AlterPath Manager E2000 Manual

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

Product Version 1.0   Document No. 1.04

Product Version: 1.0
Document Number: 1.04

Table of Contents

Chapter 2: Installing the E2000

Chapter 3: Using the E2000

Chapter 4: Configuring the E2000

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 to enable users to perform the various fault management procedures -- from user management to device management; from

console management to triggers and alerts, as
well as firmware control.

List of Figures — This is a list of all figures that appear in the document.

Typographical Conventions

Screen Labels — Words that appears on the screen are typed in
boldface.

Examples: The **Alarm** screen; the **Password**
field.

Hypertext Links — With the exception of headings and the Table of
Contents (which are already linked), all under-
lined words are hypertext links.

Screen Levels — Screen 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

E2000 — For convenience, this is the short name for Alter-
Path Manager E2000. The short name is also
commonly used in the Index.

Select — To *select* is the same as to *click your mouse*.

User(s) — *User* or *users* 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.

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.
Screen Names	The sceen names of the application's GUI do not necessarily appear on the actual window. Becuase some windows do not have titles, these names are used to distinguish each window as well as to reflect the window function.

Examples:
Console List Screen
Console Definition Screen

Symbols

This manual uses two 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.

1: Introduction

The AlterPath Manager E2000 is a robustly integrated 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, this document designates anyone who uses the E2000 application in Access mode as a **user**, regardless of whether that user is a system administrator or not. From the E2000's perspective, an administrator is anyone who is defined in the E2000 as an admin and has the authority to configure and to perform various system administrative tasks for the E2000.*

Connectivity and Capacity

The E2000 supports 256 connections to serial console ports and can control firmware upgrades on 256 separate console management devices. It can support 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:
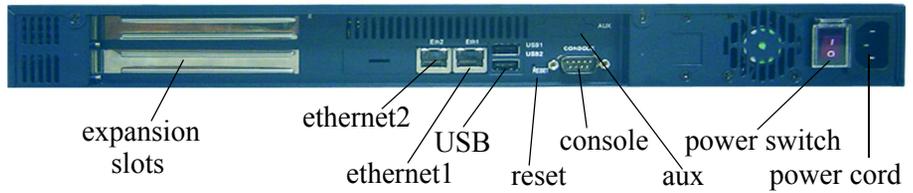
Figure 1.2 - Back view of E2000

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
- 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 E2000. The E2000 authenticates all users accessing the console ports using a local database, Radius, or LDAP.

Consolidated Views and Console Access

From the E2000 web interface, you (as an authorized user) 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 to 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 click on an icon for a particular console listed on your console screen panel. When you click a console icon, the system 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 predefined by the administrator, it will do either one or both of the following:

- Send an email to a user list
- Create a prioritized alarm entry in the Alarm database

Consequently, when an alarm is entered in the database, the system also writes 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.

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 nor access any console that does not concern them.

Command Line Interface (CLI)

For emergency access situations, the E2000 can provide you with 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) that E2000 provides. 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.
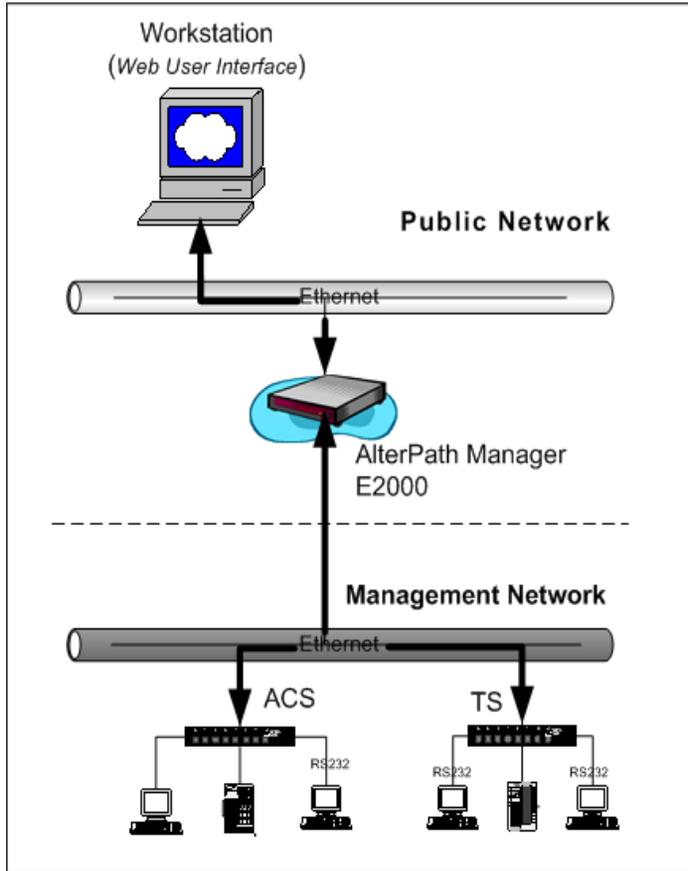
Figure: 1.3 - Private Network Topology

Single Network Diagram

The diagram below depicts how the AlterPath Manager E2000 may be set up in a single network structure.
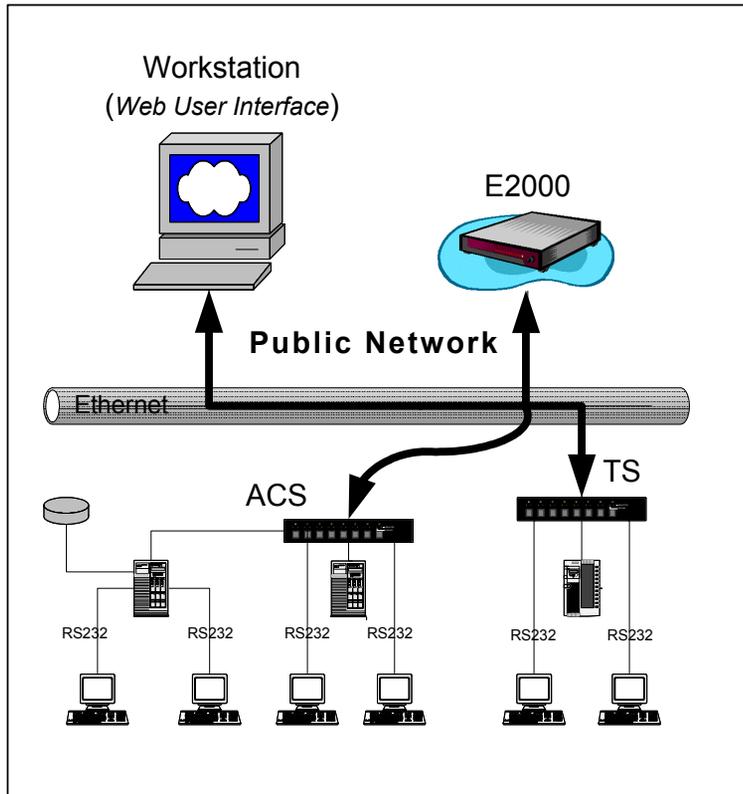
Figure 1.4 - Single Network Topology

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/htpe/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 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 terminal is used for the initial configuration (also known as *First Time Configuration* in this document) which is performed using 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:

Root Access	You will need Root Access on your local UNIX machine in order to use the serial port.
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.
IP Addresses	Have the IP/Mask addresses of the following ready:

- • All console severs
- • 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 the application only after you (as E2000 administrator) have completed the configuration procedures discussed in chapter 4.*

This page has been intentionally left blank.

3: Using the E2000

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

The chapter is broken down into the following procedures:

- User Interface Overview
- Logging In
- Using the Alarms screen
- Using the Consoles screen
- Using the Logs screen
- Using the User Profile screen

*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 screens:

Alarms	This is your default screen. Use this screen to deal with alarms such as updating the status of the alarm or closing the alarm after you resolve it.
Consoles	Use the **Consoles** screen to view a list of the consoles assigned to you. From the list, select the console you wish to access by selecting the icon on the lefthand side of the console name.

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

Accessing the E2000 Web 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** screen 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.
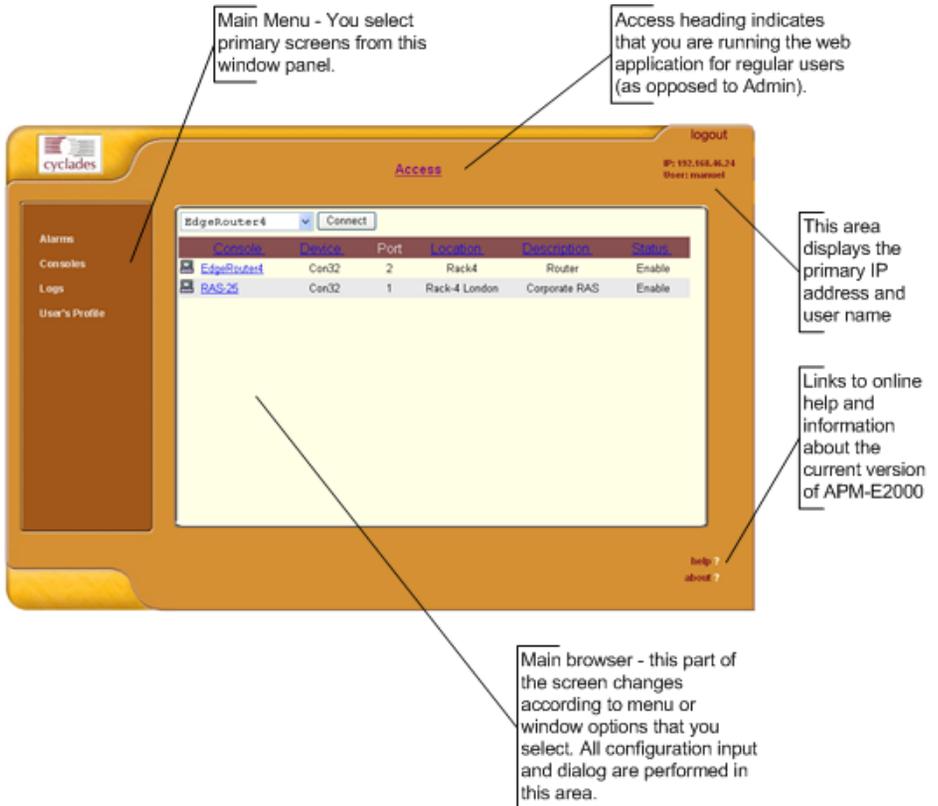
Figure 3.2 - Parts of the Access (User) Screen

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 Screen

The Alarm List screen is the default screen 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 screen. 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 screen), 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 screen or from the Logs screen (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 screen, 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 Screen

The Alarm List screen is the primary screen for alarm management. As discussed earlier, you use this screen 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 Screen

Screen Fields and Elements

Ticket	Ticket number of the alarm.
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.
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 Screen

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 screen, select the ticket you wish to examine.

    The screen 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 icon to the left of 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 screen.

Ticket Information Screen

Use the Ticket Information screen to re-assign the ticket to another user, to change the status of the ticket, or to add notes to the ticket.
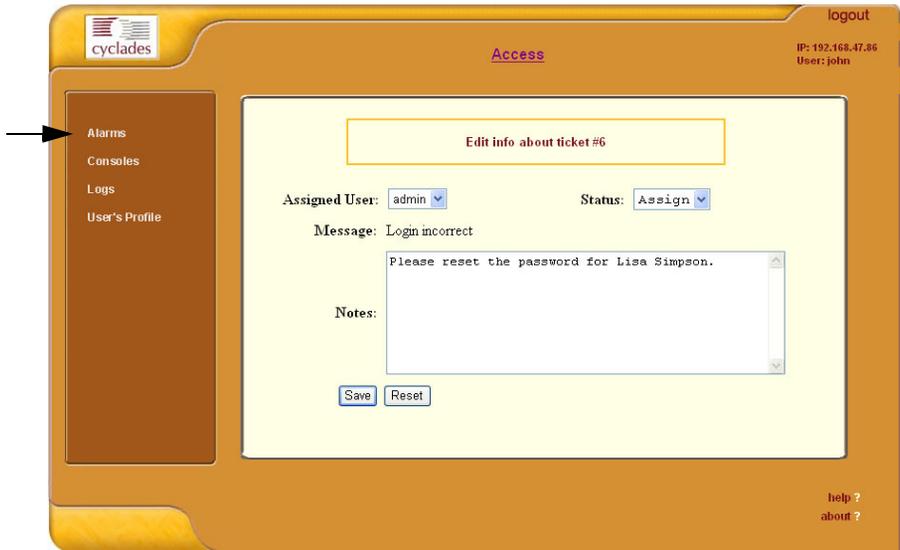
Figure 3.4 - Ticket Information Screen

Screen Fields and Elements

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 screen.
Notes	Scrollable text entry box for entering notes related to the ticket.
Save	Button to save screen entry.
Reset	Button to reset the screen.

Assigning/Re-assigning a Ticket to another User

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

1. From the Alarm List screen, select an alarm or ticket to open the Ticket Information screen.

    The system opens the Ticket Information screen.

2. From the Ticket Information screen, 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 Screen

The Console List screen, 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 Screen

Screen Fields and Elements

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 screen 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 screen, select from the Console column the console you wish to examine further.

   The Console Detail screen 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 screen, 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 screen, select the console you wish to connect to by selecting the console icon to the left of the console name.

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 screen. 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 Screen

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

You also use this screen 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 Screen

Screen Fields and Elements

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.
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. 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 Screen

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

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

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

Figure 3.7 - Console Logs Screen

Screen Fields and Elements

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.
Submit   Button to download the requested log and invoke the
                           Logs screen.

Viewing the Logs

Using the Logs screen, 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 Log from the Menu Panel
   The system brings up the main Console Logs screen.
2. From the Console drop down list, select the console from which you want
   to view the logs.

Note: 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 screen.

The logs screen provides you with three kinds of logs:

Access Log   Logs that provide logging information (*i.e.*, who
                          accessed the console, when and for how long, *etc*.)
                          about a particular console.
Events Log   Logs that provide information about notifications
                          and alarms (who handled the alarm, what action was
                          taken, etc.) 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 screen 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.
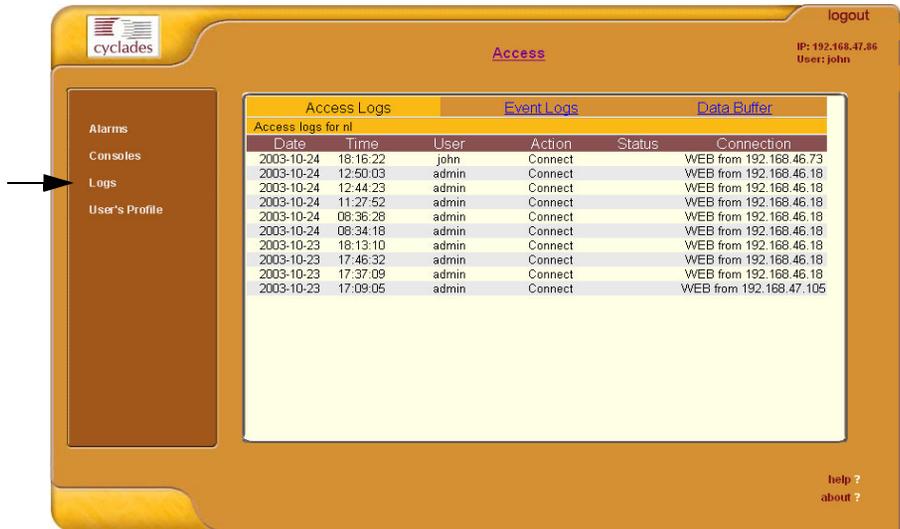
Figure 3.8 - Logs Screen

Log Fields Definition

Date	Date in which 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 or Disable)
Connection	Type of connection (SSH, Telnet)

Event Logs

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

Figure 3.9 - Event Logs Browser

Log Fields Definition

Date	Date of the event.
Time	Time of the event.
Ticket	Ticket number associated with the event.
Pattern	Name of the trigger.
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** screen.*

User Profile

The User Profile screen 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.
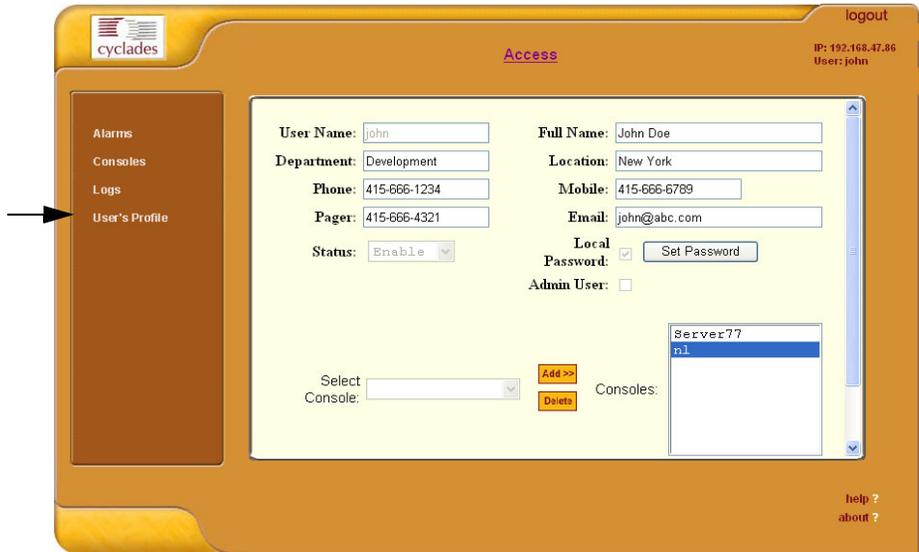
Figure 3.11 - User Profile Screen

Screen Fields and Elements

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.

4: Configuring the E2000

This chapter discusses the various procedures and underlying concepts for configuring the AlterPath Manager E2000. Since the configuration procedure is normally performed by a systems administrator, this section is addressed to the E2000 administrator.

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.
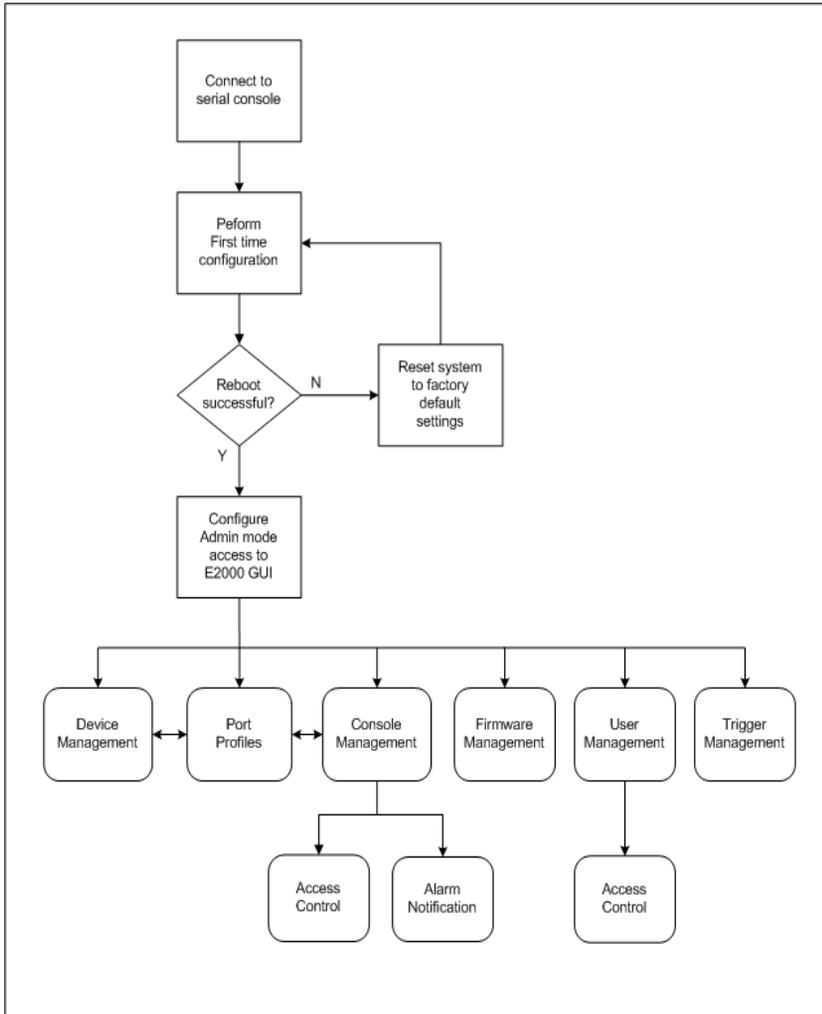
Figure 4-1: Configuration Flow Diagram

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)

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)[local]:
Current system date and time is:
    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. If you were to select Radius, the system will prompt you for the Radius *server name* and *secret*. If you were to select LDAP, the system will prompt your for the LDAP *server name* and *server base*.

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 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.

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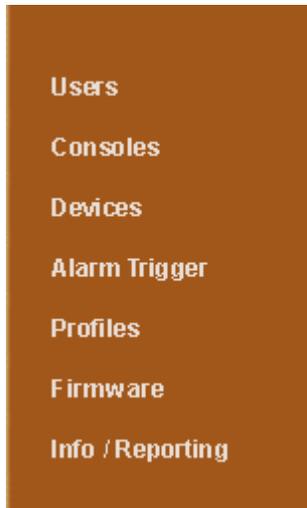
Before discussing configuration procedures using the web application, let us take a quick look at the GUI interface.

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 screen appears.

W*hen 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.
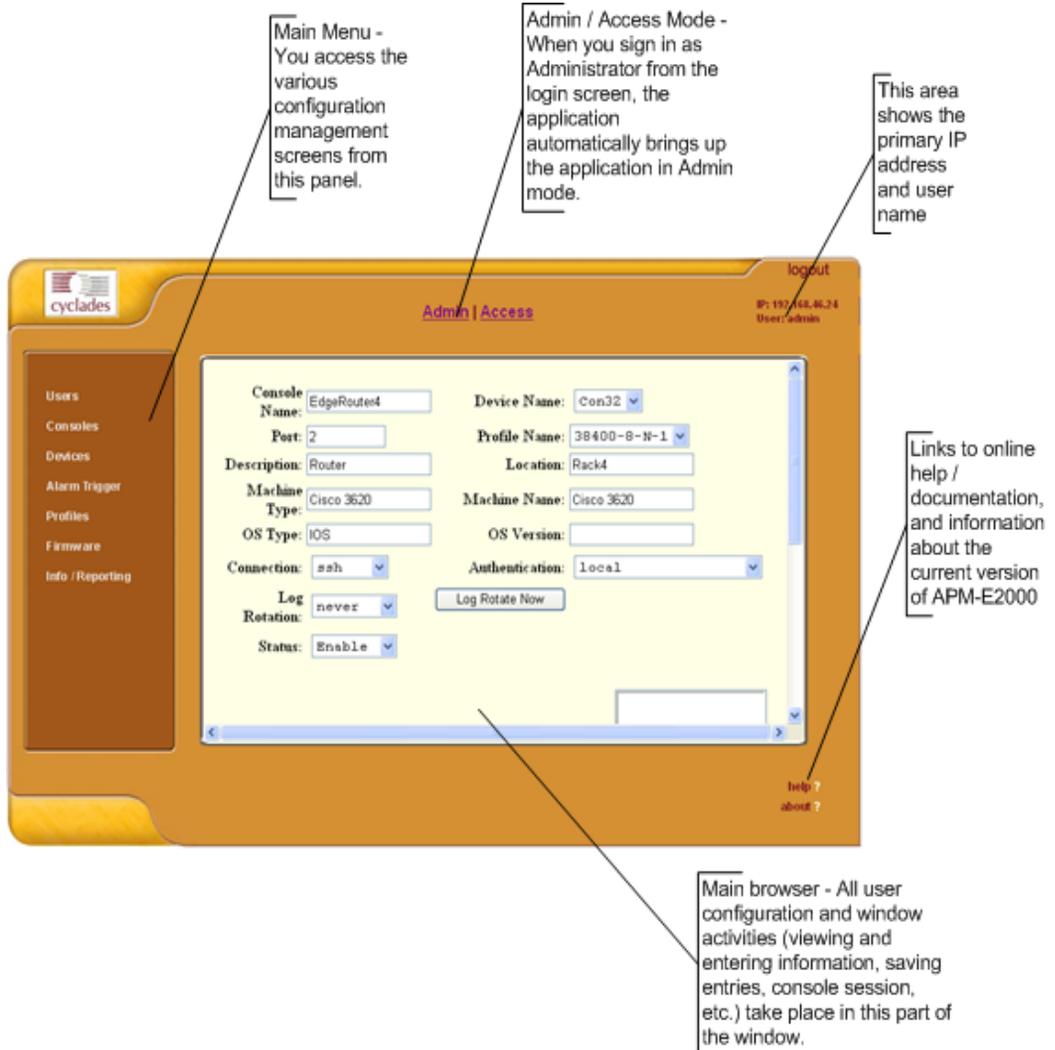
Figure 4.3 - Parts of the Application Screen

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.

Device Management consists of two screens:

- Device List screen
- Device List>Device Definition screen

The screen names do not necessarily appear on the actual window. Because some windows do not have titles, these names are used to distinguish each window as well as to reflect the window function. Most of the screens are categorized as either a List screen or a Definition screen.

Other secondary screens you may need to access in order to manage your devices are:

- Console List screen
- Console List>Console Definition screen
- Firmware Screen

Because target consoles are part of your devices, device management and console management are related. Also, you may need to refer to the **Firmware** screen 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 screen and the **Firmware/Boot** dropdown list of the Device Definition screen.

Device List Screen

The Device List screen, shown below, is the primary screen for device management.
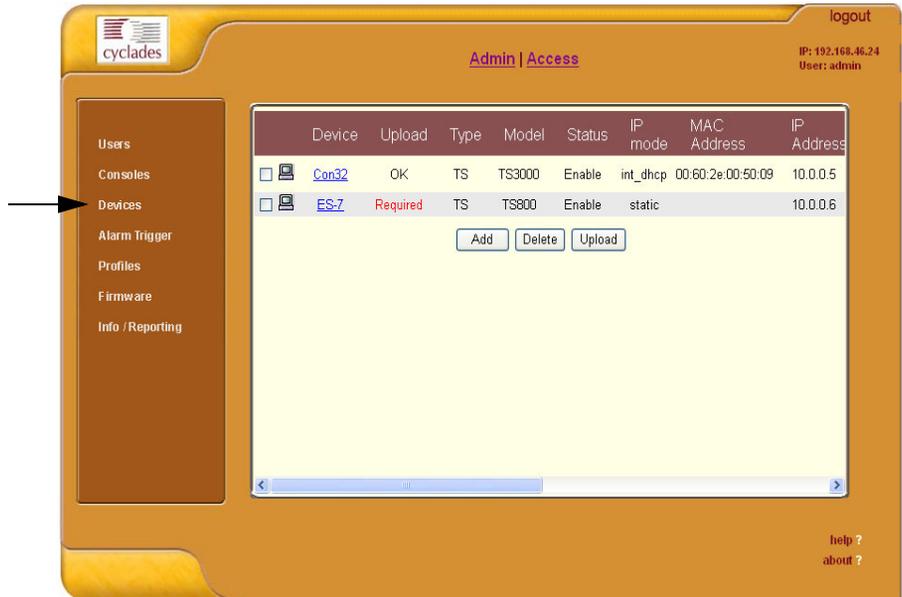
Figure 4.4 - Device List Screen

Screen Fields and Elements

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

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 Screen**, next page, and refer to the Screen 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** screen 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.

	Device	Upload	Type	Model	Status	IP mode	MAC Address	IP Address
☐ 🖥	Con32	OK	TS	TS3000	Enable	int_dhcp	00:60:2e:00:50:09	10.0.0.5
☐ 🖥	ES-7	Required	TS	TS800	Enable	static		10.0.0.6

Add Delete Upload

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 Screen

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

Figure 4.5 - Device Definition Screen

Screen Fields and Elements

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.
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 in dotted notation.
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.
	*See **Configuring Your DHCP Server**, this chapter.*
MAC Address	As indicated, in dotted notation.
Status	Pull down list to select **Enable** or **Disable**.
Auto Upload	Selecting this check box will automatically upload any configuration entries or changes you made on the current screen.
	*See **Auto Upload and Manual Upload**, this chapter.*
Firmware/Boot	Firmware to be uploaded into the console server.
Save	Button to save Device information entered through this window.
Reset	Button to reset the screen.

Configuring Your DHCP Server

A DHCP server is build into the E2000. This means that you can use either your own company's DHCP server or the E2000 as your DHCP server. Or, if you are not using a DHCP server, 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.

int_dhcp (internal)	Select this 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 screen.
ext_dhcp (external)	Select this 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 screen.

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 screen, anytime you make a change to a device or console parameter, the change is automatically uploaded to the console server after your select save from whichever screen you were making the change.

With Manual Upload (i.e., the Auto Upload in the Device Definition screen is unchecked and you upload by selecting Upload from the Device List screen) 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 screen and clicking the **Upload** button, be aware that configuring in automatic mode can lead to slow system response due to excessive uploading.

Uploading Firmware Configuration Data into the Console Devices

The E2000 can upload firmware from its firmware repository to any of the console devices. You can do this in either manual mode or automatic mode. To be in manual mode, the **Auto Upload** check box (Device Definition screen) must remain unchecked.

To upload firmware to a console device in manual mode, perform the following steps:

1. From the Device Definition Screen (Device List>Device Definition), select the firmware you wish to upload from the **Firmware/Boot** drop down list.
2. Click Save.

> *If you were on Auto Upload mode, the system should upload your con-figuration data at this point, ending the upload process.*

3. Go back to the Device List screen 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, Config-uration, 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 Screen

The **Profiles** List screen, which lists the port profiles, is used in conjunction with console management. It is designed to help you 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.

Before adding consoles, you must first define a suitable port profile.
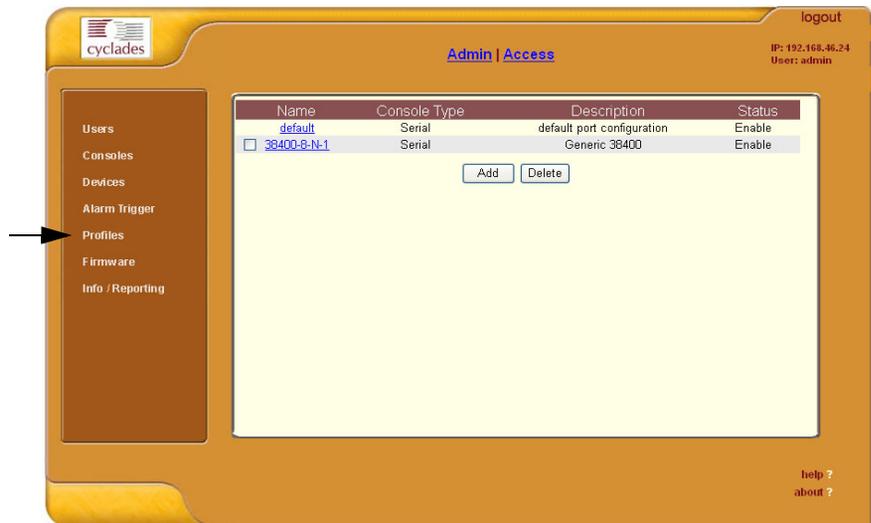
Figure 4.6 - Profiles Screen

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

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

Profile Definition Screen

Use the Profile Definition screen, below, to define your port settings.

Figure 4.7 - Profile Definition Screen

Screen Fields and Elements

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 screen entries and reset screen.

Adding a New Profile

To add a new profile, perform the following steps:
1. From the Profile List screen, select the **Add** button.

    The Profile Definition screen appears.
2. Enter profile information in the provided fields
3. Select **Save** to end.

Modifying a Profile

1. From the Profile List screen, select the profile you wish to edit.

    The Profile Definition screen appears.
2. From the Profiles Definition screen, 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

The 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 4-17.*

You perform console management using the following screens.

- 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 screen.)

Console List Screen

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

Figure 4.8 - Console List Screen

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

Sorting by Field Name

The Console List screen 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 screen, 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 screen, select the console you wish to connect to by selecting the console icon to the left of the console name.

Defining a Console

1. From Console List>Console Definition screen, 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, proceed to the next procedure, else select the **apply changes** button.
3. Return to the Consoles screen (by selecting Consoles from the menu panel) to verify your entry.

Console Definition Screen

Use the Console Definition screen 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.

Figure: 4.9 - Console Definition Screen

Screen Fields and Elements

Console Name	*Required*. Name of the console
Console Server	*Required*. (Drop down list.) Console server to which the current console is connected.
Port	*Required*. Port on the console server when the console is connected.
Profile Name	*Required*. Name of port profile.
Description	Brief description of the console.
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	*Required*. Drop down list to select the type of authentication for the E2000 to access the console port.
Status	Drop down list. Enable or Disable.
Connection	*Required*. Drop down list. Method used to establish a console connection: SSH, Socket, or Telnet.
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 screen, and to reset the screen.
Log Rotation	Frequency of the automatic log rotation process (Never, Daily, Weekly, Monthly).
Logrotate Now	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 screen, 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 screen, select the console (for the particular console log you wish to rotate) to view the Console Detail screen.
2. From the Console Detail screen, 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:

1. From the Consoles screen, select the console (for the particular console log you wish to rotate) to view the Console Detail screen.
2. From the Console Detail screen, select the Logrotate button.
3. From the dropdown list select the frequency (daily, weekly, or monthly).
4. Click **Save**.

Archiving Log Files

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

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

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 screens:

- User List screen
- User Definition screen

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 Screen

Use the User List screen, shown below, to view all E2000 system administrators and users. The screen shows a list of authorized E2000 users and other information about the user (*e.g.*, Name, Location, Phone) which you define in the User Definition screen.

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 the user management screens.
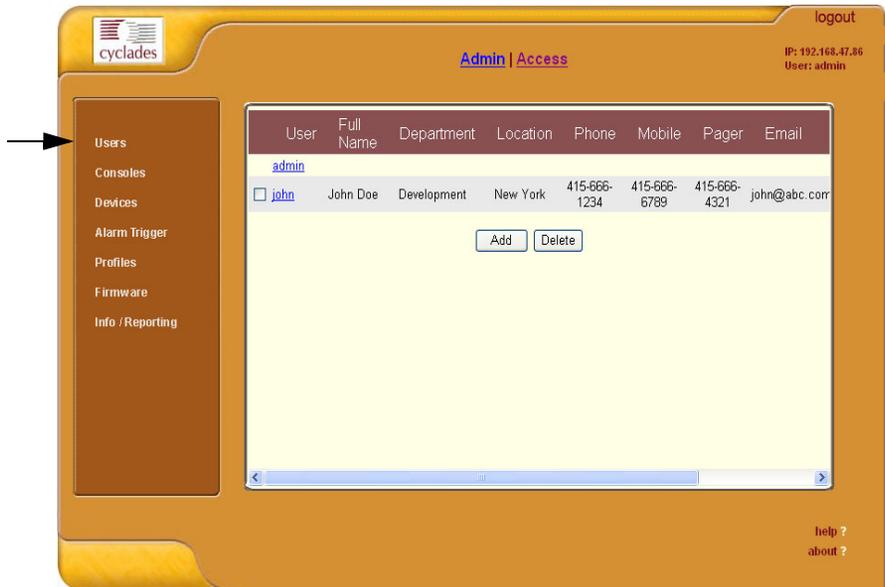
Figure 4.10 - User List Screen

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

Add	This button invokes the User Definition screen 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 screen to allow new entries.

User Definition screen

Use the User Definition screen, shown below, to define a new user or modify
an existing user.
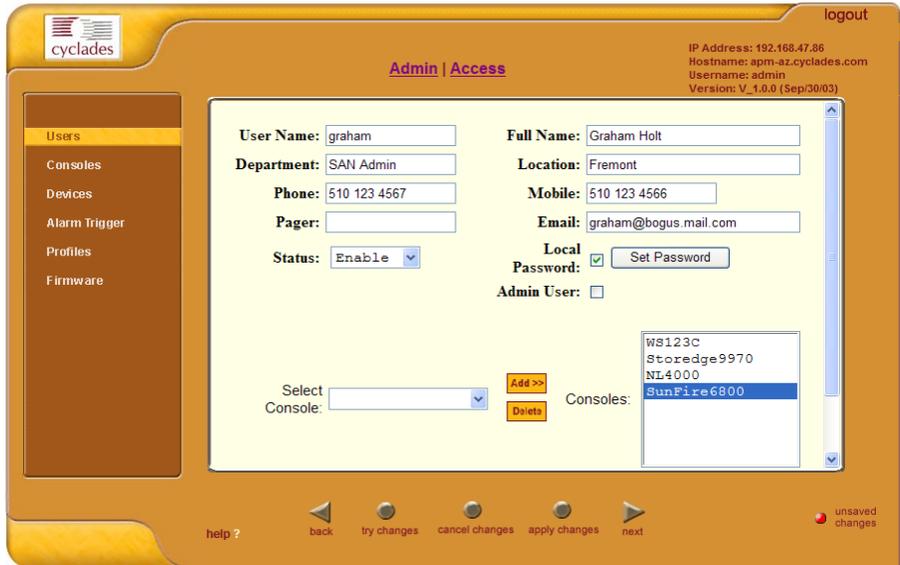
Figure 4.11 - User Definition Screen

Screen Fields and Elements

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.
Local Password	Checking this box sets the user password for local authentication.

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.*

Admin User	Check box to authorize user access to the web application in *admin* 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 screen.

Adding a User

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

1. From the User List screen, select the **Add** button. The system will bring up the User Definition screen.
2. From the User Definition screen, 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 screen, 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 screen, select the user to whom you will assign a console. The system will bring up the User Definition screen.
2. From the **Select Console** drop down menu of the User Definition screen, 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.

> *While using Radius or LDAP does not require local authentication, you may always consider setting up the local password in the AlterPath Manager. A local password is useful in cases where the authentication server may be inaccessible due to network problems or for user names which cannot easily be added to an authentication server such as 'root' and 'admin'.*

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

1. From the User List screen, select the user for whom you will set a password.

    The system will bring up the definition screen for that user.
2. If a password has not been set up, from the User Definition screen, 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 screen, click on the **Local Password** check box.
5. From the User Definition screen, 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

Screens used in Triggers and Alarms Management

Triggers and Alarms Management consists of two screens:

* Alarm List
* Alarm List>Trigger Definition

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

* User List>User Definition
  Use the User Definition screen to set user email address for user notification.

You use the User Definition screen 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 screen.*

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

Alarm Trigger List Screen

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

- Open the Trigger Alarm Definition screen
- Add or delete an alarm.
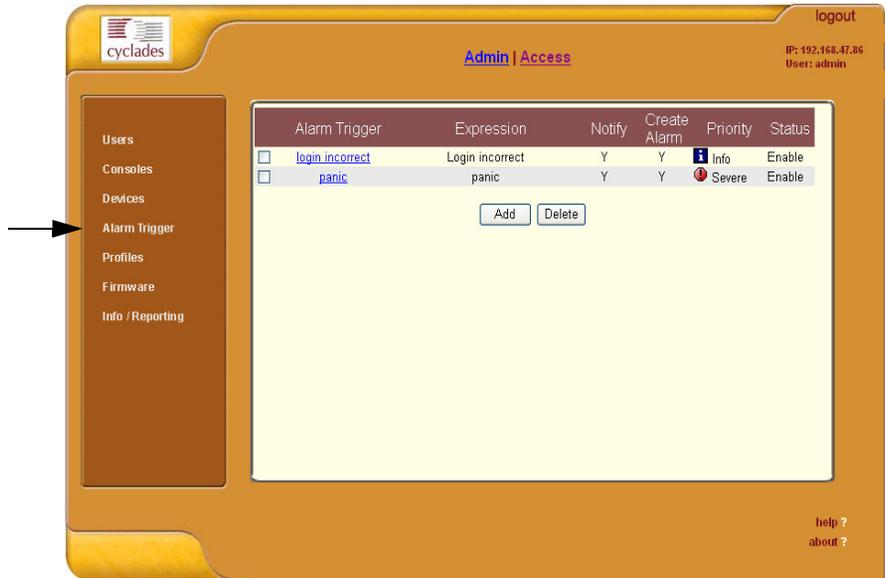
Figure 4.12 - Alarm Trigger screen

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

Adding or Deleting an Alarm

See Creating an Alarm Trigger, next section.
See Deleting an Alarm Trigger, next section.

Alarm Trigger Definition Screen

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

Figure 4.13 - Trigger Alarm Definition Screen

Screen Fields and Elements

Alarm Trigger Name	Name of the trigger. Selecting a trigger name invokes the Trigger Definition screen for that trigger.
Trigger Expression	String used to generate a trigger.
Notify	Yes or No. Indicates if system needs to notify (*i.e.*, 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 (button)	Select this button to save your trigger entry.
Reset (button)	Select this button to reset the screen 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

To create a trigger perform the following steps:

1. From the **Alarm Trigger** screen, select the **Add** button. This brings up the Trigger Definition screen.
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 screen, select the triggers to be deleted by clicking the check boxes to the left of each trigger name.
2. Select the Delete button.

Info Reporting Main Screen

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

Figure 4.14 - Info Reporting Main Screen

Screen Fields and Elements

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 Screen

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

Figure 4.15 - Info Reporting Detail Screen

Screen Fields and Elements

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 screen 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 screens:

*   Firmware List screen
*   Firmware Definition screen.

Any firmware that you add to the Firmware List screen is also reflected in the Device Definition screen (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.

Firmware List Screen

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

Figure 4.16 - Firmware Screen

For an explanation of each screen field, refer to the *Screen Fields and Elements* of the Firmware Detail screen, next screen 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 screen and click the **Import** button.

The system should add the new firmware on the Firmware List screen. The system also updates the Firmware/Boot drop down list in the Device Definition screen.

Deleting Firmware

To delete a firmware, perform these steps:

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

Uploading Firmware Configuration Data 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 Screen (Device List>Device Definition), select the firmware you wish to upload from the **Firmware** drop down list.
2. Click Save.

   If you were on Auto Upload mode, the system should automatically upload your configuration data at this point, ending the upload process.

3. Go back to the Device List screen 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 Screen

Use the Firmware Detail screen, shown below, to:

• View firmware details
• Add comments regarding a firmware.
• Assign a status to a firmware
• Access Manuals and Release Notes
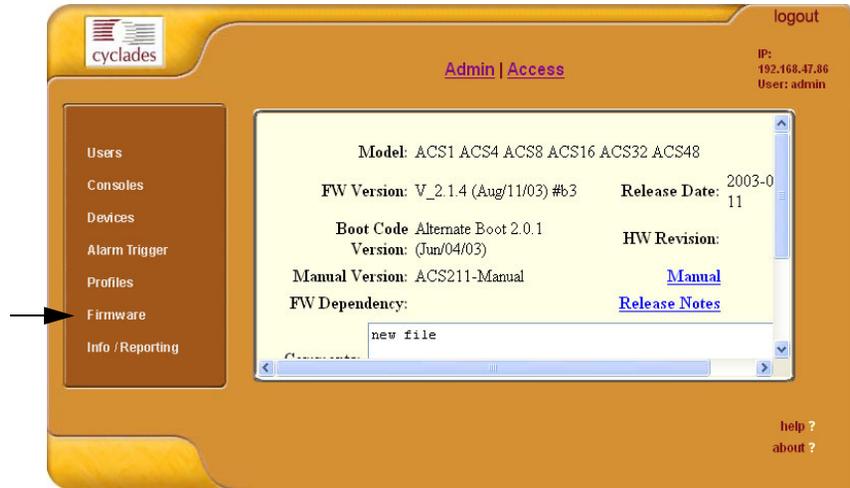
Figure 4.17 - Firmware Detail Screen

Screen Fields and Elements

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.
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 screen, select the particular Firmware Version you wish to view.

    The screen brings up the Firmware Detail screen. From the Firmware Details screen, 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.

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

This page has been left intentionally blank.

Appendix A:
E2000 Hardware Specifications

CPU	Intel® Celeron® 600MHz
Memory	256MB 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/

List of Figures

List of Figures