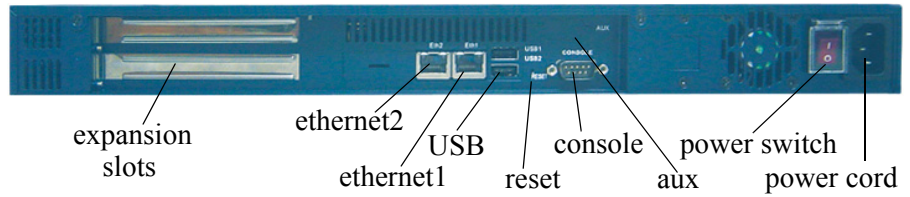


Figure 1.2 - Back view of E2000

Key Features

The key features of AlterPath Manager E2000 are:

- Single point security gateway
- Centralized authentication
- Consolidated views
- One-click access to consoles and devices
- Centralized data logging system
- Access log audit trail
- Log file compression and rotation capabilities
- Prioritized triggers and alarms
- Modem support for remote sites
- Network health monitoring
- Console wizard
- Device discovery
- Backup, restore, and replicate user data
- Automated change and configuration management
- Exhaustive reporting
- Convenient web user interface
- Easy command line interface
- Product maintenance

Single Point Security Gateway

The E2000 has been designed such that communications between users and the management network must pass through a single point of access--the E2000--to optimize security and enforce adherence to your corporate security policy.

A single, secure access point reduces management overhead for managing console servers. Moreover, the multiple authentication options available ensures compatibility with existing infrastructure.

Centralized Authentication

Centralized authentication saves you or the administrator from using a password for each TS/ACS, and thereby maintain a secure password. You need only use your password once upon logging onto the E2000. The E2000 authenticates all users accessing the console ports using a local database, RADIUS, Kerberos, or LDAP.

Consolidated Views and Console Access

From the E2000 web interface, you can view a list of all consoles to which you have authorized access. Information about each console includes console name, port, location, description, and status.

The Access Control List (ACL), which is defined by the administrator, defines which user has access to which port. For added security, users cannot view other consoles which they are not authorized to use.

One-Click Access to Consoles and Devices

Users have access to consoles; administrators, to consoles and console devices.

To access a console, you simply choose and click on any console listed on your console list screen. This opens a console session (through Secure Shell) for that particular console, allowing you to remotely fix problems related to the target console.

Centralized Data Logging System

The E2000 captures all console log messages and writes them to its internal hard disk drive. This provides a secure and permanent storage of important console log information.

The console log capacity is 20GB, which is about 80MB for each of the 256 console ports. The secure online/offline storage ensures availability of all important console messages.

Each line of the logfile contains a timestamp, a feature which prevents tampering and provides a tool for analyses and audit trailing. Each time you or any user connects to a port, E2000 adds a timestamp to the log file. The user identification timestamp is recorded in the data buffer and logged separately on the E2000 access log database.

Log File Compression and Rotation

When a log file reaches a certain size (which is specified by the administrator), the system automatically compresses the file and then creates a new file to collect a new set of console data. The file rotation should be seamless with no data loss as the system copies from one file to another.

The administrator has the option to move the compressed log file to another server for archiving.

Prioritized Triggers & Alarms

E2000's event handling feature enables the system to identify possible issues and alert the user.

As the E2000 sends a message to the hard disk for storing and consolidation, it also scans the message for triggers. A trigger is a text string pre-defined by the administrator which the system uses to detect a trigger text from messages. When the E2000 detects a trigger text, based on how the trigger was configured by the administrator, it will do the following:

- Send an email to a user list
- Create a prioritized alarm entry in the Alarm database
- Write a log message to the E2000 logging system to acknowledge the trigger.

Other Alarm Features

Notes	You can add notes to an alarm to indicate what action you have taken. These notes can be useful for future reference to similar issues.
Reports	You can generate a report to show what actions were taken by whom, and how long it took to fix the issue.

Modem Support for Remote Sites

Using point-to-point protocol (PPP), the E2000 is equipped with modem dialing capability to allow complete out-of-band access to remote console server devices. Moreover, users have the choice to use PPP as the primary mode of connection or only as a backup connection in the event that the network fails.

Health Monitoring

This feature allows enables the E2000 to monitor on a periodic basis the consoles that are running on specified device, to generate log files, and to send an alarm notifications to specified users.

Health Monitoring is designed to ensure that in the event of a network failure, remote sites are available and working properly.

An integral part of Health Monitoring is the Health Modem feature which monitors any modem that are being used to connect to a device either as a primary connection or as a backup. Like Health Monitoring, this feature has it's own alarm trigger which the administrator can configure to generate log files and send alarm notifications to users.

Console Wizard

The console wizard allows you to define the consoles connected to a device by automatically defining the consoles using default and customized values. The wizard configures the selected console(s) and applies them to the device.

Device Discovery

The Device Discovery feature enables the E2000 to recognize the current configuration of a Cyclades TS or ACS and, through the use of a wizard, autopopulate the console parameters based on the values used by the Cyclades TS or ACS.

For users who already have TS/ACS units deployed in their network, Device Discovery eradicates the time-consuming task of re-defining each console port manually.

Backup, Restore, and Replicate User Data

This feature allows users to create a backup of the E2000 configuration and data files. The backup includes data from the compact flash, configuration data from the database, and log data from the console buffer files. This feature also enables users to copy console log files to a server for further analysis and archiving.

Change and Configuration Management

Change and Configuration Management feature of the E2000 is designed such that any number of change management procedures can be configured through the E2000 rather than through the target devices or software.

- Initializing new console servers
- Setting the serial ports
- Upgrading firmware

All change management configuration is performed by the administrator.

Exhaustive Reporting

Because the E2000 consolidates all its logs and maintains its own databases, it provides in-depth reporting capabilities to suit the reporting needs of users and managers.

Simple and Easy Web User Interface

The E2000 provides a convenient and user-friendly web user interface for the regular user and the administrator. Hyperlinks enable you to access consoles, view data logs, and other information even faster. From one single interface, you can achieve just about everything you need to manage your network's consoles.

Because as a user you can only view and access those consoles you are assigned, the interface is customized to suit your needs.

The customization adds security to the system since users cannot view or access any console that does not concern them.

Command Line Interface (CLI)

For emergency access situations, the E2000 can provide you with a command line interface by making a regular Secure Shell connection to the E2000. CLI is one of two user interfaces (the other is the web interface) available to E2000 users. The CLI is also used for First Time Configuration and system recovery procedures.

Deploying the E2000

There are two typical ways (or topologies) in which the E2000 can be set up in a network, or among networks.

- Private network
- Single network

Private Network Topology

In a private network topology, one ethernet port connects E2000 to the management network; the other, to the public network. The management network comprises all fault management equipment (*i.e.*, TS, ACS), devices, and infrastructure used to manage the public network. Equipped with its own Ethernet switches, the management network is physically separate from the public network.

Because any E2000 user who needs to access console ports in the TS and ACS boxes must pass through the E2000, this is the most secure way to deploy the E2000.



See Figure 1.3 - Private Network Topology.

Single Network Topology

In a single network topology, the E2000 is connected to only one network, and the E2000 management functions are contained in the same network. While it may appear that the workstation has direct access to the TS and ACS boxes, if users attempt to access them, they will be denied because the E2000

is already controlling access to the ports. In a single network configuration, a Virtual Local Area Network (VLAN) configuration is recommended.



See Figure 1.4 - Single Network Topology.

Private Network Diagram

The diagram below depicts how the AlterPath Manager E2000 may be set up in a private network structure.

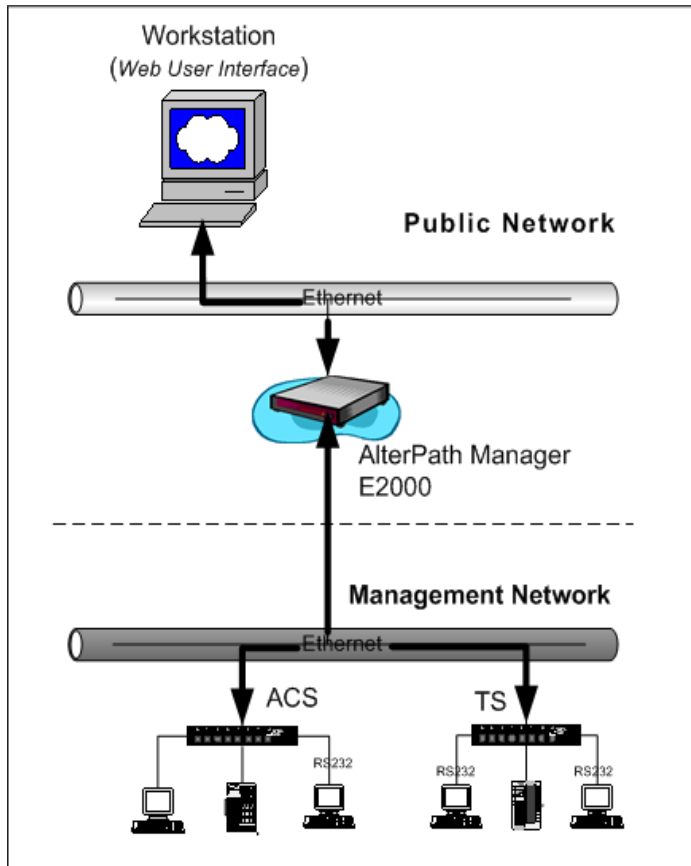


Figure: 1.3 - Private Network Topology

Single Network Diagram

The diagram below depicts how the AlterPath Manager E2000 may be set up in a single network structure.

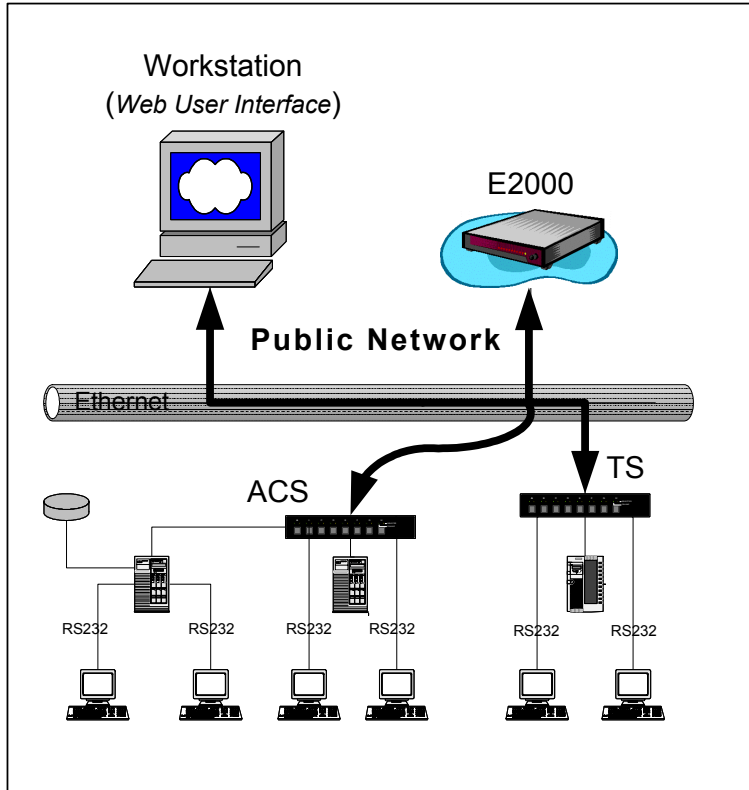


Figure 1.4 - Single Network Topology

This page has been intentionally left blank.

Chapter 2

Installing the E2000

This section discusses the procedures and requirements for installing the AlterPath Manager E2000, and is organized as follows:

- Product Installation Checklist
- Rack Mounting and Connecting E2000 to the Network
- Pre-Configuration Requirements
- Preparing Console for Initial Configuration

Product Installation Checklist

Your AlterPath Manager E2000 is shipped with the following hardware components:

- E2000 box
- Console cable (null modem)
- Power cable
- 2 Ethernet cables
- Mounting kit

Rack Mounting and Connecting the E2000

To rack-mount and connect the E2000 to your network, perform the following steps:

1. Install the mounting brackets onto the front corners of the box using a screw driver and the screws included in the mounting kit.
2. Mount the E2000 in a secure position.
Refer to the **Safety Considerations When Rack Mounting** section of this chapter to ensure safety.
3. Plug the power cable into the E2000 box.
Insert the female end of the black power cable into the power socket on the console server and the three-prong end into a wall outlet.



To help prevent electric shock, plug the E2000 into a properly grounded power source. The cable is equipped with a 3-prong plug to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from the cable. If you use an extension cable, use a 3-wire cable with properly grounded plugs.

4. Connect the console cable.

Connect one end of this cable to the port labeled **Console** on the E2000; the other end, to your PC's available COM port.

5. Connect Switch or Hub to PC and the E2000.

Your workstation and E2000 must be on the same physical LAN. Connect one RJ-45 cable from the Ethernet (1 or 2) port of the E2000 to the hub, and another from the hub to the workstation used to manage the servers.

6. Install and launch HyperTerminal, Kermit or Minicom if not already installed.

See *Configuring the COM Port Connection and Logging In*, this chapter.

You can obtain the latest update to HyperTerminal from:

<http://www.hilgraeve.com/hpe/download.html>

Safety Considerations When Rack Mounting

When rack-mounting the E2000, consider the following:

Operating Temperature

The manufacturer's recommended operating temperature for the E2000 is 50° to 112°F (10°C to 44°C).

Elevated operating ambient temperature

If you install the E2000 in a closed or multi-rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient temperature. Ensure that you install the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.

Reduced air flow

Ensure that the amount of airflow required for safe operation is not compromised.

Mechanical loading

Ensure that the equipment is mounted or loaded evenly to prevent a potentially hazardous condition.

Circuit loading

Ensure that the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Check the equipment nameplate ratings to address this concern.

Reliable Earthing

Maintain reliable earthing of rack mounted equipment by inspecting supply connections other than direct connections to the branch circuit such as power strips or extension cords.

Configuring the COM Port Connection and Logging In

The console port is used for the initial configuration (also known as *First Time Configuration* in this document) which is performed using the Command Line Interface (CLI) via serial console connection.

First Time Configuration is responsible for establishing the superusers for the CLI (hardware configuration) and the E2000 web interface and configuring the E2000 connectivity and system settings. The process is discussed in more detail in *Chapter 4: Configuring the E2000*.

Before using the terminal, make sure it is configured as follows:

1. Select available COM port.
In HyperTerminal (Start > Program > Accessories), select File > Properties, and click the Connect To tab. Select the available COM port number from the Connection dropdown.
2. Configure COM port.
Click the Configure button.
Your PC, considered here to be a “dumb terminal,” should be configured as follows:

- Serial Speed: 9600 bps
 - Data Length: 8 bits
 - Parity: None
 - Stop Bits: 1 stop bit
 - Flow Control: none
 - ANSI emulation
3. Power on the E2000
 4. Click OK on the Properties window.
You will see the E2000 booting on your screen. After it finishes booting, you should see the configuration screen.

Pre-Configuration Requirements

Before configuring E2000, ensure that you have the following system set up and information ready:

HyperTerminal,
Kermit, or Minicom

If you are using a PC, ensure that HyperTerminal is installed on your Windows operating system. If you are using the UNIX operating system, use Kermit or Minicom.



You will need Root Access on your local UNIX machine in order to use the serial port.

IP Addresses

Have the IP/Mask addresses of the following ready:

- All console servers
- SMTP
- Gateway
- DNS
- NTP (optional)

NIC Card

Ensure that you have a NIC card installed in your PC to provide an Ethernet port, and allow network access.



*To complete the configuration process, **SKIP to Chapter 4: Configuring the E2000**. Refer to *First Time Configuration* on Chapter 4, page 4-3.*

Chapter 3: Using the E2000 is designed for regular users who will use or operate the application after the E2000 administrator has completed the configuration procedures discussed in chapter 4.



*For a list of internet browsers and Cyclades device firmware versions supported by the E2000, refer to **Appendix A: Hardware Specifications**.*

This page has been left intentionally blank.

Chapter 3

Using the E2000

This chapter explains the procedures for using the web user interface of AlterPath Manager E2000 for regular users. Recall that there are two GUI-based modes for using E2000 based on the type of user: **Access** and **Admin**. This chapter is devoted to the user using the system in *Access* mode, and is organized as follows:

- User Interface Overview
- Accessing the E2000 Web Management Interface
- Logging In
- Using the Alarms form
- Using the Consoles form
- Using the Logs form
- Using the User Profile form
- Working from a Command Line Interface (CLI)



*If you are an E2000 system administrator, refer to “4: **Configuring E2000**” chapter of this document.*

User Interface Overview

The E2000 user interface provides you with four main menu options, or four basic forms:

Alarms	This is your default form. Use this form to deal with alarms such as updating the status of the alarm or closing the alarm after you resolve it.
Consoles	Use the Consoles form to view a list of the consoles assigned to you. From the list, select the console you wish to access, or select the console from the drop down menu on the top left, and then click on Connect .

Logs	Use the Logs form to view the Access Logs , Events Logs , and Data Buffer for a particular console. The Logs form is used in conjunction with the Consoles form.
User Profile	Use the User Profile to view or modify user information.

Accessing the E2000 Web Management Interface

To open the E2000 web application, perform the following steps:

1. Type in the following URL from your web browser:

`https://nnn.nnn.nnn.nnn`

Where: **nnn.nnn.nnn.nnn** is the IP address provided to you by your E2000 administrator.

The IP address works for both encrypted (https) and non-encrypted (http) versions. Cyclades recommends that you use the encrypted version.

2. When the Login screen appears, enter your user name and password (as provided by your system administrator).

Login Screen

The AlterPath Manager E2000 Login screen is shown below:

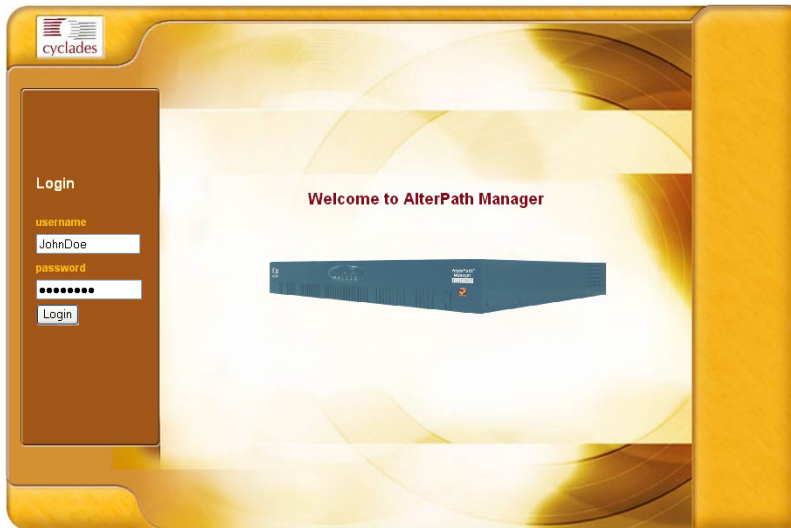


Figure 3.1 - E2000 User Login Screen

Logging In

To log in, follow the following steps:

3. Type in your username and password in the corresponding fields of the Login screen. (See Figure 3.1 - Login Screen.)
4. Select the **Login** button.

Upon successful login, the **Alarms** form appears.



When E2000 launches your application screens for the first time, the process will be slow. Once the screens are stored into your cache, subsequent retrieval of screens should be fast.

General Screen Features

Before continuing, familiarize yourself with the general features of the E2000 screens by selecting some of the items in the menu. The sample screen below is for illustration only; it is not the first screen that you should see when you log in as a regular user.

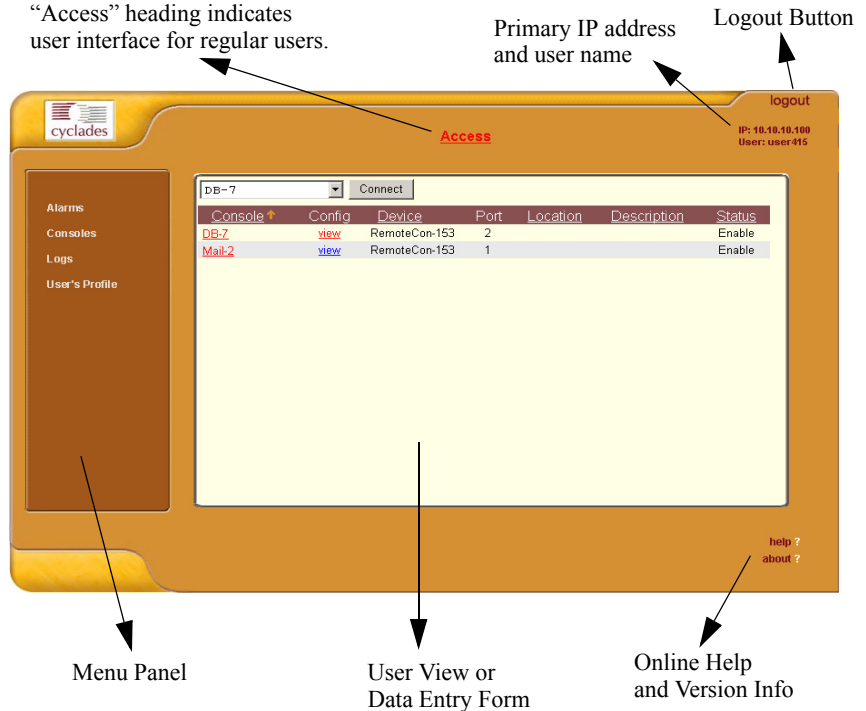


Figure 3.2 - Parts of the Access (User) Screen

The four main menu options are always displayed in a group box on the left. Your user name and IP address appears on the top right hand corner of the screen.

No matter what browser you are using you should be able to resize or maximize the main window to fit your screen.

Be sure you select the **Logout** button on the top right hand corner after you finish your session.

Using the Alarm List Form

The Alarm List form is the default form of the E2000 user interface (*i.e.*, using the application in **Access** mode). An alarm is a brief message alerting you of a possible problem that requires an action.

When E2000 detects an alarm, it sends the alarm to the user's Alarm List form. As a user, you should see only those alarms assigned to you by your administrator.

If the trigger for the alarm has been configured to send an email, then you should also receive an email notification regarding the alarm. Apart from the alarm itself (which is the **Trigger Name** in the Alarms form), each alarm in the list includes a timestamp, a priority level, and a status.

The system not only stores each alarm in a database, but also maintains a log for each alarm. You can view the log directly from the Alarms form or from the Logs form (Main Logs>Access Logs>Data Buffer).

Responding to an alarm

Outlined below is a “typical” procedure for responding to an alarm. Since no two issues are exactly the same, you have several ways to respond to an alarm depending on the nature and severity of the alarm.

When you first receive an alarm through the Alarms form, you can respond as follows:

- Accept the ticket or assignment
- Reassign the ticket or assignment to another user, and optionally add notes about the ticket.

Once assigned, the user working on the ticket can perform any of the following procedures to resolve the alarm or complete the ticket.

- View Console Log and other related logs
- Edit information ticket by changing the status and adding notes.
- Connect to the console.
- Run a console session.
- If problem is fixed, change status of alarm and close the ticket
- Or, re-assign the ticket to another user

Alarm List Form

The Alarm List form is the primary form for alarm management. As discussed earlier, you use this form to view the list of alarms, to reassign an alarm, to connect to a console (i.e, console SSH session), and to view console logs.



Figure 3.3 - Alarms form

Form Fields and Elements

<i>Field Name</i>	<i>Definition</i>
Console	Console from which the alarm originated. Selecting the console icon to the left of the console name enables a text-based console session.
Alarm Trigger	Trigger name that reflects the nature or type of alarm.
Ticket	Ticket number of the alarm.
User Assigned	User assigned to the alarm.
Status	Status of the alarm.
Console Log	Select this to navigate to the Data Buffer log pertaining to the console.

Options Available from the Alarm List Form

When you receive an alarm, one of the first steps you need to do is open the ticket window and review the information associated with the ticket. To view ticket information follow the following steps:

1. From the Alarm List form, select the ticket you wish to examine.
The form brings up the Alarm Detail window.
2. From the Alarm Detail window you may perform any of the following tasks, as needed:
 - a. Re-assign the ticket by selecting the appropriate user from the **Assigned User** drop list box.
 - b. Change the status of the ticket or alarm by selecting the correct status from the **Status** drop down list box.
 - c. View console details by selecting the particular console name.
 - d. View the Console Log for a particular console by selecting a log under the **Console Log** column. (This is a shortcut link to **Logs > Data Buffer**.)
 - e. Perform a console session (through SSH) by selecting the link to the console name. (This is a shortcut link to **Consoles > Console**.)
 - f. Add notes or comments about the current ticket by typing them into the **Notes** text entry box.
3. Select **Save** when completing steps a, b and f.
4. Verify some of your changes by selecting Alarms from the main menu panel to re-open the **Alarm** List form.

Ticket Information Form

Use the Ticket Information form to re-assign the ticket to another user, to change the status of the ticket, or to add notes to the ticket.

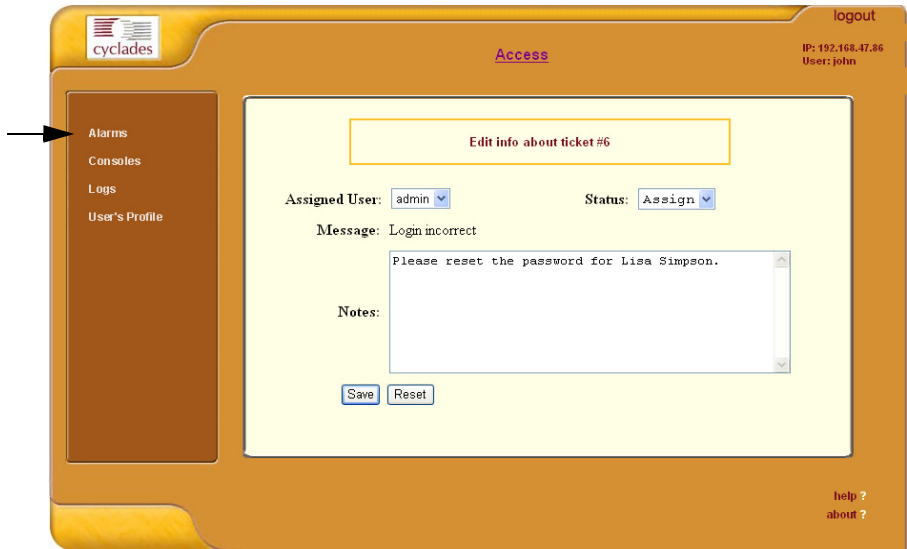


Figure 3.4 - Ticket Information form

Form Fields and Elements

<i>Field Name</i>	<i>Definition</i>
Assigned User	Drop down list. User to whom the ticket is assigned.
Status	Drop down list. Status of the ticket.
Message	System or alarm message that appears on the Alarm List form.
Notes	Scrollable text entry box for entering notes related to the ticket.
Save	Button to save form entry.
Reset	Button to reset the form.

Assigning/Re-assigning a Ticket to another User

To assign or re-assign a ticket, follow these steps:

1. From the Alarm List form, select an alarm or ticket to open the Ticket Information form.
The system opens the Ticket Information form.
2. From the Ticket Information form, select user from the Assigned User drop down list box.
3. If applicable, select the status from the **Status** drop down list box.
4. If applicable, type in your notes or comments in the **Notes** text entry box.
5. Select Save to complete your entry.

Adding Notes to an Alarm

See previous procedure, *Assigning/Re-assigning a Ticket to Another User*.

Using the Console List Form

The Console List form, shown below, allows you to:

- View detailed information about the consoles assigned to you.
- Connect to your target console and do a command line console session



Figure 3.5 - Console form

Form Fields and Elements

<i>Field Name</i>	<i>Definition</i>
Console	Console name
Device	Console server used by the console.
Port	Port number used by the console.
Location	Location of the console.
Description	A brief description of the console
Status	Operating status (enabled or disabled) of the console.

Sorting by Fieldname

The Console List form allows you to sort by fieldname. For example, to sort by location, simply click the column name (or fieldname), **Location**.

Viewing Console Details

To view console details, follow these steps:

1. From the Consoles form, select from the **Config** column the **edit** link adjacent to the console you wish to view.
The Console Detail form appears.

Connecting to a Console

There are two ways to connect to a console using Secure Shell (SSH):

Method 1: Using the dropdown menu.

1. From the Console List form, select the console you wish to connect to from the console dropdown menu (located on the upper left corner of the main panel).
2. Click on **Connect**.

Method 2: Using the main list.

1. From the Console List form, select the console you wish to connect to by selecting the console name.



Regardless of the method, if a modem is connected to a remote site, you will experience a slight delay before connecting to a console.

Multiple Users and Read/Write Access

Because the E2000 supports multiple connections to the same port, this makes it possible for multiple users to view the same form. Note, however, that only the first user to connect to that port can have full *Read and Write* (R/W) access to the Console panel while the rest can have *Read only* (R) access.

Console Detail Form

Use the Console Detail form to view specific information about a particular console (*i.e.*, the *target* console). You can invoke this form from either the Alarm List form or the Console List form.

If you have admin privileges, you also use this form to select user(s) to notify of the alarm and select user(s) to have access to the current console.

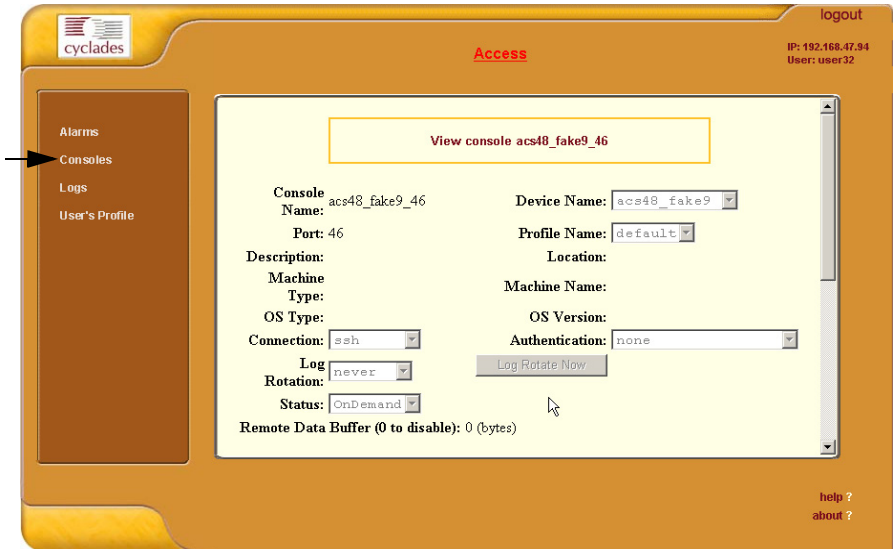


Figure 3.6 - Console Detail form

Form Fields and Elements

Field Name	Definition
Console Name	Name of (target) console.
Device Name	Name of device used by the console.
Port	Name of port used by the console.
Profile Name	Port profile name.
Description	A brief description of the target system.
Location	Location of the target system.
Machine Type	Type of target system.

<i>Field Name</i>	<i>Definition</i>
Machine Name	Other applicable system name.
OS Type	Operating system used by the console.
OS Version	Version of operating system.
Status	Status of the target console (able or disable).
Connection	Connection type between console and device.
Log Rotation	Indicates the frequency of the automatic log rotation. This feature can only be configured by the Administrator.
Log Rotation Now	Button to initiate log rotation. This feature is also for Administrator use only.
Select User to Notify	Drop down list to select user(s) you wish to be notified of alarms from the current console.
Add	Button to add user to be notified.
Delete	Button to delete user to be notified.
Select User to Access Console	Drop down list to add user(s) who can access the current console.
Add	Button to add user to access the current console.
Delete	Button to delete user to access the current console.

Using the Logs Form

The Logs form allows you to view three types of logs pertaining to the console assigned to you. For that reason, the Logs form is often used in connection with Console Management (*i.e.*, the Console forms). The Logs main form has three selectable tabs:

- Access Logs (default browser)
- Event Logs
- Data Buffer

When you select Logs from the menu panel, the initial logs form, shown below, will prompt you for a range of dates from which to retrieve your logs.

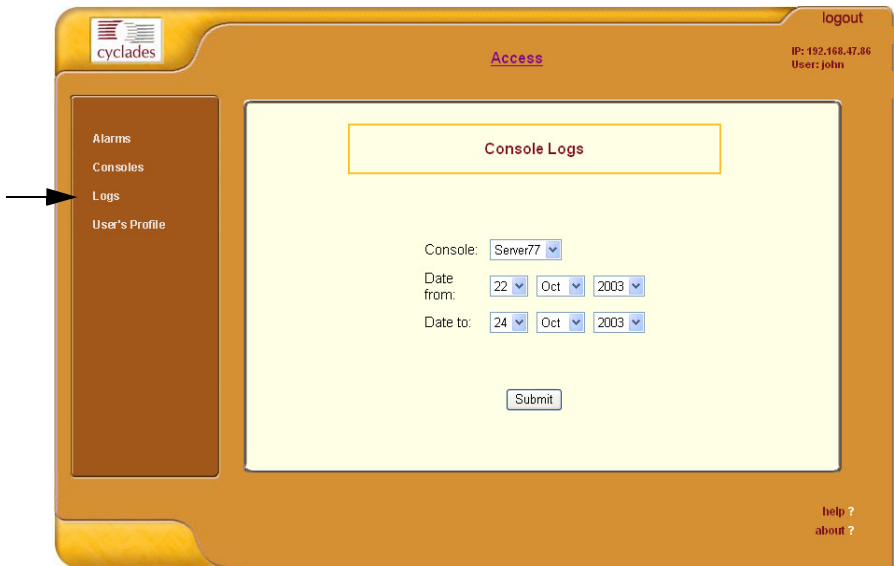


Figure 3.7 - Console Logs form

Form Fields and Elements

<i>Field Name</i>	<i>Definition</i>
Console	Drop down list to select console.
Date From	Drop down list to select starting date of log to be viewed.
Date To	Drop down list to select end date of log to be viewed.

<i>Field Name</i>	<i>Definition</i>
Submit	Button to download the requested log and invoke the Logs form.

Viewing the Logs

Using the Logs form, you have the option to view the various logs available for a specified console (to which you have authorized access).

To view the logs, perform the following steps.

1. Select **Logs** from the Menu Panel
The system brings up the main Console Logs form.
2. From the Console drop down list, select the console from which you want to view the logs.



You can only view or access the logs of consoles to which you have authorized access.

3. Select a range of dates from which to base your logs by selecting from the **Date From** and **Date to** drop down lists.

The system brings up the Logs Detail form.

Three Types of Logs

The Logs form provides you with three types of log:

<i>Log Type</i>	<i>Definition</i>
Access Log	Logs that provide logging information (<i>i.e.</i> , who accessed the console, when and for how long, <i>etc.</i>) about a particular console.
Events Log	Logs that provide information about notifications and alarms (who handled the alarm, what action was taken, <i>etc.</i>) triggered by a particular console.
Console Log Buffer	This is a log of all transaction data generated on the console.

All three logs are made immediately available for the specified console. All you need to do is select the appropriate tab to view the type of log you want. As with consoles and alarms, you can only view the logs of systems to which you have authorized access.

Access Logs

Use Access Logs form to view the Access Logs, Event Logs, and Data Buffer Logs. The Access Logs (default log browser) provide all access information (e.g., who accessed the console, access date, action taken, etc.) about your target console.

The name of the console/port/device to which the logs apply to is shown below the tab titles.

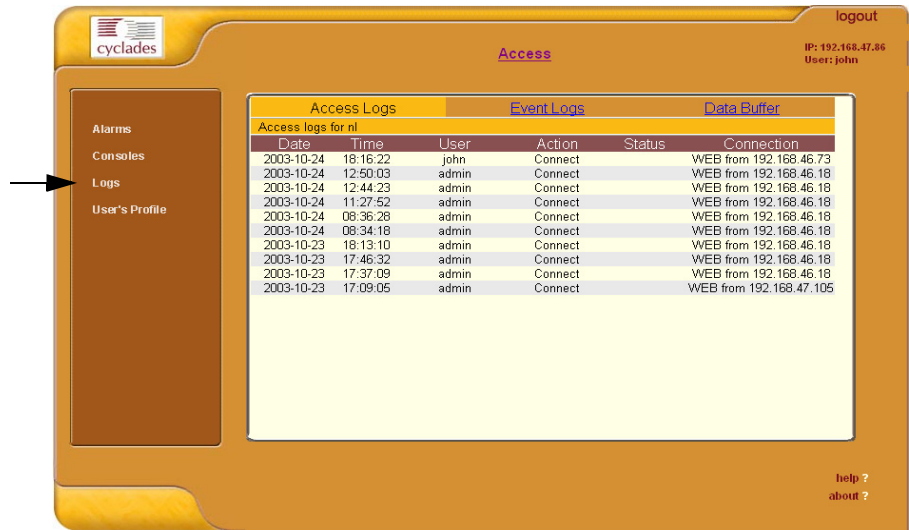


Figure 3.8 - Logs form

Log Field Definition

Field Name	Definition
Date	Date in which the event occurred.
Time	Time of the event.
User	User who connected to the console.
Action	What the user did in response to the alarm.
Status	Status of the console (Enable / Disable).
Connection	Type of connection (SSH / Telnet).

Event Logs

Use the Event Logs browser to view all events that occurred (within a specified range of time) on your target console.

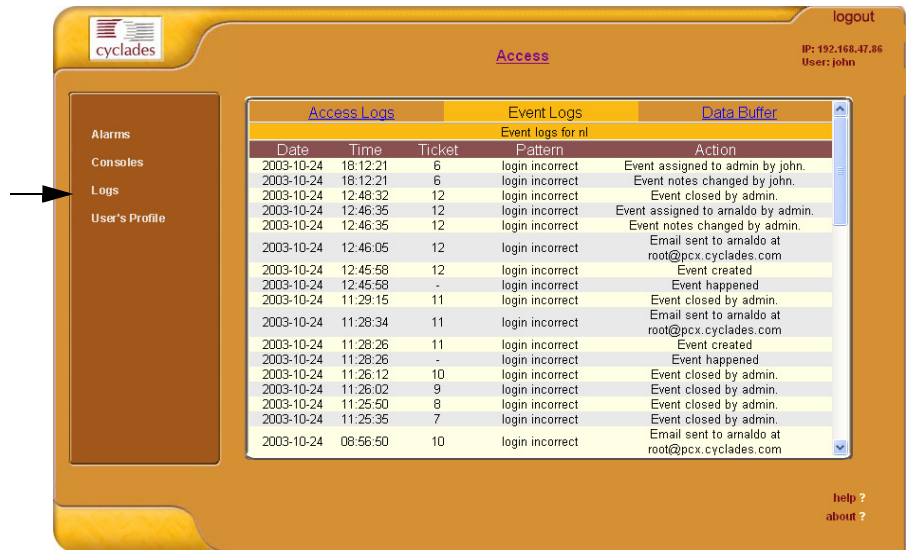


Figure 3.9 - Event Logs Browser

Log Field Definition

<i>Field Name</i>	<i>Definition</i>
Date	Date of the event.
Time	Time of the event.
Ticket	Ticket number associated with the event.
Pattern	Trigger Expression
Action	Action taken to resolve event.

Console Log Buffer

Use the Console Log Buffer browser to view the contents of the data buffer generated by a target console.



Figure 3.10 - Data Buffer Browser



*You can also access the Console Buffer log from the **Alarms** form.*

User Profile

The User Profile form allows you to view your profile or contact information and modify a limited number of fields. The system does not allow you to view other user profiles other than your own.

The screenshot shows the 'User Profile' form in the 'cyclades' interface. The form is titled 'Access' and displays the following information:

- User Name:** john
- Full Name:** John Doe
- Department:** Development
- Location:** New York
- Phone:** 415-666-1234
- Mobile:** 415-666-6789
- Pager:** 415-666-4321
- Email:** john@abc.com
- Status:** Enable
- Local Password:** Set Password
- Admin User:**
- Consoles:** Server77, n1

Figure 3.11 - User Profile form

Form Fields and Elements

<i>Field Name</i>	<i>Definition</i>
Full Name	User's full name.
Department	User's department.
Location	Location of department.
Phone	User's phone number.
Mobile	User's mobile phone number.
Pager	User's pager number.
Email	User's email. This is the same field name used by the system for event notification.

Working from a Command Line Interface (CLI)

The E2000 allows you to use a command line interface (CLI) as an alternative to the web interface. You may use Linux or Windows-based secure shell (SSH) client. The same restrictions to the web interface apply to the CLI.

Logging In

To connect to the E2000, enter the following shell commands:

```
> ssh -l <username> <IP address of E2000>  
> <password>
```

If you are an administrator, the system will display a menu. You can either run the console shell from the menu

- OR -

Go directly to the system prompt.

See sample print of a CLI session at the end of this chapter.

If you are a regular user, you will get the console shell alone, without a menu or system prompt.

Shell Commands

A list of commonly used CLI commands for operating the E2000 are as follows:

<i>Command</i>	<i>Use this command to:</i>
man list	list the available commands
man <command name>	get a definition of a command
consolelist	list all consoles allocated to you as defined in the access control list.
console <console name>	connect to the console.
page <console name>	display the content of the data buffer file for the specified console.
searchlog	search the data log files for alarms.

Copying and Pasting Text within the Console Applet Window

The APM allows you to copy and paste text within your console (Java applet) window to facilitate any command line configuration of a device and other similar operations.

To use the *copy & paste* feature, right click your mouse. This invokes a pop-up menu with the following options:

<i>Menu Option</i>	<i>Use this option to . . .</i>
Copy	Copy text from the applet window or another source.
Paste	Paste text to the applet window.
Disconnect	Close the applet window and disconnect your SSH session.
Send Break	Cause an OK prompt to appear on the applet screen..

The copy and paste feature follows the standard Windows/GUI convention of clicking the mouse, dragging it over the text to be copied, releasing the mouse to capture the entire text, and then positioning your cursor to the desired destination as you select the Paste option.

Connecting Directly to Ports

It is possible to connect to console ports using the E2000 as a security proxy. Using SSH on your workstation, type in:

```
ssh <user name>:<console name>@<IP address of E2000>
```

This command opens a SSH connection to the manager, checks the username and password, checks the access control list to verify user access, and then establishes the connection to the appropriate console.

Sample Command Line Interface

An example of a command line interface as accessed by an admin is shown below:

```
*****
```

```
login as: [This field is absent if the user is logged in as an admin.]
```

```
Password:
```

```
-----  
AlterPath Manager  
-----
```

Please choose from one of the following options:

- 1.CLI
- 2.Shell Prompt
- 3.Quit

```
Option ==> 1
```

```
User: admin
```

```
AlterPath Manager @(#)V_1.1.0b (Mar/19/2004) - CLI
```

```
admin@Mgr>
```

```
admin@Mgr>
```

```
admin@Mgr> man list
```

```
console      - connects to a console
```

```
consolelist  - lists all monitored consoles
```

```
page         - prints all lines in a console's logfile
```

```
searchlog    - prints lines in a console's logfile  
                that match a pattern
```

```
man <command> - to get help text of <command>
```

```
admin@Mgr>
```

```
admin@Mgr> consolelist
```

```
Mail-2 - port 1
```

```
DB-7 - port 2
```

```
admin@Mgr>
```

```
admin@Mgr>
```

```
admin@Mgr> console Mail-2
```

```
[Enter `^Ec?' for help]
```

```
[Enter `^Ec.' to disconnect]
```

```
*****
```

CLI Commands

For your convenience, the CLI key commands (accessible by pressing ^Ec?) are summarized in the table below. Each command must be preceded by ^Ec (i.e., <Ctrl><Esc>)

<i>Key(s)</i>	<i>Command</i>	<i>Key(s)</i>	<i>Command</i>
.	disconnect	a	attach read/write
b	send broadcast message	c	toggle flow control
d	down a console	e	change escape sequence
f	force attach read/write	g	group info
i	information dump	l?	break sequence list
l0	send break per config file	l1-9	send specific break sequence
o	(re)open the tty and log file	p	replay the last 60 lines
r	replay the last 20 lines	s	spy read only
u	show host status	v	show version info
w	who is on this console	x	show console baud info
z	suspend the connection	<cr>	ignore/abort command
?	print this message	^R	replay the last line
\ooo	send character by octal code		

To exit from the CLI, press: <cr> <shift>_
(i.e., <Ctrl> <Shift> <underscore>)

Changing the Escape Sequence

There are two ways to change the escape sequence:

- Locally: From the console session, use option ^Ece (refer to the table of help above for 'e') to change the escape sequence. It applies only to the current console session. Once you log off, the escape sequence is deleted.
- Globally: Change file **/var/apm/bin/con** as below. To make it permanent, you must include this file in the **/etc/files.list** and then run **saveconf**.

```
#original line in /var/apm/bin/con
exec /var/apm/bin/console -Mlocalhost -l$USR $1
```

```
#modify this line to have -e <escape seq>. In this example esc seq= ^Az
exec /var/apm/bin/console -Mlocalhost -e^Az -l$USR $1
```

The result of this change in the console session is as follows:

```
[arnaldo@hp arnaldo]$  
[arnaldo@hp arnaldo]$ ssh -ladmin:acs8_02 192.168.47.86  
Password:  
Console on-demand, please wait...  
[Enter `^Az?' for help]  
[Enter `^Az.' to disconnect]
```

Re-defining the Interrupt Key

The key sequence **Ctrl+C** in the file **/var/apm/bin/apmrun.sh** has been changed to **Ctrl+_** (that is: **^_**) to prevent the system from directing this command to any application running on the foreground rather than to the console server. Unlike **^C**, the latter is not a valid key combination for most servers including Sun, and should enable you to interrupt the console server as necessary.

If, however, you need to re-define the command, you may do so from the **apmrun.sh** file as shown:

```
/var/apm/bin/apmrun.sh  
# Redefine CTRL+C here. Customize it as you wish.  
stty intr ^_
```

Chapter 4

Configuring the E2000

This chapter presents the procedures and underlying concepts for configuring the AlterPath Manager E2000. Addressed to the E2000 administrator, the primary user of the web configuration interface, the chapter is organized as follows:

- Operational Modes
- Configuration Process Flow
- Using the First Time Configuration Wizard
- Connecting to the E2000 Web Interface
- Using the Admin Mode
- Logging Into the E2000 Web Interface
- E2000 Web User Interface
- Device Management
- Configuring Your DHCP Server
- Auto Upload and Manual Upload
- Configuring Modem Dialing Capability
- Managing Modems via Command Line Interface
- Configuring the Health Monitoring System
- Using the Console Wizard
- Device Discovery
- Uploading Firmware into the Console Devices
- Profile List Form
- Console Management
- User Management
- Triggers and Alarms Management
- Info Reporting Main Form
- Firmware Management
- Backing Up User Data
- Backup and Restore Scenarios
- Backup and Restore Commands
- System Recovery Procedures

Operational Modes

The E2000 provides you with two operational modes:

- First Time Configuration (CLI / text-based)
- Admin Mode (GUI-based)

As the name implies, you use the First Time Configuration mode the first time you configure E2000 and the devices associated with it.

The admin user, by default, is the system administrator of the E2000 web interface and runs the application in **Admin** mode. This designation cannot be revoked. Your users will be using the application in Access mode. An administrator, however, can assign admin roles to new users.

As the administrator, you have the authority to add users, consoles, devices (console servers) alarms, and other configuration procedures.



*Refer to the previous chapter, **Using the E2000**, for information on using the system in Access mode.*



*The only other time you may need to use CLI is during system recovery. The Recovery procedure is discussed in more detail in the **System Recovery** section of this chapter.*

Configuration Process Flow

The process flow below is designed to guide you through the configuration process. By mapping the procedures, you may understand how one procedure relates to another, and how they relate to the entire configuration process.

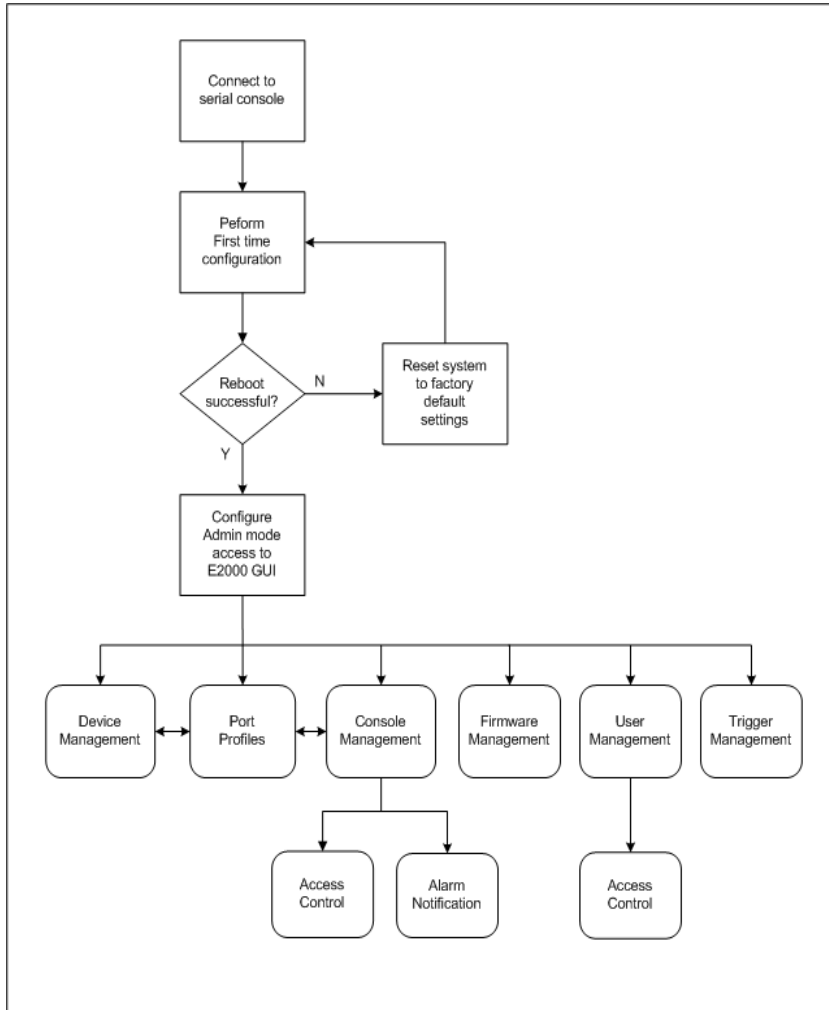


Figure 4-1: Configuration Flow Diagram

You perform the first part of the configuration process (see Figure 4.1: Configuration Flow Diagram) using the command line interface. Once completed, you perform the rest of the configuration process and all daily administration procedures through the E2000 web interface.

To configure all your devices with the E2000 (using the web interface), you must first configure the console servers (Device Management and Profiles windows), and then connect consoles to the devices (Consoles Management windows).

Firmware Management is used to update firmware and to enable you to select from different versions of firmware, or just to view information about a particular firmware.

Once you have configured the consoles, you can define users and assign them to access the target consoles (User Management windows), and define the triggers that will create alarms and send email notifications (Trigger Alarm Management windows) to users.

First Time Configuration

Before you proceed with First Time Configuration, check to ensure that your system is set up properly. If you are using a PC, ensure that HyperTerminal is installed on your Windows operating system. If you are using the UNIX operating system, use Kermit or Minicom.

Ensure that you have a NIC card installed in your PC to provide an Ethernet port, and allow network access.

Refer to Chapter 2: Installing the E2000 for procedures on how to prepare for First Time Configuration.

This section is organized as follows:

- Using the First Time Configuration Wizard
- First Time Configuration Wizard: An Example
- Re-setting Configuration to Default Settings

Using the First Time Configuration Wizard

The first time configuration process is designed to:

- Establish user as root, the superuser for the CLI.
- Establish user as Admin, the superuser for the E2000 web user interface.
- Initialize your system and user settings to ensure full connectivity and functionality of the E2000.

The two important requirements of First Time Configuration is that you must:

- Connect to a serial console
- Log in as *root*

1. Connect management console to E2000.
2. Boot your management console.
3. Follow the configuration wizard. You may configure the following manually, or press **Return** to accept the default value(s).
 - Enter Root password (and re-type)
 - Enter Admin password (and re-type)
 - Enter Authentication Method (Local/RADIUS/LDAP/Kerberos)



If you select **RADIUS**, the system will prompt you for the RADIUS *server name* and *secret*; if you select **LDAP**, the system will prompt you for the LDAP *server name* and *server base*.

- Enter Date (format MM/DD/YYYY)
- Enter System's Hostname (30 characters max)
- Enter Primary Ethernet (Static/None).
- Enter Primary Ethernet IP address
- Enter Primary Ethernet subnet mask
- Enter Secondary Ethernet (Static/None)
- Enter Secondary Ethernet IP address
- Enter Secondary Ethernet subnet mask
- Enter Ethernet default gateway
- Enter Domain name (60 characters max)
- Enter Primary nameserver's IP address
- Enter Secondary nameserver's IP address
- Enter SMTP server (IP or hostname)

Resetting Configuration to Factory Default Settings

If you make a mistake during the First Time Configuration (or if you need to make a change in the configuration), you can reset the configuration to its factory default settings and start over. To reset the configuration, follow these steps:

1. Log in to the management console as root.
2. Type in: **defconf** and press <Enter>.
3. Type in: **reboot** and press <Enter>.

Example:

```
E2000 login: root
Password:
.
.
[root@E2000 root]# defconf
```

```
WARNING: this will erase all of your current configuration and restore the
system's factory default configuration. This action is irreversible!
```

```
Are you sure you wish to continue? (Y/N) y
Restoring default configuration ... done.
```

```
The new configuration will take effect after the next boot.
[root@E2000 root]# reboot
```

Refer to the sample First Time Configuration, next section, to view how the parameters are entered into the system.

4. Save and reboot.

Once saved, the E2000 applies the new configuration to the system and saves the information on a Compact Flash card.

First Time Configuration Wizard: An Example

The First Time Configuration sample session shown below shows the portion of the command line data where the user configuration begins. This is commenced by the heading, Welcome to Cyclades-APM!

CAUTION: *Before the Welcome heading appears, the system will prompt you for the following:*



Do you want to re-create hard disk partitions? (y/n) [n]
 Do you want to re-create the System file system? (y/n) [n]
 Do you want to re-create the Console Log file system? (y/n) [n]
 Do you want to re-create the Configuration file system? (y/n) [n]

*Be sure to answer **no** to the above questions. Once completed, you should see the configuration text as shown in the example below.*

The afore discussed parameters are represented in **boldface**.

Welcome to Cyclades-APM!

Since this is the first time you are booting your APM, you need to answer some basic configuration questions. Once this is done, the other APM configuration parameters can be set through its Web Management Interface (WMI).

Press any key to continue.

You must now set a password for 'root', the system administrative account.

WARNING: this is a very powerful account, and as such it's advisable that its password is chosen with care and kept within the reach of system administrators only.

New password:

Re-enter new password:

Password changed

You must now set a password for 'admin', the administrative account for the Web Management Interface (WMI).

WARNING: this is a very powerful account, and as such it's advisable that its password is chosen with care and kept within the reach of system administrators only.

New password:

Re-enter new password:

Password changed

Choose the desirable authentication method: (local/radius/ldap/kerberos/tacacs+)[local]:

Current system date and time is:

4: Configuring the E2000

```
Wed Nov 19 03:57:41 GMT 2003
Press ENTER to accept it or specify new ones.
Enter date in MM/DD/YYYY format:
Wed Nov 19 03:57:00 GMT 2003
Enter the System's Hostname
(max 30 characters, ENTER for default: 'E2000'):
Primary Ethernet IP address: [S]tatic or [N]one? (S/n)

Enter Primary Ethernet's IP address: 192.168.46.24
Enter Primary Ethernet's Subnet Mask: 255.255.252.0
Secondary Ethernet IP address: [S]tatic or [N]one? (S/n)

Enter Secondary Ethernet's IP address: 10.0.0.1
Enter Secondary Ethernet's Subnet Mask: 255.0.0.0
Enter Ethernet Default Gateway (ENTER for none): 192.168.44.1
Enter the System's Domain Name
(max 60 chars, ENTER for default: 'localdomain'): cyclades.com
Enter the Primary Nameserver's IP address (ENTER for none): 192.168.44.21
Enter the Secondary Nameserver's IP address (ENTER for none):
Enter the NTP server: 192.168.44.1
Enter the NTP client network address: 192.168.44.0
Enter the NTP client network mask: 192.16      255.255.252.0
Enter the email (SMTP) server: mail.cyclades.com
Saving configuration files to flash (/flash/config/config.tgz) ... done.
Removing init_config flag... done.
mount: Mounting /proc on /proc failed: Device or resource busy
Checking root file system...
SYSTEM: clean, 3528/577152 files, 66985/1152655 blocks
.
.
done.
```

[At this point, First Time Configuration is complete. Close the terminal session at the point and proceed to the web interface.]

The sample First Time Configuration uses *local* as the Authentication Method to be used.

Depending on the type of authentication service that you select, you will be prompted for questions relating to the authentication service of your choice. For example, if you select RADIUS, the system will prompt you for the RADIUS server name and the secret. Selecting TACACS+ will prompt you for the TACACS+ server IP address and the shared secret.

Connecting to the E2000 Web Interface

Now that the installation is complete, you can begin the configuration using the web interface.

1. Type in the following URL from your web browser:

`http://nnn.nnn.nnn.nnn`
(*Non-encrypted version*)

- OR -

`https://nnn.nnn.nnn.nnn`
(*Encrypted version*)

Where: **nnn.nnn.nnn.nnn** is the IP address of either the first or second Ethernet interface that you defined during the First Time Configuration.

2. When the Login screen appears, enter **admin** as the username and the password (as specified in the First Time Configuration wizard).

The admin user is by default the manager of the E2000 web interface and runs the application in **admin** mode. This designation cannot be revoked.

Disabling HTTP to Use Only HTTPS

The E2000 is configured to allow both HTTP and HTTPS access. You can, however disable HTTP access by commenting out its configuration in the E2000 unit by using the command line. To do so, perform the following steps:

1. Edit the file: `/opt/tomcat/conf/server.xml`
2. Using the exclamation mark (!) and the double dash (--), comment out the following XML paragraph:

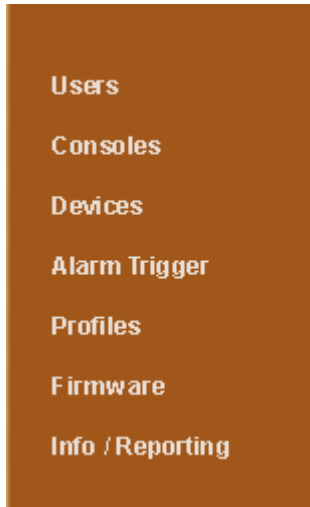
```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8080 -->
<!-- Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="80" minProcessors="5" maxProcessors="75"
enableLookups="true" redirectPort="443"
acceptCount="100" debug="0" connectionTimeout="20000"
useURIValidationHack="false" disableUploadTimeout="true" /-->
```

3. Restart the web server using the following command:

```
/etc/init.d/tomcat stop
/etc/init.d/tomcat start
```

Using the Admin Mode

Now that you have completed the First Time Configuration procedure, you can now log into the E2000 web application (GUI interface) and use the system in Admin Mode. Using the Admin mode, you have seven areas of configuration management as shown on the menu panel:



Before discussing configuration procedures using the web application, let us take a quick look at the GUI interface.

Logging Into the E2000 Web Interface

To log in, follow the following steps:

1. Type in your username and password in the corresponding fields of the Login screen:

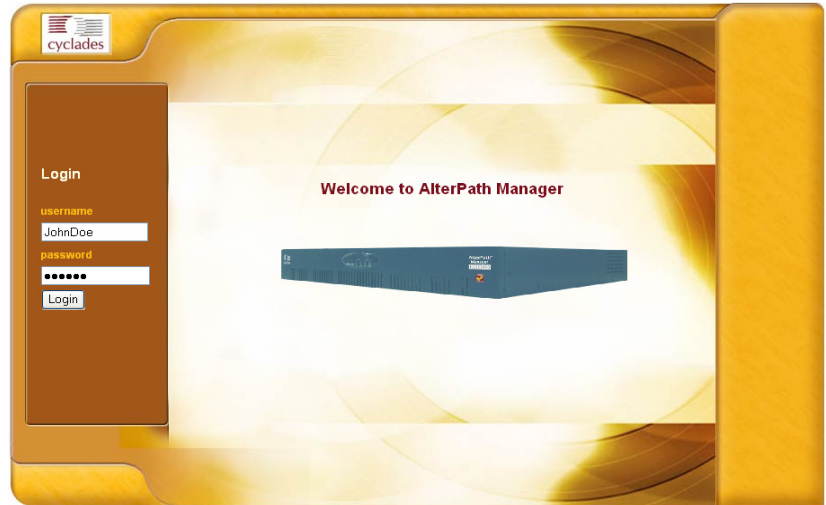


Figure 4.2 - E2000 Login Screen

2. Select the **Login** button.

Upon successful login, the User List form appears.



When E2000 launches your application screens for the first time, the process tends to be slow. The system needs to build all the web pages in the E2000 Manager. Once the screens are stored, their subsequent retrieval should be fast.

E2000 Web User Interface

Shown below are the basic features of the E2000 Web User Interface. The screen example is for illustration purposes only; it is not the first screen to appear in the web application.

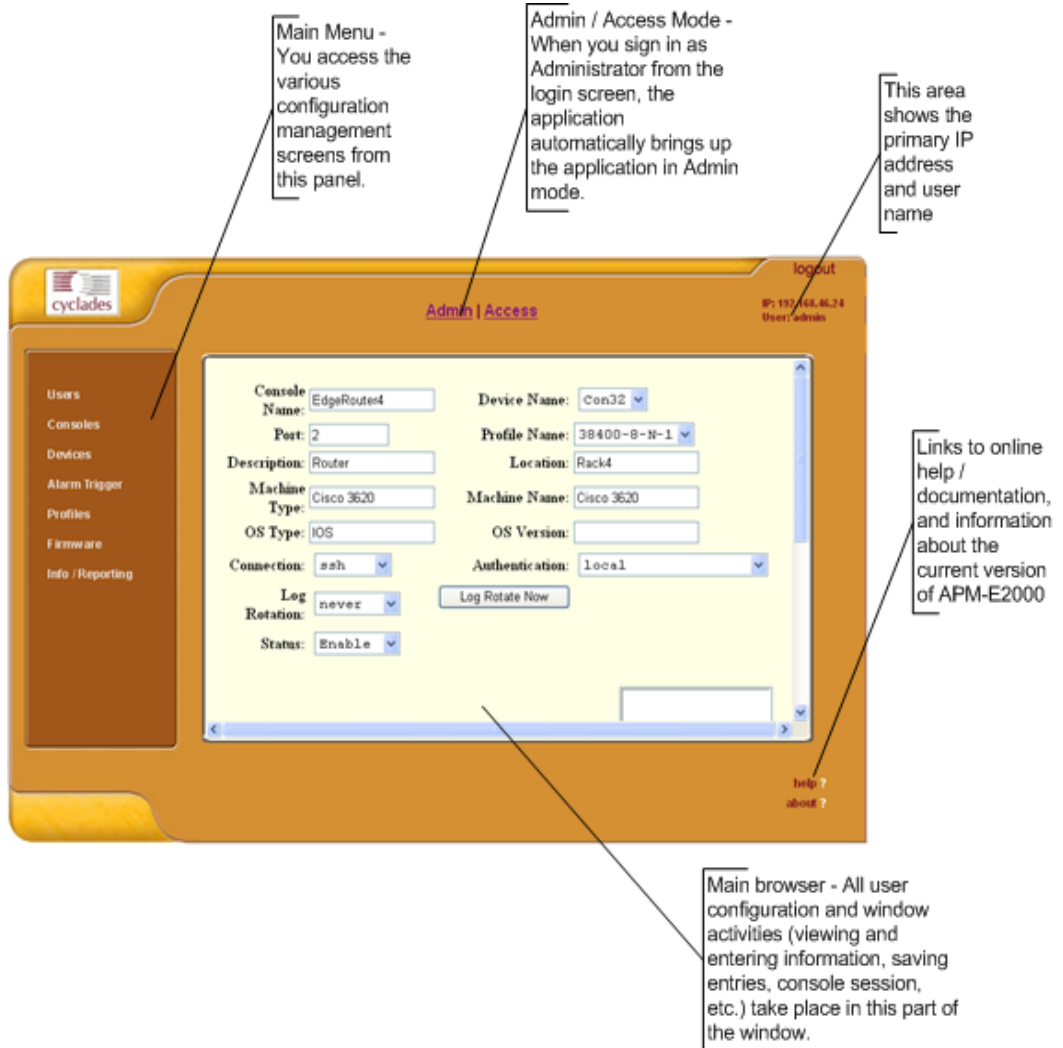


Figure 4.3 - Parts of the Application Screen

Device Management

Device management is the process by which you configure E2000 to:

- Define all devices (*i.e.*, serial console servers such as Cyclades' ACS family) you want to connect to E2000
- Upload device firmware/bootcode or configuration
- Set up health monitoring of devices
- Configure PPP connection for out-of-band access to remote devices.
- Run the Console Wizard

Device Management consists of two forms:

- Device List form
- Device List>Device Definition form



The form names do not necessarily appear on the actual form. Because some forms do not have titles, these names are used to distinguish each form as well as to reflect its form function. Most forms are categorized as either a List or Main form, or a Definition or Detailed form.

Other forms you may need to access to manage your devices are:

- Console List form
- Console List > Console Definition form
- Firmware form

Because target consoles are part of your devices, device management and console management are related. Also, you may need to refer to the **Firmware** form for any information you might need pertaining to device and firmware.

Normally, when a new firmware is imported to E2000, the new firmware is added to the database and reflected in the Firmware List form and the **Firmware/Boot** dropdown list of the Device Definition form.

Device List Form

The Device List form, shown below, is the primary form for device management.

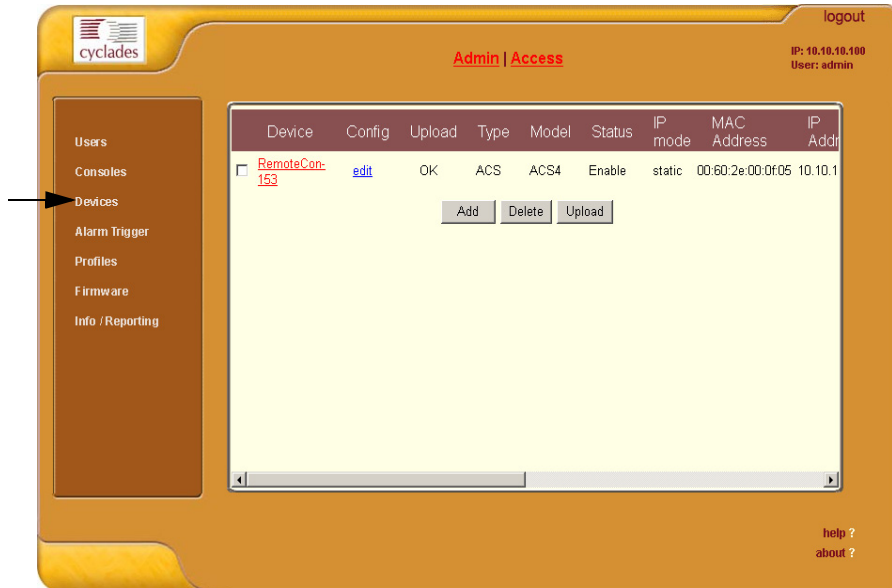


Figure 4.4 - Device List form

Form Fields and Elements

For a definition of the fieldnames on this form, refer to the *Form Fields and Elements* heading of the *Device Definition* form. Selectable buttons on this form are:

<i>Field Name</i>	<i>Definition</i>
Add	Button used to add new devices.
Delete	Button used to delete the devices.
Upload	Button used to upload the configuration or firmware to the selected device.

Adding a Device

To add a device, perform the following steps:

1. From the Device List window, select the **Add** button.
The system brings up the Device Definition Window.
2. From the Device Definition window, enter all the necessary device information.



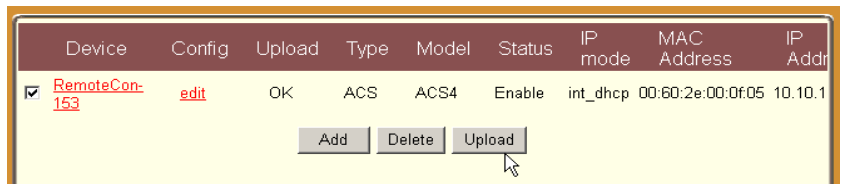
See **Device Definition Form**, next page, and refer to the **Form Fields and Elements** section for an explanation of each field.

3. Select **Save**
4. Select **Devices** from the main menu panel to return to the **Devices** form and verify your entry.

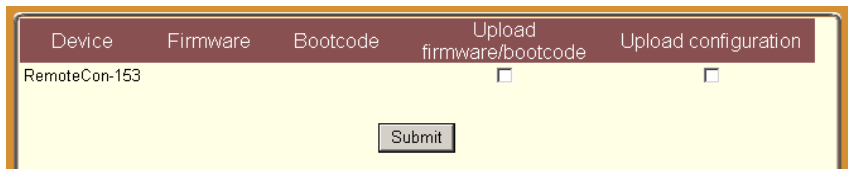
Uploading Firmware to a Device

To upload firmware to a device:

1. From the Device List window, select the device (from which you wish to update or upload the firmware) by clicking the check box to the left of the device name.



2. Click **Upload**.
The system brings up the *Device Firmware Upload* window.





The Required flag in the Upload column indicates that, based on your device or any configuration changes you did to a device, you will need to upload the configuration or the firmware or both.

Deleting a Device

To delete (or unlink) a device from E2000, follow the steps below:

1. From the Device window, select any device you wish to delete by clicking on the checkbox on the lefthand side of the console icon.
2. Select the Delete button.

Device Definition Form

Use the Device Definition form, shown below, to configure a device.

Figure 4.5 - Device Definition form

Form Fields and Elements

Field Name	Definition
Device Name	Symbolic name linked to the console server device.
Type	Type of console server (currently supported servers are Cyclades TS and Cyclades ACS).
Model	Model of TS or ACS selected.

<i>Field Name</i>	<i>Definition</i>
Location	Physical location of the device.
Admin Username	Admin superuser of the device.
Admin Password	Button to invoke a dialog box used to define the Admin user's password. This password is used to access the console server port, but NOT to change the password. You must enter the SAME password registered in the console server.
IP Address	IP address of console server for IP mode: int_dhcp or static .
Netmask	As indicated, in dotted notation.
Default Gateway	As indicated, in dotted notation.
DNS	As indicated, in dotted notation.
Base Port	TCP port number allocated in the first serial port of the console server.
Connection	Drop down list to select connection method used between E2000 and console serial port (SSH or Telnet).
IP Mode	Drop down list. Select int_dhcp if APM E2000 is the DHCP server for this device, or ext_dhcp if DHCP is served by another server), or Static if using a static IP. <i>See Configuring Your DHCP Server, this chapter.</i>
MAC Address	The MAC address if IP mode: int_dhcp is used.
Status	Pull down list to select: Enable - connection between the E2000 and the device/console is ALWAYS established. Disable - no connection is established, and all child consoles follow this configuration. OnDemand - connection is established only upon user's request.
Auto Upload	Check Auto Upload if you want your configuration automatically uploaded when you save it. <i>See Auto Upload and Manual Upload, this chapter.</i>
PPP Device IP	<i>Optional.</i> If this is blank, the device IP is used for PPP modem connection.
PPP Local IP	<i>Optional.</i> If this field is blank, the E2000 IP is used for PPP.

<i>Field Name</i>	<i>Definition</i>
PPP Phone	<i>Required for PPP connection.</i> Enter the PPP phone to establish PPP connection to a device or console via web interface, CLI, or SSH.
Modem Mode	Select how you want your PPP connection to be used: Disabled - default value. Primary Network - uses a modem connection as the primary way to connect to a device. The connection is dropped when the last user disconnects. Network Backup - uses a modem connection only if the network connection is unavailable.
Wizard: Create Consoles	Button to initiate the Console Wizard.
Health Monitor	Select the frequency of the Health Monitoring feature. Choices: Never (default), Daily, Weekly or Monthly.
Firmware/Boot	Firmware to be uploaded into the console server.
Reset	Button to reset the form.
Save	Button to save Device information entered from this window.
Save / Create Consoles	Button to initiate the Console Wizard and save the resulting settings.
Save / Auto Discover	Button to initiate the ACS and TS device discovery wizard and save the resulting settings.



For Health Monitoring to work with alarms, you must create the alarm triggers. See Configuring Health Monitoring in the Device section of this chapter.

Configuring Your DHCP Server

A DHCP server is build into the E2000. You can use either your company's DHCP server or the E2000 as your DHCP server. If you are not using a DHCP server, then you may use a static IP address.

The Device Definition window provides three IP modes in which to configure your DHCP server or static IP address. The IP address that you use depends on what type of mode you use.

<i>IP Mode</i>	<i>When to use this mode</i>
int_dhcp (internal)	Select this mode if you are using the E2000 as your DHCP server. You decide on what IP address you wish to use and then save the configuration in the Device Definition form.
ext_dhcp (external)	Select this mode if you already have a DHCP server in your LAN that you wish to use. You will need to get from your System Administrator the IP address allocated for your company's DHCP server.
Static	Select this if using a static IP address. When using the static mode, you (or your LAN/System Administrator) must first connect to the console server using the serial console to enter the IP address. You must then enter that same IP address in the E2000 through the Device Definition form.

About the Status: OnDemand

The **Status** field of the Device Definition form indicates the connection type of the E2000 based on whether the connection is **Abled** (*i.e.*, permanently connected), **Disabled** (no connection established), or **OnDemand**.

OnDemand means that the connection between the E2000 and the device/console is established only upon the user's request, and the connection is disabled when the last user on the console/device logs out. When disconnected, no data buffer or alarm is available.

About Auto Upload and Manual Upload

From the E2000 interface, there are two ways in which you can upload your device configuration to the console server(s):

- Auto Upload
- Manual Upload

When the **Auto Upload** box is checked from the Device Definition form, anytime you make a change to a device or console parameter, the change is automatically uploaded to the console server after you select save from whichever form you were making the change.

With Manual Upload (i.e., the Auto Upload in the Device Definition form is unchecked and you upload by selecting Upload from the Device List form) all changes are cached into the E2000 until you select the **Upload** button.

While automatic uploading saves you from having to open the Device List form and clicking the **Upload** button, be aware that configuring in automatic mode can lead to slow system response due to excessive uploading.

Modem Dialing Capability for Remote Access to Devices

The E2000 has modem dialing capability to enable complete out-of-band access to remote console server devices. The protocol used to dial out is PPP. To use this feature, you must set the Status to **OnDemand** from the Device Definition form, and configure the appropriate PPP settings.

The E2000 checks the same configuration in conjunction with Health Monitoring.

You can establish PPP connection using any of the following methods:

- Clicking on a console or device from the web interface.
- Starting a SSH session to the E2000 and entering the username as follows:
`<username>:<console name>`
- Uploading device configuration

Modem Mode

There are three modes of PPP connection:

- Disabled - This is the default value.
- Primary Network - If you select this, the E2000 establishes a PPP connection whenever a user connects to a device or console. The modem connection remains as long as there is a console port open.
- Network Backup - If you select this, the connection between the E2000 and the device will preferably be done via Ethernet. In the event that the device becomes unreachable via Ethernet, a PPP connection is established as a backup network whenever a device/console access is requested.

Health Monitoring and PPP Settings

The E2000 uses the same PPP settings to enable Health Monitoring. The Health Monitoring feature is not affected regardless of whether the Mode selected is **Primary Network** or **Network Backup**.

Actions Not Recommended While Using PPP

Changing the Device IP or the Device Name (including deleting or disabling it) to which the console belongs while running PPP will cause a disconnection if no upload is in progress. Any device change during an upload will not save your upload.

Configuring the Modem Dialing Capability

To configure the modem dialing capability, follow the procedure below:

1. From the Device Definition form (Devices > Add > Device Definition form), select the **Modem Mode**:

Modem Mode provides three choices:

<i>Option:</i>	<i>Use this option if you want to use PPP:</i>
Primary Network	As the primary mode of connection.
Network Backup	Only when the network fails.
Disable	Default value. (If you select this, then you don't need to do this procedure.)

2. For Status, you must select **On Demand**.
3. Complete the PPP settings as follows:
 - PPP Device IP *Optional*. Enter the IP address for the current device.
 - PPP Local IP *Optional*. Enter the local IP address for using PPP.
 - PPP Phone *Required*. Enter the complete PPP phone number.
4. Select the **Save** button to complete the procedure.

Modem Management via Command Line Interface

Depending on the customer order, your APM unit may or may not come with internal modems. This section present three common command line procedures for managing modems, with examples using four modems:

- Checking your modems
- Excluding modems from the modem pool
- Viewing the latest status of each modem

Checking Your Modems

The internal modems are detected during bootup, and all modem devices present are included automatically in the modem pool. To view which modems are in use or which ones are available, use SSH to connect to **APM**, login as **root**, and use the following commands:

```
check_modem ( -d | -s ) [tty]
```

Where: -d disconnect

-s status

[tty] If no tty is specified, then the command applies to all modems.

To check what modems are available, type in: `check_modem -s`

Example:

```
[root@Penguin root]# check_modem -s
ttyPS0 Available
ttyPS1 Available
ttyPS2 Available
ttyPS3 Available
```

Excluding Modems from the Modem Pool

If your configuration requires less than four modems, then you must exclude the unnecessary modem(s) from the pool to prevent a dial-up failure. When you exclude modems, be sure to run and save your configuration as follows:

1. Using VI, edit the following file: **vi /var/apm/apm.properties**
<Enter>
2. Type in: **modem.pool.exclude=ttyPS**
For example, to exclude ttyPS2 and ttyPS3, type in:
modem.pool.exclude=ttyPS2 ttyPS3
3. Once a modem has been excluded, you must initialize the configuration by typing in:
/etc/init.d/modem_pool restart

WARNING: Be sure that no upload is in progress when you run this command otherwise all PPP connections will be disconnected. The same is true when disconnecting a modem (**check_modem -d <tty>**).

4. To save your configuration to flash, type in: **saveconf**
5. Verify your new configuration by typing in: **check_modem -s**

Viewing the Latest Status of Each Modem

The modems in the modem pool are allocated in a round robin sequence to ensure all modems are exercised to the same degree. If a modem fails to dial out, the system will allocate the next modem in the modem pool. The **/var/log/modem_status** file contains the result of the last attempted usage of a modem. Containing the modem, date, time, and status, it is created the first time a connection is attempted.

Example:

```
[root@Penguin root]# cat /var/log/modem_status
ttyPS0 2004/04/12 09:40:12 Dial out to acs48failed
ttyPS1 2004/04/12 09:42:35 Connected to acs32
ttyPS2 2004/04/12 09:32:23 Connected to acs32
ttyPS3 2004/04/12 09:35:00 Dial out to acs48 failed:
      NO DIAL TONE
```

Configuring the Health Monitoring System

The Device Health Monitoring feature enables the E2000 to monitor on a periodic basis the consoles that are running on specified devices, as well as to create log files, and to send an alarm notification to specified users. The users must have a valid email address as configured in the Users Definition form (Users > User Definition form).

1. From the Device Definition form (Device List>Device Definition), select the frequency of monitoring from the **Health Monitoring** drop down list. Your choices are:

Never	System will never run Health Monitoring for this device (default).
Daily	System will run Health Monitoring at 2 am everyday.
Weekly	System will run Health Monitoring at 3 am every Saturday.
Monthly	System will run Health Monitoring on the first of each month.
2. To complete the procedure for configuring Device Health Monitoring, go to the **Alarm Trigger Definition Form** section of this chapter.

Using the Console Wizard

The console wizard allows you to define the consoles connected to a device by automatically defining the consoles using default and customized values. The wizard configures the selected console(s) and applies them to the device.

If you use the wizard to define a new device which has no consoles defined, then all the consoles listed will be checked, and the console names generated automatically in the form: <device name>_nnn (where nnn = port number).

If you use the wizard to edit a device which already has consoles defined, then it will detect and list the consoles, but keep them unchecked. You can then decide which console should be checked and have the configuration overridden.

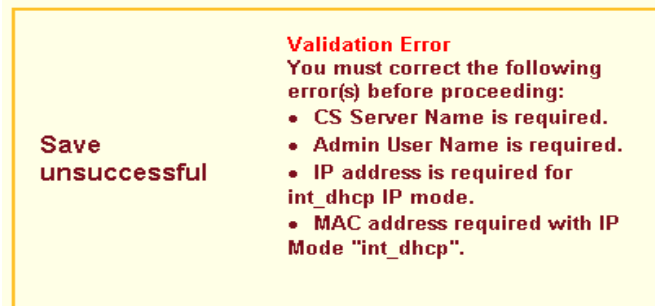
Summary of the Console Wizard Forms

The console wizard is composed of a series of configuration pages or forms. Once the wizard is activated, the forms will appear in the following order:

<i>Wizard Form</i>	<i>Function</i>
Warning	This page warns you about any data to be overwritten and the choices you have before going ahead with the wizard.
Defaults	Sets the profile, connection protocol, and authentication type.
Lists Edit	Selects the users to be notified and who can access the console(s).
Console Selection	Lists all consoles that have not been configured for this console server. Select the console(s) to be configured by the wizard.
Edit Consoles	Edits any settings for consoles connected to this console server.
Confirmation	Confirms your previous edits and selections. Select Finish to save configuration or select Back to re-edit.
Console in Use	Displays any consoles that are in use to allow you to ensure that users are logged out and their sessions closed.
Upload Progress	Indicates the percentage complete and displays any messages or errors. This page is shown if you did not check autoupload in the Device Configuration form.
Console Creation Finish	This page is shown if you did not select Autoupload from the Device Configuration form.

To Run the Console Wizard:

1. From the Device List form, select the device you wish to configure and then select **Edit** to modify an existing device, or select **Add** to configure a new device.
2. From the Device Definition form complete the following required fields for using the Console Wizard:
 - Device Name
 - Type (ACS or TS)
 - Admin User Name
 - IP address for IP mode: "int_dhcp" or "static"
 - MAC address if IP Mode: "int_dhcp" is used.
 - Check **Auto Upload** if you want your configuration to be uploaded automatically when you **save** it.
3. Select the **Create Consoles** button to invoke the console wizard.
If the Device Definition form is configured incorrectly, an error message such as the one shown below appears:

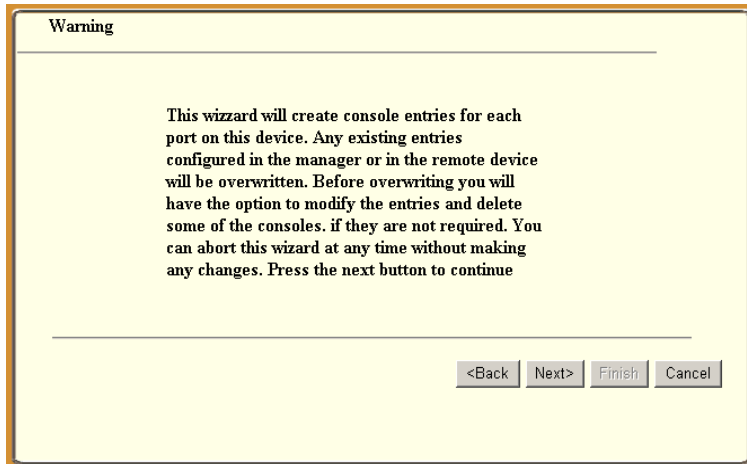


**Save
unsuccessful**

Validation Error
You must correct the following error(s) before proceeding:

- CS Server Name is required.
- Admin User Name is required.
- IP address is required for int_dhcp IP mode.
- MAC address required with IP Mode "int_dhcp".

If the Device Definition form is configured correctly, then the wizard invokes a warning message:



Warning

This wizard will create console entries for each port on this device. Any existing entries configured in the manager or in the remote device will be overwritten. Before overwriting you will have the option to modify the entries and delete some of the consoles, if they are not required. You can abort this wizard at any time without making any changes. Press the next button to continue

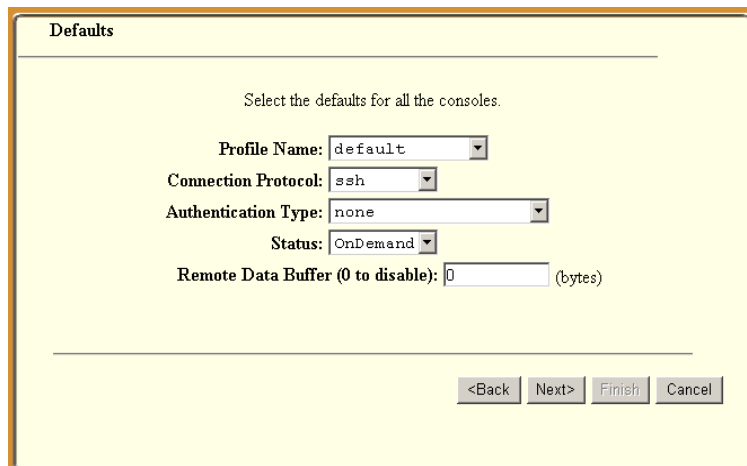
<Back Next> Finish Cancel



Use the **Back**, **Next**, and **Finish** buttons to navigate through the forms. Pressing the **Next** button saves your current form settings.

4. Select the **Next** button.

The system brings up the Defaults form which allows you to set the default profile, connection protocol, and authentication type for all consoles.



Defaults

Select the defaults for all the consoles.

Profile Name: default

Connection Protocol: ssh

Authentication Type: none

Status: OnDemand

Remote Data Buffer (0 to disable): 0 (bytes)

<Back Next> Finish Cancel

5. Complete the above fields, and then select the next button when done. The system brings up the **Lists edit** form:

Lists edit

Select the users to be notified and who can use the consoles...

Select User to Notify: user Users:

Select User To Access Console: user Users:

6. From the form, select or edit the users to be notified and who can access the console(s), and then select the **Next** button when done. The system brings up the Console Selection form:

Console selection

Below is a list of all consoles that have not been configured for this console server. Select the one(s) you wish to configure using the wizard.

Configure?	Console Name
<input type="checkbox"/>	Con-153_1
<input type="checkbox"/>	Con-153_2
<input checked="" type="checkbox"/>	Con-153_3
<input checked="" type="checkbox"/>	Con-153_4

<Back Next> Finish Cancel

7. From the form, select the unconfigured consoles that you wish to configure, and then select the **Next** button.

The system brings up the **Edit Consoles** form:

Console Name	Device Name	PortProfile	Connection	Authentication
Con-153_3	Con-153	3	default	ssh
Con-153_4	Con-153	4	default	ssh

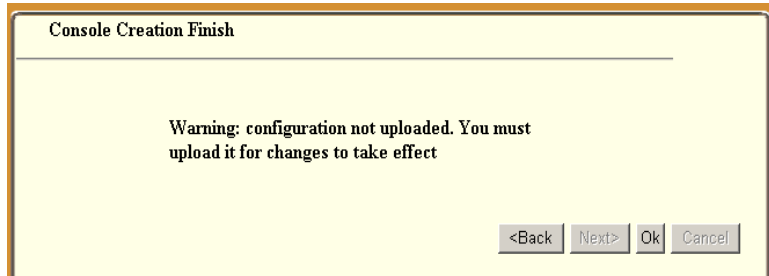
8. Follow the form instructions, and then select the **Next** button. To confirm your modified consoles settings, the system brings up the **Confirmation** form:

Console Name	Device Name	PortProfile	Connection	Authentication	Notify	Access Control
Con-153_3	Con-153	3	default	ssh	<input type="checkbox"/>	<input type="checkbox"/>
Con-153_4	Con-153	4	default	ssh	<input type="checkbox"/>	<input type="checkbox"/>

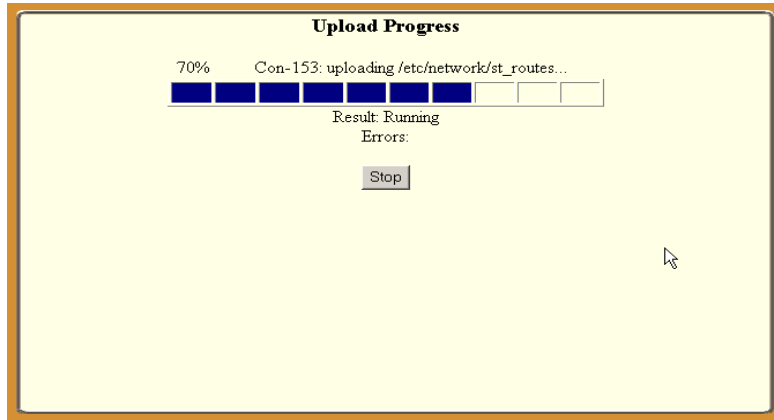
9. If information is incorrect, select the **Back** button and repeat steps 7 and 8, otherwise select the **Next** button.

4: Configuring the E2000

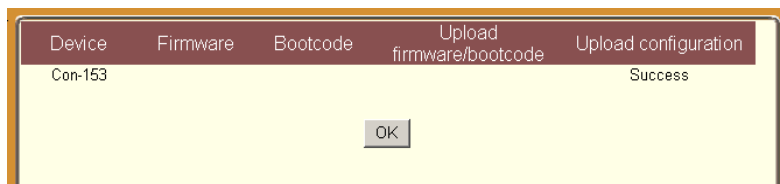
If you did not select **Autoupload** from the Device Configuration form, then the following message form appears:



Otherwise, the following form appears:



Once upload is complete, the system displays the uploaded device:



10. Select **OK** to complete the procedure.

Device Discovery

The Device Discovery feature enables the E2000 to recognize the current configuration of a Cyclades TS or ACS and, through the use of a wizard, autopopulate the console parameters based on the TS or ACS configuration settings.

Configuration Requirements

For the Auto Discovery button to work, you must complete the following required fields in the Device Definition form:

- IP Address
- Netmask or MAC Address
- Admin Username
- Admin Password

Using Device Discovery

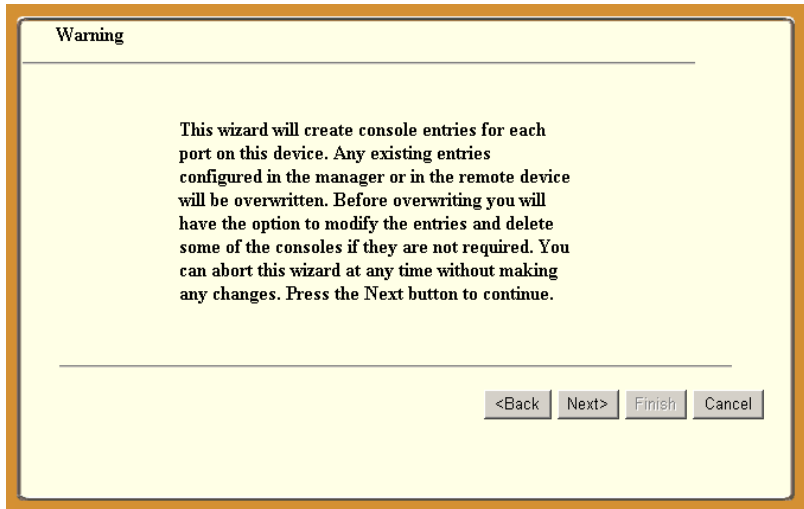
The procedure for running the Device Discovery Wizard is as follows:

1. Log in as admin to the E2000
2. From the menu, select **Devices**.
3. From the Device List form, select the **Add** button to configure the ACS/TS.
4. From the resulting Device definition form, if you are using **static IP mode**, complete the input fields with particular attention to the following:
 - Device Name
 - Type and Model must match
 - Enter the Admin Username and Admin Password from the configured ACS or TS.
 - IP Address and Netmask from the configured ACS or TS.
 - Select IP Mode as **Static**
 - Check mark the **Auto Upload** box.

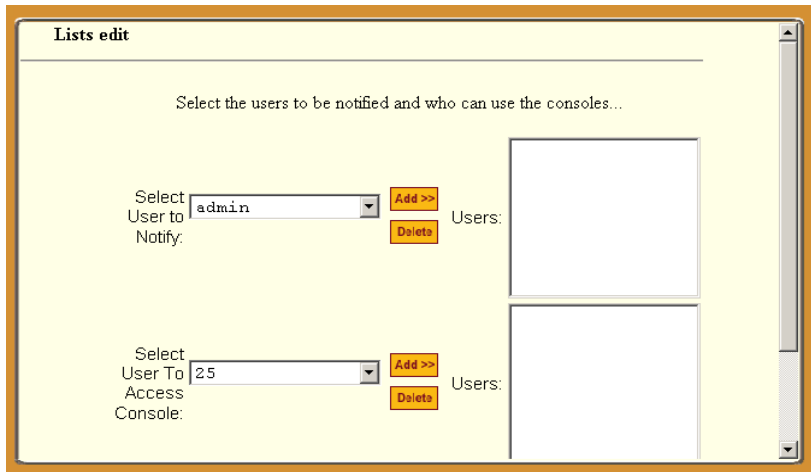
If you are using internal DHCP mode, select IP Mode as **int_dhcp** and also include the ACS/TS MAC Address.

5. To start the Console Wizard, select the **Save / Auto Discover** button. The system invokes Warning page which may include any configuration errors that you may need to fix in the Device definition form before you can select the **Next** button.

The **Warning** page typically looks like this:



6. Select the **Next** button.
The **Lists edit** form appears:



7. Complete the form as necessary, and then select the **Next** button.

The **Edit consoles** form appears:

Edit consoles

Edit any settings for the consoles for this console server. You can press Advanced to edit other console settings.

Console Name	Device Name	Port	Profile	Connection	Authentication
AReal1_01	AReal1	1	9600-8-none-1	ssh	local
AReal1_02	AReal1	2	9600-8-none-1	ssh	local
AReal1_03	AReal1	3	9600-8-none-1	ssh	local
AReal1_04	AReal1	4	9600-8-none-1	ssh	local
AReal1_05	AReal1	5	9600-8-none-1	ssh	local
AReal1_06	AReal1	6	9600-8-none-1	ssh	local
AReal1_07	AReal1	7	9600-8-none-1	ssh	local
AReal1_08	AReal1	8	9600-8-none-1	ssh	local

- From the **Edit consoles** form, make any edits if needed, else select the **Next** button.

The Confirmation form appears:

Confirmation

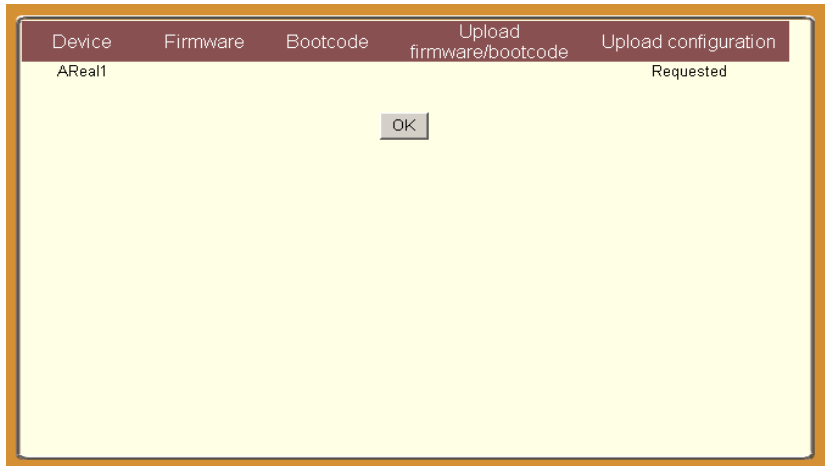
This screen confirms your previous edits and selections. Pressing Finish will save these changes. Press back to reedit.

Console Name	Device Name	Port	Profile	Connection	Authentication
AReal1_01	AReal1	1	9600-8-none-1	ssh	local
AReal1_02	AReal1	2	9600-8-none-1	ssh	local
AReal1_03	AReal1	3	9600-8-none-1	ssh	local
AReal1_04	AReal1	4	9600-8-none-1	ssh	local
AReal1_05	AReal1	5	9600-8-none-1	ssh	local
AReal1_06	AReal1	6	9600-8-none-1	ssh	local
AReal1_07	AReal1	7	9600-8-none-1	ssh	local
AReal1_08	AReal1	8	9600-8-none-1	ssh	local

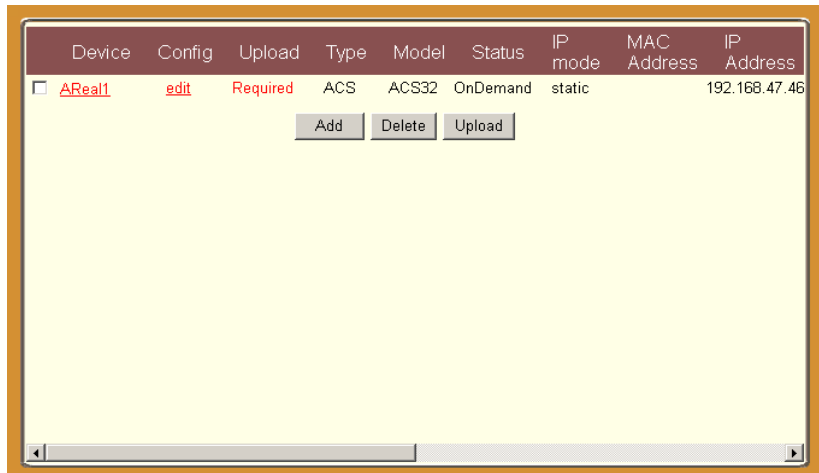
From this point, if you select the **Back** button, the system will return you to the Device definition form.

4: Configuring the E2000

9. Press the **Finish** button; wait for the discover process and the resulting form to appear:



10. Press the **OK** button.
The “upload” form appears:



11. Click on the check box that refers to the ACS or TS to upload, and then select the **Upload** button.

The “submit” form appears:


Device	Firmware	Bootcode	Upload firmware/bootcode	Upload configuration
AReal1			<input type="checkbox"/>	<input checked="" type="checkbox"/>

12. Click on the **Submit** button.

The system uploads the configuration, providing a status form during the process.

Upload Progress

30% AReal1: uploading /etc/portslave/pslave.conf..


Result: Running
Errors:

4: Configuring the E2000

Once the upload is completed, the following form appears indicating that the upload was successful.

Device	Firmware	Bootcode	Upload firmware/bootcode	Upload configuration
AReal1			(not selected)	Success

13. Select the **OK** button top complete the procedure.

Uploading Firmware into the Console Devices

Using the Device Definition form, you can configure the E2000 to upload firmware from its firmware repository to any of the console devices.

1. From the Device Definition form (Device List>Device Definition), select the firmware you wish to upload from the **Firmware/Boot** drop down list.
2. Click **Save**.
3. Go back to the Device List form and select the device(s) that need to be uploaded by clicking the corresponding checkbox, and then click **Upload**.
4. Select Upload Firmware/Configuration to select either Firmware, Configuration, or both).
5. Click **Submit**.



*The **Upload Firmware/Bootcode** option appears even if the E2000 firmware repository is empty. If you click on it, you must wait for a while before a message appears to let you know that the firmware repository is empty.*

Profile List Form

The **Profiles** List form, which lists the port profiles, is used in conjunction with console management. It allows you to configure the port profile that the target console uses. Port profiles define a standard set of parameters that are common to many consoles such as port speed, data bits, stop bits, and the like.

There is a default profile, and there may be other profiles generated by the Device Discovery feature. You may want to define your own profile before adding consoles because it is more convenient, but you can also edit individual consoles to use a different profile at a later time, if necessary.



Figure 4.6 - Profiles form

For a definition of the fieldnames on this screen, refer to the *Form Fields and Elements* heading of the *Profile Definition* form below.

Use the **Add** button on this form to invoke the Profile Definition form.

Profile Definition Form

Use the Profile Definition form to define your port settings.

The screenshot shows the 'Profile Definition form' in the 'cyclades' web interface. The interface has a top navigation bar with 'Admin | Access' and 'logout' links, and a user information section showing 'IP: 192.168.47.86' and 'User: admin'. A left sidebar contains menu items: 'Users', 'Consoles', 'Devices', 'Alarm Trigger', 'Profiles', 'Firmware', and 'Info / Reporting'. The 'Profiles' menu item is highlighted with a black arrow. The main content area contains the form with the following fields and values:

- Profile Name: cisco
- Console Type: Serial
- Description: cisco serial port
- Status: Enable
- port speed: 19200
- port data size: 8
- port stop bits: 1
- port parity: none
- port flow: none
- DCD sensitive: off
- break sequence: -break

Buttons for 'Save' and 'Reset' are located at the bottom right of the form. A 'help ?' and 'about ?' link is visible in the bottom right corner of the interface.

Figure 4.7 - Profile Definition form

Form Fields and Elements

<i>Field Name</i>	<i>Definition</i>
Profile Name	Port name.
Console Type	Drop down list to select type of console supported.
Description	Brief description of the profile.
Status	Port status (Enable or Disable).
Port Speed	Serial port baud rate.
Port Data Size	Number of data bits (7 or 8).
Port Stop Bits	Number of stop bits (1 or 2).
Port Parity	None, even, or odd.
Port Flow	Flow control (none, hardware, or software).
DCD Sensitive	How the console server responds to changes to DCD signal.
Port Break Sequence	As indicated.
Save / Reset	Buttons to save form entries and reset the form.

Adding a New Profile

To add a new profile, perform the following steps:

1. From the Profile List form, select the **Add** button.
The Profile Definition form appears.
2. Enter profile information in the provided fields
3. Select **Save** to end.

Modifying a Profile

To edit a profile, perform the following steps:

1. From the Profile List form, select the profile you wish to edit.
The Profile Definition form appears.
2. From the Profiles Definition form, make your changes.
3. Select **Save** to end.

Console Management

Console management is the process by which you configure E2000 to:

- Define all consoles to be accessed by E2000 users.
- Provide system information about each console.
- Select the type of user authentication to access a console.



The system authenticates users from the console server.

- Assign each console to any number of users
- Select users to be notified in the event of a console alarm
- Add or delete a console

If you chose not to use the Console Wizard under Device Management, then next step in the configuration process is to add consoles attached to the recently added device.



After adding a console, you must upload the configuration to the device before the console can become active. To prevent multiple uploads, it is advisable to add many consoles and then do one upload for the device to enable all the consoles that were added.

*See also the **Auto Upload** feature on page 4-20.*

You perform console management using the following forms.

- Console List
- Console List>Console Definition
- And to some degree, User List>User Definition (You allocate or assign from one to as many consoles to a user from this form.)

Console List Form

The Console List form, shown below, is the default form for Console Management.



Figure 4.8 - Console List form

For an explanation of each form field, refer to the Form Fields and Elements of the Console Definition form, next form section.

Sorting by Field Name

The Console List form allows you to sort by field name. For example, to sort by location, simply click the column name (or field name), **Location**.

Connecting to a Console

There are two ways to connect to a console using Secure Shell (SSH):

Method 1: Using the dropdown menu.

1. From the Console List form, select the console you wish to connect to from the console dropdown menu (located on the upper left corner of the main panel).
2. Click **Connect**.

Method 2: Using the main list.

1. From the Console List form, select the console you wish to connect to by selecting the link for the console name.

Defining a Console

1. From Console List > Console Definition form, type in the console information into the field boxes, and select the appropriate choices from the drop down menus.
2. If you wish to select the current user to receive notifications, select the **Add** button, or use the drop down menu to select other users and then **Add**.
3. If you wish to select the current user to access the console, select the **Add** button, or use the drop down menu to select other users and then select **Add**.
4. Select the **Save** button when finished.
5. Select the **apply changes** button.
6. Return to the Consoles form (by selecting Consoles from the menu panel) to verify your entry.

Console Definition Form

Use the Console Definition form to define in detail a target console, to select users to receive alarm notifications pertaining to the console, and to select users to have authorized access to the console.

Data buffering, data logging, and event notification are valid definitions only for consoles with permanent connections (*i.e.*, data status is enabled).

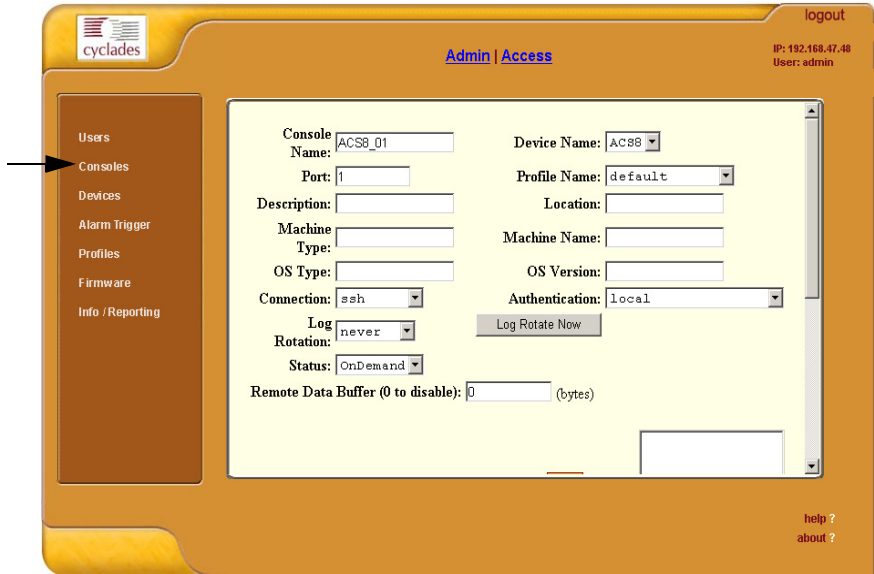


Figure: 4.9 - Console Definition form

Form Fields and Elements

<i>Field Name</i>	<i>Definition</i>
Console Name	<i>Required.</i> Name of the console
Console Server	<i>Required.</i> (Drop down list.) Console server to which the current console is connected.
Port	<i>Required.</i> Port on the console server when the console is connected.
Profile Name	<i>Required.</i> Name of port profile.
Description	Brief description of the console.

<i>Field Name</i>	<i>Definition</i>
Machine Type	Type of machine connected to the console.
Machine Name	Name of machine connected to the console.
OS Type	Type of operating system.
OS Version	Version of operating system.
Authentication	<i>Required.</i> Drop down list to select the type of authentication for the E2000 to access the console port.
Connection	<i>Required.</i> Drop down list. Method used to establish a console connection: SSH, Socket, or Telnet.
Log Rotation	Frequency of the automatic log rotation process (Never, Daily, Weekly, Monthly).
Status	Drop down list. Enable, Disable, OnDemand.
Remote Data Buffer (0 to disable)	The size of the remote data buffer in bytes. Filling in this field enables remote data logging by ACS/TS.
Select User to Notify	Drop down list. User selected to receive alarm notification pertaining to the target console.
Add / Delete	Buttons used to add or delete selected users (to be notified) from the Users list box.
Select User to Access Console	Drop down list. User selected to have authorized access to the target console.
Add / Delete	Buttons used to add or delete selected users (to access console) from the Users list box.
Save / Reset	Buttons to save entries or edits on the form, and to reset the form.
Logrotate Now	This field appears only if you selected Edit instead of the New button. Use this button to close and compress the console buffer log file, and to open a new file to receive new log entries. This process overrides the Log Rotation automatic setting.

Selecting Users to be Notified

Assigning a user to a console enables the system to direct to the user all notifications (email or alarm) pertaining to the console. You can assign one or more users to receive the notification.

1. From the **Console List**>**Console Definition** form, select a user from the **Select User to Notify** drop down menu.
2. Select the **Add** button.
The system should add the selected user into the **Users** view panel on the right.
3. To select another user, repeat steps 1 and 2.

Log Rotate Now

Periodically, the system automatically compresses the file and then creates a new file to collect a new set of console data. The file rotation is seamless with no data loss as the system copies from one file to another.

As administrator, you have the option to manually compress the log file, archive it, and then open a new file to accept new logs.

To initiate the logrotation perform the following steps:

1. From the **Consoles** form, select the console (for the particular console log you wish to rotate) to view the **Console Detail** form.
2. From the **Console Detail** form, click **Logrotate Now**.

Setting Log Rotation in Auto Mode

You can also set the log rotation to be automatically performed on a daily, weekly, or monthly basis. To set the system to automatically initiate log rotation on a regular basis, perform the following steps:

From the **Consoles** form, select the console (for the particular console log you wish to rotate) to view the **Console Detail** form.

1. From the **Log Rotation** field of the **Console Detail** form, select the frequency (daily, weekly, or monthly) of the log rotation.
2. Click on **Save**.

Where Log Files are Archived

Once log files are rotated, the system stores them in:

/var/log/consolos/rotated

You can back up these files to another server using the secure shell SCP program.

Backing Up Log Files to a Remote Server

You can copy rotated logs to another server that is more suited for holding large amounts of log data using the following command line syntax:

```
save_rotated_log [[user@]host:]file [ -flush ] [ -now ]
```

Where:

-flush deletes the current rotated logs

-now forces an immediate log rotation

The destination file is mandatory and must be the first argument. The order of the options (**-flush** and **-now**) does not matter; the system will perform the actions in the same order (save-flush-rotate) regardless of the options given.

If you supply *user@host*, the logs are transferred to a remote machine under the privileges of the specified user. If you do not supply *user@*, the system will assume that the current user is the remote one.

For remote destination, ensure that the remote machine is prepared to accept connections to ssh service on port 22. If only the file name is supplied, the system will copy the logs locally. You can include pathnames as part of the file name.

User Management

User management is the process by which you configure the E2000 to:

- Add or delete a user
- Authorize a user to access consoles
- Provide user information
- Set, change or reset a user password
- Define a user as a regular user or as an administrator
- Assign any number of consoles to a user

User management consists of two forms:

- User List form
- User Definition form



*Any user who will use the E2000 application **MUST** be entered in the E2000 database in order to access the application. This is regardless of whether you are using any other authentication services, remote, local, or none.*

User List Form

Use the User List form to view all E2000 system administrators and users. The form, shown below, lists all authorized E2000 users including information about each user (e.g., Name, Location, Phone) which you define in the User Definition form.

Any user who will use the E2000 application *must* be entered in the E2000 database in order to have access to the application, regardless of whether you are using any other authentication services or not. RADIUS users, for example, must still be registered in the E2000 database through these user management forms.

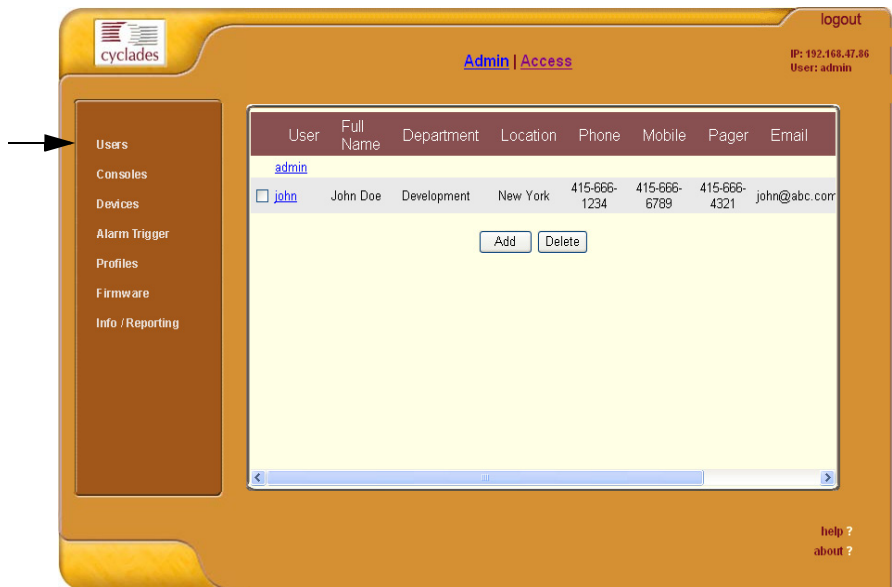


Figure 4.10 - User List form

For an explanation of each form field, refer to the *Screen Fields and Elements* of the User Definition screen, next screen section.

<i>Button Name</i>	<i>Function</i>
Add	This button invokes the User Definition form and allows you to enter a new user or modify an existing user, which you select from the current window.
Reset	This button resets the form to enable new entries.

User Definition Form

Use the User Definition form, shown below, to define a new user or an existing user.

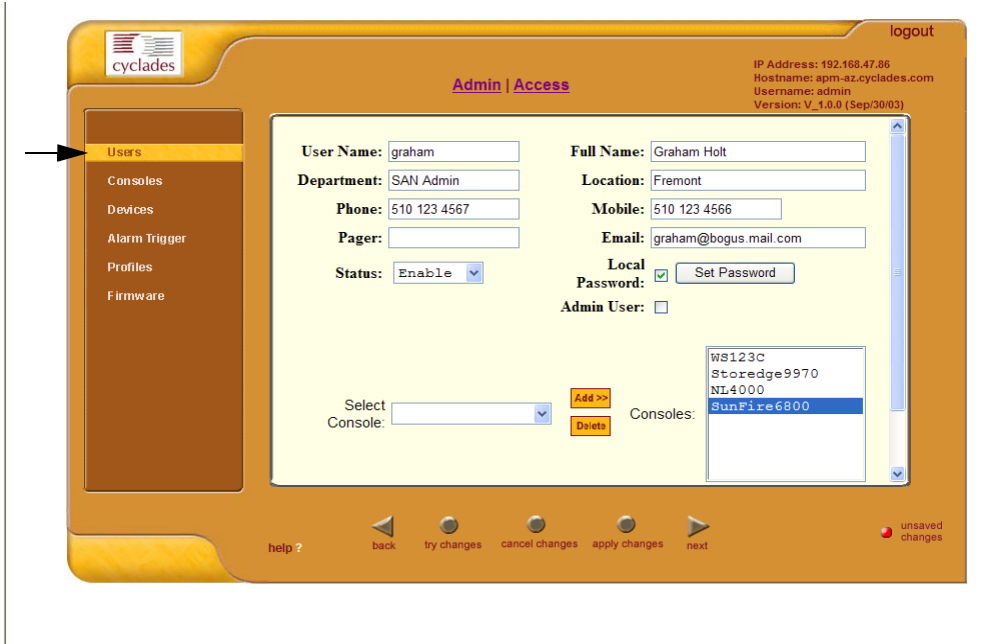


Figure 4.11 - User Definition form

Form Fields and Elements.

<i>Field Name</i>	<i>Definition</i>
User Name	User's login ID.
Full Name	User's complete name.
Department	As indicated.
Location	As indicated.
Phone	As indicated.
Mobile	As indicated.
Pager	As indicated.
Email	As indicated. This field is also used by the trigger to notify the user of any event or issue relating to consoles and other system areas delegated to him.

<i>Field Name</i>	<i>Definition</i>
Local Password	Checking this box sets the user password for local authentication.
	<i>NOTE: Even though you may be using another server authentication (e.g., LDAP, RADIUS), it is advisable that you activate the password for local authentication in the event that your authentication server fails.</i>
Admin User	Check box to authorize user access to the web application in <i>admin</i> mode.
Select Console	Assigns console(s) to the current user.
Consoles list panel	Lists all consoles to which the current user has access. This can also be set in the Console Definition form.

Adding a User

To add a user who will access a console port, perform the following steps:

1. From the User List form, select the **Add** button. The system will bring up the User Definition form.
2. From the User Definition form, type in the user information into the field boxes, and select the appropriate status from the **Status** drop down menu.
3. If you are ready to assign consoles to the current user, select each applicable console from the **Select Console** drop down menu, and then select the Add button. Otherwise, click the apply changes button to complete the user entry.

Deleting a User

From the User List form, click the check box on the left hand side of the user name, and then select the **Delete** button.

You can delete as many users as you need to at one time.

Selecting Consoles for a User

To select consoles for a user, perform the following steps:

1. From the User List form, select the user to whom you will assign a console. The system will bring up the User Definition form.
2. From the **Select Console** drop down menu of the User Definition form, select the console you want to assign to the current user.
3. Select the **Add** button.
4. To add another console, repeat steps 2 and 3.

Setting Up the Local Password

You can set up users to have local authentication by setting the Local Password, and defining the user name and password.

A local password is used if the authentication setting for the E2000 is **Local**. The local password is also used as a backup when server-based authentication is being used. In this case, if the authentication server is unavailable due to network problems then the system can use the local password. It is therefore advisable that you set a local password for some users even when server-based authentication is being used.

To set up local authentication for a user, follow the following steps:

1. From the User List form, select the user for whom you will set a password.
The system will bring up the definition form for that user.
2. If a password has not been set up, from the User Definition form, select set password.
System brings up the Password dialog box.
3. From the password dialog box, enter the password twice, and then click **Submit**.
4. From the User Definition form, click on the **Local Password** check box.
5. From the User Definition form, click **Save**.

Triggers and Alarms Management

Triggers and alarms management is the process by which you configure the E2000 to:

- Create and define trigger strings
- Modify or delete a trigger
- Create an alarm for each string, as needed, and prioritize the alarm.
- Create notification events (email list).
- Allocate an alarm to one or more users

Forms used to Manage Triggers and Alarms

Triggers and Alarms Management consists of two forms:

- Alarm List
- Alarm List>Trigger Definition

Additionally, you will need the following forms to define the following:

- User List>User Definition
Use the User Definition form to set user email address for user notification.

You use the User Definition form in Alarm Trigger management to define or verify the email that is used when a user is notified of an event.



Users who use the application in Access Mode also have the capability to change their email address through the User Profile form.

- Console List>Console Definition
Use the Console Definition form to assign users to be notified of an alarm originating from a specified console.

Alarm Trigger List Form

The Alarm Trigger List form, shown below, is used to:

- Open the Trigger Alarm Definition form
- Add or delete an alarm.

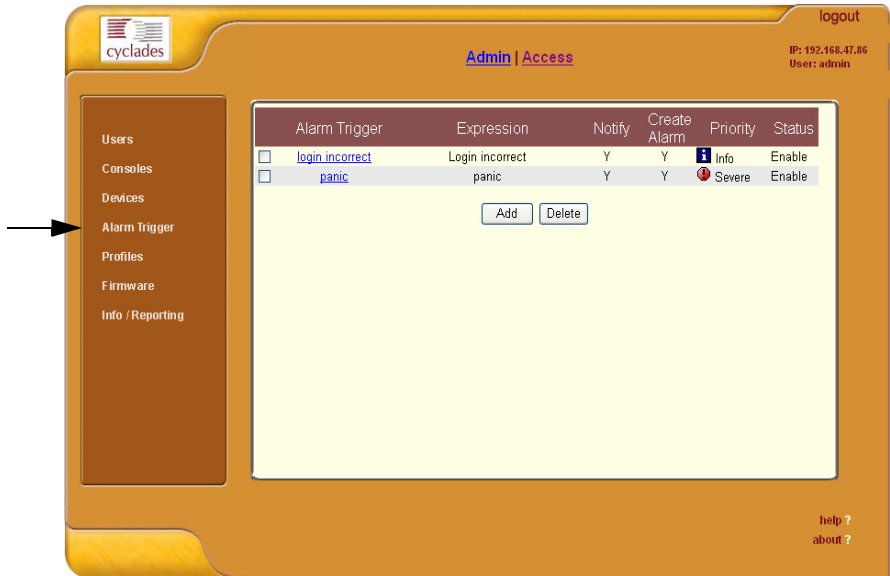


Figure 4.12 - Alarm Trigger form

For an explanation of each form field, refer to the *Form Fields and Elements* of the Alarm Trigger Definition form, next form section.

Adding or Deleting an Alarm

See Creating an Alarm Trigger, next section.

See Deleting an Alarm Trigger, next section.

Alarm Trigger Definition Form

Use the Alarm Trigger Definition form, shown below, to define triggers to generate user notifications and alarms.

Figure 4.13 - Trigger Alarm Definition form

Form Fields and Elements

<i>Field Name</i>	<i>Definition</i>
Alarm Trigger Name	Name of the trigger. Selecting a trigger name invokes the Trigger Definition form for that trigger.
Trigger Expression	String used to generate a trigger.
Notify	Yes or No. Indicates if system needs to notify (<i>i.e.</i> , send an email to) the user.
Create Alarm	Yes or No. Indicates if system needs to send an alarm to the user.
Priority	Indicates the priority or severity level of the alarm.
Status	Enable or disable a trigger.
Save	Select this button to save your trigger entry.
Reset	Select this button to reset the form to create a new trigger entry.

Creating an Alarm Trigger

A trigger is a text string that you create to generate any one or combination of the following:

- Email notification for users or administrators
- Alarm

By default, there are two pre-existing trigger entries:

- HeaLth_MoNiToR
- HeaLth_MoDeM

You can edit both trigger entries or create new ones.

For health monitoring triggers to work, you must create alarm triggers using the Alarm Trigger definition form. See Health Monitoring in the Device Management section of this chapter.

To create a trigger perform the following steps:

1. From the **Alarm Trigger** form, select the **Add** button. This brings up the Trigger Definition form.
2. Fill in the fields and select the selectable fields.



*The trigger string from which the system will base the trigger search is defined in the **Trigger** field.*

3. Else, select the **apply changes** button to complete the procedure.

Deleting an Alarm Trigger

1. From the main Alarm Trigger form, select the triggers to be deleted by clicking the check boxes to the left of each trigger name.
2. Select the **Delete** button.

Configuring Alarms for Device Health Monitoring

To enable the Device Health Monitoring feature of the E2000, you must also configure its alarm trigger(s). As discussed in the Device Management section, this feature is designed to monitor devices on a periodic basis as well as to create log files, and to send an alarm notification to specified users. Users must have a valid email address as configured in the Users Definition form (Users > User Definition form) to receive alarm notifications.

Configuration Requirement: Device Definition Form

For Health Monitoring to work, you must define the frequency of monitoring from the **Health Monitor** user entry field of the Device Definition form (Device List > Device Definition) as shown below:

The screenshot shows a web-based configuration form for a device. The fields are as follows:

- Device Name: acs48
- Type: ACS
- Model: ACS48
- Location: (empty)
- Admin Username: root
- Admin Password: Set Password
- IP Address: 192.168.46.203
- Netmask: (empty)
- Default Gateway: (empty)
- DNS: (empty)
- Base Port: 7001
- Connection: ssh
- IP Mode: static
- MAC Address: (empty)
- Status: OnDemand
- Auto Upload:
- Modem Mode: Primary Network
- PPP Phone: 203
- PPP Device IP: (empty)
- PPP Local IP: (empty)
- Health Monitor: daily
- Firmware/Boot: - none / none

Buttons at the bottom: Save / Create Consoles, Save, Reset, Auto Discover.

The available choices from the **Health Monitoring** drop down list are:

- | | |
|----------------|--|
| Never | System will never run Health Monitoring for this device (default). |
| Daily | System will run Health Monitoring at 2 am everyday. |
| Weekly | System will run Health Monitoring at 3 am every Saturday. |
| Monthly | System will run Health Monitoring on the first of each month. |

Once you have done this, proceed to the Alarm Trigger Definition form to define the Health Monitoring Alarm Trigger.

Using the Logical AND in the Alarm Trigger Expression

To create a logical AND in the alarm trigger expression, use the period and asterisk: `.*`

The alarm trigger is also capable of processing substrings. OK, for example, is a substring of NOK. Therefore, both types of messages will cause alarms if `.*OK` is appended to the `HeaLth_MoNiToR` trigger string.

Defining the Health Monitoring Alarm Trigger

1. To create an alarm trigger to be associated with the Health Monitoring, go to the Alarm Trigger Definition form (**Alarm Trigger List > Add > Alarm Trigger** Definition form):

The screenshot shows a web form for defining an alarm trigger. The fields are as follows:

- Alarm Trigger Name:** Health_Alert
- Trigger Expression:** HeaLth_MoNiToR.*NOK
- Notify:** Y
- Create Alarm:** Y
- Priority:** Severe
- Status:** Enable

Buttons: Save, Reset

2. From the Alarm Trigger Definition form, complete the fields as follows:

<i>Field Name</i>	<i>Field Definition</i>
Alarm Trigger Name	Provide a name to be associated with this particular alarm trigger.

<i>Field Name</i>	<i>Field Definition</i>
Trigger Expression	Type in: HeaLth_MoNiToR NOTE: To effectively filter the alarm trigger to generate only messages relating to failure, it is recommended that the Trigger Expression be restricted to: HeaLth_MoNiToR.*NOK (see explanation, next section).
Notify	Select Yes if you want users to receive email notifications regarding the alarm.
Create Alarm	Select Yes if you want alarms to be generated based on the trigger expression.
Priority	Select a priority to be associated with the alarm.
Status	Select Enable to enable this particular alarm trigger.

How Health Monitoring Works

Based on the aforementioned configuration settings, the program gets from the database a list of devices to check. The monitoring results are ultimately stored in a log file using the following line format for each device:

```
Device_Name,IP,Device_IP,Phone_Number,Date,Time, Result_Status
```

Each line is a syslog message generated by Health Monitoring, and contains the string identifier, **HeaLth_MoNiToR** which is used by the alarm trigger. Moreover, the `Result_Status` field will have two leading strings:

- OK (indicates that the device is okay)
- NOK (indicates a problem)

It is for this reason that the trigger expression needs to be restricted further to: **HeaLth_MoNiToR.*NOK** in order for users to get messages that only relate to failure, and not be bombarded by a large amount of unnecessary messages.

User Notification is Based on the Lowest Enabled Console Port

The Health Monitor is designed to monitor devices, and yet the current version does not support user notification per device, only per console. So how does the Health Monitoring and user notification work on the device level? To address this, the system creates an alarm and sends out a notification email based on the *notify users list* for the console connected to the lowest port number; not necessarily Port 1, but the lowest port used.



As far as Health Monitoring is concerned, you must add users to the *notify users list* associated with the lowest, enabled console port of the device, and ensure that users have a valid email address to receive email.

Info Reporting Main Form

Info Reporting is composed of two forms: Info Reporting main form and Info Reporting detail form. The Info Reporting main form lists all console access information by users and administrators.



Figure 4.14 - Info Reporting Main form

Form Fields and Elements

Button Name	Function
Session Start Date	Date when the session started.
Session Start Time	Time when the session started.
Session End Date	Date when the session ended.
Session End Time	Time when the session ended.
User Name	Name of session user.
Session ID	As indicated.

Info Reporting Detail Form

Use the Info Reporting Detail form to view information (console name, action taken, result) about console activities by users and administrators alike.



Figure 4.15 - Info Reporting Detail form

Table Fields

<i>Field Name</i>	<i>Definition</i>
Console Name	Name of console.
Action	Action taken pertaining to a console issue or alarm.
Result	Result of that action.

Firmware Management

AlterPath Manager E2000 contains a firmware repository. Each time a new firmware is released for the ACS, TS, PMxx, or KVM, Cyclades will release a package for E2000 to import.

The package contains firmware, boot code, release notes, user manual and dependency file. The dependency file is used to ensure you do not load the firmware to the wrong device or perform invalid upgrade operations.

The Firmware form provides a management tool for you to:

- Import firmware updates
- Keep track of firmware updates
- Document any comments regarding the particular firmware
- Access manuals and release notes

Firmware Management consists of two forms:

- Firmware List form
- Firmware Definition form.

Any firmware that you add to the Firmware List form is also reflected in the Device Definition form (specifically, the **Firmware/Boot** list fieldbox). The next time you create a new device, the system will prompt you to upload the new firmware, as necessary.

The last part of this section provides instructions on how to upgrade the E2000 firmware.

Firmware List Form

You use the Firmware List form to open the Firmware Definition form, and to add or delete a firmware.



Figure 4.16 - Firmware form

For an explanation of each form field, refer to the *Form Fields and Elements* of the Firmware Detail Form, next form section.

Adding Firmware

Firmware files (.tgz) are normally downloaded from the web and copied into the E2000 via Secure Copy (SCP). To add or import new firmware, follow this procedure:

1. From the web (www.cyclades.com), download the firmware to your computer.
2. Using the CLI, use the SSH **scp** command to copy the firmware to E2000.
Example: scp v214.tgz root@<ip_address>:/usr/fw
3. Open the Firmware List form and click the **Import** button.
The system should add the new firmware on the Firmware List form. The system also updates the Firmware/Boot drop down list in the Device Definition form.

Deleting Firmware

To delete a firmware, perform these steps:

1. From the menu panel, select Firmware.
2. From the Firmware List form, select the checkmark box of the firmware you wish to delete.
3. Select the Delete button, accordingly.

Uploading Firmware into the Console Devices

The E2000 can upload firmware from its firmware repository to any of the console devices. To upload firmware to a console device, perform the following steps:

1. From the Device Definition form (Device List > Config edit), select the firmware you wish to upload from the **Firmware/Boot** drop down list.
2. Click **Save**.
3. Go back to the Device List form and select the device(s) that needs to be uploaded, and then click **Upload**.
4. Select Upload Firmware Configuration (you have the choice to select either Firmware, Configuration, or both).
5. Click **Submit**.

Firmware Detail Form

Use the Firmware Detail form, shown below, to:

- View firmware details
- Add comments regarding a firmware.
- Assign a status to a firmware
- Access Manuals and Release Notes

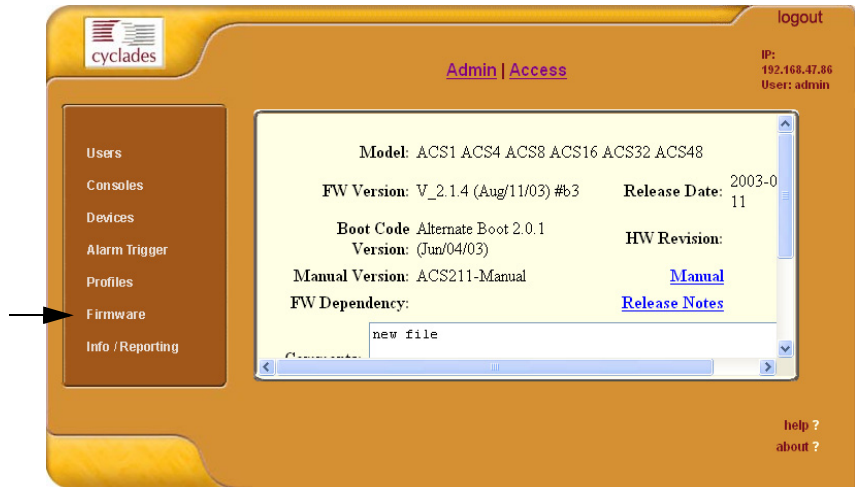


Figure 4.17 - Firmware Detail form

Form Fields and Elements

<i>Button Name</i>	<i>Function</i>
Model	Models to which firmware is applied.
FW Version	Firmware version.
Release Date	Firmware's release date.
Boot Code Version	As indicated.
HW Revision	Hardware revision, if any.
Manual Version	As indicated.
Manual	Hyperlinks to firmware documentation.
FW Dependency	As indicated.
Release Notes	Links to release notes.

<i>Button Name</i>	<i>Function</i>
Comments	Text entry box for user comments.
Status	Drop list to select Enable or Disable .

Viewing and Accessing Firmware Information

To view and access firmware details, follow these steps:

1. From the Firmware List form, select the particular Firmware Version you wish to view.
The form brings up the Firmware Detail form. From the Firmware Details form, you can do any of the following:
 2. To access firmware documentation, select **Manual**.
 3. To access Release Notes for the current firmware, select **Release Notes**.
 4. Type in notes in the Notes input text box and then select **Save** to enter notes and comments about the current firmware.
 5. If needed, enter the status (Enable/Disable) of the firmware installation or update.

Upgrading the E2000 Firmware

You may upgrade the E2000 firmware by downloading the upgraded software from the web to the E2000.

1. From the Cyclades website (www.cyclades.com), download and copy the firmware to the E2000 via Secure Copy (SCP).
The firmware is composed of two files:
 - E2000_v110.tgz
 - E2000_v110.md5sum.tgz
2. Copy the two files to the E2000 /tmp directory as follows:

```
scp E2000_v110.tgz root@E2000_IP:/tmp
scp E2000_v110.md5sum.tgz
```

3. Login to the E2000 as **root**, and then change the directory to **/tmp** as follows:

```
ssh root@E2000_IP
cd /tmp
```

4. Install the new software to compact flash as follows:

```
installimg all all.tgz
reboot
```

Backing Up User Data

Using CLI, you can back up and restore the configuration and data files of the E2000 to a local or a remote destination. This feature allows you to backup and restore (either independently or altogether) the following data types:

<i>Data Type</i>	<i>Definition</i>
System Configuration	Data related to the E2000 host settings such as IP Address, Authentication Type, and Host Name.
Configuration Data	Data related to the configuration of consoles, users and so forth, which are stored in the data-base.
Data Buffers	The ASCII data collected from the consoles.

Backup and Restore Scenarios

For illustration purposes, there are two scenarios in which you can perform the backup.

- Replicating data to a hot spare machine - You back up the configuration data and data buffers and restore them to a second E2000 unit. This method enables you to keep the network identity of each E2000 unit, but maintain the same configuration for both units. The second unit serves as a spare system.
- Replacing the existing E2000 - You back up ALL data to an external server. The E2000 is then replaced with a new unit to which all data is restored. The new unit will have the same configuration as the original unit.

Backup and Restore Commands

Using CLI, the command line for backup and restore are as follows:

```
> backup {log | sys[tem] | conf[iguration] | all}
[[user@]host:]file

> restore {log | sys[tem] | conf[iguration] | all}
[[user@]host:]file
```

If you do not specify a user, then the current username will be used.
If you do not specify a host then the backup will be done to a local file.

The backup/restore functions by using secure copy (scp). The file is saved as a ***.tgz** file.

System Recovery Procedures

In the event that the E2000 goes down, on restart, the system will check the integrity of the file system. If any problem is found, then the system should attempt to repair any damage that may have occurred.

When performing a recovery procedure to the E2000, if there is too much damage, you have the option to stop the booting process and take recovery actions through the serial console as follows:

1. Rebuild system partition
2. Rebuild database
3. Rebuild data log partition

The rest of the configuration process is done through the GUI/web interface.

If the E2000 goes down, you will still have direct access to ports and consoles, but you will need to redefine the devices.

This page has been left intentionally blank.

Appendix A:

E2000 Hardware Specifications

CPU	Intel® Celeron® 850MHz
Memory	512MB SDRAM 256MB CompactFlash
Interfaces	2 Ethernet LAN 10/100BT 1 RS-232 serial console port
Operating System	Netlinos Open Source Networking OS
Security	RADIUS, LDAP, SSHv2, SSL
Management	Text-based console shell access, Cyclades Web-based management (CWM) interface
Dimensions	17in x 1.75in x 14in (1U rack-mountable unit)
Power	150W, 115/230 VAC input (auto-range)
Operating Temperature	50°F to 112°F (10°C to 44°C)
Certifications	FCC Class A, CE

Supported web browsers and java runtime systems:

- Mozilla 1.0.2/java plugin 1.4.2
- Netscape 7.1/java plugin 1.4.2
- Internet Explorer 6.0/java plugin 1.4.2

The Java Runtime plugin is available from the Sun web site at:
<http://java.sun.com/products/plugin/>

This page has been left intentionally blank.

Appendix B:

Modem Access in ACS

The AlterPath Manager E2000 allows you to automatically dial out to remote console servers such as the AlterPath Console Server (ACS) or Terminal Server Series (TS) if the network connection is lost.

In the remote console server, you can connect an external modem to a serial port, or use a PCMCIA modem in the case of the ACS. This section explains the procedure for configuring either modem.

PCMCIA Modem Configuration

To use a PCMCIA modem, configure the **pap-secrets** in the ACS (**/etc/ppp/pap-secrets**) to accept any password by inserting the following line:

```
#* hostname "" *
* * "" * ← Insert this line.
```

External Modem Configuration

To configure your external modem, perform the following steps:

1. Ensure that you do not configure the console where the modem is attached otherwise any upload process on the console will overwrite your configuration.
2. Edit the **/etc/portslave/pslave.conf** for the modem port as follows:

```
-----
#all.initchat      TIMEOUT 10 \
#                  "" \d\l\dATZ \
#                  OK\r\n-ATZ-OK\r\n "" \
#                  TIMEOUT 10 \
#                  "" ATM0 \
#                  OK\r\n "" \
#                  TIMEOUT 3600 \
#                  RING "" \
#                  STATUS Incoming %p:I.HANDSHAKE \
#                  "" ATA \
#                  TIMEOUT 60 \
#                  CONNECT@ "" \
#                  STATUS Connected %p:I.HANDSHAKE
.
```

```

.
.
#all.autoppp %i:%j novj \
#       proxyarp modem asyncmap 000A0000 \
#       noipx noccp login auth require-pap refuse-chap \
#       mtu %t mru %t \
#       ms-dns 192.168.160.5 ms-dns 0.0.0.0 \
#       plugin /usr/lib/libpsr.so
.
.
#all.pppopt %i:%j novj \
#       proxyarp modem asyncmap 000A0000 \
#       noipx noccp mtu %t mru %t netmask %m \
#       idle %I maxconnect %T \
#       ms-dns 192.168.160.5 ms-dns 0.0.0.0 \
#       plugin /usr/lib/libpsr.so

```

-
- a. Uncomment all lines (*i.e.*, remove all # symbols) from the **all.initchat** and **all.autoppp** sections.
 - b. Change the first line of **all.initchat...** to **sxx.initchat...** (where xx is the serial port # where the modem is attached).
 - c. In the **all.autoppp** and **all.pppopt** sections, for the E2000 to assign remote and local IPs, you must replace **%i:%j** with **0.0.0.0:0.0.0.0**

Where 0.0.0.0:0.0.0.0 is <Local IP>:<Remote IP>

- d. If the Local IP in the APM is blank, then use: **%i:%j**
- e. In the **all.autoppp** and **all.pppopt** sections, remove the line beginning with “**plugin /usr...**”
- f. Be sure to remove the continuation symbol or the backward slash (\) from the last line of **all.autoppp** and **all.pppopt**.
- g. Add “**require-pap refuse-chap **” to **all.pppopt** after “**noipx noccp**” and then press <Enter><Tab> to put “**mtu %...**” on a new line. See the example below.
- h. After “**sxx.tty ttySxx**” add the following lines:

```

sxx.protocol      ppp
sxx.authype       local
sxx.speed         57600
sxx.dcd           1
sxx.flow          hard

```


The modified file:

```

-----
sxx.initchat TIMEOUT 10 \
    "" \d\l\DATZ \
    OK\r\n-ATZ-OK\r\n "" \
    TIMEOUT 10 \
    "" ATM0 \
    OK\r\n "" \
    TIMEOUT 3600 \
    RING "" \
    STATUS Incoming %p:I.HANDSHAKE \
    "" ATA \
    TIMEOUT 60 \
    CONNECT@ "" \
    STATUS Connected %p:I.HANDSHAKE
.
.
all.autoppp 0.0.0.0:0.0.0.0 novj \
    proxyarp modem asyncmap 000A0000 \
    noipx noccp login auth require-pap refuse-chap \
    mtu %t mru %t
.
.
all.pppopt 0.0.0.0:0.0.0.0 novj \
    proxyarp modem asyncmap 000A0000 \
    noipx noccp require-pap refuse-chap \
    mtu %t mru %t netmask %m \
    idle %I maxconnect %T \
    ms-dns 192.168.160.5 ms-dns 0.0.0.0
.
.
s1.tty      ttyS1
s2.tty      ttyS2
.
.
sxx.tty      ttySxx
sxx.protocol ppp
sxx.authype  local
sxx.speed    57600
sxx.dcd      1
sxx.flow     hard
-----

```

3. As with PCMCIA modem configuration, configure the **pap-secrets** in the ACS or TS to accept any password by inserting the following line in the **/etc/ppp/pap-secrets** under:

```
#* hostname "" *
* * "" * ← Insert this line.
```

4. Ensure that the filename **/etc/ppp/pap-secrets** is listed in **/etc/config_files**. If not, add that line to **/etc/config_files** by typing:
echo /etc/ppp/pap-secrets
and pressing <Enter>.
5. If for any reason you are enabling syslog-ng on the ACS or TS, it is not advisable to use “root” as the Admin Username for this device. Instead, create a user in the ACS or TS which will be the Admin Username in the APM for that device.
6. After creating the user in the ACS or TS, give it root privileges by editing **/etc/passwd** for the user by changing the UID and GID fields to 0.

A sample user with the fields changes to 0 is as follows:

```
edson:fTEQb6zEnuIEQ:0:0:Embedix User...:/home/  
edson:/bin/sh
```

7. Change the ownership of the user’s home directory to root as follows:

```
chown root /home/edson
```

8. Edit the file **/etc/ssh/sshd_config** to remove the comment symbol (#) in front of the line:

```
AuthorizedKeysFile /etc/ssh/authorized_keys
```

Appendix C:

Installing SSL Certificates

This section explains how to add or import your own SSL certificate to the E2000 instead of using the Cyclades default SSL certificate.

A certificate for the HTTP security is created by a Certification Authority (CA). Using a public algorithm such as RSA or X509, certificates are commonly obtained by generating public and private keys.

To obtain and install a SSL certificate, follow the procedure below:

Step 1: Enter OpenSSL command.

On a Linux computer, you can generate a key using the Open SSL package through the command:

```
# openssl req -new -nodes -keyout private.key -out public.csr
```

If you use this command, the following information is required:

<i>Parameter</i>	<i>Description</i>
Country Name (2-letter code) [AU]:	The 2-letter country code.
State or Province Name (full name) [Some-State]:	Enter the full name (not the code) of the state.
Locality Name (e.g., city) []:	Enter the name of your city.
Organization Name (e.g., company) [Internet Widgits Ltd]:	Organization that you work for or want to obtain the certificate for.
Organizational Unit Name (e.g., section) []:	Department or section where you work.
Common Name (e.g., your name or your server's hostname) []:	Name of the machine where the certificate must be installed.
Email Address []:	Your email address or the administrator's.

You may skip the other requested information.

The command generates a Certificate Signing Request (CSR) which contains some personal (or corporate) information and its public key.

Step 2: Submit the CSR to the CA

Once generated, submit the CSR and some personal data to the CA. You can request this service by selecting from a list of CAs at the following URL:

`pki-page.org`

The service is not free. Before sending the certificate, the CA will analyze your request for policy approval.

Step 3: Upon receipt, install the certificate

Once the CSR is approved, the CA sends a certificate (*e.g.*, `jcertyfile.cer`) to the origin and stores a copy on a directory server.

If you are satisfied that the certificate is valid, then you can import the certificate to your keystore using the **-import** command:

```
keytool -import -alias joe -file jcerty.cer
```

The certification becomes effective in the next reboot.

More About Importing Certificates

There are many sources of information regarding certificate management on the web. The information below has been excerpted and modified from the `keytool` document which you can access from the following web site:

<https://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html>

You import a certificate for two reasons:

1. To add it to the list of trusted certificates, or
2. To import a certificate reply received from a CA as the result of submitting a Certificate Signing Request (see the **-certreq** subcommand) to that CA.

Which type of import is intended is indicated by the value of the **-alias** option. If the alias exists in the database, and identifies an entry with a private key, then it is assumed you want to import a certificate reply. `Keytool` checks whether the public key in the certificate reply matches the public key stored with the alias, and exits if they are different. If the alias identifies the other type of keystore entry, the certificate will not be imported. If the alias does not exist, then it will be created and associated with the imported certificate.

Be sure to check a certificate very carefully before importing it as a trusted certificate! View it first (using the **-printcert** subcommand, or the **-import** subcommand without the **-noprompt** option), and make sure that the displayed certificate fingerprint(s) match the expected ones.

For example, suppose someone sends or emails you a certificate, and you put it in a file named /tmp/cert. Before you consider adding the certificate to your list of trusted certificates, you can execute a **-printcert** subcommand to view its fingerprints, as in:

```
keytool -printcert -file /tmp/cert
  Owner: CN=ll, OU=ll, O=ll, L=ll, S=ll, C=ll
  Issuer: CN=ll, OU=ll, O=ll, L=ll, S=ll, C=ll
  Serial Number: 59092b34
  Valid from: Thu JUL 01 18:01:13 PDT 2004
             until: Wed SEP 08 17:01:13 PST 2004
  Certificate Fingerprints:
  MD5: 11:81:AD:92:C8:E5:0E:A2:01:2E:D4:7A:D7:5F:07:6F
  SHA1: 20:B6:17:FA:EF:E5:55:8A:D0:71:1F:E8:D6:9D:C0:37:1
```

Then call or contact the person who sent the certificate, and compare the fingerprint(s) that you see with the ones that they show. Only if the fingerprints are equal is it guaranteed that the certificate has not been replaced in transit with somebody else's (for example, an attacker's) certificate. If such an attack took place, and you did not check the certificate before you imported it, you would end up trusting anything the attacker has signed (for example, a JAR file with malicious class files inside).

Note: it is not required that you execute a **-printcert** subcommand prior to importing a certificate, since before adding a certificate to the list of trusted certificates in the keystore, the **-import** subcommand prints out the certificate information and prompts you to verify it.

You then have the option of aborting the import operation. Note, however, this is only the case if you invoke the **-import** subcommand without the **-noprompt** option. If the **-noprompt** option is given, then there is no interaction with the user.

If you are satisfied that the certificate is valid, then you can add it to your key store as follows:

```
keytool -import -alias tomcat -file jcertfile.cer
```

This creates a trusted certificate entry in the keystore, with the data from the file jcertfile.cer, and assigns the alias tomcat to the entry.

This page has been left intentionally blank.