

AlterPath Manager E2000 User Manual

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

Product Version 1.3.0
Revision No. 10



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, 2005

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, AlterPath KVM/net, 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.

IBM, IBM BladeCenter, ServerGuide and ServeRAID are registered trademarks of IBM Corporation.

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, 3541 Gateway Boulevard, Fremont, CA 94538, USA. Telephone (510) 771-6100. Fax (510) 771-6200. www.cyclades.com.

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	1-3
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
Multiport Ethernet	1-5
Dial Back Support	1-5
Health Monitoring	1-5
Console Wizard	1-6
Device Discovery	1-6
Support for KVM/net	1-6
Support for IPMI	1-7
Device, Console, and User Group Management	1-7
Blade Module	1-7
Backup, Restore, and Replicate User Data	1-8
Change and Configuration Management	1-8

Exhaustive Reporting	1-8
Simple and Easy Web User Interface	1-8
Deploying the E2000	1-9
Private Network Topology	1-9
Private Network Diagram	1-10
Single Network Diagram	1-11
KVM/net Support	1-12
Typical Configuration of E2000 and KVM	1-12
E2000 Features Unsupported by KVM/net	1-13

Chapter 2: E2000 Installation

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: E2000 Web Access

User Interface Overview	3-1
Accessing the E2000 Web Application	3-2
General Screen Features	3-3
Sorting a List Form by Column/Field Name	3-4
Search and Filter Functions	3-5
Alarms	3-5
Alarm Logs	3-5
Responding to an alarm	3-6
Alarm List Form	3-6
Viewing the Alarm Detail Form	3-8
Viewing Alarm or Console Logs	3-10
Assigning/Re-assigning a Ticket to a User	3-10

Consoles	3-11
Viewing the Console List	3-11
Connecting to a Console	3-13
Multiple Users and Read/Write Access	3-13
Viewing a Blade or Switch	3-13
Console Detail Form	3-14
Viewing the (Console) Access Form	3-15
Viewing the (Console) Notify Form	3-16
Viewing the (Console) Groups Form	3-17
Viewing IPMI Sensors	3-18
Logs	3-19
Viewing the Logs	3-20
Access Logs	3-21
Event Logs	3-22
Data Buffer	3-23
User's Profile	3-24
Changing Your Password	3-25
Viewing the User Access Form	3-26
Viewing the User Groups Form	3-26
Viewing the Security Form	3-28

Chapter 4: E2000 Web Administration

Operational Modes	4-2
Configuration Process Flow	4-3
First Time Configuration Wizard	4-4
Using the First Time Configuration Wizard	4-5
Resetting Configuration to Factory Settings	4-5
First Time Configuration Wizard:	
An Example	4-6
Setting the Authentication Method	4-8
Configuring Active Directory	4-8
Limitation of Tacacs Plus in	
ACS Console Access	4-9
Hostname Configuration Must	

Table of Contents

Follow RFC Standard	4-9
Multiport Ethernet Card Configuration	4-9
Connecting to the E2000 Web Interface	4-9
Disabling HTTP to Use Only HTTPS	4-10
E2000 Web Interface: Admin Mode	4-10
Logging Into the E2000 Web Interface	4-11
Parts of the Web Management Interface	4-12
Sorting, Filtering, and Saving a List Form	4-13
Using the Form Input Fields	4-14
Devices	4-14
Device List Form	4-16
Supported Devices	4-18
Adding a Device	4-19
Proxies	4-23
Proxy Types	4-23
Configuring the Web Proxy	4-25
Verifying your Proxy Setting	4-26
Disabling the Proxy	4-26
Direct Access	4-26
Configuring Ports to be Proxied	4-26
Dial Up and Dial Back	4-26
Configuring Dial Up / Dial Back	4-27
Other Requirements for Dial Back (ACS Only)	4-29
KVM/net Device Detail Form	4-30
Configuring KVM Ports	4-30
Assigning KVM Device Groups	4-31
IPMI Device Detail Form	4-31
Using the IPMI Device Detail Form to Add a Console	4-32
Using the IPMI Console Detail Form to Add a Console	4-32
Viewing Sensors or Logs from the BMC	4-32

Configuring Your DHCP Server	4-33
Function of the Status Field	4-34
Difference between Auto Upload and Manual Upload	4-34
Modem Dialing Capability for Remote Access to Devices	4-34
Modem Management via Command Line Interface	4-37
Configuring the Health Monitoring System	4-37
Console Wizard	4-37
Summary of Console Wizard Forms	4-38
Running the Console Wizard	4-39
Device Discovery (Auto Discovery)	4-45
Running the Device Discovery Wizard	4-46
Connecting to a Device	4-47
Deleting a Device	4-48
Deleting a Device from a Group	4-48
Deleting a Device Group	4-49
Uploading Firmware to a Console Device	4-49
KVM/net Device Configuration	4-50
Configuring Escape Sequences and Idle Timeout	4-51
Cascading a Secondary KVM to a Primary KVM	4-54
Alarm Trigger	4-57
Alarm Trigger Management	4-57
Viewing the Alarm Trigger List Form	4-58
Creating an Alarm Trigger	4-59
Deleting an Alarm Trigger	4-60
Configuring Alarms for Device Health Monitoring	4-60
Using the Logical AND in the Alarm Trigger Expression	4-62
Defining the Health Monitoring Alarm Trigger	4-62
How Health Monitoring Works	4-63

Table of Contents

Profiles	4-64
Adding a New Profile	4-65
Modifying a Profile	4-67
Consoles	4-67
Viewing the Console List	4-69
Adding a Serial Console	4-70
Console Type: KVM	4-73
Selecting Users to Access the Console	4-74
Selecting Users to be Notified	4-75
Assigning the Console to a Group	4-76
Deleting a Console from a Group	4-77
Deleting a Console Group	4-77
Connecting to a Console	4-77
Log Rotate Now	4-77
Initiating Log Rotate (Manual Operation)	4-78
Setting Log Rotation in Auto Mode	4-78
Using the Console Detail Form to Add an IPMI Console	4-78
Users	4-79
User List form	4-79
Adding a User	4-80
Selecting Consoles for a User	4-82
Selecting User Group(s) for a User	4-84
Assigning a Security Profile for a User	4-85
Deleting a User	4-85
Deleting a User from a Group	4-85
Deleting a User Group	4-86
Local Password	4-86
Configuring the Local Password	4-86
Setting a User's Security Profile	4-87
Groups	4-87
Creating a Group	4-88

Deleting a Group	4-90
Firmware	4-90
Firmware List Form	4-91
Adding Firmware	4-91
Deleting Firmware	4-92
Uploading Firmware to Console Devices	4-92
Firmware Detail Form	4-93
Viewing and Accessing	
Firmware Information	4-93
Upgrading the E2000 Firmware	4-94
Backing Up User Data	4-95
Backup and Restore Scenarios	4-95
System Recovery Guidelines	4-95
E2000 Database Transaction Support	4-96
Responding to the Warning Message	4-96
Changing the Default Configuration	4-97
Info / Reporting	4-97
Info / Reporting Details	4-98
Blade Management Module	4-99
Activating the Blade Module	4-100
Forms Used to Configure the	
Blade Module 4-	4-100
Devices	4-103
Adding or Editing the Chassis	4-103
Selecting a Group to Access the Chassis	4-106
Proxies	4-107
Configuring the Chassis Switch	4-107
Two Methods of Blade Configuration	4-109
Running the Blade Wizard	4-109
Configuring the Blades and Switches	4-114
Consoles List Form	4-115
Adding a Blade or Switch	4-116
Editing a Blade or Switch	4-116
Security Profiles	4-117
Adding or Editing a Security Profile	4-118

Security Profiles: Source IP	4-119
Security Profiles: VLAN/Subnet	4-121
Security Profile: Date/Time Configuration	4-123
Security Profile: Author. Configuration	4-124
Deleting a Security Profile	4-126

Chapter 5: Advanced Configuration

Working from a CLI	5-2
Logging In	5-2
Shell Commands	5-2
Copying and Pasting Text within the Console Applet Window	5-3
Connecting Directly to Ports	5-4
Sample Command Line Interface	5-4
CLI Commands	5-5
Set Commands	5-6
Re-defining the Interrupt Key	5-11
Changing the Number of Lines in the SSH Applet	5-11
Enabling Telnet	5-12
Changing the ACS/TS Admin Name	5-13
Ethernet Port Configuration	5-13
Modem Card Configuration	5-14
Checking Your Modems	5-14
Excluding Modems from the Modem Pool	5-15
Viewing the Latest Status for Each Modem	5-15
Serial Card Configuration	5-16
How to Detect Modems Connected to the Ports	5-16
Checking Your Modems	5-16
Viewing the Latest Status of Each Modem	5-17
How to Define Different Scripts for Each tty Device	5-17
Modem Dial Back for ACS	5-18
Required CLI configuration	5-18
Optional CLI Configuration	5-18
For external modems:	5-19

For PCMCIA modem:	5-19
Changing the Ports to be Proxied	5-19
NIS Configuration	5-20
User Authentication	5-21
Creating the krb5.keytab for	
Kerberos Authentication	5-22
How Kerberos Works	5-22
Creating the krb5.keytab in the E2000	5-23
Active Directory Configuration	5-24
Disabling HTTP to Use Only HTTPS	5-25
Firmware 25	
Adding Firmware	5-25
Upgrading the E2000 Firmware	5-25
Backing Up User Data	5-26
Backup and Restore Scenarios	5-27
Backup and Restore Commands	5-27
Managing Log Files	5-27
Where Log Files are Archived	5-27
Backing Up Log Files to a Remote Server	5-28
System Recovery Guidelines	5-28
Changing the Database Configuration	5-29
Installing SSL Certificates	5-29
More About Importing Certificates	5-31
Appendix A: <i>Hardware Specifications</i>	A-1
Appendix B: <i>Modem Access in ACS</i>	B-1
Glossary	

Table of Contents

Before You Begin

Welcome to the AlterPath Manager E2000 Manual! This manual is designed to help you install, configure, and operate the E2000, as well as to guide you in your day-to-day operations of the product.

Note: *For convenience, this manual refers to the AlterPath Manager E2000 as simply **E2000**. In some instances such as the CLI, the term **APM** (AlterPath Manager) is also used.*

Audience

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

Document Organization

The document is organized as follows:

Chapter	Content Description
1: Introduction	Defines and explains the overall product features and uses of the E2000.
2: E2000 Installation	Explains the procedure for installing the E2000 and preparing it for web configuration and access.
3: E2000 Web Access	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

Chapter	Content Description
4: E2000 Web Administration	Explains to the system administrator how to 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 more. Configuration settings include user access, alarm triggers, device management, firmware control, as well as running the configuration wizards.
5: Advanced Configuration	Addressed to the advanced user, provides configuration procedures using CLI. It includes such procedures as modem card configuration, backing up log files and user data, and installing SSL certificates.

Typographical Conventions

This manual uses the following typographical conventions:

Print Element	Convention
Form/Window Labels	Words that appear on forms, windows, or any part of the user interface are typed in boldface . <i>Examples:</i> The Alarm definition form; the Password field.
Hypertext Links	With the exception of headings and the Table of Contents (which are already linked), all <u>underlined</u> words are hypertext links.
Form/Window Levels	Form levels are indicated by the “greater than” symbol (>), starting from the parent screen to child. Most E2000 screens or windows contain only two levels. <i>Example:</i> Consoles List > Console Detail

Naming Conventions

This manual uses the following conventions:

Name	Convention
Administrator	Also referred to as the <i>Admin User</i> . The system administrator of the E2000 who has the authority to configure and manage the E2000.
APM	AlterPath Manager. Synonymous with E2000, “APM” is often used in the Command Line Interface.
E2000	The short name for AlterPath Manager E2000.
Form	The form is the largest area as well as the basic unit of the web graphical 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 Detail forms. The configuration forms of the E2000 (<i>i.e.</i>, Devices, Consoles, Users, Alarm Trigger) use the two types of forms.</p> <p><i>Examples:</i> Console List form; Console Definition form.</p>
Regular User	Refers to one who uses the E2000 application as a regular user (<i>i.e.</i> , the web management interface is on Access mode, not Admin mode) even though the user may be a system administrator
Select	To <i>select</i> is the same as to <i>click your mouse</i> .

Command Line Syntax

While this manual is primarily designed for using the E2000 web interface, some special features show you how to configure the E2000 using the Command Line Interface (CLI). CLI configuration is discussed in Chapter 5 (Advanced Configuration) of the manual. 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.pmusers: 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>]...
```

Change the ChapterTitle variable

Chapter 1

Introduction

The AlterPath Manager E2000 is a feature-rich, out-of-band (OOB) manager designed to provide out-of-band infrastructure (OOBI) 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, the E2000 regular user can easily view and access consoles, view consolidated logs and reports, and respond to triggers, alarms, and other system issues that may arise.

Through the same web interface (in Admin Mode) or through CLI, the system administrator can configure and manage the E2000 and all its users from a single location without having to work directly on a target device or server console.

Note: 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** is anyone who has the exclusive authority to configure and administer the E2000 and its users.

Connectivity and Capacity

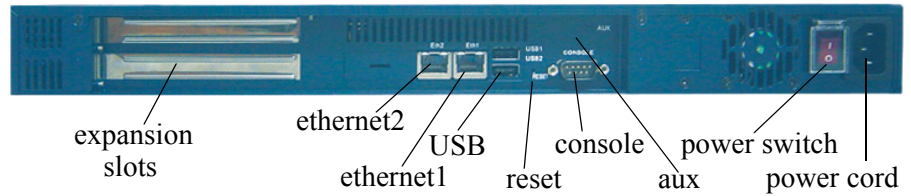
The E2000 allows you to configure 2048 devices, 5000 console ports and maintain 256 simultaneous connections to consoles and devices. You can perform firmware upgrades on 256 separate console management devices. The E2000 also supports up to 30 simultaneously connected users, and allow multi-user access to each port.

Front view of the E2000:



1: Introduction

The port connections available from the E2000 box are shown below (*back view of the 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
- Multiport Ethernet
- Dial Back Support
- Network health monitoring
- Console wizard
- Device discovery
- Support for KVM/net
- Support for IPMI
- Device, Console, and User Group Management
- 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 communication 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. 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 device (*e.g.*, TS, ACS, KVM/net), and thereby maintain a secure password. You need only use your password once upon logging onto the E2000. For all users who access the console ports, the E2000 provides the following authentication methods: local database, RADIUS, LDAP, Kerberos, Tacacs+ and NIS.

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 consoles which they are not authorized to use.

One-Click Access to Consoles and Devices

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

To access a console, 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.

If the Blade Module is enabled, the Console List form also shows the console name for each supported blade server. Right-clicking a console name, enables the user to select KVM or SOL, or to power on or power off, based on the user's access rights defined in the **Security Profile**.

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

Note: Alarm triggers work only with serial and IPMI consoles.

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 - Allows you to add notes to an alarm to indicate what action you have taken. These notes can be useful for future reference to similar issues.

Reports - Allows you to 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.

Multiport Ethernet

The E2000 supports up to two multiport PCI Ethernet cards for secure networks that use multiple network segments. This enables the E2000 to physically separate devices and connect to multiple network segments.

The Ethernet cards are detected by the configuration wizard during boot time.

Dial Back Support

The E2000 provides options for integrated modems to automatically dial to remote locations when the network fails. In the absence of network connectivity, the dial back feature enables the E2000 to initiate a call to a remote AlterPath ACS unit, and then have the ACS dial back the connection using a predefined number.

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 modems 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. The console wizard is designed to work with all types of devices, including KVM/net units and secondary units that are connected to the KVM/net units.

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.

Support for KVM/net

Among other console types, the E2000 supports viewing of Keyboard-Video-Mouse-based consoles through the use of an AlterPath KVM/net installed in the network. The user connects through a client software over an IP connection and the KVM/net switch routes the application to one of its ports to connect the user application to the KVM ports of a target server.

The KVM/net supports physical cascading of unit to provide or support more ports. The admin user configures the cascading through the E2000.

Note: E2000 is compatible with AlterPath KVM/net version 1.1.0 and above.

Support for IPMI

The E2000 supports servers that are based on IPMI (Intelligent Platform Management Interface), the open standard for machine health and control (including remote control). IPMI defines common interfaces to the "intelligent" hardware that is used to monitor server physical health characteristics, such as temperature, voltage, fans, power supplies and more.

These monitoring capabilities provide E2000 users information that allow power control of servers, recovery, and asset tracking.

The E2000 allows multiple, concurrent IPMI SOL (Serial Over LAN) sessions, up to 256 sessions.

Note: IPMI is a paid-for option for E2000 users. The feature is hidden from users who do not need it.

Device, Console, and User Group Management

Devices, consoles, and users can be grouped to further simplify the organization and management of these system components. The administrator may create, update and delete any of the groups at anytime through the web management interface. Users can view only those groups to which they belong or have access.

Blade Module

The E2000 supports blade management (that is, the IBM Blade Center) through the plugged-in Blade Module. Blade configuration and management is available through the web interface or CLI. The Blade Module, once enabled, supports up to 2048 chassis and 5000 blades/switches, just like any device or console.

Using the Blade Wizard, an admin user can create 14 blades and 4 switches. All blades provide authorized users with CLI, KVM/IP, virtual media, and power options. For security, Blade users are controlled by the Access Control List (ACL) which is configured through the Security Profile option of the web interface.

Note: The Blade Management Module is a paid-for option for E2000 users, and is hidden from users who do not need it.

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.

As a user you can only view and access those consoles you are assigned. This 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.

Note: See *Private Network Diagram*, this chapter.

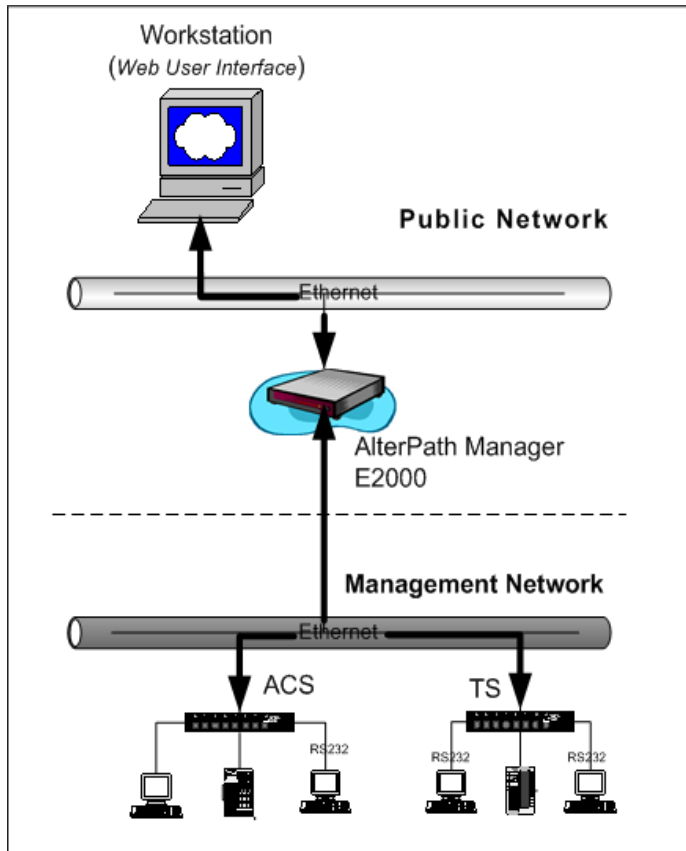
Single Network Topology

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.

Note: See *Single Network Diagram*, this chapter.

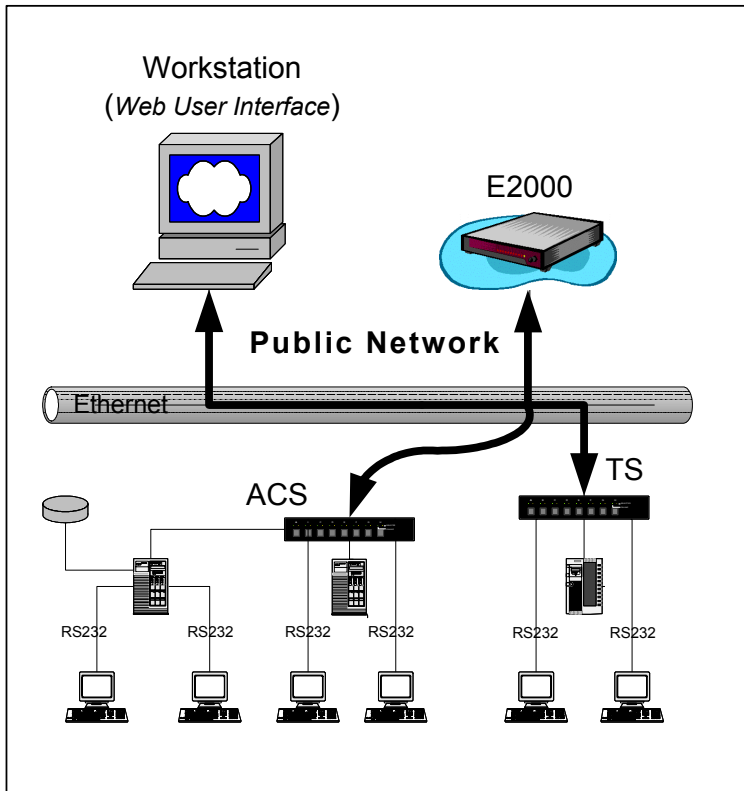
Private Network Diagram

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



Single Network Diagram

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

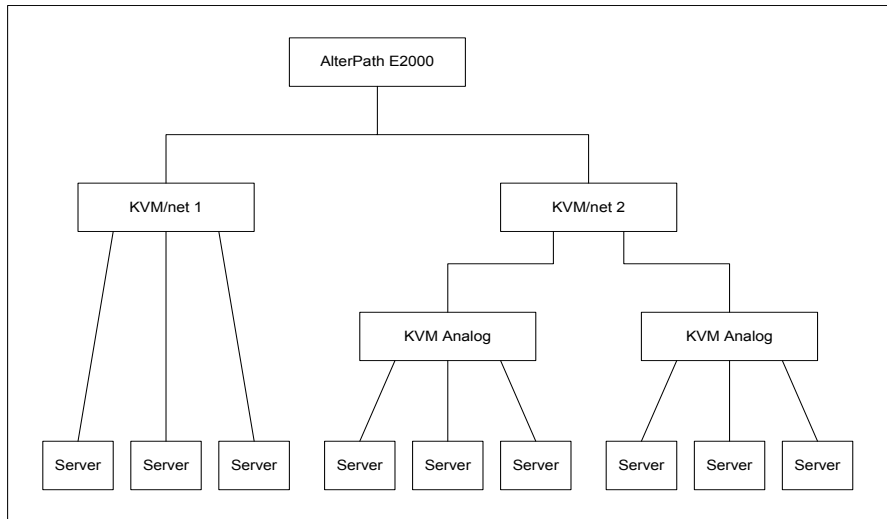


KVM/net Support

The AlterPath KVM/net is a Cyclades stand-alone networking device similar in concept to a console server. The user connects through a program over an IP connection and the KVM/net switch routes the application to one of its ports to connect directly to the keyboard, video, and mouse ports of a target server. You can install in the network a KVM/net with 16 or 32 KVM ports (i.e., AlterPath KVM/net 16 or AlterPath KVM/net 32).

Typical Configuration of E2000 and KVM

The configuration below shows the E2000 managing four KVM switches. Two KVM/net switches are accessed directly through IP. The other two are physically cascaded to KVM/net 2. KVM analog switches (as well as KVM Expanders) are normally used as cascaded units since they cost less than KVM/net switches.



Each secondary KVM switch may have one or two connections to a primary KVM/net switch while a primary KVM/net switch may have one or more secondary switches connected.

In the diagram, if the KVM/net 2 is a 16-port device and the two analog switches are also 16-port devices, then the KVM/net 2 will have 44 ports available to the user; 32 ports from the two analog switches and 12 ports from the KVM/net 2. The four ports in the KVM/net 2 are used to connect to the slave units.

Regular users only see the ports to which they can connect. Authentication, authorization, and access accounting (logging) functions in the same manner as for serial console ports. Health Monitoring will consist of periodic checking as defined in the Device Detail form. It will connect to the KVM/net interface and login to the unit to ensure that the IP is valid, including the

username and password. Errors are reported by email to the admin user, and an alarm generated.

E2000 Features Unsupported by KVM/net

When using the KVM/net, logs are available only for access to KVM consoles. The Logs form defaults to Access Logs, and Event Logs. Data Buffering is inactive.

Alarms are generated only for KVM/net Health Monitoring events. The Alarm list form is the same as for serial console alarms, but without the data buffer link.

1: Introduction

Chapter 2

E2000 Installation

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.
3. Refer to the **Safety Considerations When Rack Mounting** section of this chapter to ensure safety.
4. 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.

Note: *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.

5. 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.

6. 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.

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

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

You can obtain the latest update to HyperTerminal from:

<http://www.hilgraeve.com/hpte/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. Configuration through the web interface is discussed 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:

2: E2000 Installation

- 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:

Requirement	Description
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. NOTE: You must have 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: <ul style="list-style-type: none">- All console servers- Gateway- DNS Optional addresses: <ul style="list-style-type: none">- NTP- SMTP (only when using the alarms feature.)
NIC Card	Ensure that you have a NIC card installed in your PC to provide an Ethernet port, and allow network access.

Note: To complete the configuration process, go to **Chapter 4: Web Administration, First Time Configuration** section, page 4-3.

Note: **Chapter 3: E2000 Web Access** 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.

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

Activating IPMI or Blade Module

The E2000 provides two optional features:

- IPMI
- Blade Module

To activate IPMI, follow the steps below:

1. Execute the script: **`/var/apm/bin/apm_enable_ipmi.sh`**
2. Enter the password provided to you when you register for this feature.

To activate the Blade Module:

1. Execute the script: **`/var/apm/bin/apm_enable_bladeModule.sh`**
2. Enter the password provided to you when you register for this feature.

2: E2000 Installation

Chapter 3

E2000 Web Access

The web interface provides two modes for using the E2000 based on the type of user: **Access** (for operation by regular users) and **Admin** (for configuration by system administrators). This chapter explains the procedures for operating the E2000 web interface in Access Mode.

Addressed specifically to regular users, this chapter is organized as follows:

- User Interface Overview
- Accessing the E2000 Web Management Interface
- Logging In
- Using the **Alarms** forms
- Using the **Consoles** forms
- Using the **Logs** forms
- Using the **User Profile** forms

Note: If you are an E2000 system administrator, refer to **Chapter 4: E2000 Web Administration**.

User Interface Overview

The E2000 user interface provides you with four main menu options:

Table 3-1: Access Mode Menu Summary

Menu Selection	Description
Alarms	The Alarms list form is the first form that you see (or the default form) when you log in. Use this form to view alarms, update the status of an alarm or close an alarm after resolving it

Table 3-1: Access Mode Menu Summary

Menu Selection	Description
Consoles	Use the Consoles form to view a list of 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 . For IMPI and Blade Module users, the Consoles list form provides access to the IPMI SOL as well as the chassis blades and switches.
Logs	Use the Logs form to view the Access Logs , Events Logs , and Data Buffer for a particular console or device. You can also access logs from the Console List form.
User's Profile	The User's Profile form displays the profile of only the user currently logged in. Use the User Profile to view or modify your own user information, as well as your own security profile.

>> **Accessing the E2000 Web Application**

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

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

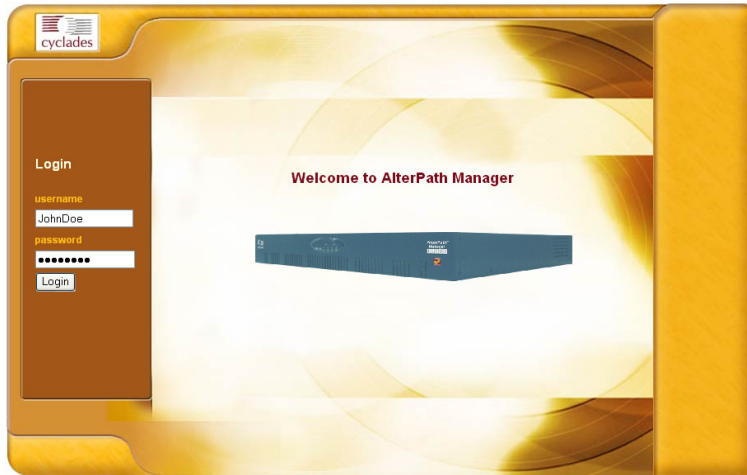
`https://nnn.nnn.nnn.nnn`

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.

Note: See *Chapter 5: Advanced Configuration* for the procedure on how to configure the encrypted version.

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



3. Select the **Login** button.

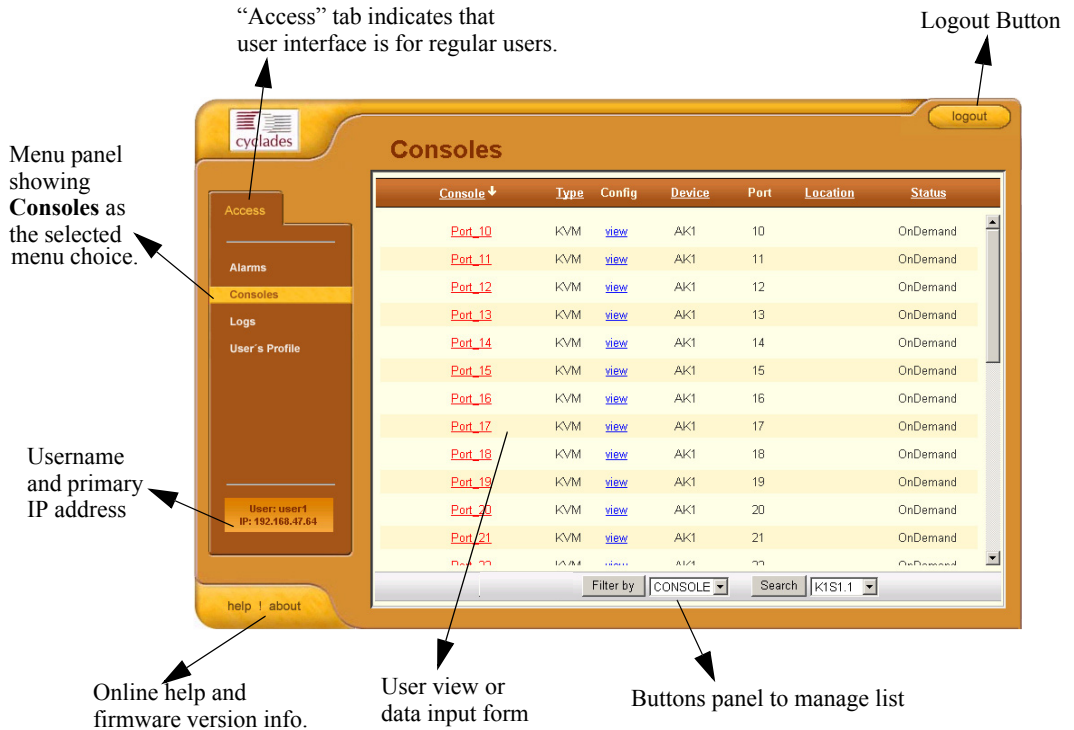
Upon successful login, the **Alarms** form appears.

Note: 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

The diagram below shows the general features of the E2000 Web Management Interface (WMI). The sample form is for illustration only; it is not the first screen that you see when you log in as a regular user.

3: E2000 Web Access



The menu panel highlights the currently selected menu option.

Your user name and IP address appears on the lower left hand corner of the screen.

The Admin tab (not visible in the example above) is visible to regular users with admin rights.

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

Sorting a List Form by Column/Field Name

Most, if not all, list forms provide sort, search, and filter functions.

An underlined column name indicates that the list can be sorted by the column name. The Console List form, for example, allows you to sort by Console, Type, Device, Location, or Status. To sort by Location, simply click the column name, **Location**.

The arrow adjacent to the heading indicates that the list is sorted based on that heading. The position of the arrowhead indicates the sort order. A downward arrowhead indicates that the list is alphanumerically arranged in ascending order; an upward arrowhead, in descending order. You can change the sort order by clicking on the heading or the arrow.

Search and Filter Functions

When available, you will find the **Search** and **Filter by** buttons at the bottom of the List form.

This allows you to search through a List form by selecting the search category (*i.e.*, Console group) from the dropdown field and selecting the **Search** button. You can also filter your search by selecting a category from the Filter by dropdown field and selecting the **Filter by** button.

The view generated by selecting the **Filter by** button is automatically saved.

Alarms

The Alarm List form is the default form of the E2000 Web Interface 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 along with a ticket number 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. Each alarm or ticket in the list includes a timestamp, a priority level, and a status.

Alarm Logs

The E2000 not only stores each alarm in a database, but also maintains a log for each alarm. There are two ways in which you can view alarm logs:

- From the Alarms List form
- From the Logs form (**Logs > Data Buffer**)

Responding to an alarm

Since no two issues are exactly the same, you have several ways to respond to an alarm depending on its nature and severity. A “typical” procedure for responding to an alarm is 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 the alarm status and close the ticket.
- Re-assign the ticket to another user.

Alarm List Form

When you first log in to the E2000 as a regular user or select Alarms from the menu, the Alarm List form is the first form that you will see. Use this form to view the list of alarms, to connect to a console, and to view console logs. To

Alarms

re-assign the current ticket, change the ticket status, and add notes or comments, use the Alarm Detail (or Ticket Info) form.



Table 3-2: Alarms List Form - Fieldnames and Elements

Fieldname	Definition
Ticket	Ticket number assigned to an alarm. The symbol above the ticket number indicates the severity level of the alarm. Select the number to display the Alarm Detail form.
Console	Console from which the alarm originated. Click on the console name to enable a console session according to the type of configured device and console. For example, a serial console will establish a text-based session; a KVM console will launch the KVM viewer, and an IPMI console will launch the SSH applet and connect to the IPMI SOL console.

Table 3-2: Alarms List Form - Fieldnames and Elements

Fieldname	Definition
Console Config	Console configuration. Select this to view the Console Detail form (which includes the secondary form: Console Notify, Console Access, and Console Group) for the particular console record.
Alarm Trigger	The Alarm Trigger name. Click on the name to view the Alarm Trigger Detail form.
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.

>> **Viewing the Alarm Detail Form**

The Alarm Detail form contains detailed information about the ticket as generated by an alarm. It allows you to re-assign the ticket, update the status, and enter notes regarding the alarm or ticket.

To view the ticket information for an alarm, follow the steps below:

1. From the Alarm List form, click on the ticket number.

The form brings up the Alarm Detail form.

Table 3-3: Alarms Detail Form - Fieldnames and Elements

Fieldname / Button	Definition
--------------------	------------

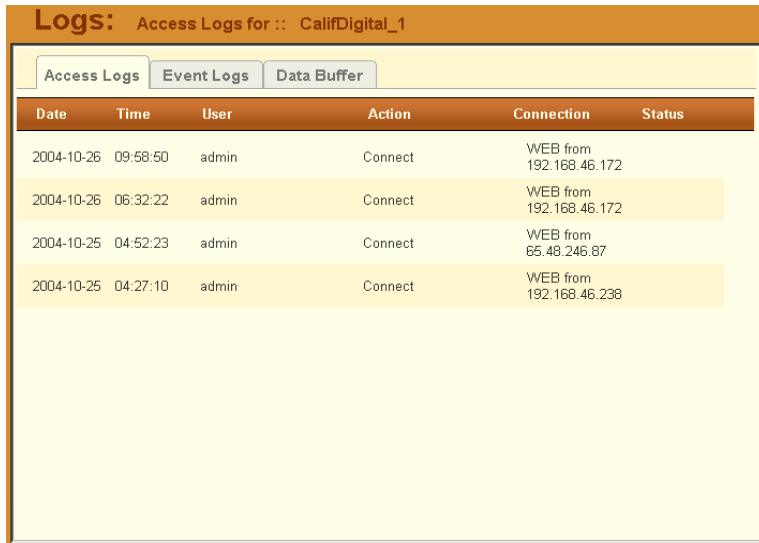
Assigned Users	Dropdown box that lists all the assigned users for the current alarm. Select a user to assign or re-assign ticket to another individual user.
Status	Dropdown box to select the status of the ticket.
Messages	The system-generated message(s) pertaining to the alarm.
Notes	Text entry box for entering notes or comments about the current ticket or alarm.
Back	Button to return to the Alarm List form.
Save	Button to save your entries.
Reset	Button to reset the form to its original or default values.

>> Viewing Alarm or Console Logs

You can view the console log for a particular alarm or ticket from the Alarm List form. To view the console log, follow the step below:

1. From the Alarm List form, under the Console Log column heading, select the corresponding view link for the console log you wish to view.

The system displays the Logs form:



Logs: Access Logs for :: CalifDigital_1					
Access Logs Event Logs Data Buffer					
Date	Time	User	Action	Connection	Status
2004-10-26	09:58:50	admin	Connect	WEB from 192.168.46.172	
2004-10-26	06:32:22	admin	Connect	WEB from 192.168.46.172	
2004-10-25	04:52:23	admin	Connect	WEB from 65.48.246.87	
2004-10-25	04:27:10	admin	Connect	WEB from 192.168.46.238	

>> Assigning/Re-assigning a Ticket to a 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 Alarm Detail or Ticket Information form.

The system opens the Alarm Detail form.

2. From the Ticket Information form, select user from the **Assigned Users** dropdown list box.
3. If applicable, select the status from the **Status** dropdown list box.
4. If applicable, type in your notes or comments in the **Notes** text entry box.
5. Select **Save** to complete your entry.

Consoles

Selecting **Consoles** from the menu brings up the Consoles List form which allows you to:

- View detailed information about the consoles assigned to you.
- Connect to your target console.

To “*connect to a target console*” means that depending on the type of configured device and console, selecting a console from the Console List form may:

- Open a command line console session (for TS and ACS)
- Launch the KVM Viewer and connect you to a KVM port (for KVM/net)

Optional Features

For the following optional, paid-for options, the **Consoles** menu also allows you to:

- Connect to an IPMI Serial Over Lan (SOL) console.
- View individual blades and switches of the chassis, as part of the Blade Module.

>> Viewing the Console List

The Console List form allows you to view the consoles to which you have authorized access.

To view the Console List form, follow this step:

1. From the Consoles form, under the **Config** column, select the **view** link adjacent to the console you wish to view.

The Console List form appears.



Table 3-4: Consoles List form: Fieldnames and Elements

Column/Button	Definition
Console	Console name. Clicking on a Console Name launches a connection to the console. (The example shows a KVM console; clicking on a console will connect you to the KVM port.)
Type	The type of console as defined in the Console Detail form.
Config	For each line, select the link to view the console detail form of the selected console.
Device	Console server used by the console.
Port	Port number used by the console.
Location	Location of the console.
Status	Operating status (Enabled, Disabled, OnDemand) of the console.

Table 3-4: Consoles List form: Fieldnames and Elements

Column/Button	Definition
Filter By	Button to filter your search by Console Group Name which you select from the dropdown box.
Search	Button to search by individual console name which you select from the dropdown box.

>> **Connecting to a Console**

To connect to a console:

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

Note: If a modem is connected to a remote site, you will experience a slight delay before connecting to a console.

The system normally connects you to a console through Secure Shell (SSH).

In KVM/net, the listed console names are the KVM/net ports. Clicking on the console name launches the ActiveX application and connects to the port.

If the console name is an IPMI console, clicking on the console name launches an SSH session and connects to the IPMI SOL (Serial Over LAN) console.

Regardless of the type of “console,” the E2000 handles the authentication.

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.

Viewing a Blade or Switch

Note: *This feature is available only to users of the optional **Blade Module**.*

The E2000 allows you to view individual blades and switches from the Consoles List form. To view a blade or switch, place the mouse cursor over the blade/switch name to display the list of connect options: **CLI** (command

line interface), **KVM**, **VM**, **On** (i.e., to power on the blade server), and **Off** (i.e., to power off the blade server).

Like all other consoles, as a regular user, you can only view those blade servers to which you have access. You may also view your user profile with regards to blade access from the **User's Profile** option of the menu, **Security** form.

Console Detail Form

Use the Console Detail form to view specific information about a particular 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. The sample forms in this section uses an IPMI console as an example.

The screenshot shows a web interface titled "Consoles: viewing IPMI console :: CalifDigital_1". It features a tabbed interface with "Details" selected. The details form includes the following fields and values:

- Console Name: CalifDigital_1
- Device Name: CalifDigital_1
- Description: IPMI Server
- Location: Fremont
- Machine Type: x86
- Machine Name: Noah
- OS Type: Linux
- OS Version: Suse9.0
- IPMI Authentication: straight password
- Encryption Type: none
- Log Rotation: never
- Status: OnDemand

Additional elements include a "Log Rotate Now" button, and "Back" and "Sensors" buttons at the bottom.

Table 3-5: Consoles, Details Form - Fieldnames and Elements

Field Name	Definition
Details	Button to display the Console Detail form.

Table 3-5: Consoles, Details Form - Fieldnames and Elements

Field Name	Definition
Access	Button to view users who are authorized to access the current console.
Notify	Button to view users who can be notified of an alarm pertaining to the current console.
Groups	Button to view the group(s) to which the current console belongs.
Power	Button to view power management information.
Console Name	Name of the (target) console.
Device Name	Name of the device used by the console.
Port	Name of port used by the console.
Description	A brief description of the console.
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.
Location	Physical location of the console.
Status	Status of the target console (Able, Disable, On Demand).
Back	Button to return to the previous page or form.

>> Viewing the (Console) Access Form

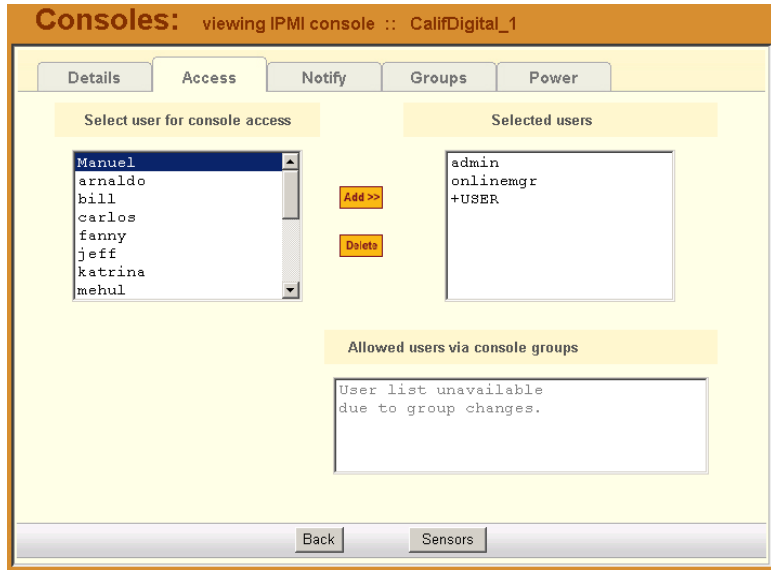
The Console Access form shows the users who are authorized to access the current console.

To view the Console Access form:

3: E2000 Web Access

1. From the Console Detail form, click on Access.

The system displays the Console Access form:



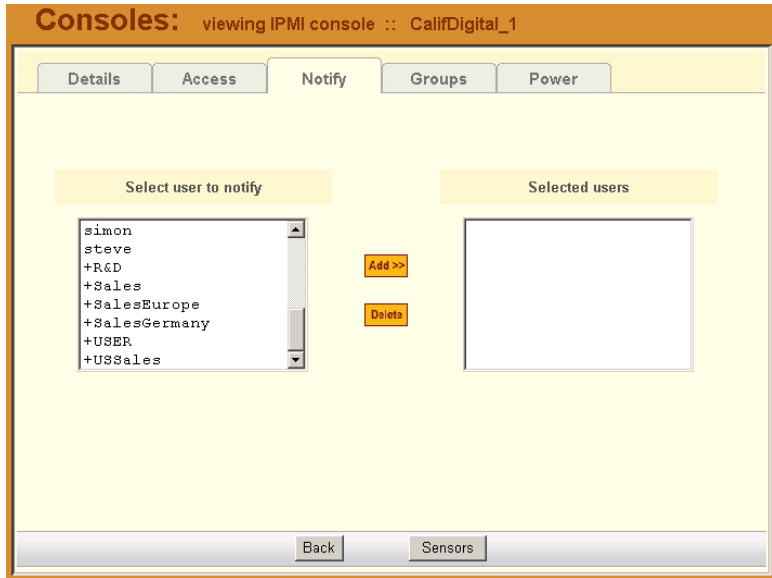
>> Viewing the (Console) Notify Form

The Console **Notify** form shows the users who are notified when an alarm pertaining to the current console is generated.

To view the Console Notify form:

1. From the Console Detail form, click on Notify.

The system displays the Console **Notify** form:



In the selection box, a plus (+) sign indicates a group, as opposed to a user. USER is the default list which contains all users.

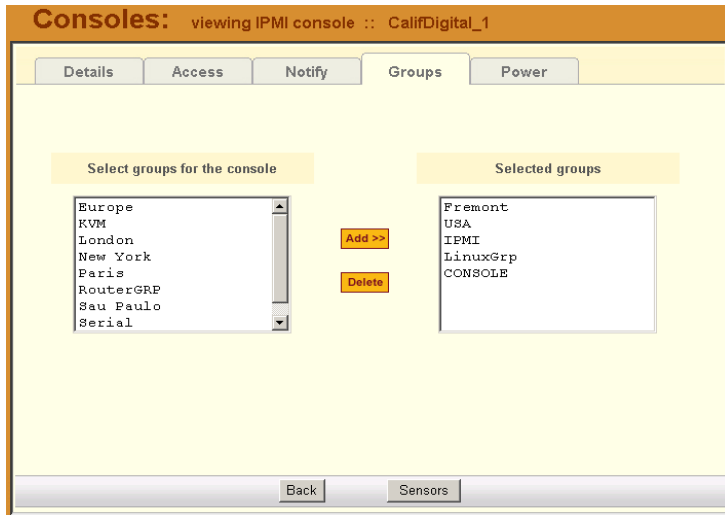
>> **Viewing the (Console) Groups Form**

The Console Groups form shows the group(s) to which the current console belongs.

To view the Console Group form:

1. From the Console Detail form, click on **Groups**.

The system displays the Console Group form:



>> Viewing IPMI Sensors

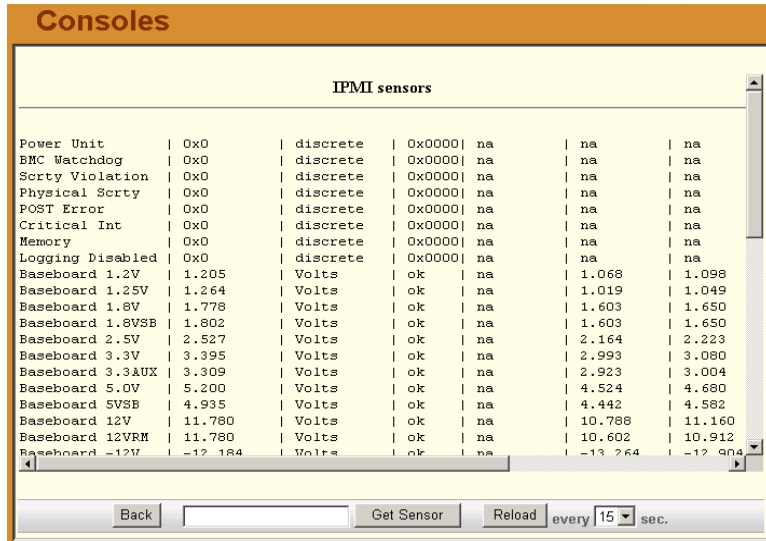
Note: IPMI is a paid-for feature of E2000, which is available only to IPMI users.

The IPMI Sensor screen is used to view IPMI-based servers. IPMI (Intelligent Platform Management Interface) is the open standard for machine health and control (including remote control). The screen allows you to monitor server physical health characteristics, such as temperature, voltage, fans, power supplies and more.

To view IPMI Sensors, perform the following procedure:

1. From the Consoles list form, select an IPMI console to view.
2. From the Console detail form, click on the Sensor button.

The system displays the IPMI Sensors form:



Logs

The Logs option of the menu allows you to select and view three types of logs pertaining to the console assigned to you:

Log Type	Definition
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.
Data Buffer	This is a log of all transaction data generated on the console.

All three logs are available for the specified console. To access each log, select the appropriate log type from the title bar. As with consoles and alarms, you can only view the logs of systems to which you have authorized access.

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

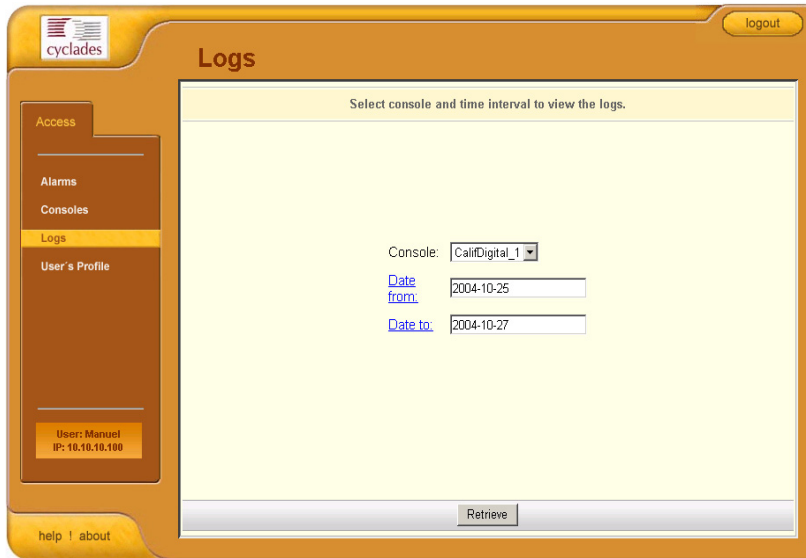


Table 3-6: Logs Form - Fieldnames and Elements

Field Name	Definition
Console	Drop down list to select a console that will be the basis of the log(s) to be retrieved.
Date From	Drop down list to select the starting date of the log(s) to be viewed.
Date To	Drop down list to select the end date of the log(s) to be viewed.
Retrieve	Button to download the requested log(s) and display the Log forms.

>> Viewing the Logs

To view the logs available for a specified console (to which you have authorized access), perform the following steps:

1. Select **Logs** from the menu.

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.

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

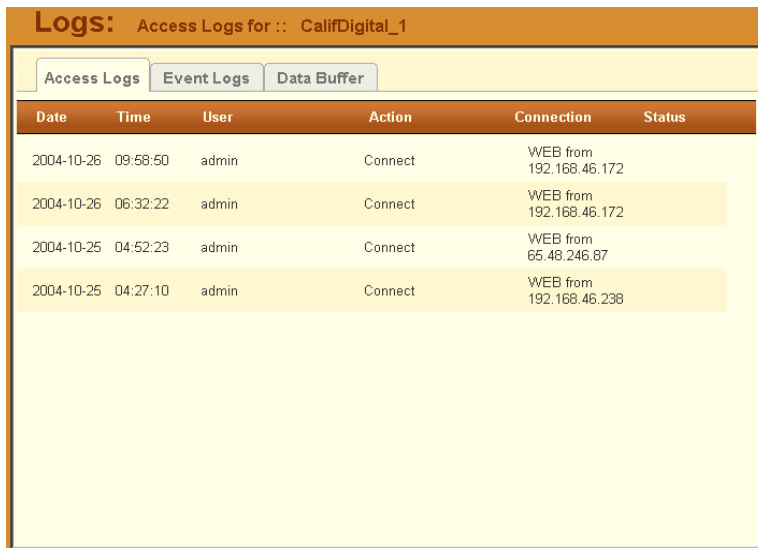
3. Select a range of dates from which to base your logs by selecting from the **Date From** and **Date to** drop down lists.

The system brings up the Logs Detail form.

Access 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.



Date	Time	User	Action	Connection	Status
2004-10-26	09:58:50	admin	Connect	WEB from 192.168.46.172	
2004-10-26	06:32:22	admin	Connect	WEB from 192.168.46.172	
2004-10-25	04:52:23	admin	Connect	WEB from 65.48.246.87	
2004-10-25	04:27:10	admin	Connect	WEB from 192.168.46.238	

Table 3-7: Access Logs Form - Fieldnames

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 (e.g., SSH, Web); IP address used.

Event Logs

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

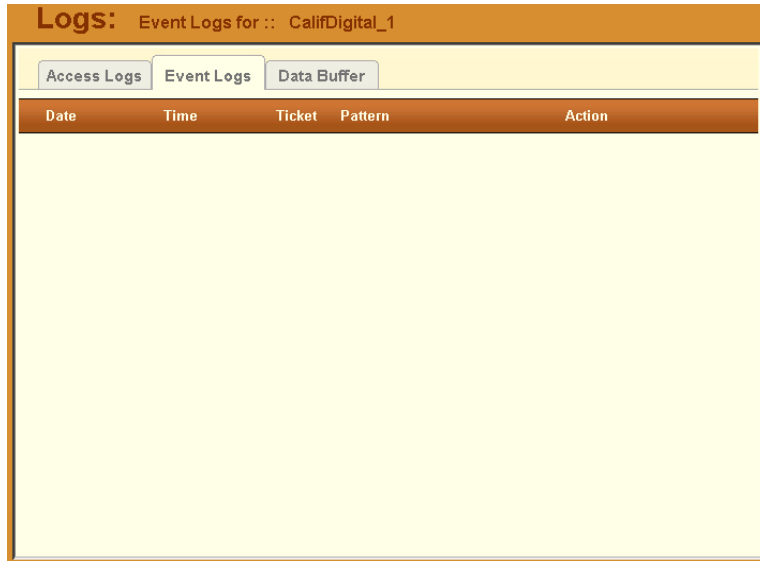
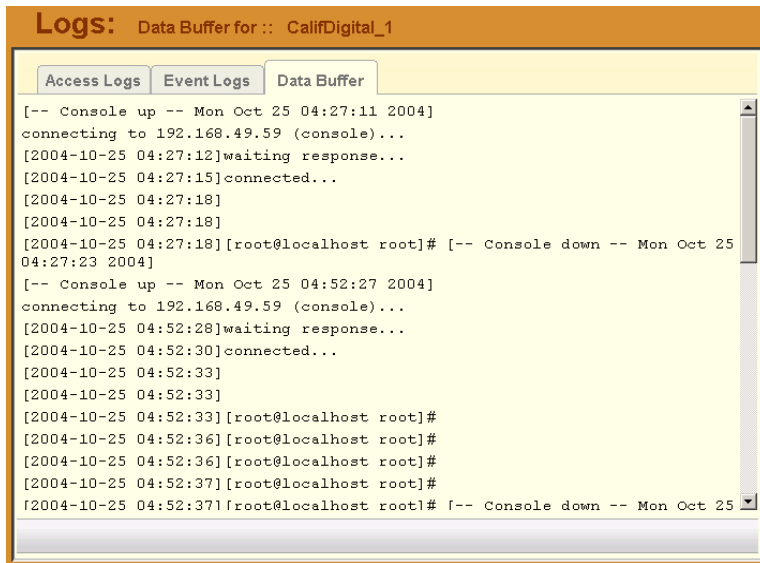


Table 3-8: Event Logs Form - Fieldnames

Field Name	Definition
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.

Data Buffer

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



Note: You can also access the Data Buffer log from the *Alarms* form.

User's Profile

The User's Profile form allows you to view your profile or contact information and modify a limited number of fields. The system allows you to view only your own profile.

Table 3-9: Users, Details Form - Fieldnames and Elements

Field Name	Definition
Details	Tab or button to display the User Detail form. This is also the primary form of User's Profile .
Access	Button to display the User Access form which shows all consoles assigned to the current user.
Groups	Button to display the User Group form which shows all groups to which the current user belongs.
User Name	The user name used to log into the E2000.

Table 3-9: Users, Details Form - Fieldnames and Elements

Field Name	Definition
Admin User	Check box to indicate that the user has Admin privileges, and also belongs to the Admin user group.
Security Profile (<i>For Admin use only</i>)	Check box to indicate that a security profile has been assigned to the user. Designed to prevent admin users from locking themselves out, the check box is available only to admin users. NOTE: In case the admin user is locked out when this check box is selected, the admin user can edit the script file <code>/var/apm/bin/apm_unlock_admin.sh</code> through CLI.
Local Password	Check box to indicate that local authentication applies to the user.
Full Name	User's full name.
Email	User's email. This is the same field name used by the system for event notification.
Department	User's department.
Location	Location of department.
Phone	User's phone number.
Mobile	User's mobile phone number.
Pager	User's pager number.
Status	Indicates whether the user is enabled or disabled .

>> **Changing Your Password**

To change your password, perform the following steps:

1. From the User's Profile detail form, click on **Set Password**.
2. From the password dialog box, enter the new password twice.

3. Click on **Submit**.

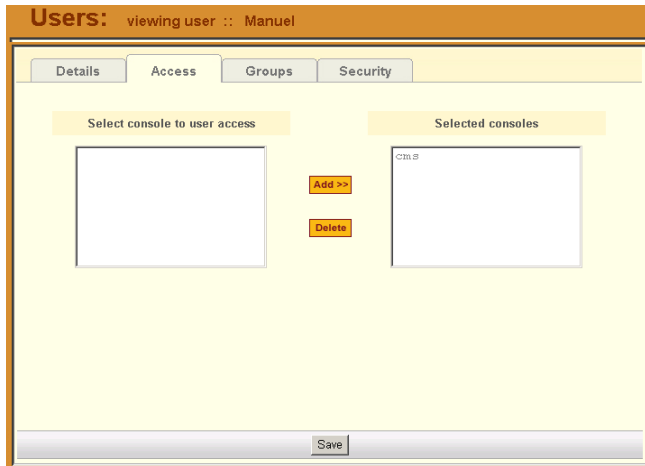
>> **Viewing the User Access Form**

The User Access form shows the consoles that the current user can access.

To view the User Access form:

1. From the User Detail form, click on **Access**.

The system displays the User Access form:



The screenshot shows a web application window titled "Users: viewing user :: Manuel". The window has a navigation bar with tabs for "Details", "Access", "Groups", and "Security". The "Access" tab is selected. The main content area is divided into two sections: "Select console to user access" on the left and "Selected consoles" on the right. The "Selected consoles" section contains a list with one entry, "cms". Between the two sections are two buttons: "Add >>" and "Delete". At the bottom of the window is a "Save" button.

>> **Viewing the User Groups Form**

The User Groups form displays the groups to which you belong.

To view the User Group form:

1. From the User Detail form, click on **Groups**.

The system displays the User Group form:

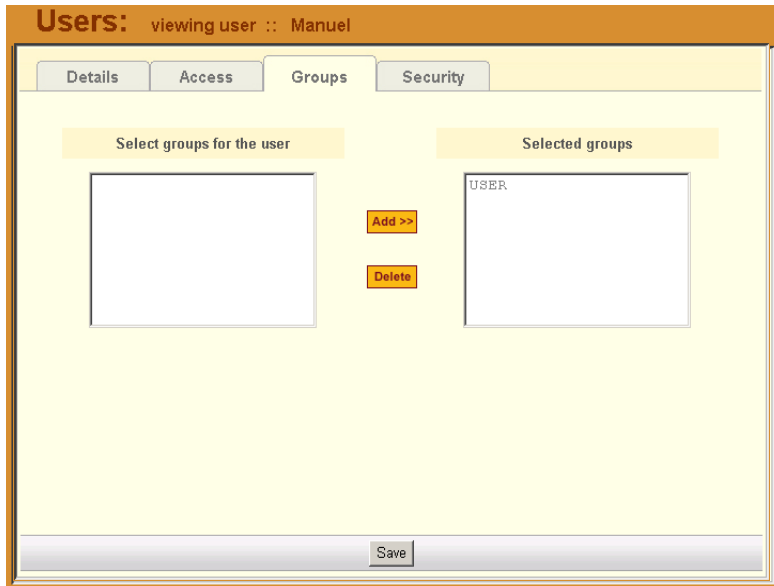


Table 3-10: User's Profile, Groups Form - Fieldnames and Elements

Field Name	Definition
Groups	Tab or button to select the current form.
Select groups for the user	List box from which to select a possible list of user groups assignable to the current user.
Add	Button to add a selected user group (left list box) to the Selected groups list box.
Delete	Button to delete a selected user group (right list box) and return it to the Select groups for the user list box.
Selected Groups	The list box that shows the group(s) assigned to the current user.

>> Viewing the Security Form

The Security form shows the current security profile assigned to you (as well as any other profiles to which you have access). A security profile defines a user's access control to a device as well as through which user group that profile is assigned.

For Blade Module users, the Security Profile includes access to blades and switches.

To view the Security form:

1. From the menu, select **User's Profile**; from the **Details** form, select the **Security** tab.

The system displays the **Security** tabbed form:

Table 3-11: User's Profile, Security Form - Fieldnames and Elements

Field Name	Definition
Security	Tab or button to select the current form.
Select security profile	List box from which to select a possible list of security profiles assigned to the current user.

Table 3-11: User's Profile, Security Form - Fieldnames and Elements

Field Name	Definition
Add	Button to add a selected security profile (left list box) to the Selected security profiles list box.
Delete	Button to delete a selected security profile (right list box) and return it to the Select security profile list box.
Selected security profiles	The list box that shows the Security Profile assigned to the current user.
Security profiles via user groups	The list box that shows the Security Profile assigned to a user group. This can be the default USER group or any other defined user groups.

Chapter 4

E2000 Web Administration

This chapter presents the procedures for configuring the AlterPath Manager E2000 through the web interface. Addressed to the E2000 administrator who must use the E2000 web interface in **Admin** Mode, 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
- Firmware Management
- Backing Up User Data
- Backup and Restore Scenarios
- System Recovery Procedures

- Info/Reporting
- Blade Module

Operational Modes

The E2000 provides two operating modes for configuration:

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

Before you can use the E2000 Web Management Interface (WMI) you must first run the First Time Configuration wizard.

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. Unless a regular user has been configured to be an admin user as well (through the User Detail form), regular users can use the application only in Access mode.

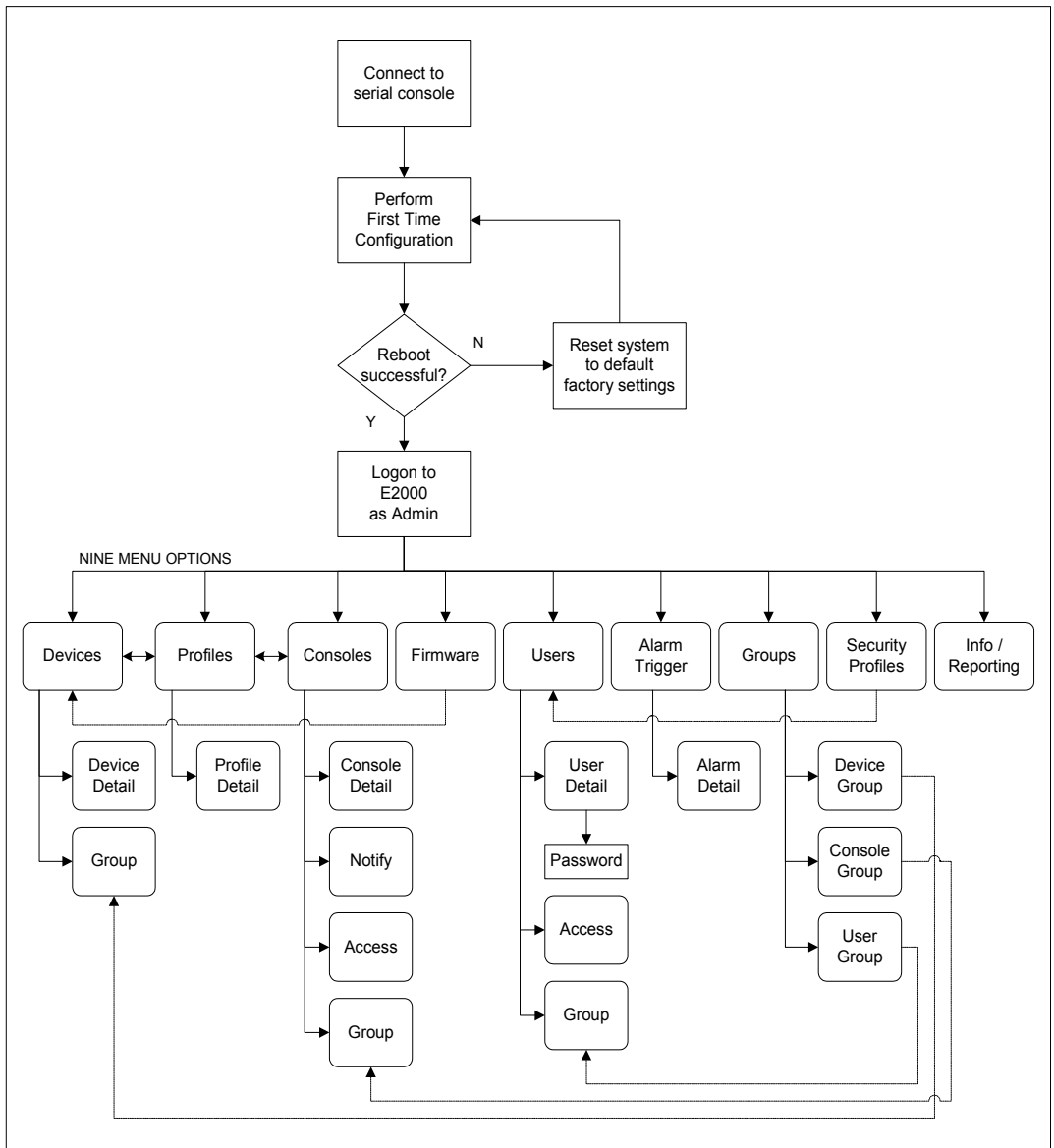
Only an administrator or admin user can use the WMI in Admin Mode which allows them to assign admin roles to new users; to add users, consoles, devices (console servers) alarms, and other configuration procedures.

Note: For information on how to use the system in Access mode, refer to the previous **Chapter 3: E2000 Web Access** .

Note: Certain configurational procedures (e.g., System Recovery, Modem Card Configuration) require the use of the CLI by advanced users. These procedures are discussed in **Chapter 5: Advanced Configuration**.

Configuration Process Flow

The entire configuration process through the WMI is as follows:



You must perform the First Time Configuration process (see Configuration Flow Diagram) using the command line interface. Once completed, you may 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 devices such as console servers or a KVM switch (menu options: **Devices** and **Profiles**), and then configure the consoles or ports associated with the devices (menu option: **Consoles**).

The **Firmware** option is used to update firmware and to enable you to select from different versions of firmware, or 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 (menu option: **Users**), and define the triggers that will create alarms and send email notifications (menu option: **Alarm Trigger**) to users.

First Time Configuration Wizard

Before you run 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: E2000 Installation** for procedures on how to prepare for First Time Configuration.

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.

First Time Configuration requires that you:

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

>> **Using the First Time Configuration Wizard**

To run the First Time Configuration Wizard, follow the steps below:

1. Connect the management console to the E2000 unit.
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)
 - Select Time Zone
 - Enter Date (format MM/DD/YYYY)
 - Enter Primary Ethernet IP Address (Static/None)
 - Enter Secondary Ethernet IP Address (Static/None)
 - Configure Ethernet Subinterfaces (Yes/No/List)
 - Configure Ethernet VLANs (Yes/No/List)
 - Enter Ethernet default gateway
 - Enter System's Hostname (30 characters max)
 - Enter System's Domain name (60 characters max)
 - Enter Primary nameserver's IP address
 - Enter the NTP Server
 - Enter email (SMTP) server
 - Enter Authentication Method (local/radius/tacacs+/ldap/kerberos/nis/active_directory)

Note: Depending on the Authentication Method that you select, the system will prompt you for additional information. See "Setting the Authentication Method" on page 4-8 for more information.

>> **Resetting Configuration to Factory Settings**

If you make a mistake during the First Time Configuration (or if you need to change 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 restart your computer.

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.*

First Time Configuration Wizard

Note: Default values are enclosed in angled brackets after each question or prompt. Press <Enter> to accept the default value.

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

Please choose the time zone where this machine is located.

Current system date and time is:

Tue Apr 5 17:11:18 PDT 2005

Press ENTER to accept it or specify new ones.

Enter date in MM/DD/YYYY format: 48

Enter date in MM/DD/YYYY format:

Tue Apr 5 17:11:00 PDT 2005

Primary Ethernet IP address: (S)tatic or (N)one ? [S]:

Secondary Ethernet IP address: (S)tatic or (N)one ? [S]:

Configure Ethernet Subinterfaces: (Y)es, (N)o or (L)ist ? [N]: n

Configure Ethernet VLANs: (Y)es, (N)o or (L)ist ? [N]: n

Enter Ethernet Default Gateway [none]:

Enter the System's Hostname

(max 30 characters) [E2000]:

Enter the System's Domain Name

(max 60 chars) [localdomain]:

Enter the Primary Nameserver's IP address [none]:

Enter the NTP server:

Enter the email (SMTP) server:

Choose the desirable authentication method

(local/radius/tacacs+/ldap/kerberos/nis/active_directory) [local]:

Cyclades-APM V_1.3.0 (Apr/03/2005) - Console (kernel 2.4.25)

APM login:

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

Setting the Authentication Method

The sample First Time Configuration selects *local* as the Authentication Method to use to authenticate a user.

Depending on the type of authentication service that you select, the wizard will prompt 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, the shared secret, and the available service (system).

If you select NIS, the system will prompt you for the NIS Domain Name and the NIS Server. For the NIS Domain Name, the system will accept **localdomain** or you may leave the field blank.

Note: If you use NIS Authentication and the NIS server fails, APM will not allow you to add the user in the local database since it already exists in the NIS server. This is due to the way NIS centralizes and distributes user account information into common local files. For more detailed information, refer to the “NIS Configuration” on page 5-21 of **Chapter 5: Advanced Configuration**.

Configuring Active Directory

To use Active Directory as your authentication method, select **ldap** and then proceed to the “Active Directory Configuration” on page 5-25 of **Chapter 5: Advanced Configuration**.

Limitation of Tacacs Plus in ACS Console Access

Beware that access to an ACS console through the AlterPath Manager is currently not possible if the ACS serial port is configured to use Tacacs Plus authentication.

Hostname Configuration Must Follow RFC Standard

When configuring the hostname, the name must comply with RFC 608 which states that the hostname is a string composed of:

- Up to 48 characters drawn from the alphabet (A-Z)
- Digits (0-9), and the minus sign (-)
- No blank or space characters allowed
- No distinction between upper and lower case letters
- First character is a letter
- Last character is NOT a minus sign

Any deviation from this standard may cause the web browser to disable APM cookies and prevent the user from logging into the E2000 web application.

Multiport Ethernet Card Configuration

The E2000 supports up to two multiport Ethernet cards to allow connection to network segments. The E2000 supports the Multiport 10/100Mbps NIC - ADLINK PCI 8213 or the AEI-P430TX cards. The First Time Configuration Wizard will detect any multiport Ethernet card that is installed in the E2000 and will prompt you for network information. If you are using this feature, be ready to provide the network IP addresses.

Note: To configure the Ethernet ports (such as changing the speed/duplex settings), go to Configuring the Ethernet Ports, Chapter 5: Advanced Configuration.

>> *Connecting to the E2000 Web Interface*

Once the First Time Configuration is complete, you may connect to the web interface to begin web configuration.

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.

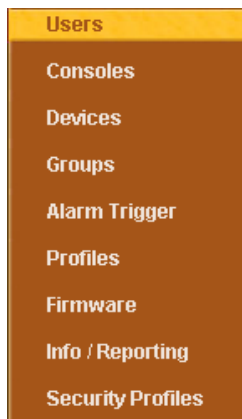
Disabling HTTP to Use Only HTTPS

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.

Note: See “Disabling HTTP to Use Only HTTPS” on page 5-26 of **Chapter 5: Advanced Configuration** for the procedure on how to configure the encrypted version.

E2000 Web Interface: Admin Mode

Once you have completed the First Time Configuration procedure, you may login to the E2000 web interface and use the system in Admin Mode. The Admin menu panel contains the following selections:



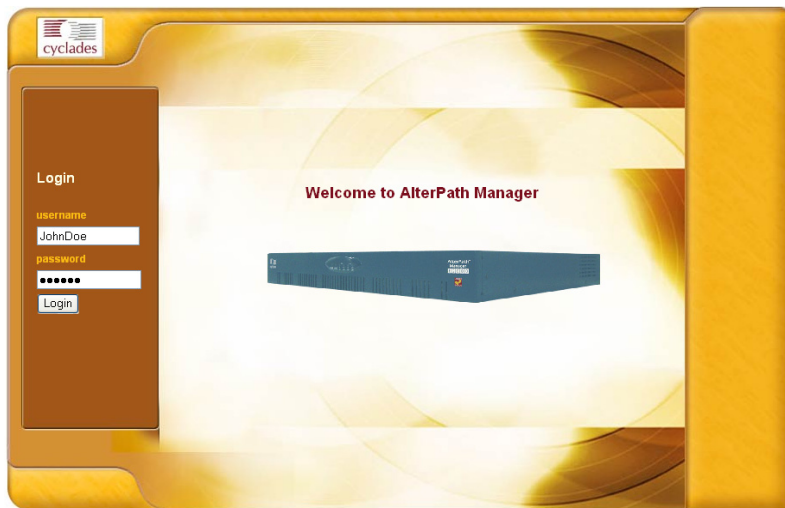
Configuring the E2000 requires using the menu in a certain order. To facilitate the configuration process, the menu choices are discussed in the following order:

- Devices
- Alarm Triggers
- Profiles

- Firmware
- Consoles
- Users
- Groups
- Info/Reporting
- Security Profiles

>> **Logging Into the E2000 Web Interface**

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



2. Select the **Login** button.

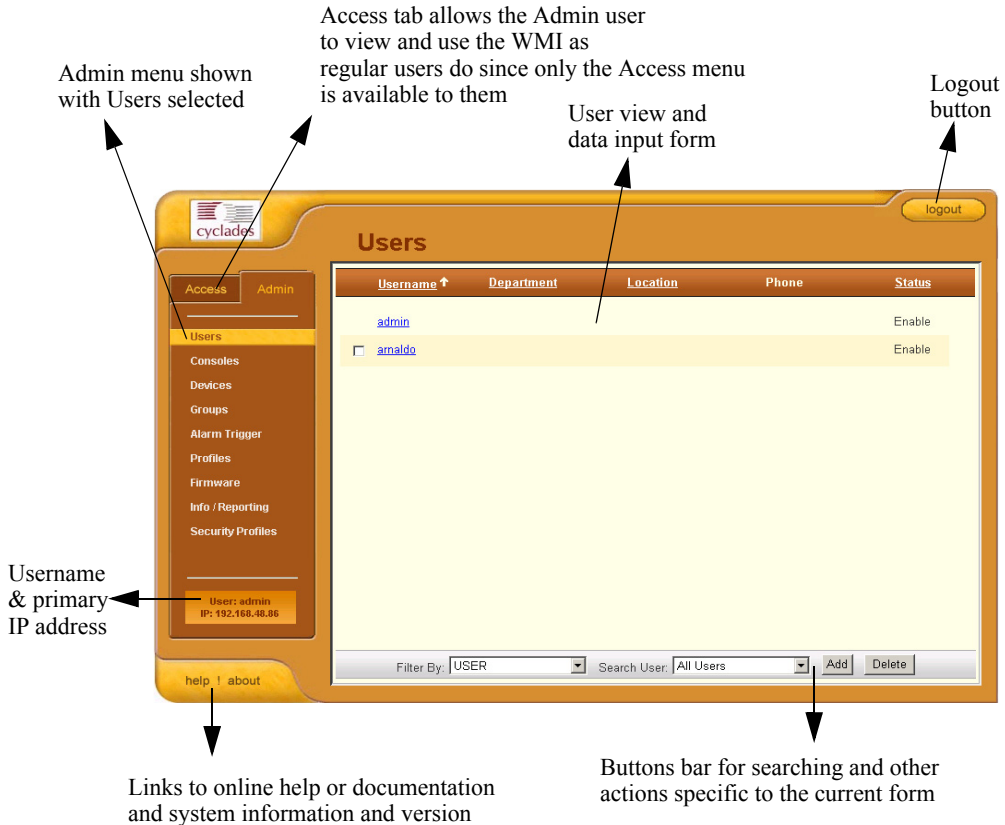
Upon successful login, the User List form appears.

Note: *When the 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, retrieving them should be fast.*

Note: *All procedures in this chapter assumes that you are already logged in.*

Parts of the Web Management Interface

Before proceeding to the web configuration process, familiarize yourself with the graphical user interface. Shown below are the basic features of the E2000 Web Management Interface in Admin Mode. The form example shows the Users List form, the first form to appear in the web interface.



The first form to appear when you select an option from the menu panel is called the primary form. The Users List form, for example, is the primary form of the menu option, **Users** (User Management).

In this manual, all primary forms are shown in their entirety (*i.e.*, the entire screen which includes the menu panel and form). Non-primary forms are shown only as individual forms (*i.e.*, without the menu panel and other GUI elements outside the form).

Sorting, Filtering, and Saving a List Form

An underscored column heading on any of the list forms indicates that the list may be sorted based on that column heading. For example, you can sort the previously shown User List form by Username, Department, Location or Status by clicking on the heading.

Where there are several underscored headings on a list, an arrow appears adjacent to the heading on which the sort is based. The position of the arrowhead indicates the sort order. A downward arrowhead indicates that the list is alpha-numerically arranged in ascending order; an upward arrowhead, in descending order. You can change the sort order by clicking on the heading or the arrow.

Example:

<u>Console</u> ↑	<u>Type</u>	<u>Config</u>	<u>Device</u>	<u>Port</u>	<u>Location</u>	<u>Status</u>
<input type="checkbox"/> ACS_02	Serial	edit	ACS	2	OnDemand	OnDemand
<input type="checkbox"/> ACS_03	Serial	edit	ACS	3	OnDemand	OnDemand
<input type="checkbox"/> ACS_04	Serial	edit	ACS	4	OnDemand	OnDemand
<input type="checkbox"/> ACS_05	Serial	edit	ACS	5	OnDemand	OnDemand
<input type="checkbox"/> ACS_06	Serial	edit	ACS	6	OnDemand	OnDemand
<input type="checkbox"/> ACS_07	Serial	edit	ACS	7	OnDemand	OnDemand
<input type="checkbox"/> ACS_08	Serial	edit	ACS	8	OnDemand	OnDemand
<input type="checkbox"/> ACS_09	Serial	edit	ACS	9	OnDemand	OnDemand
<input type="checkbox"/> ACS_10	Serial	edit	ACS	10	OnDemand	OnDemand
<input type="checkbox"/> ACS_11	Serial	edit	ACS	11	OnDemand	OnDemand
<input type="checkbox"/> ACS_12	Serial	edit	ACS	12	OnDemand	OnDemand

Filter By: CONSOLE Search For:

The Console List form shown above is sorted by Console in ascending order. You can further sort this form by Type, Device, Location, and Status.

To filter your list by group, use the **Filter by** button. The list generated by selecting the **Filter by** button is automatically saved.

To search for a particular console, use the **Search** button.

Using the Form Input Fields

When typing in data into any of the input fields, note the following conventions:

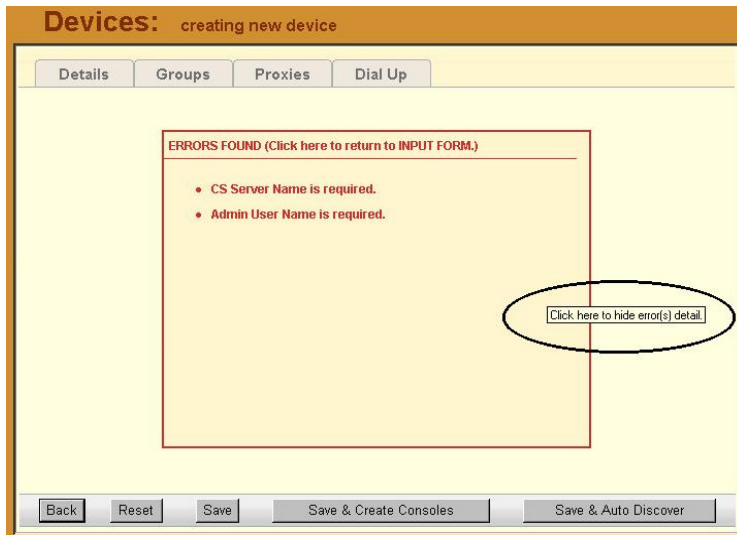
- In the web form (as it appears on the screen), all required fields are shown in RED.
- With some exceptions, fields cannot contain special or reserved characters. If you enter an invalid character, the system generates the message: “Fields cannot contain special characters.”
- Only the following special characters are allowed:

`_!@%&()[]{}<>?=-*/,.;:^~`

Verifying Error Messages

To verify an error message, you can view the form or screen in question by clicking on the error message. This feature allows you to verify or check the error message against the form.

Example:



Clicking the error message, generates the form in error:

Devices

Note: For Device forms associated with the Blade Module, see the **Blade Module** section of this chapter.

The **Devices** option allows you to perform device management operations as summarized by the table below:

Table 4-1: Summary of Devices Forms

Form Function	Form(s) Used
Add and configure new devices (<i>i.e.</i> , ACS, TS, KVM/net or IPMI).	Device list form (Add button) > Select Device Type form > Device detail form.
Edit devices.	Device list form (Edit link) > Device detail form.
Delete devices.	Device list form (Delete button).
Upload device firmware, bootcode or configuration.	Device list form (Upload button).

Table 4-1: Summary of Devices Forms

Form Function	Form(s) Used
Configure device health monitor.	Device detail form (Health Monitor input field).
Configure Dial Up and enable PPP connection for out-of-band access to remote device (ACS)	Dial Up form
Run the Device Discovery Wizard.	Device detail form (Save / Auto Discover button).
Run the Console Wizard.	Device Discovery form (Save / Create Console button).
Configure KVM Viewer.	KVM Viewer form (Device detail form > KVM Viewer form).
Search, sort, and save list of devices.	Devices List form.
Assign type of web proxy to access a target device through the web.	Proxies form.
Configure modem user, password and related parameters to enable dial up / dial out functions.	Dial Up

Note: 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 the form function. For example: Device List form.

Supporting forms that you may need to access and manage your devices are:

- Console list form
- Console detail form

- Firmware form
- Profiles form

Because target consoles are part of your devices, it is often necessary to work with device and console management forms together. Also, you may need to refer to the **Firmware** form for any information you might need pertaining to a device 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 detail form.

Device List Form

The Device List form, the primary form of **Devices**, allows you to view a list of devices that are configured in the E2000. From this form, you can add, modify, or delete devices. .



Table 4-2: Device List Form - Fieldnames and Elements

Fieldname / Element	Definition
[checkbox adjacent to each device name]	Checkbox to select the device to add or upload firmware (refer to the buttons below the form to enable these commands).
Device	Device name. Click on the device name to connect to the console server or device. Click on the column title (Device) to change the sort order.
Type	The type of device (i.e, TS, ACS, KVM/net or IPMI).
Config	The device configuration. Click on Edit to display the Device Detail form for selected device record or line.
Upload	This column indicates if the device requires a firmware or configuration upload. If required, then select the checkbox adjacent to the device name and click on the Upload button. NOTE: The E2000 supports firmware and configuration upgrades for the following products: - ACS and TS: Firmware and Configuration - KVM: Configuration only
Firmware	The firmware version for this device.
Log	Device log buffer. Click on Log to view the log for this device.
Status	Status of the device: Enabled, Disabled or OnDemand. OnDemand means that the device is enabled only upon user connection.

Table 4-2: Device List Form - Fieldnames and Elements

Fieldname / Element	Definition
Filter by	From the dropdown box, select the field by which to filter the list and then click on the Filter by button.
Search	From the dropdown box, select the device you wish to search, and then click on Search .
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.

Supported Devices

The E2000 supports the following types of devices:

- ACS
- TS
- KVM/net
- IPMI (Optional)
- Chassis (Optional. See Blade Module section.)

Important: For TS Users: If you are using older versions of TS100/400/800 which may have less than 32 MB of RAM, you **MUST** increase the RAM in the TS equipment.

Note: For Device forms associated with the Blade Module, see the **Blade Module** section of this chapter.

Note: IPMI Activation. *IPMI is a paid-for option for E2000 users. The feature is hidden from users who do not need it. To activate IPMI:*

- a. *Execute the script: `/var/apm/bin/apm_enable_ipmi.sh`*
- b. *Enter the password provided to you by Cyclades when you registered for the IPMI feature.*

>> **Adding a Device**

To add any of these devices, follow the steps below:

1. From the menu panel select **Devices**
The system displays the Device List form.
2. From the Device List form, click on **Add** located at the bottom of the form.

The system displays the Select Device Type form:



The screenshot shows a web form titled "Devices: creating new device". The main content area is titled "Select device type" and contains a dropdown menu with "ACS" selected. At the bottom of the form is a "Submit" button.

3. From the Select Device Type form, select from the type of device (TS, ACS, KVMnet, or IPMI) you wish to add, and then click on **Submit**.

The system displays the Device detail form based on the selected device type. The example below shows the Device Detail form for the device type, ACS:

- Complete the Detail form, as necessary, using the table below as a guide.

Note: In all the forms, the required fields are printed in red; in all tables, the required fields (under the Fieldname column) are printed in **boldface**.

Table 4-3: Devices, Detail Form - Fieldnames and Elements

Fieldname	Definition
Details	Currently selected tab.
Groups	Click this tab to assign or re-assign user to a user group.
Proxies	Click this tab to assign a web proxy type to access the web interface of the current device.
Device Name	The symbolic name linked to the console server device.
Type	Type of device (e.g., ACS, KVM, etc.)

Table 4-3: Devices, Detail Form - Fieldnames and Elements

Fieldname	Definition
Model	Dropdown list box to select the model of the current device.
Location	Physical location of the device.
Admin Name	The admin username (superuser) of the device.
Admin Password	Button to invoke a dialog box used to define the Admin'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 Mode	Dropdown list box. 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 <i>Configuring Your DHCP Server</i> , this chapter.
MAC Address	The MAC address if the selected IP mode is int_dhcp .
IP Address	The IP address of the device 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.
Connection	Dropdown list box to select the connection protocol used between the E2000 and the console serial port: ssh or telnet .
Domain	Domain Name

Table 4-3: Devices, Detail Form - Fieldnames and Elements

Fieldname	Definition
Base Port	TCP port number allocated in the first serial port of the console server.
Status	Dropdown list box 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.
Health Monitor	The frequency in which the Health Monitor operates to monitor the system (Never, Daily, Weekly or Monthly).
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>
Firmware/Boot	Dropdown list to select any firmware or bootcode to upload.
Back	Button to return to the previous page.
Reset	Button to reset the form.
Save	Button to save all Device configuration entered in this form.
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.

5. Click on the **Save** button when done.

6. Select **Devices** from the main menu panel to return to the Device List form and verify your entry.

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

The Device detail form for TS is similar to that of the ACS. The **Model** dropdown box provides you with a list of TS models to select from.

Proxies

The E2000 includes a web proxy server so that connections to the native web interface of any supported device go through the E2000. This feature enables the E2000 to:

- Connect users through the E2000 to remote servers that it controls (*e.g.*, IBM Blade, KVM/net switches, ACS/TS units, and other servers) in connection with any web interface.
- Provide a secure mechanism for E2000 clients to access remote servers.
- Configure remote AlterPath devices directly from the E2000.

Proxy Types

There are three types of proxy you can configure for a device:

Table 4-4: Types of Web Proxy

Proxy Type	Function
Reverse Proxy	Reverse proxy allows any web server to be viewed through the proxy agent. The web server appears to the user as a subdirectory of the proxy server's document tree. Advantages: Target server does not need to have a routable IP address; not accessible outside the E2000; user workstation and network does not need to know about the target web server.

Table 4-4: Types of Web Proxy

Proxy Type	Function
Forward Proxy with ARP	<p>A forward proxy acts as a gateway for a client's browser, sending HTTP requests on the client's behalf to the Internet. The proxy protects your inside network by hiding the client's actual IP address and using its own instead. When the outside HTTP server receives the request, it sees the request or address as originating from the proxy server, not from the actual client.</p> <p>Proxy ARP is the technique in which one host answers ARP requests intended for another machine. By assuming its identity, the router accepts responsibility for routing packets to the intended destination. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway.</p>
Forward Proxy without ARP	As indicated.

Warning: *When you assign **Forward Proxy Using ARP** or **Forward Proxy without ARP**, all ports of the proxied device are reachable from the workstation from which the user is logged in. It is important that all console ports are configured with an authentication type other than **None**.*

The constraints that are set for all proxies rely on IP addresses only. Any user from a workstation where there is another user logged into the E2000 will have access (as long as the device does not require authentication) to all devices that are being proxied for that user.

Warning: Reverse Proxy does NOT work with Java applets and Active X applications. Consequently, the E2000 web interface cannot support the following connections:

- Serial console connection to the ACS/TS.
- Remote access to the IBM Blade devices.

- Use the KVM viewer to access KVM/net console.

>> **Configuring the Web Proxy**

To create or configure a proxy for a device, follow the steps below:

1. Open the Device List form
2. If the device is new, click on the **Add** button.
(If the Device already exists, highlight the device and click on the **Edit** button.)
3. From the Device Edit form, select the **Proxies** tab.

The system displays the **Proxies** tabbed form.



The screenshot shows a web browser window titled "Devices: creating new device". The interface has a yellow background and a brown header. At the top, there are four tabs: "Details", "Groups", "Proxies", and "Dial Up". The "Proxies" tab is currently selected. Below the tabs, there is a label "Proxy type:" followed by a dropdown menu showing "Reverse Web Proxy". At the bottom of the form, there are five buttons: "Back", "Reset", "Save", "Save & Create Consoles", and "Save & Auto Discover".

4. From the **Proxies** tabbed form select the type of web proxy you wish to assign for the current device.

Note: If you select Forward Proxy, then you must set your PC's default gateway and the device's default gateway to the IP addresses of the E2000 if your PC and the device are in different networks.

5. Click on **Save** to complete the procedure.

>> **Verifying your Proxy Setting**

1. To verify your configuration, return to the Devices List form, and under the Web Proxy column, select **YES**.

A pop up window will display to show the web pages of the selected device.

Disabling the Proxy

Setting the Type of Proxy to none will display none under the Web column of the Device List form. Any admin user currently viewing the proxy will receive a message indicating that they are not authorized to access the proxy.

Direct Access

To enable the E2000 to forward any http(s) data from any client workstation to the target web server (such as the IBM BladeCenter Management Module), select the checkbox for **Allow Direct Access**.

Warning: *Allowing direct access provides no protection to the device or the web user interface.*

Configuring Ports to be Proxied

When Forward Proxy (with or without ARP) is enabled for a device, the default proxied ports are 80 and 443. To change the opened ports, see “Changing the Ports to be Proxied” on page 5-19, **Chapter 5: Advanced Configuration**.

Dial Up and Dial Back

The **Dial Up** form allows you to configure the current device for dial-up connection to the network.

The same form is also used to configure the device for **dial back**. Currently, the Dial Back feature only applies to ACS devices. When an ACS unit is configured for dial back, the E2000 can dial out to the remote ACS unit and authenticate with the ACS. Once authenticated, the ACS drops the line and dials out to a pre-defined number. Simultaneously, the E2000 sets its modems into a state where it is ready to receive a call. The system allows all remote sites to call back to the same number and support multiple, simultaneous call back connections to the E2000.

When the E2000 receives the dial back call, the authentication is repeated. Upon successful authentication, the system establishes a PPP session and opens the console connection.

Call back connections are included in the log messages.

Note: For dial back to work, you must configure it from the web interface and the CLI.

>> **Configuring Dial Up / Dial Back**

To configure Dial Up or Dial Back, follow the steps below:

1. Go to Devices > Dial Up.

The system displays the **Dial Up** tabbed form:

The screenshot shows a web interface titled "Devices: creating new device" with a "Dial Up" tab selected. The form contains the following fields and controls:

- Modem Mode:** A dropdown menu set to "Disable".
- PPP Device IP:** A text input field.
- PPP Auth Method:** A dropdown menu set to "PAP".
- PPP User:** A text input field.
- PPP Phone:** A text input field.
- PPP Local IP:** A text input field.
- Dialback Mode:** A dropdown menu set to "Disable".
- PPP Password:** A text input field with a "Set Password" button next to it.

At the bottom of the form, there are five buttons: "Back", "Reset", "Save", "Save & Create Consoles", and "Save & Auto Discover".

2. Complete the form using the table below as a guide:

Table 4-5: Dial Up Form - Fieldnames and Elements

Field Name	Definition
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.
PPP Phone	<i>If Modem Mode is enabled (either as Primary or Network Backup), then this field is required for PPP connection.</i> Enter the complete PPP phone to establish PPP connection to a device or console via web interface, CLI, or SSH.
PPP Device IP	If this is blank, the device IP is used for PPP modem connection.
PPP Local IP	If this field is blank, the E2000 IP is used for PPP.
PPP Auth Method	Select the authentication method: PAP or CHAP
Dialback Mode	Select whether to enable or disable dialback mode.
PPP User	The username of the modem or dialback user.
PPP Password	The password to be used to authenticate the dial back user.

3. Click on **Save** to save.

4. If you are configuring for dial back, ensure that you have fulfilled the other requirements outlined in the next section.

Other Requirements for Dial Out / Dial Back

To enable device or console access through dial out or dial back, you must configure the following:

From the E2000:

1. Go to the web interface: **Consoles** Detail Form:
 - Status: Be sure to select **OnDemand** for this field.
2. From the **Dial Up** form, provide the following parameter values:
 - PPP User - The user that you have configured in the APM as the admin user for the ACS.
 - PPP Password
 - PPP Auth Method - Select PAP or CHAP.

Note: If the PPP User is not configured in the APM, then the main user is used for dial out and dial back.

From the ACS:

3. Using CLI, create a new user and password from the ACS using the commands:
 - **adduser** <ppp_user>
 - **passwd** <ppp_user>

Note: See Chapter 5: Advanced Configuration, “Modem Dial Back for ACS” on page 5-17.

Other Requirements for Dial Back (ACS Only)

Currently, the dial back feature works for ACS only. To set an ACS device for dial back, you must also configure the following:

From the E2000:

1. Using CLI, edit the file `/var/apm/apm.properties` and add the E2000 dial number in the following parameter: **dial.apm_phone_number**=<phone number>

KVM/net Device Detail Form

The example below shows the Device Detail form that is used to configure the device type, KVM/net:

The input fields and buttons of the KVM/net Device Detail form are similar to that of the ACS or TS with the exception of the following:

GUI Element	Definition
KVM Viewer	Button to display the configuration form for the KVM Viewer. The resulting form is used to configure the Idle Timeout and the various escape sequences for operating the KVM Viewer.
Save / List Cascade	Button used to display the list of cascaded KVM devices and/or to configure cascaded KVM devices.

>> **Configuring KVM Ports**

The procedure for configuring the KVM ports is the same as that of serial console ports.

1. Go to **Consoles**: Console List.
2. From the Console List form, select **Add**.
3. From the Add Console form, select KVM

See the **Consoles** section of this chapter for more detailed information.

Assigning KVM Device Groups

Use the **Groups** tabbed form to assign a KVM device to groups. This form functions the same way as you would group users and consoles.

See also: “KVM/net Device Configuration” on page 4-50, this chapter.

IPMI Device Detail Form

Note: IPMI Activation. *IPMI is a paid-for option for E2000 users. The feature is hidden from users who do not need it. To activate IPMI:*

- a. *Execute the script: `/var/apm/bin/apm_enable_ipmi.sh`*
- b. Enter the password provided by Cyclades.

The example below shows the Device Detail form for the device type, IPMI. The device configuration for IPMI is actually the configuration for the IPMI Baseboard Management Controller (BMC) that is embedded in the system.

The input fields and buttons for this form are also similar to the other Device Detail forms with the exception of the following:

Table 4-6: Devices, Details Form (IPMI) - Fieldnames and Elements

Fieldname / Element	Definition
Authentication Information	Dropdown box to select the authentication type.
Encryption Required	Dropdown box to select the encryption type.
Group Membership	The groupname to which the device belongs.
Power Control Enabled	(Y/N) to enable/disable power control.
Power On	Button to switch on the IPMI server.
Power Off	Button to switch off the IPMI server.

Table 4-6: Devices, Details Form (IPMI) - Fieldnames and Elements

Fieldname / Element	Definition
Display Sensors/Log	Button to display a new form that contains two tabs for viewing sensors or logs from the BMC, respectively.

When you configure an IPMI device, the E2000 will allow you to create one console which uses the device name as a root and adds “_01”. There are two ways you can create this console:

- From the current IPMI Device Detail form.
- From the Console Detail form.

>> **Using the IPMI Device Detail Form to Add a Console**

1. Open the IPMI Device Detail form (**Devices**: Device List > Device Detail).
2. From the IPMI Device Detail form, click on the **Save/Create Console** button.

The system launches the Console Wizard.

3. Follow the system instructions and enter all relevant information, as needed.

Note: You may change the default console name which is the same as the device name.

4. Once you have saved the Console configuration, the system returns you to the Device Detail form.

Using the IPMI Console Detail Form to Add a Console

*See same heading in the **Consoles** section of this chapter.*

>> **Viewing Sensors or Logs from the BMC**

To view the sensors and logs from the BMC:

1. From the IPMI Device Detail form, click on the **Display Sensors/Logs** button.

The system displays a form containing two tabs:

- **Sensors** tabbed form (default) - displays the current values of all sensors. This form refreshes every 15 seconds.
- **Logs** tabbed form - displays all logs read from the BMC. You may clear the log database by clicking on the **Clear** button, but be careful because this command will erase all logs from the BMC database and it cannot be undone.

Configuring Your DHCP Server

A DHCP server is build into the E2000. You can use 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.

IP Mode	When to use this mode
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.

Function of the Status Field

The **Status** field of the Device Detail form indicates whether the connection between the E2000 and the device/console is **Abled** (*i.e.*, permanently connected), **Disabled** (no connection established), or **OnDemand**.

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

Difference between 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, every time you make a change to a Device or Console parameter, or the Device Default Gateway, the change is automatically uploaded to the console server after you select **Save** from the form.

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 Detail 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:

Connection Mode	Definition
Disabled	This is the default mode.
Primary Network	Select this to establish 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	Select this to use Ethernet to connect to a device. In the event that the device becomes unreachable via Ethernet, the E2000 establishes a PPP connection 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

Do not change the Device IP or the Device Name (including deleting or disabling it) while running PPP as this 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 steps below:

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

Modem Mode provides three choices:

Option	Use this option if you want to use PPP . . .
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. From the Status field of the Devices Detail form, select **On Demand**.
3. Complete the PPP settings as follows:

PPP Setting	Definition
PPP Device IP	<i>Optional.</i> IP address for the current device.
PPP Local IP	<i>Optional.</i> Local IP address for using PPP.
PPP Phone	<i>Required.</i> The complete PPP phone number.
PPP Auth Method	Select the authentication method: PAP or CHAP
PPP User	Username of the modem user.
PPP Password	Password of the modem user.

4. Click on **Save** 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. There are three commonly used command line procedures for managing modems.

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

If you need to use any of these procedures, please refer to *Chapter 5: Advanced Configuration*.

>> Configuring the Health Monitoring System

The Device Health Monitoring feature enables the E2000 to monitor, on a periodic basis, the consoles that run on specified devices, 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 User Detail form (Go to: **Users**: User List form > User Detail form).

1. From the Device Detail form, select the frequency of monitoring from the **Health Monitor** dropdown list box. Your choices are:

<i>Selection</i>	<i>Definition</i>
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, you must complete an Alarm Trigger Detail form.

See the **Triggers** section of this chapter.

Console Wizard

The **Save/Create Consoles** button is used to run the Console Wizard which allows you to configure those consoles connected to a device by following the wizard's prompts, options, and default values. The wizard automatically configures the 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 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:

Table 4-7: Summary of Console Wizard Forms

Wizard Form	Function
Warning	This page warns you about any data to be overwritten and the choices you have before proceeding with the wizard.
Defaults	Sets the profile, connection protocol, and authentication type.
Access	Select the users who can access the consoles.
Notify	Selects the users to who will be notified in the case of an event.
Groups	Select the groups to which the console(s) belong.
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.

Table 4-7: Summary of Console Wizard Forms

Wizard Form	Function
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.

>> *Running the Console Wizard*

To Run the Console Wizard follow the steps below:

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.

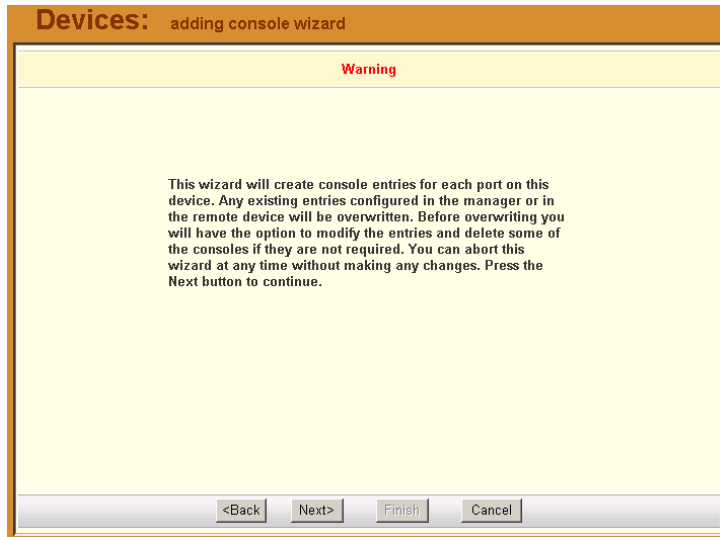
The system displays the Device Definition form:

2. From the Device Definition form, complete the following required fields for using the Console Wizard:
 - Device Name

- Admin Name
- IP address (for IP mode: **int_dhcp** or **static**)
- Netmask (for IP mode: **static**)
- Base Port
- MAC address (for IP Mode: **int_dhcp** or **ext_dhcp**)

3. Select the **Save / Create Consoles** button to invoke the Console Wizard.

The Console Wizard begins with a warning message to notify you of any data to be overwritten and the choices you have before going ahead with the wizard.

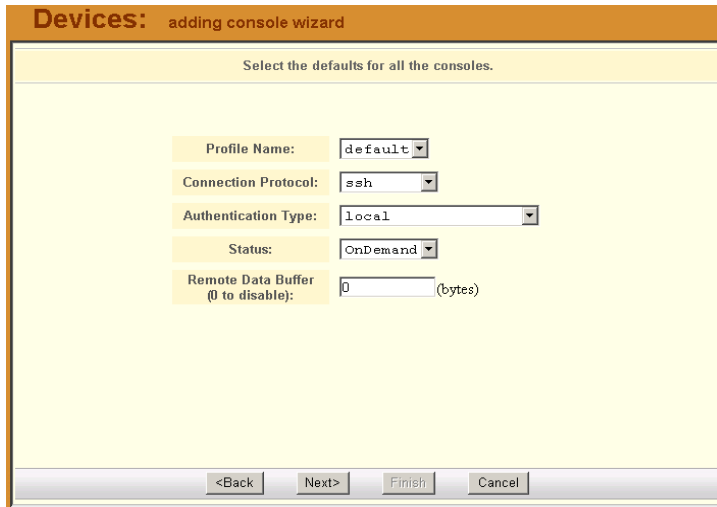


Note: Use the **Back**, **Next**, and **Cancel** buttons to navigate through the forms. Pressing the **Next** button saves your current form settings.

4. Select the **Next** button.

4: E2000 Web Administration

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

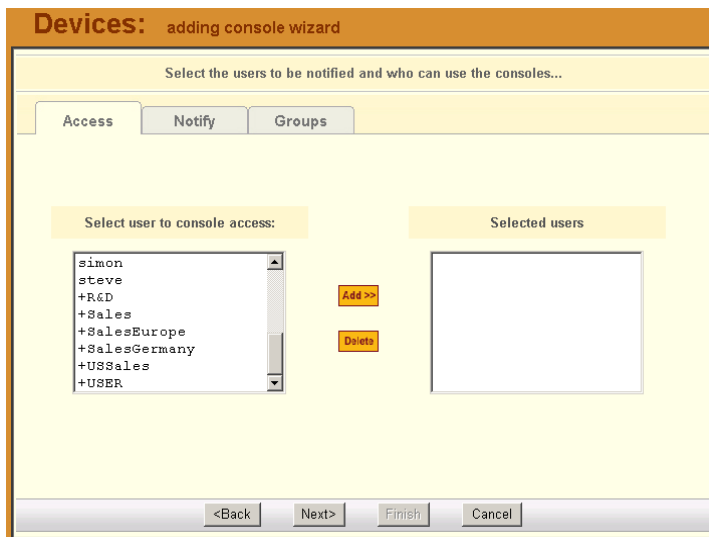


The screenshot shows a web-based configuration window titled "Devices: adding console wizard". The main heading is "Select the defaults for all the consoles." Below this, there are several configuration fields:

- Profile Name: default (dropdown menu)
- Connection Protocol: ssh (dropdown menu)
- Authentication Type: local (dropdown menu)
- Status: OnDemand (dropdown menu)
- Remote Data Buffer (0 to disable): 0 (text input field)

At the bottom of the form, there are four buttons: "<Back", "Next>", "Finish", and "Cancel".

5. Complete the above fields, and then select the **Next** button when done. The system brings up the User Access form:



The screenshot shows a web-based configuration window titled "Devices: adding console wizard". The main heading is "Select the users to be notified and who can use the consoles...". There are three tabs: "Access", "Notify", and "Groups". The "Access" tab is selected.

Below the tabs, there are two main sections:

- Select user to console access:** A list box containing the following items: simon, steve, +R&D, +Sales, +SalesEurope, +SalesGermany, +USSales, and +USER.
- Selected users:** An empty list box.

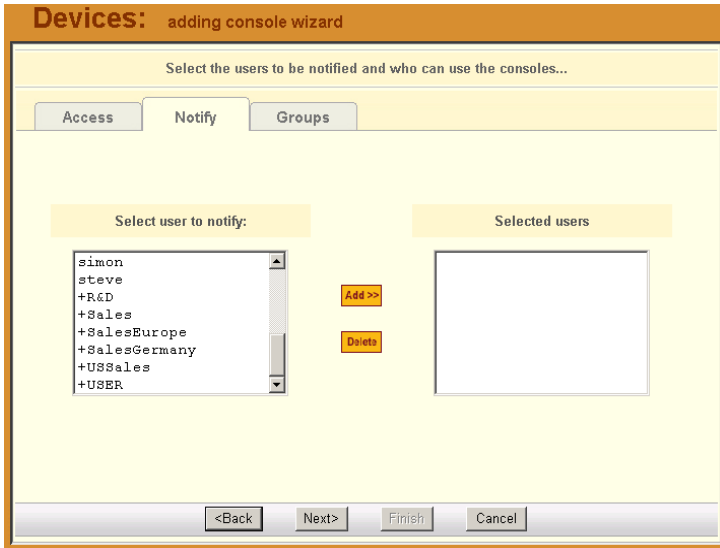
Between the two list boxes are two buttons: "Add >>" and "Delete".

At the bottom of the form, there are four buttons: "<Back", "Next>", "Finish", and "Cancel".

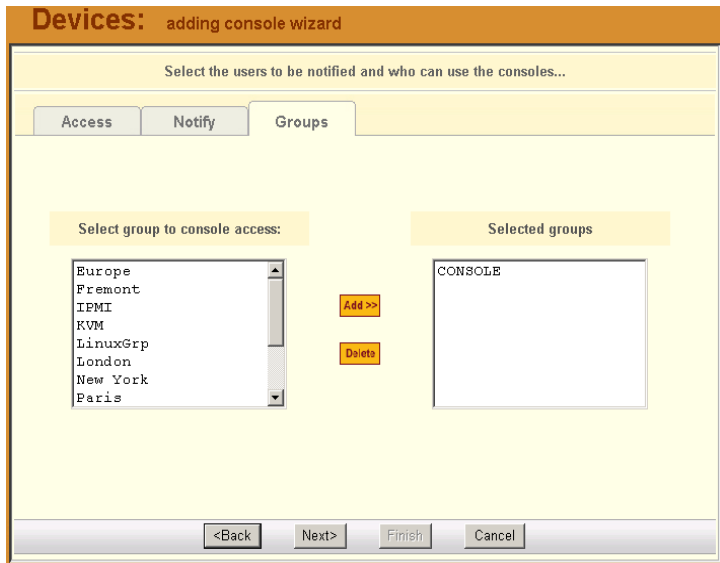
USER+ is the default list which contains all users.

The system also adds a plus (+) sign to any added user group that appears in the selection box.

6. Follow the instructions for the User Access form and then click on the Notify tab to proceed to the User Notification form:



From the User Notification form, select the user(s) you wish to be notified and then select the Groups tab to display the Groups form:



- Complete the Groups form, as necessary, and then select the **Next** button to display the Unconfigured Consoles form:

Devices: adding console wizard

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 checked="" type="checkbox"/>	server16_01
<input checked="" type="checkbox"/>	server16_02
<input checked="" type="checkbox"/>	server16_03
<input checked="" type="checkbox"/>	server16_04
<input checked="" type="checkbox"/>	server16_05
<input checked="" type="checkbox"/>	server16_06
<input checked="" type="checkbox"/>	server16_07
<input checked="" type="checkbox"/>	server16_08
<input checked="" type="checkbox"/>	server16_09
<input checked="" type="checkbox"/>	server16_10
<input checked="" type="checkbox"/>	server16_11

<Back Next> Finish Cancel

- Select the unconfigured console(s) that you wish to configure, and then select the **Next** button to display the Edit Settings form:

Devices: adding console wizard

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

Page 1/2 Page 2/2

Console	Port	Profile	Connection	Authentication
A_01	1	default	ssh	local
ACS_02	2	default	ssh	local
ACS_03	3	default	ssh	local
ACS_04	4	default	ssh	local
ACS_05	5	default	ssh	local
ACS_06	6	default	ssh	local
ACS_07	7	default	ssh	local
ACS_08	8	default	ssh	local

Console Prefix <Back Next> Finish Cancel

Note: If you need to change the prefix of the console names, type in the new prefix in the **Console Prefix** field and then click on the **Console Prefix** button. The system applies the new prefix to all console names.

- From the resulting form, modify any settings as needed, and then click on the second tab (**Page 2/2**) to continue the same form:

Console	Notify	Access	Data Buffer	Status	Advanced
A_01	<input type="text"/>	<input type="text"/>	0	OnDemand	advanced
ACS_02	<input type="text"/>	<input type="text"/>	0	OnDemand	advanced
ACS_03	<input type="text"/>	<input type="text"/>	0	OnDemand	advanced
ACS_04	<input type="text"/>	<input type="text"/>	0	OnDemand	advanced
ACS_05	<input type="text"/>	<input type="text"/>	0	OnDemand	advanced
ACS_06	<input type="text"/>	<input type="text"/>	0	OnDemand	advanced

- From the resulting form, modify any settings as needed, and then click on the next button to proceed to the Confirm Edits form:

Console	Port	Profile	Connection	Authentication
A_01	1	default	ssh	local
ACS_02	2	default	ssh	local
ACS_03	3	default	ssh	local
ACS_04	4	default	ssh	local
ACS_05	5	default	ssh	local
ACS_06	6	default	ssh	local
ACS_07	7	default	ssh	local
ACS_08	8	default	ssh	local

- Check your console settings from the Confirm Edits form (the second tab included). If information is incorrect, select the **Back** button and repeat steps 8 and 9, otherwise select the **Finish** button.

Device Discovery (Auto 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 existing TS or ACS configuration settings.

Warning: Consoles with the same names will cause the wizard to fail. Since ACS was designed to accept multiple ports with the same name, in the event that the wizard fails due to ports sharing the same name, you have two options: (1) Fix the configuration problem in the ACS and then run the Device Discovery wizard again. (2) Create consoles through the console wizard and then upload the configuration to ACS to overwrite the old one.

Configuration Requirements

For the **Auto Discovery** button to work, you must complete the required fields which are highlighted in red in the Device Definition form:

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

>> Running the Device Discovery Wizard

To run the Device Discovery Wizard follow the steps below:

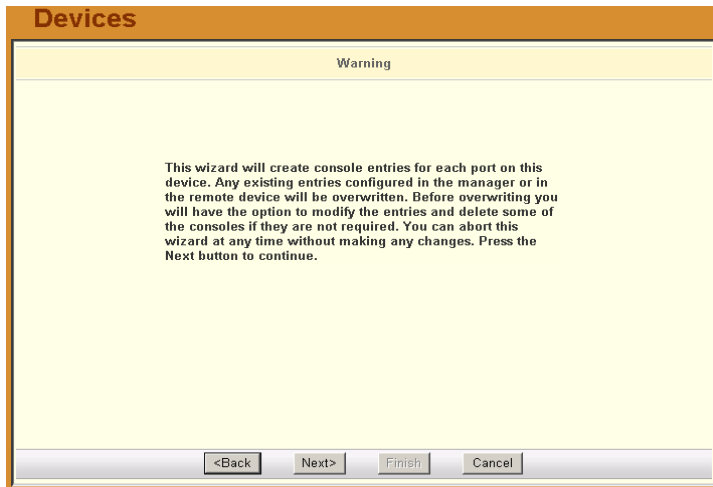
1. Log in as **admin** to the E2000
2. From the menu, select **Devices**.
3. From the Device List form, select the **Add** button to configure the ACS/TS.
4. From the resulting Device definition form, if you are using **static IP mode**, complete the input fields with particular attention to the following: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

- IP Address and Netmask form 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 displays the 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.



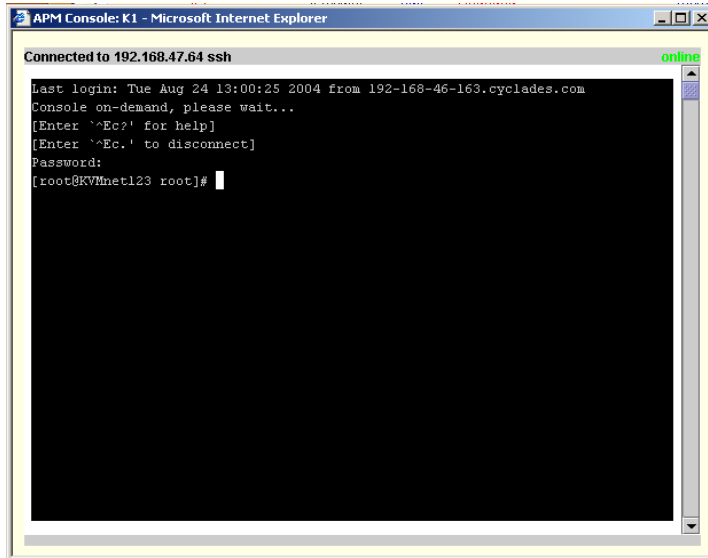
6. Select the **Next** button and follow the same procedure outlined in the Console Wizard section.

>> Connecting to a Device

To connect to a device, follow the steps below:

1. From the Device List form, click on the device name to which you wish to connect.

In the example below, the selected device is a KVM/net switch and the configured connection type is SSH:



If the type of device defined is IPMI, when you connect to a device, the system connects you to the BMC command line.

>> *Deleting a Device*

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

1. From the Device List form, select any device you wish to delete by clicking on the checkbox adjacent to the Device name.
2. Select the **Delete** button.

>> *Deleting a Device from a Group*

To delete a device from one or more groups, follows the steps below:

1. From the menu panel, select **Devices**.
The system displays the Device List form.
2. Under the Config column of the Console List form, click on the **Edit** link of the device you wish to remove from a group.
3. The system displays the Device Detail form for the selected device.

4. From the Device Detail form, click on Groups.
The system displays the Device Group form.
5. From the **Selected Groups** view panel of the Console Group form, select the group or groups from which you wish to remove the current device.
6. Click on the **Delete** button.
7. Click on the **Save** button to complete the procedure.

Deleting a Device Group

You cannot delete a device group using the Device Group form. To delete a device group, select **Groups** from the menu and refer to the Groups section of this chapter.

>> *Uploading Firmware to a Console Device*

Using the Device Detail form, you can configure the E2000 to upload firmware from its firmware repository to any console device.

1. From the Device Detail form (**Devices**: Device List > Device Detail), select the firmware you wish to upload from the **Firmware/Boot** drop down list.
2. Click on **Save**.

- 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**.

Device	Firmware	Bootcode	Upload firmware/bootcode	Upload configuration
ACS48			<input type="checkbox"/>	<input type="checkbox"/>

Submit

- Select **Upload Firmware/Configuration** to select either Firmware, Configuration, or both).
- Click on **Submit**.

Note: *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.*

KVM/net Device Configuration

When connected to a KVM/net switch, the **Devices** option also allows you to use the following KVM/net forms:

Table 4-8: Forms Used to Configure KVM/net

Form	Use this form to:
Device List	View KVM/net devices. Create, edit or delete a KVM/net device.

Table 4-8: Forms Used to Configure KVM/net

Form	Use this form to:
Device Detail	Configure the currently selected KVM/net device (e.g., Model, IP Address, MAC Address, etc.)
Groups	Assign the current KVM/net switch to one or more groups.
Proxies	Select the type of proxy if a KVM web proxy is required.
KVM Viewer	Configure the Idle Timeout and escape sequences for using the KVM Viewer

>> **Configuring Escape Sequences and Idle Timeout**

A main component of the KVM/net settings is defining the (keyboard) key sequences for users when using the AlterPath Viewer. An *escape sequence* is a sequence of special characters used to send a command to a device or program. In this case the escape sequence is sent to the KVM/net application. Typically, an escape sequence is coupled with a special character.

The Console KVM Viewer form shows the default Idle Timeout and escape sequences that are pre-configured in the KVM program. You can, however, change any of these values.

Idle Timeout refers to the time (in minutes) it takes the system to timeout (or drop the connection) after it remains idle.

To configure the aforementioned settings for the KVM viewer, follow the steps below:

1. From the menu, select Devices.
The system displays the Device List form.
2. From the Device List form, select the Edit column of the KVM device you wish to configure.

The system displays the KVM Device **Details** form:

The screenshot shows the 'Devices: editing device :: KVMDemo' interface. The 'Details' tab is active, displaying various configuration fields for the KVM device. The fields are organized into two columns. The left column includes fields for Device Name (KVMDemo), Model (KVM/net16), Admin Name (root), IP Address (10.10.10.31), Default Gateway (10.10.10.1), IP Mode (static), Status (OnDemand), Modem Mode (Disable), PPP Device IP, Health Monitor (never), and KVM Proxy (checked). The right column includes fields for Type (KVMnet), Location, Admin Password (Set Password), Netmask (255.255.255.0), DNS, Mac Address (five empty boxes), Auto Upload (unchecked), PPP Phone, PPP Local IP, and Connection (ssh). At the bottom, there are buttons for <Back, Reset, Save, Save / List Cascade, Save / Create Consoles, and Save / Auto Discover.

- From the Console Detail form, click on the KVM Viewer button.

The system displays the **KVM Viewer** form:

The screenshot shows the 'Devices: editing device :: KVMDemo' interface with the 'KVM Viewer' tab active. The form contains several input fields for configuring the KVM viewer. At the top, there are fields for Idle Timeout (3) and Escape Sequence (rk). Below this is a section titled 'Escape Sequences' with a yellow background, containing fields for Quit (q), Mouse/Keyboard Sync (s), Switch Next (.), Port Info (i), Power Management (p), Video Control (v), and Switch Previous (,). At the bottom, there are buttons for <Back, Reset, Save, Save / List Cascade, Save / Create Consoles, and Save / Auto Discover.

Table 4-9: Devices, KVM Viewer Form: Fieldnames and Elements

Button/Field Name	Definition
Details	Tab that links to the Device Detail form.
Groups	Tab that links to the Device Group form.
KVM Viewer	Tab that links to the KVM Viewer form (currently displayed).
Idle Timeout	The time (in seconds) it takes before the KVM viewer switches to idle mode after a period of inactivity. Default value = 3
Escape Sequence	The special character (keyboard key) to be used by the user to send a system command when using the KVM viewer or OSD. The “primary” escape sequence or key is combined with the various escape sequences that follow. Default value = ^K
Escape Sequences:	
Quit	Closes the session to a port and takes you back to the KVM/net Main Menu.
Power Management	Initiates a power control session.
Mouse/Keyboard Sync	Resets the keyboard and mouse synchronization if either one becomes unavailable after adding a new server to the KVM/net.
Video Control	Controls screen brightness and contrast.
Switch Next	Switches from the currently connected server to the next server that you are authorized to access.
Switch Previous	Switches from the currently connected server to the previous server.

Table 4-9: Devices, KVM Viewer Form: Fieldnames and Elements

Button/Field Name	Definition
Port Info	Displays any information about the current port.
Back	Button to return to the previous form.
Reset	Button to reset the input fields of the current form.
Save	Button to save the configuration to Flash.
Save/List Cascade	Displays the Cascade List form which shows a list of cascaded KVM devices, if configured.
Save/Create Consoles	Button to initiate the Console Wizard.
Save/Auto Discover	Button to initiate the Device Discovery Wizard.

4. From the KVM Viewer form, make the necessary changes and then click on **Save**.

>> ***Cascading a Secondary KVM to a Primary KVM***

The Devices Detail form for a KVM allows you to add a secondary KVM to be cascaded (or connected) to a primary KVM switch.

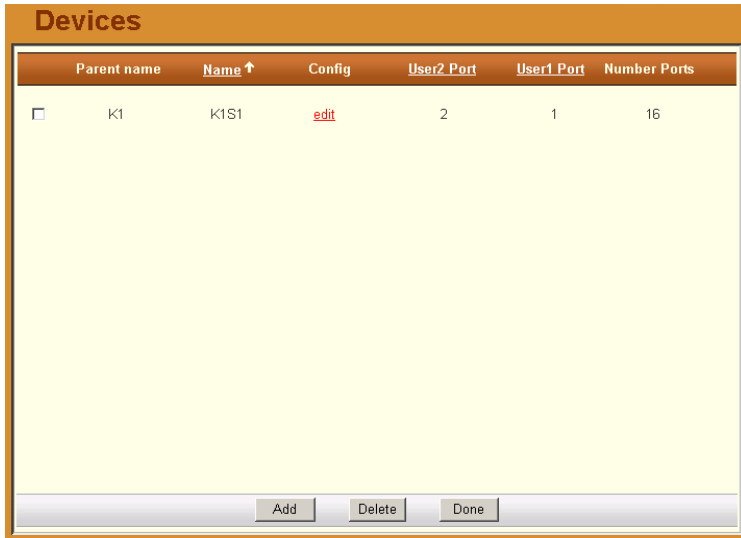
Please refer to the KVM User Manual or the KVM/net User for more detailed information about cascading.

To connect a Secondary KVM to a Primary KVM switch, follow the steps below:

1. From the menu, select **Devices**
The system displays the Device List form.
2. From the Device List form, select the **Edit** column of the KVM device you wish to configure.
The system displays the Device Detail form.

Devices

- From the Console Detail form, click on the Save/List Cascade button.
The system displays the Device Cascade List form:



Parent name	Name ↑	Config	User2_Port	User1_Port	Number Ports	
<input type="checkbox"/>	K1	K1S1	edit	2	1	16

Buttons: Add, Delete, Done

For a definition of the column fields, refer to the Field Definition table of the Cascade Detail form, next step.

- To configure a new device for cascading, click on **Add**.
- OR -

From the Device Cascade List form, select the KVM device that you wish to use as the primary device for cascading by clicking on **Edit**.

The system displays the Cascade Detail form:

The screenshot shows a web form titled "Devices" with a light yellow background and an orange border. At the bottom center is a "Save" button. The form contains the following fields:

- Device Name:
- Parent Name:
- User 2 Port:
- User 1 Port:
- Number of ports:

5. Complete the dialog box as follows:

Field Name	Definition
Device Name	Name of the secondary device or KVM switch.
Parent Name	The name of the primary KVM switch to which you are connecting the secondary device or KVM switch.
Number of Ports	Number of ports contained in the device to be cascaded.
Port Connected to User 2	The secondary KVM port to be connected to the User 2 port of the primary KVM/net.
Port Connected to User 1	The secondary KVM port to be connected to the User 1 port of the primary KVM/net.

6. Click on **Save** to complete the configuration

Alarm Trigger

Note: Alarm triggers work only with serial and IPMI consoles.

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

- Email notification for users or administrators
- Alarm

There are two pre-existing trigger entries:

- HeaLth_MoNiToR
- HeaLth_MoDeM

These alarm triggers are used in connection with the Health Monitor feature of the E2000, which includes the monitoring of any modems configured. You can modify these alarm triggers, but you cannot delete them.

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

Alarm Trigger Management

Use the Alarm Trigger forms to perform the following Alarm Trigger management procedures:

Table 4-10: Forms Used to Configure Alarms

Form Function	Form(s) Used
Add a new trigger string.	Alarm Trigger list form (Add button) > Alarm Trigger detail form.
Edit an alarm trigger.	Alarm Trigger list form (Alarm Trigger name) > Alarm Trigger detail form.
Delete an alarm trigger.	Alarm Trigger list form (Delete button).
Create an alarm for the trigger string and prioritize the alarm.	Alarm Trigger detail form (Input fields: Create Alarm and Priority).
Create notification events (email list).	Alarm Trigger detail form (input field: Notify).

Table 4-10: Forms Used to Configure Alarms

Form Function	Form(s) Used
Assign one or more user to receive an email or alarm.	Console Detail form (Notify button). Go to: Consoles: Console List > Console Detail.
Define or verify the email that is used when a user is notified of an event.	User List form > User Detail form.

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

>> Viewing the Alarm Trigger List Form

The Alarm Trigger List form allows you to view all the alarm triggers configured for the E2000 as well as to create, edit, and delete alarm triggers from the list.

To view the Alarm Trigger List form, follows the steps below:

1. From the menu, select Alarm Trigger.

The system displays the Alarm Trigger list form:



Alarm Trigger

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

To view or edit the configuration of an alarm trigger, click on the alarm trigger name.

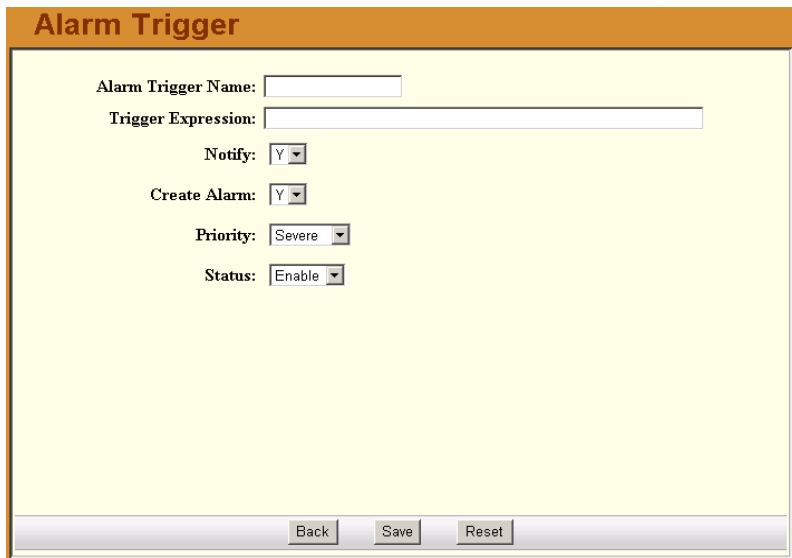
>> **Creating an Alarm Trigger**

Use the Alarm Trigger Detail form to define triggers to generate user notifications and alarms.

To create an alarm trigger, follows the steps below:

1. From the menu, select Alarm Trigger.
The system displays the Alarm Trigger List form.
2. From the Alarm Trigger List form, click on the Add button.

The system displays the Alarm Trigger Detail form:



Alarm Trigger

Alarm Trigger Name:

Trigger Expression:

Notify:

Create Alarm:

Priority:

Status:

Table 4-11: Alarm Trigger Detail Form - Fieldnames and Elements

Field Name	Definition
Alarm Trigger Name	Name of the trigger. Selecting a trigger name invokes the Alarm Trigger Detail 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.
Back	Button to return to the previous page or form.
Save	Button to save your trigger entry.
Reset	Button to reset the form to create a new trigger entry.

3. Complete the fields, as necessary.
4. Click on **Save** 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 Alarm Trigger name.
2. Click on 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 User Detail form (**Users:** User List > User Detail) to receive alarm notifications.

Configuration Requirement: Device Detail Form

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

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

Selection	Definition
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 defined, proceed to the Alarm Trigger Detail form to define the Health Monitoring Alarm Trigger.

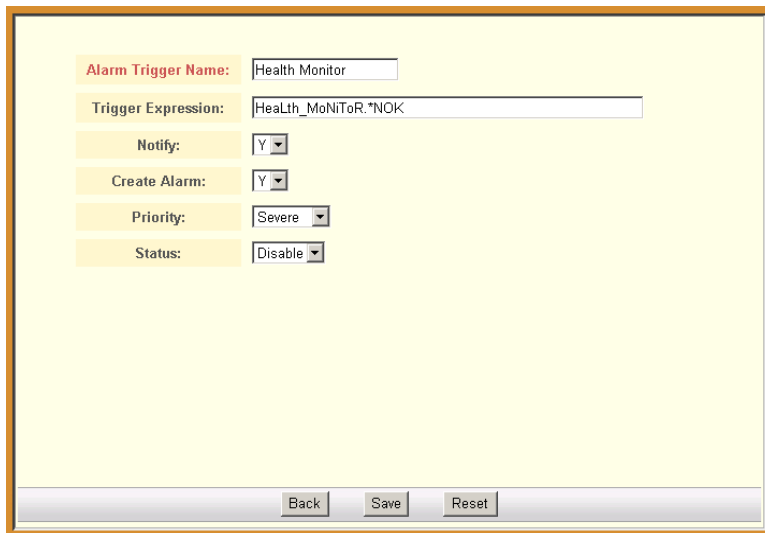
Using the Logical AND in the Alarm Trigger Expression

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 Health Monitoring, go to the Alarm Trigger Definition form (**Alarm Trigger List** > **Add** button > **Alarm Trigger** Detail form):



The screenshot shows a web form for defining an alarm trigger. The form has a light yellow background and a brown border. It contains the following fields and controls:

- Alarm Trigger Name:** Text input field containing "Health Monitor".
- Trigger Expression:** Text input field containing "HeaLth_MoNiToR.*NOK".
- Notify:** Dropdown menu with "Y" selected.
- Create Alarm:** Dropdown menu with "Y" selected.
- Priority:** Dropdown menu with "Severe" selected.
- Status:** Dropdown menu with "Disable" selected.

At the bottom of the form, there are three buttons: "Back", "Save", and "Reset".

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

Input Fieldname	Definition
Alarm Trigger Name	Provide a name to be associated with this particular alarm trigger.
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.

Important: For Health Monitoring to work properly, 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.

Profiles

The **Profiles** option allows you to configure the port profile for a target console. Port profiles define a standard set of parameters that are common to many consoles such as port speed, data bits, and stop bits.

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

Table 4-12: Summary of Profiles Forms

Action	Form(s) Used
Add a new profile.	Profile list form (Add button) > Profile detail form.
Edit a profile.	Profile list form (name link) > Profile detail form.
Delete a profile.	Profile list form (Delete button).

The Profiles List form is shown below:

Name	Console Type	Description	Status
default	Serial	default port configuration	Enable
<input type="checkbox"/> 9600-8-none-1	Serial	autogenerated profile	Enable
<input type="checkbox"/> 19200-8-none-1	Serial	autogenerated profile	Enable

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

Use the **Add** button on this form to invoke the Profile Detail 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 Detail form appears:

Table 4-13: Profiles Detail Form - Fieldnames and Elements

Field Name	Definition
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).

Table 4-13: Profiles Detail Form - Fieldnames and Elements

Field Name	Definition
DCD Sensitive	How the console server responds to changes to DCD signal.
Port Break Sequence	As indicated.
Back / Save / Reset	Buttons for the indicated actions.

2. Enter your port settings and other profile information in the provided fields
3. Select **Save** to complete the configuration.

>> **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 Detail form appears.
2. From the Profiles Definition form, make your changes.
3. Select **Save** to complete the configuration.

Consoles

Note: *For console forms associated with the Blade Module, see the **Blade Module** section of this chapter.*

The **Consoles** option allows you to perform the following console management procedures:

Table 4-14: Summary of Console Forms

Action	Form(s) Used
Add a new console to connect to the E2000 and for user access.	Console list (Add button) > Select Console Type > Console detail.

Table 4-14: Summary of Console Forms

Action	Form(s) Used
Configure blade(s) as part of the Blade Module.	The Blade Module is a paid-for option. See the Blade Module section (page 4-n) for more detailed information.
Select or change the authentication method for console access.	Console detail form (Input field: Authentication). NOTE: The E2000 authenticates users from the console server.
Assign the current console to any number of users.	Console detail form (Access button) > Console Access form.
Select the users to be notified of any alarms from the current console.	Console detail form (Notify button) > Console Notify form.
Edit a console.	Console list form (edit link under the Config column) > Console detail form.
Delete console.	Console list form (Delete button).
Assign or remove console(s) from the console group.	Console detail form (Groups button) > Console Groups.
Search, sort, and save list.	Console list form.

If you choose not to use the Console Wizard (**Devices:** Device List > Device Detail), then you can add consoles attached to the added device using the Console List and Console Detail forms.

Note: 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.

Note: See “Difference between Auto Upload and Manual Upload” on page 4-35 of this chapter.

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

Limitation of Tacacs Plus in ACS Console Access

Beware that access to an ACS console through the AlterPath Manager is currently not possible if the ACS serial port is configured to use Tacacs Plus authentication.

>> Viewing the Console List

To view the Console List form, perform the following steps:

1. From the menu panel, select Consoles.

The system displays the Console List form:



From the Console List form, you can add, edit, or delete a console by selecting the appropriate button or link.

Note: For console forms associated with the Blade Module, see the **Blade Module** section of this chapter.

Changing the Number of Consoles per Page

You can change or configure the number of consoles that you can view for each page. By default the number of consoles (or lines) per page is set to 512.

If you want to change this setting go to “Changing the Number of Consoles per Page” on page 5-12, Chapter 5: Advanced Configuration.

>> **Adding a Serial Console**

This procedure uses the serial console as an example of adding a new console. While there are variations to the Console Detail form based on the console type to be configured, there is a standard procedure for adding a console.

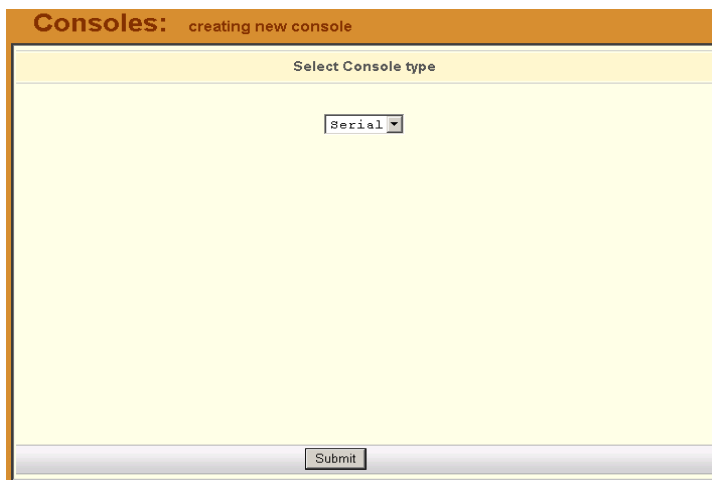
To add a console, follow the steps below:

1. From the menu, select **Consoles**.

The system displays the Console List form.

2. From the Console List form, click on the **Add** button.

The system displays the Adding Console form:



The screenshot shows a web form titled "Consoles: creating new console". The main content area is titled "Select Console type" and contains a dropdown menu with "Serial" selected. At the bottom of the form is a "Submit" button.

3. From the Adding Console form, select the type of console you wish to add.

The system displays the Console Detail form:

Table 4-15: Consoles, Details Form - Fieldnames and Elements

Fieldname	Definition
Details	Button to display the Console Detail form which is the currently displayed form.
Notify	Button to display the Console Notify form used to assign users to be notified when an alarm pertaining to the current console or device occurs.
Access	Button to display the Console Access form used to assign or authorize users to access the current console.
Groups	Button to display the Select Console Group form used to assign the current console to one or more console groups.
Console Name	<i>Required.</i> Name of the console
Device Name	(Drop down list.) Console server to which the current console is connected.

Table 4-15: Consoles, Details Form - Fieldnames and Elements

Fieldname	Definition
Port	Port on the console server when the console is connected. NOTE: In the Blade Module, if you are adding a switch console, the Port number corresponds to the switch number (go to Devices > Switch 1 through 4).
Profile Name	Name of port profile.
Description	Brief description of the console.
Location	Physical location 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.
Connection	Drop down list. Method used to establish a console connection: SSH, Socket, or Telnet.
Status	Drop down list. Enable, Disable, OnDemand.
Log Rotation	Frequency of the automatic log rotation process (Never, Daily, Weekly, Monthly).
Authentication	Drop down list to select the type of authentication for the E2000 to access the console port.
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.
Back	Button to revert to the last page or form.
Save	Button to save the configuration.

Table 4-15: Consoles, Details Form - Fieldnames and Elements

Fieldname	Definition
Logrotate Now	This field appears only if you selected Edit instead of the New button from the Console List form. Use this button to close and compress the console buffer log file, and to open a new file to receive new log entries. This operation overrides the Log Rotation automatic setting.

4. Complete the Console Detail form, as necessary.
5. Click on **Save** to complete the procedure.

Console Type: KVM

Selecting KVM as the Console Type displays the Console Detail form below. The Console Detail form for KVM allows you to configure the KVM/net ports for the KVM/net switch.

The screenshot shows a web-based form titled "Consoles: editing KVM console". At the top, there are four tabs: "Details", "Access", "Notify", and "Groups". The "Details" tab is selected. The form contains several input fields and dropdown menus arranged in two columns:

- Console Name:** A text input field.
- Device Name:** A dropdown menu with "KVMDemo" selected.
- Port:** A dropdown menu with "4" selected.
- Description:** A text input field.
- Machine Type:** A text input field.
- Machine Name:** A text input field.
- OS Type:** A text input field.
- OS Version:** A text input field.
- Location:** A text input field.
- Status:** A dropdown menu with "OnDemand" selected.

At the bottom of the form, there are two buttons: "Back" and "Save".

Refer to the previous Form Fields and Elements for a definition of the buttons and fieldnames.

>> **Selecting Users to Access the Console**

Use the Console Access form to assign and authorized one or more users to access the current console.

1. From the Console Detail form (**Consoles**: Console List > Console Detail), click on the **Access** button.

The system displays the Console Access form:

The screenshot shows a web interface titled "Consoles: editing KVM console ::". It has four tabs: "Details", "Access", "Notify", and "Groups". The "Access" tab is selected. Below the tabs, there are two main sections: "Select user to console access" and "Selected users". The "Select user to console access" section contains a list box with the following items: "simon", "steve", "+R&D", "+Sales", "+SalesEurope", "+SalesGermany", "+USER", and "+USSales". To the right of this list box are two buttons: "Add >>" and "Delete". The "Selected users" section is currently empty. At the bottom of the form, there are two buttons: "Back" and "Save".

2. From the resulting form, select a user from the **Select User to Console Access** view panel.

In the selection box, **+USER** is the default list which contains all users. The plus (+) sign is also used to indicate all defined groups.

3. Select the **Add** button.

The system transfers the selected user to the **Selected Users** view panel on the right.

4. To select another user, repeat steps 1 and 2. You can also use the <Shift> key to select multiple users.
5. Click on **Save** to complete the procedure.

>> **Selecting Users to be Notified**

Use the Console Notify form to assign one or more users to whom the system can send all notifications (email or alarm) pertaining to the current console.

1. From the Console Detail form (**Consoles**: Console List > Console Detail), click on the **Notify** button.

The system displays the Console Notify form:

2. From the resulting form, select a user from the **Select User to Notify** view panel.

In the selection box, **+USER** is the default list which contains all users. The plus (+) sign is also used to indicate all defined groups.

3. Select the **Add** button.

The system transfers the selected user to the **Selected Users** view panel on the right.

4. To select another user, repeat steps 1 and 2. You can also use the <Shift> key to select multiple users.
5. Click on **Save** to complete the procedure.

>> Assigning the Console to a Group

You can assign the current console to one or more groups using the Console Groups form. To use this form, however, a console group must already exist. To create a new group, you must select **Groups** from the main menu.

To assign a console to a group, follow the steps below:

1. From the Console Detail form (**Consoles**: Console List > Console Detail), click on the **Groups** button.

The system displays the Console Groups form:

The screenshot shows a web interface titled "Consoles: editing KVM console ::". It has four tabs: "Details", "Access", "Notify", and "Groups". The "Groups" tab is selected. The main content area is divided into two sections: "Select console groups" on the left and "Selected groups" on the right. The "Select console groups" section contains a list box with the following items: Europe, Fremont, IPMI, KVM, LinuxGrp, London, New York, and Paris. The "Selected groups" section contains a list box with the item "CONSOLE". Between these two sections are two buttons: "Add >>" and "Delete". At the bottom of the form are two buttons: "Back" and "Save".

2. From the resulting form, select a group from the **Select Console Groups** view panel.

Note: As with USER, CONSOLE is the default list which contains all consoles.

3. Select the **Add** button.

The system transfers the selected group to the **Selected Groups** view panel on the right.

4. To select another group, repeat steps 1 and 2. You can also use the <Shift> key to select multiple groups.
5. Click on **Save** to complete the procedure.

>> **Deleting a Console from a Group**

To delete a Console from one or more groups, follows the steps below:

1. From the menu panel, select **Consoles**.
The system displays the Console List form.
2. Under the Config column of the Console List form, click on the **Edit** link of the Console you wish to remove from a group.
The system displays the Console Detail form.
3. From the Console Detail form, click on **Groups**.
The system displays the Console Group form.
3. From the Selected Groups view panel of the Console Group form, select the group or groups from which you wish to remove the current console.
4. Click on the **Delete** button.
5. Click on **Save** to complete the procedure.

Deleting a Console Group

You cannot delete a console group from the Console Group form. To delete a console group or any group, you must select **Groups** from the menu.

See the **Groups** section of this chapter.

>> **Connecting to a Console**

To connect to a console using Secure Shell (SSH), follow the following step:

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

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.

>> **Initiating Log Rotate (Manual Operation)**

To initiate the logrotation perform the following steps:

1. From the Console List form, select the console for the particular console log you wish to rotate.

The system displays 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**.

>> **Using the Console Detail Form to Add an IPMI Console**

1. Open the Console List form (**Consoles**: Console List).
2. From the Console List form, click on **Add**.
3. The system opens the Adding Console form.
4. From the Adding Console form, select **IPMI** as the console type.
5. The system displays the IPMI Console Detail form.
6. Complete the fields, as necessary.

Use the Access Control List for Power to select users who can view the sensor display.

Note: IPMI Activation. *IPMI is a paid-for option for E2000 users. The feature is hidden from users who do not need it. To activate IPMI:*

- i. *Execute the script: `/var/apm/bin/apm_enable_ipmi.sh`*
- ii. *Enter the password provided by Cyclades when you register:*

Users

The Users option provides forms that enable the following user management tasks:

Table 4-16: Summary of User Forms

Action	Form(s) Used
Add a new user.	User list (Add button) > User detail.
Authorize the current user to access one or more consoles.	User detail (Access button) > User Access form.
View or edit user information	User list (username link) > User detail.
Set or change a user password.	User detail (Set Password button).
Define user as an administrator.	User detail (Admin User checkbox).
Assign a user to one or more groups.	User detail (Groups button) > User Groups form.
Delete a user.	User list (Delete button).
Search, sort, and save list	User list.

Note: Regardless of the authentication type (remote, local or none) or service, any user who will use the E2000 application **MUST** be entered in the E2000 database in order to access the application.

User List form

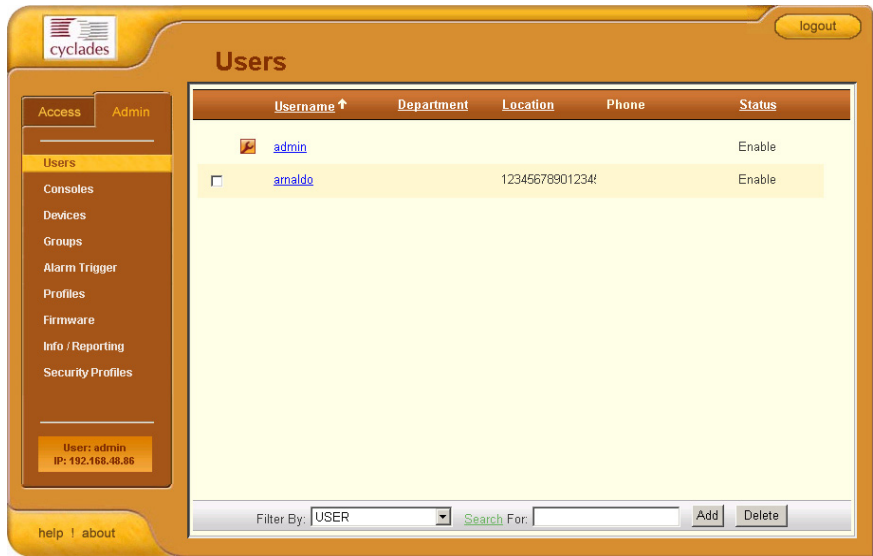
Use the User List form to view all E2000 system administrators and regular users. The list includes information about each user (*e.g.*, Name, Location, Phone) which you define in the User Detail form.

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

4: E2000 Web Administration

example, must still be registered in the E2000 database through the User Detail form:

Below is the User List form:



For an explanation of field column, refer to the *Screen Fields and Elements* of the User Detail form in the next section.

>> Adding a User

To add a new user, perform the following steps:

1. From the menu, select **Users**.
The system displays the User List form.
2. From the User List form, click on the **Add** button.

The system displays the User Detail form:

3. Complete the User Detail form, as necessary.

Table 4-17: Users, Details Form - Fieldnames and Elements

Fieldnames	Definition
Details	Tab to display the User Detail form (currently displayed).
Access	Click this tab to assign one or more consoles to the current user.
Groups	Click this tab to assign or re-assign the current user to one or more user groups.
Security	Click this tab to assign one or more security profiles to the current user.
Username	As indicated.
Admin User	Checkbox to indicate if the user is an admin and to authorize user access to the web application in <i>admin</i> mode.

Table 4-17: Users, Details Form - Fieldnames and Elements

Fieldnames	Definition
Security Profile	This check box appears only if you are in edit mode and a Security Profile can be assigned to the user group of this user.
Local Password	Checkbox to enable local authentication for the user. <i>NOTE: Even if you are 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>
Set Password	Button to display the password dialog box for setting the user password.
Full Name	The full name of the user.
Email	As indicated. This field is also used by the Alarm Trigger to notify the user of any event or issue relating to consoles and other system areas delegated to the user.
Department	The department to which the user belongs.
Location	The physical location of the user or department.
Phone	The phone number of the user.
Mobile	As indicated.
Pager	As indicated.
Status	Status of the user. Select enable or disable .
Back	Button to return to the previous page or form.
Save	Button to save the configuration.

4. Click on **Save** to complete the procedure.

>> **Selecting Consoles for a User**

The User Access form allows you to assign one or more consoles for the current user.

To assign consoles to a user, follow the steps below:

1. From the menu, select **Users**.

The system displays the User List form.

2. From the User List form, select the user to whom you wish to assign console access.

The system displays the User Detail form.

3. From the User Detail form, click on the **Access** button.

The system displays the User Access form:

The screenshot shows a web interface for managing users. The title bar reads "Users: creating new user". Below the title bar are four tabs: "Details", "Access", "Groups", and "Security". The "Access" tab is selected. The main content area is divided into two panels. The left panel, titled "Select console to user access", contains a text input field with the following text: "h", "l", "+CONSOLE", and "+mine_consoles". Below this input field are two buttons: "Add >>" and "Delete". The right panel, titled "Selected consoles", is currently empty. At the bottom of the form are two buttons: "Back" and "Save".

4. From the resulting form, select from the **Select Console to User Access** view panel the console you wish to assign to the user.

In the selection box, the plus (+) sign is used to indicate defined groups. The Console (or +CONSOLE) group is the default console group.

5. Select the **Add** button.

The system transfers the selected group to the **Selected Consoles** view panel on the right.

6. To select another console, repeat steps 4 and 5. You can also use the <Shift> key to select multiple groups.
7. Click on **Save** to complete the procedure.

>> **Selecting User Group(s) for a User**

The User Group form allows you to assign a user to one or more user groups. The user group, however, must already exist to be able to assign a user to the user group. Otherwise, select **Groups** from the menu to create a user group.

To assign a user to one or more groups, follow the steps below:

1. From the menu, select **Users**.

The system displays the User List form.

2. From the User List form, select the user to whom you wish to assign one or more groups.

The system displays the User Detail form.

3. From the User Detail form, click on Groups.

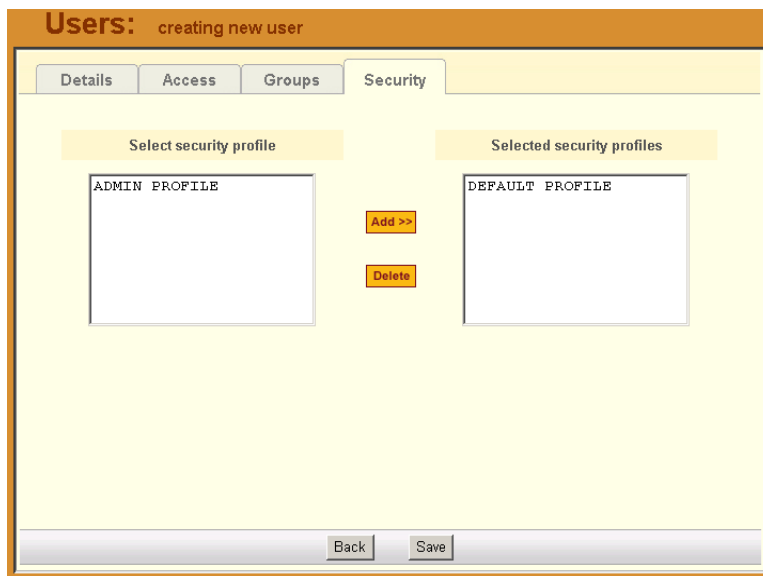
The system displays the User Groups form:

The screenshot shows a web interface for managing users. The main title is "Users: creating new user". Below the title are four tabs: "Details", "Access", "Groups", and "Security". The "Groups" tab is selected. The interface is divided into two main sections: "Select groups for the user" and "Selected groups". The "Select groups for the user" section contains a text input field with the value "mine_user". The "Selected groups" section contains a text input field with the value "USER". Between these two sections are two buttons: "Add >>" and "Delete". At the bottom of the form are two buttons: "Back" and "Save".

4. From the resulting form, select from the **Select Groups for the User** view panel the group you wish to assign to the user.
5. Select the **Add** button.
The system transfers the selected group to the **Selected Groups** view panel on the right.
6. To select another user group, repeat steps 4 and 5. You can also use the <Shift> key to select multiple user groups.
7. Click on **Save** to complete the procedure.

>> **Setting a User's Security Profile**

The **Security** tabbed form of the User's Profile allows you to assign/delete a security profile to/from a user group (to which the current user belongs). You can assign a security profile to a user or a user group.



>> **Deleting a User**

To delete one or more users from the User List, follow the steps below:

1. From the User List form, click the check box to the left of the username that you wish to delete.
2. Click on **Delete**.

>> **Deleting a User from a Group**

To delete a user from one or more groups, follows the steps below:

1. From the menu panel, select **Users**.
The system displays the User List form.
2. From the User List form, click on the user name you wish to remove from a group.
The system displays the User Detail form for the selected user.
3. From the User Detail form, click on **Groups**.
The system displays the User Group form.
4. From the **Selected Groups** view panel of the User Group form, select the group or groups from which you wish to remove the current user.
5. Click on the **Delete** button.
6. Click on the **Save** button to end the procedure.

Deleting a User Group

You cannot delete a user group from the User Group form.

See “Groups” on page 4-87 of this chapter.

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.

>> **Configuring the Local Password**

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.

Groups

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**.

Groups

The **Groups** option allows you to create new groups of users, consoles, or devices, as well as to edit or delete these groups. The E2000 has three default groups:

- Device,
- Console
- User

The system does not allow you to edit or delete these groups. You can edit and delete only those groups that you have created.

While you can assign devices, consoles, and users to groups using their respective menu options (**Devices**, **Consoles**, and **Users**), it is only through the **Groups** menu option that you can create groups.

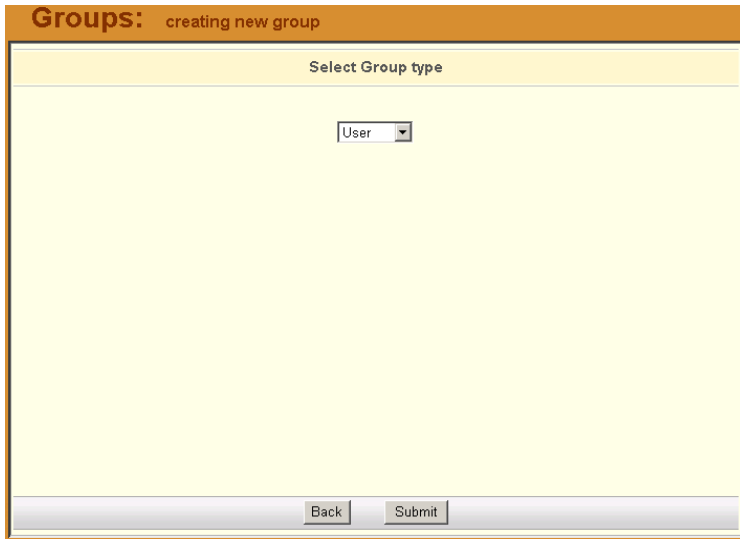


>> **Creating a Group**

To create a new group, follows the steps below:

1. From the menu, select **Groups**.
The system displays the Group List form (shown previously).
2. From the Group List form, click on the **Add** button.

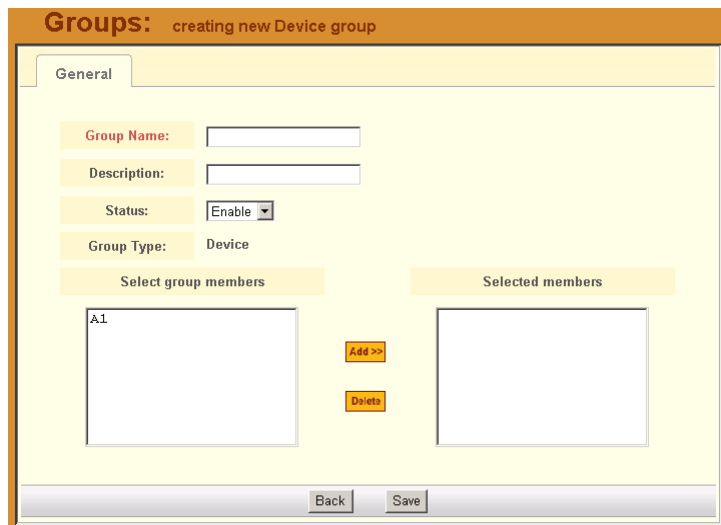
The system displays the Adding Group form:



The screenshot shows a web form titled "Groups: creating new group". The main content area is titled "Select Group type" and contains a single dropdown menu with the option "User" selected. At the bottom of the form, there are two buttons: "Back" and "Submit".

3. From the resulting form, select the group type you wish to create (**Device**, **Console**, or **User**).

Based on your selection, the system displays the Group Detail form. The example below uses the Group Detail form for the Group Type, User:



The screenshot shows a web form titled "Groups: creating new Device group". It has a "General" tab. The form contains several fields: "Group Name" (text input), "Description" (text input), "Status" (dropdown menu with "Enable" selected), and "Group Type" (text input with "Device" selected). Below these fields are two list boxes: "Select group members" (containing the item "A1") and "Selected members" (empty). Between the list boxes are two buttons: "Add >>" and "Deletes". At the bottom of the form, there are "Back" and "Save" buttons.

4. Enter the Group Name, Description, and Status of the new group.

5. Click on **Save** to complete the procedure.

>> **Adding Members to a Group**

To add members to a group, follow the steps below:

1. From the menu, select **Groups**.
2. From the resulting Group List form, select the type of group you want to configure.
3. From the resulting **General** tabbed form, choose from the left list box the members you wish to add to the group.

>> **Deleting a Group**

Note: *You cannot delete the following system-generated default groups:
Device, Console, and User.*

To delete a group, follow the steps below:

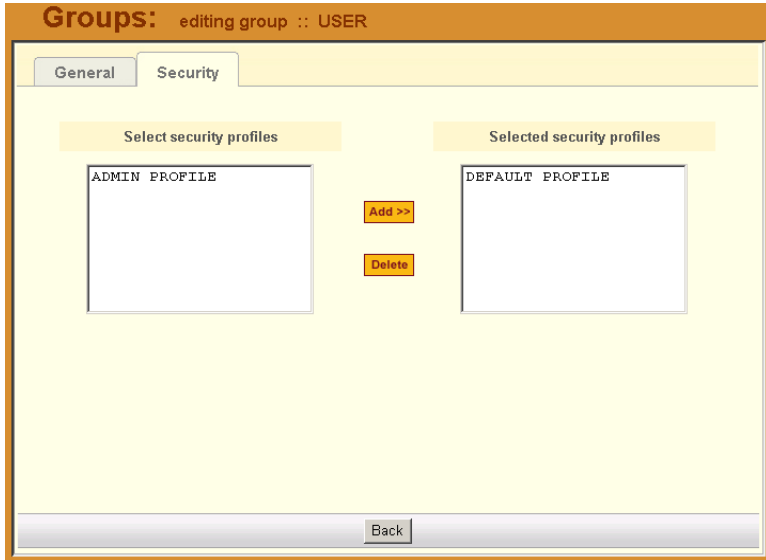
1. From the menu, select **Groups**.
The system displays the Group List form.
2. From the Group List form, click on the checkbox of the group that you wish to delete.
3. Click on **Delete**.

>> **Assigning a Security Profile to a User Group**

The User Group includes an additional tab, Security, which allows you to assign one or more Security Profiles to the current user group.

To assign a Security Profile:

1. Select the security profile from the Select Security Profile box and then click on the **Add** button.



Firmware

AlterPath Manager E2000 contains a firmware repository and supports firmware upgrades for TS and ACS. Each time a new firmware is released for the ACS and TS, 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:

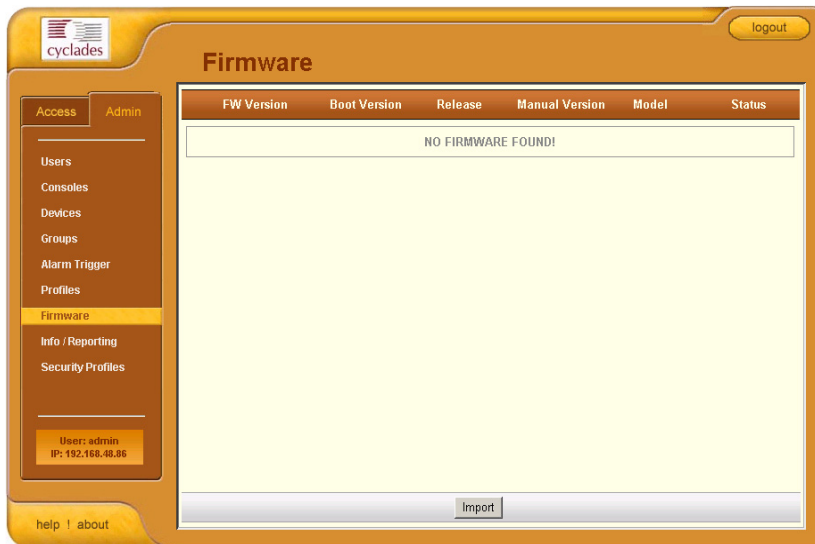
- Firmware List form
- Firmware Detail form.

Any firmware that you add to the Firmware List form is also reflected in the Device Detail form (specifically, the **Firmware/Boot** list field box). 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.



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 to 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**.

Note: 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.

Firmware Detail Form

Use the Firmware Detail form to:

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

The table below defines all the fields in the Firmware Detail form.

Table 4-18: Firmware Detail Form - Fieldnames and Elements

Field Name	Function
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 Enable or Disable the current firmware.

>> *Viewing and Accessing Firmware Information*

To view and access firmware details, follow these steps:

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:

1. To access firmware documentation, select **Manual**.
2. To access Release Notes for the current firmware, select **Release Notes**.
3. Type in notes in the Notes input text box and then select **Save** to enter notes and comments about the current firmware.
4. 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:

Data Type	Definition
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 database.
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.

To use the Backup and Restore commands in CLI, please refer to *Chapter 5: Advanced Configuration*.

System Recovery Guidelines

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

When performing a recovery procedure, 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.

E2000 Database Transaction Support

The E2000 commits all successful database transactions to the E2000 database. To ensure data integrity, the E2000 roll will roll back any failed database transaction in the event that:

- There are concurrent users updating the same record at the same time or
- A system fault caused the database transaction to fail.

When multiple users who are logged in as admin update the same record simultaneously, the system will generate a warning message to one of the users:

Validation Error

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

- **This record has been updated by another user. The changes you made will not be saved. Please reload and edit again.**

>> Responding to the Warning Message

When you receive the above warning message, you must perform the following steps:

1. Click on the **Reload** button located at the bottom of the screen.

The system displays the screen that you were updating.

4: E2000 Web Administration

1. Verify the information to determine if you still need to update the form. If you need to update the form, then proceed to re-update the form and then click on **Save**.

Optimistic locking is a mechanism to lock objects in multi-user systems to preserve integrity of changes so that one person's changes do not accidentally get overwritten by another. It offers reduced concurrency, higher performance, and avoids deadlocks.

Changing the Default Configuration

This configuration procedure is for advanced users only. To change the default database configuration of the E2000, please refer to **Chapter 5: Advanced Configuration**.

Info / Reporting

Info/Reporting is a list that summarizes all console access information by users and administrators as shown:

User	Session Start	Session End	Action	Connect Type	Source IP
admin	2005-03-28 16:31:27		logged in	WEB	192.168.46.163
admin	2005-03-28 16:24:24	2005-03-28 16:31:27	logged out	WEB	192.168.46.163
admin	2005-03-28 14:51:00		logged in	WEB	192.168.48.88
admin	2005-03-28 14:50:34	2005-03-28 14:50:42	login failed for user jane	WEB	192.168.48.88
admin	2005-03-28 14:50:34	2005-03-28 14:50:39	login failed for user jane	WEB	192.168.48.88
admin	2005-03-28 14:50:34	2005-03-28 14:50:56	login failed for user admin	WEB	192.168.48.88
admin	2005-03-28 14:26:04	2005-03-28 14:26:13	logged out	SSH	192.168.48.88
admin	2005-03-28 14:25:21	2005-03-28 14:52:51	logged out	SSH	192.168.48.88

Table 4-19: Info / Reporting List Form - Fieldnames and Elements

Field Name	Definition
User	Name of session user. To sort by User, click on the column name.
Session Start	Date and time when the session started. To sort by Session Start, click on the column name. Down arrow indicates that the list is in descending order; up arrow, in ascending order.
Session End	Date and time when the session ended.
Action	The user's action or the system action generated by the user. To sort by Action, click on the column name.
Connect Type	Connection type used by the session.
Source IP	The source IP address used.
Next>>	Button to view the next page.
<<Back	Button to return to the previous page.

Info / Reporting Details

To view a more detailed information about a particular user from a detail line, select from under the **User** column the particular user you wish to view.

When you select a user from the Info/Reporting List screen, the system displays the following detail list:



Date/Time	Information
2004-10-23 08:39:21	consolename= Win,actionattempted= Connect
2004-10-23 08:39:21	consolename= CalifDigital_1,actionattempted= Connect
2004-10-23 08:39:21	consolename= Router1,actionattempted= Connect

Blade Management Module

The Blade Module is an optional plug-in feature that enables the E2000 to provide console management of chassis, blades and switches. Once configured, the module allows authorized users to remotely manage the blades by providing access to the remote console and remote disk of a blade server.

All blades provide authorized users with Command Line Interface (CLI), KVM/IP, virtual media, and power options. Like most devices supported by the E2000, alarm notification, continuous logging, group and user management are integrated into the module. For security, blade users are controlled by the Control Access List (ACL) which is configured through the Security Profiles settings.

The Blade Module also comes with a Blade Wizard which enables the admin user to configure up to 14 blades and 4 switches for each chassis. There is no limit to the number of chassis that the Blade Module can support.

>> **Activating the Blade Module**

To activate the Blade Module, follow the steps below:

1. Execute the script: `/var/apm/bin/apm_enable_bladeModule.sh`
2. Enter the password provided to you when you registered for this feature.

Forms Used to Configure the Blade Module

The Blade Module in Admin mode comprises the following forms:

Table 4-20: Summary of Blade Module Forms

Menu Option	Forms and their Functions
Devices	<p>Device List - View list of chassis; add, edit or delete chassis; view logs.</p> <p>Device Details - Edit chassis configuration details; set or change admin password; run blade wizard.</p> <p>Groups - Select the group(s) to access the chassis.</p> <p>Proxies - Select the type of web proxy to use when accessing the Blade Center Management Module.</p> <p>Switch 1 - Configure a switch for the chassis.</p> <p>Switch 2 - Configure a second switch for the chassis.</p> <p>Switch 3 - Configure a third switch for the chassis.</p> <p>Switch 4 - Configure a fourth switch for the chassis.</p>
Consoles	<p>Console List - View list of blades/switches; add, edit or delete blades/switches.</p> <p>Console Details - View or edit blade configuration details (<i>e.g.</i>, connection type, log rotation, etc.)</p> <p>Access - Select user(s) to access the current blade.</p> <p>Notify - Select user(s) to be notified of an alarm regarding the current blade.</p> <p>Groups - Select blade groups.</p>

Table 4-20: Summary of Blade Module Forms

Menu Option	Forms and their Functions
Alarm Triggers	<p>Alarm Trigger List - View alarm trigger list; add, edit or delete an alarm trigger.</p> <p>Alarm Detail - View or configure a selected alarm trigger.</p>
Users	<p>User List - View list of users; add, edit or delete users.</p> <p>Details - View or configure a selected user.</p> <p>Access - Select blades and switches to which the current user can access.</p> <p>Groups - Select one or more groups to which a user can belong.</p> <p>Security - Select one or more security profiles to apply to the current user.</p>
Groups	<p>Group List - View list of groups according to user, blade or switch.</p> <p>Chassis > General - Select group members for the selected chassis group.</p> <p>Blade > General - Select group members for the selected blade group.</p> <p>User > General - Select group members for the current user group.</p> <p>Security - Select security profile to be applied to the current user.</p>

Table 4-20: Summary of Blade Module Forms

Menu Option	Forms and their Functions
Security Profile	<p>Security Profile List - View list of security profiles; add, edit or delete a security profile.</p> <p>General - Enable or disable the current security profile.</p> <p>Source IP - Define the source IP addresses allowed or not allowed.</p> <p>VLAN/Subnet - Define the VLANs/subnets allowed or not allowed.</p> <p>Date/Time - Define the date and time in which system access is allowed or not allowed.</p> <p>Authorization - Select the types of action allowable for the current security profile.</p>
Info Reporting	<p>Info / Reporting List</p> <p>Detail</p>

Note: *In Access Mode, a regular user can only view an individual blade/switch detail information from the Devices List form, but can not perform any add, delete, or edit functions. See **Chapter 3: E2000 Web Access** for more detailed information about the BladeManager web interface in Access Mode.*

Devices

The Devices List form allows you to perform the following:

- Connect to the Blade Management Module Web GUI through a web proxy of the native web interface or by telnet access (or whatever default session type is configured from the Devices Detail form).
- Access add/edit forms (Details, Groups, Proxies, Switch 1 through 4) to add/edit chassis.
- Delete a blade chassis.
- Run the Blade Wizard (to automatically create and configure the blades/switches for the currently selected chassis).
- View chassis access log.

>> Adding or Editing the Chassis

To add or edit a chassis, follow the steps below:

1. From the menu, select **Devices**.

The system displays the Device list form:



2. If you are adding a new chassis, from the Device list form, select the **Add** button.

3. Select Device Type form appears; from this form, select **IBM Blade Center**.

- OR -

If you are editing an existing chassis, from the Device list form, select the chassis you want to edit, and then click on the **edit** link (**Config** column, same row).

The system displays the Devices detail form:

4. Complete or modify the Details tabbed form as defined by the following table:

Note: In the Fieldname column, required fields are printed in **boldface**.

Table 4-21: BladeModule: Devices, Details Form - Fieldnames & Elements

Fieldname	Definition
Device Name	The symbolic name linked to the chassis.
Type	IBM Blade Center is the only supported type of device or chassis.

Table 4-21: BladeModule: Devices, Details Form - Fieldnames & Elements

Fieldname	Definition
Location	Physical location of the device or chassis.
Status	Dropdown list box to select: Enable - connection between the E2000 and the device is ALWAYS established. Disable - no connection is established, and all child consoles follow this configuration. OnDemand - connection is established only upon user's request.
Admin Name	The admin username (superuser) of the device.
Admin Password	Button to invoke a dialog box used to define the Admin's password. This password is used to access the IBM Blade Center port, but NOT to change the password. You must enter the SAME password registered in the blade server.
IP Address	The IP address of the device for IP mode: int_dhcp or static .
Netmask	As indicated, in dotted notation.
IP Mode	Dropdown list box. Select int_dhcp if APM E2000 is the DHCP server for this device, or Static if using a static IP. <i>See Configuring Your DHCP Server, this chapter.</i>
Mac Address	Specify the MAC address if the selected IP mode is int_dhcp .
Default Gateway	As indicated, in dotted notation.
DNS	As indicated, in dotted notation.
Back	Button to return to the previous page.
Reset	Button to reset the form.
Save	Button to save your configuration.

Table 4-21: BladeModule: Devices, Details Form - Fieldnames & Elements

Fieldname	Definition
Save / Create Blades	Button to activate the Blade Wizard.

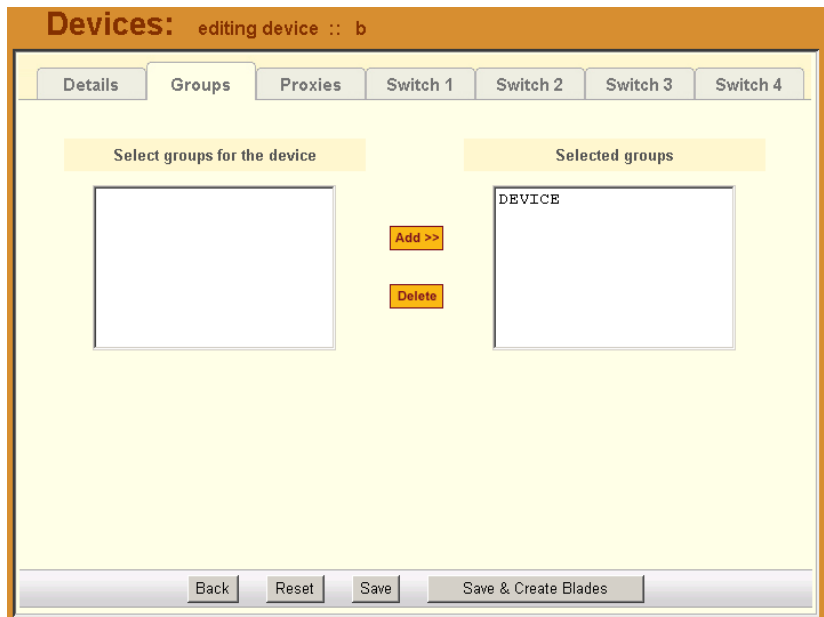
- Click on the **Save** button, and proceed to the next tabbed form, as necessary.

>> **Selecting a Group to Access the Chassis**

The Groups tabbed form allows you to specify one or more groups to access the currently selected chassis. To configure Groups, perform the following steps:

- From the menu, go to **Devices** (click on **Add** or **edit**) > **Details** > **Groups**.

The system displays the **Devices - Groups** tabbed form:



- Select (or highlight) from the left list box the device group that the current chassis supports.

Note: Unless a device is configured for another group, the **DEVICE** group is the default group for all devices.

3. Click on **Add**.
4. Repeat steps 2 and 3 if you have another group to add.

Note: To delete any entries from the **Selected Groups** box, highlight the group you wish to delete and then click on **Delete**.

5. Click on **Save** and proceed to the next tabbed form, as necessary.

Proxies

To create or configure a web proxy for a device, see “Proxies” on page 4-24.

>> *Configuring the Chassis Switch*

The switch tabbed form allows you to specify the parameters to access the switch management interface through Telnet or the web interface. You can configure up to four chassis switches for the currently selected chassis. To configure a switch, perform the steps below:

1. From the menu, go to **Devices** (click on **Add** or **edit**) > **Details** > **Groups** > **Switch 1**.

The system displays the **Devices - Switch 1** tabbed form:

2. Complete the **Switch 1** form, as necessary.

Table 4-22: Blade Module: Devices, Switch 1 - Fieldnames & Elements

Fieldname	Definition
IP Address	The IP address of the switch which uses the IP mode: int_dhcp or static .
Type	The symbolic name linked to the chassis switch. IBM Blade Center is the only supported type of chassis.
Admin Name	The admin username (superuser) of the device.
Admin Password	Button to invoke a dialog box used to define the Admin's password. This password is used to access the IBM Blade Center port, but NOT to change the password. You must enter the SAME password registered in the blade server.

Table 4-22: Blade Module: Devices, Switch 1 - Fieldnames & Elements

Fieldname	Definition
Status	Dropdown list box to select: Enable - connection between the E2000 and the device is ALWAYS established. Disable - no connection is established, and all child consoles follow this configuration. IMPORTANT: The system will not allow you to add and configure a switch console unless you set this field to Enable .
Netmask	As indicated, in dotted notation.
IP Mode	Dropdown list box. Select int_dhcp if APM E2000 is the DHCP server for this device, or Static if using a static IP. <i>See Configuring Your DHCP Server, this chapter.</i>
MAC Address	The MAC address is required if the IP mode is int_dhcp .
Default Gateway	As indicated, in dotted notation.
DNS	As indicated, in dotted notation.
Back	Button to return to the previous page.
Reset	Button to reset the form.
Save	Button to save your configuration.
Save / Create Blades	Button to activate the Blade Wizard.

3. Click on Save to save your configuration.
4. To configure another switch, click on the next Switch tabbed form.

Two Methods of Blade Configuration

Once the chassis has been defined and configured, you can configure the blades and switches in two ways:

- Through the Blade Wizard
- Through the **Consoles** forms

As with the chassis, Admin users may edit only those blades or switches to which they are authorized as defined in the **Security Profiles** form.

Running the Blade Wizard

The Blade Wizard is designed to help you configure and automatically generate blades/switches for the current chassis.

To activate the Blade Wizard, click on the **Save/Create Blades** button from any of the Device forms.

The series of screens comprising the Blade Wizard, in sequential order are as follows:

Table 4-23: Summary of Blade Wizard Forms

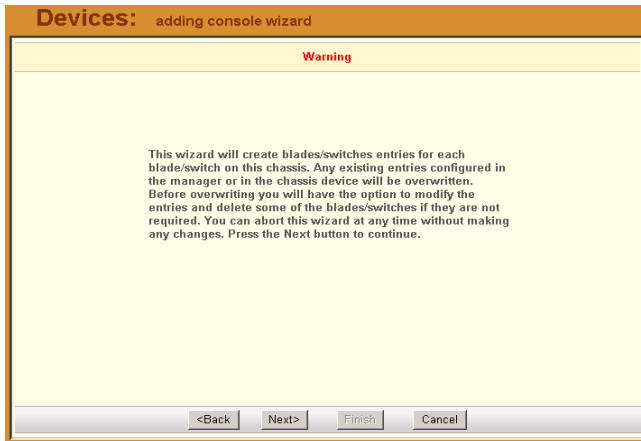
Form Name	Function
Warning	Warns the users that existing entries for chassis/blades in the E2000 or chassis device will be overwritten.
Connection Method	Sets the default connection protocol for the blades or switches.
User Access, Notification & Groups	These three tabbed forms define who can access the blades/switches, the user(s) to be notified, the authorized group(s).
Console (blade/switch) selection.	Allows you to select each blade/switch to be configured from the list of unconfigured blades/switches.
Edit Configuration	Allows you to edit any of the configured blades/switches. This form provides advanced configuration options.

Table 4-23: Summary of Blade Wizard Forms

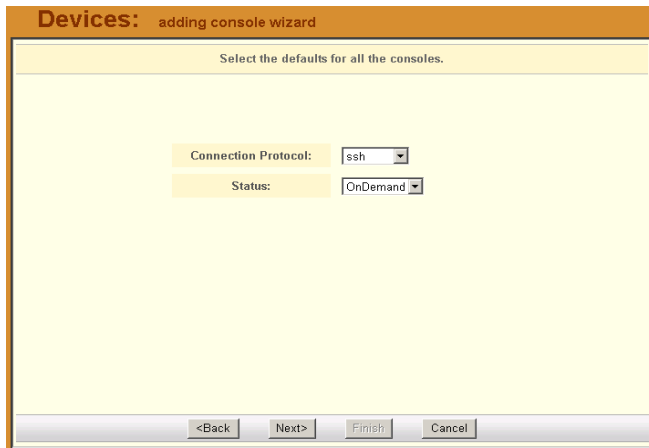
Form Name	Function
Confirmation	Prompts you to review and confirm the configuration.
Completion	Message to indicate successful completion.

The Blade Wizard screens are shown as follows:

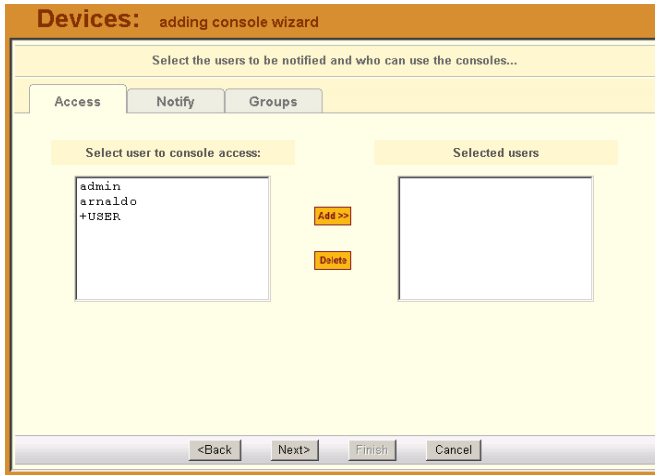
Warning Message:



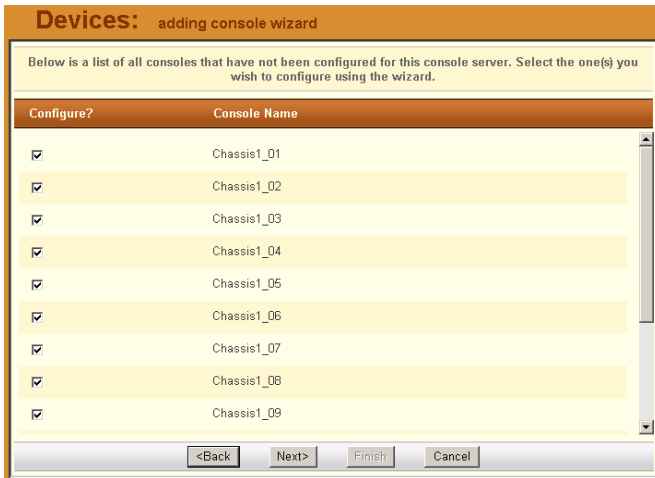
Connection Method:



User Access & Notification:



Console (Blade/Switch) Selection:



4: E2000 Web Administration

Edit Configuration:

Devices: adding console wizard

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

Page 1/2 Page 2/2

Console	Port	Connection
Chassis1_01	1	ssh
Chassis1_02	2	ssh
Chassis1_03	3	ssh
Chassis1_04	4	ssh
Chassis1_05	5	ssh
Chassis1_06	6	ssh
Chassis1_07	7	ssh

<Back Next> Finish Cancel

Confirmation:

Devices: adding console wizard

This screen confirms your previous edits and selections. Pressing Finish will save these changes.

Page 1/2 Page 2/2

Console	Port	Connection
Chassis1_01	1	ssh
Chassis1_02	2	ssh
Chassis1_03	3	ssh
Chassis1_04	4	ssh
Chassis1_05	5	ssh
Chassis1_06	6	ssh
Chassis1_07	7	ssh
Chassis1_08	8	ssh

<Back Next> Finish Cancel

From the Confirmation form, click on **Finish** to complete the configuration process.

Configuring the Blades and Switches

The blades and switches are configured from the Consoles forms in the same way you would configure consoles. The forms are the same except that they now fully support blade configuration.

The Consoles List form shows one console name for each blade or switch. For each blade, the E2000 provides serial console, KVM, power and virtual media connections; and for each switch, CLI and web connections.

All users' access rights to blades and switches and the types of action they are allowed to do are defined in the **Security Profiles** forms.

Table 4-24: Blade Module: Summary of Console Forms

Form Name	Use this form to:
Consoles List	View list of blades/switches; add, edit or delete blades/switches.
Details tabbed form	View or edit blade configuration details (<i>e.g.</i> , connection type, log rotation, etc.)
Access tabbed form	Select user(s) to access the current blade or switch.
Notify tabbed form	Select user(s) to be notified of an alarm regarding the current blade.
Group tabbed form	Select blade groups. NOTE: To create a new group, go to menu: Groups .

Consoles List Form

The Consoles List form displays all the blades configured and supported by the E2000. The form allows you to:

- Connect to a blade server or switch - When you move your cursor over the blade or switch name, a pop-up window displays options to provide you the following connection types:

Connection Type	Applies to:	Use this connection to:
CLI	Blade servers and switches.	Launch a CLI session using either Telnet or SSH. NOTE: Power control is available through ^ec sequence.
KVM	Blade servers only	Launch the remote console applet session for KVM.
VM	Blade servers only	Launch the remote console applet and remote disk of the currently selected blade server.
ON	Blade servers only	Power on the blade server.
OFF	Blade servers only	Power off the blade server.
Web	Switches only	Launch the web application.

- Add, edit, or delete blades.
- Access the other blade/switch console management forms: Details, Access, Notify, and Groups.

Consoles						
Console ↑	Type	Config	Device	Port	Location	Status
<input type="checkbox"/> IBM_01	Blade	edit	IBM	1		OnDemand
<input type="checkbox"/> IBM_02	Blade	edit	IBM	2		OnDemand
<input type="checkbox"/> IBM_03	Blade	edit	IBM	3		OnDemand
<input type="checkbox"/> IBM_04	Blade	edit	IBM	4		OnDemand
<input type="checkbox"/> IBM_05	Blade	edit	IBM	5		OnDemand
<input type="checkbox"/> IBM_06	Blade	edit	IBM	6		OnDemand
<input type="checkbox"/> IBM_07	Blade	edit	IBM	7		OnDemand
<input type="checkbox"/> IBM_08	Blade	edit	IBM	8		OnDemand
<input type="checkbox"/> IBM_09	Blade	edit	IBM	9		OnDemand
<input type="checkbox"/> IBM_10	Blade	edit	IBM	10		OnDemand
<input type="checkbox"/> IBM_11	Blade	edit	IBM	11		OnDemand

Filter By: CONSOLE Search For:

>> Adding a Blade or Switch

To add a blade or switch:

1. Select **Consoles** from the menu.
2. From the Consoles List form, select the **Add** button.
3. From the Select Console Type form, select **Blade** or **Switch**.

Important: If you are adding a switch, be sure that you have set the switch to **Enable** (go to Chassis > Switch) in the switch device form otherwise you will receive an error message.

4. Complete the rest of the tabbed forms, as necessary.

>> Editing a Blade or Switch

To edit a blade or switch:

1. Select **Consoles** from the menu.
2. From the Consoles List form, select the blade or switch you wish to edit, and then select the **edit** link.

3. Complete the rest of the tabbed forms, as necessary.

Note: For more detailed information on how to use the Consoles **Details**, **Access**, **Notify**, and **Groups** forms, see “Consoles” on page 4-67 of this chapter.

Security Profiles

A security profile defines a set of rules or conditions regarding a user’s access permissions and limits for accessing the E2000 and its features. The **Security Profiles** feature allows the administrator to centrally create these rules for as many profiles as necessary. Each time a user requests a page, the system checks the security profile.

Security Profiles deal with IP filtering, VLAN restriction, time and date restrictions, and authorization rules that are applied to each user. The default rule of security profiles is **Deny**.

You can apply security profiles to users and user groups. The **Default Profile** is the profile of the default group, **User**. Whatever condition(s) you configure in the Default Profile is automatically applied to all users except Admin users. This profile cannot be deleted.

Note: To configure users and user groups, go to **Users > Groups**.

The Default Profile already allows users to log on. You may change it to block connections by default and then allow the valid users. If the chosen rule is **Allow**, you must select at least one action from the **Authorization** tab.

Security profile management is composed of the following forms:

Table 4-25: Summary of Security Profile Forms

Form Title	Use this form to:
Security Profiles List	View a list of available profiles along with the description, status, and default rule of each profile.
General	Enter the security profile name, description, status (Enabled , Disabled or Deleted) and rule (Allow or Deny).
Source IP	Enter the client workstation IP addresses from which you may allow a user to connect.

Table 4-25: Summary of Security Profile Forms

Form Title	Use this form to:
LAN/ITF	Enter the LAN interfaces and subnets to which you may allow a user to connect.
Date/Time	Enter the date and time in which the user can access the system.
Authorization	Define the specific authorized action (e.g., Connect to a console, connect to a KVM/net, Connect to the web management interface, etc) for this profile.

Security Profile List

The Security Profile List form displays a list of all Security Profiles that you can assign to a user or user group. The list contains four columns:

Column Name	Definition
Profile Name	The name of the profile and, if applicable, the source IPs allowed for this profile.
Description	A brief description of the profile and, if applicable, the interfaces and the date/time allowed for this profile.
Status	States if the profile is enabled or disabled ; if applicable, lists all authorized actions for the current profile.
Rule	States whether the rule is to allow or deny .



>> Adding or Editing a Security Profile

To add or edit a security profile, perform the following steps:

1. From the menu select Security Profile.
The system displays the Security Profile list form (see previous page).
2. Select the **Add** button to add, or select an existing profile to edit.

The system displays the **Security Profiles - General** tabbed form:



The screenshot shows a web form titled "Security Profile: creating new security profile". The form has five tabs: "General", "Source IP", "LAN ITF", "Date/Time", and "Authorization". The "General" tab is selected. The form contains the following fields:

- Profile Name:** A text input field.
- Description:** A text input field.
- Status:** A dropdown menu with "Enabled" selected.
- Rule:** A dropdown menu with "Allow" selected.

At the bottom of the form, there are two buttons: "Back" and "Save".

3. From the **General** tabbed form, enter the profile name (required), a brief description of the profile, its status (Enabled, Disabled, Deleted), and the rule to be applied to the entire profile (Allow or Deny).
4. Click on **Save**.

>> **Security Profiles: Source IP**

1. Click on the **Source IP** tab to configure the conditions for accepting source pages for the current profile.

The system displays the **Source IP** tabbed form:

2. Complete or modify the form, as needed.

Table 4-26: Security Profiles, Source IP - Fieldnames and Elements

Field Name	Function
Source IP (tab)	Title of the current tabbed form.
Rule	The default rule (Allow or Deny) that applies to the entire security profile. The default rule is configured from the General tabbed form.
Add Source IP Conditions	This section allows you to define the Source IP that will be used as the conditions for applying it to the rule.
IP	The IP address to be added to the Added Source IP Conditions list box.
Netmask	The netmask to be added to the Added Source IP Conditions list.

Table 4-26: Security Profiles, Source IP - Fieldnames and Elements

Field Name	Function
Add	Button to add to the conditions list the address you just entered in the IP or Netmask field.
Delete	Button to delete a selected IP address from the adjacent Source IP Conditions list box.
Added Source IP Conditions	List of source IP addresses to be applied to the rule.
Back	Button to return to the previous page.
Save	Button to save your configuration.

3. Click on **Save**.

Security Profiles: LAN ITF

The LAN ITF (Local Area Network Interfaces) tabbed form allows you to define the interfaces to which a user is either allowed to connect, or denied access. This feature is designed for situations where multiple network or LAN segments are used or defined.



Table 4-27: Security Profiles, LAN ITF - Fieldnames & Elements

<i>Field Name</i>	<i>Function</i>
LAN ITF (tab)	Tab to select the current form.
Rule	The default rule (Allow or Deny) that applies to the current form and the entire security profile. The rule is configured from the General tabbed form.
Select LAN ITF Conditions	List box that lists all LAN interfaces. Select the LAN interface(s) that will be applied to the rule.
Add	Button to select items from the Select LAN ITF Conditions (left box) and add to the Selected LAN ITF Conditions list box (right box).
Delete	Button to remove any selected LAN ITF conditions from the right list box.
Selected LAN ITF Conditions	List of selected LAN ITF conditions that will be applied by the rule to the policy.
Back	Button to return to the previous page.
Save	Button to save your configuration.

Security Profile: Date/Time Configuration

The **Date/Time** tabbed form allows you to specify the time in which the profile will allow or deny access to the system.

Table 4-28: Security Profiles, Date/Time Form - Fieldnames and Elements

Field Name	Function
Date/Time (tab)	Tab title to select the current form.
Rule	The rule (Allow or Deny) that applies to the entire security profile. The default rule is configured from the General tabbed form.
[Day/Time Table]	The table represents the days of a week (rows) and the hours of a day (columns). Clicking inside a segment selects a specific one-hour period of a day.
Add Time Period Conditions	Define below this title the time period conditions that applies to the default rule by clicking the appropriate boxes.

Table 4-28: Security Profiles, Date/Time Form - Fieldnames and Elements

Field Name	Function
Sun - Sat (check boxes)	Select the day(s) to be applied to the default rule.
Start Time	Specify a Start Time to be applied to the selected day(s), as part of the time conditions.
End Time	Specify an End Time to be applied to the selected day(s), as part of the time conditions.
Add	Button to add the day and time settings to the Added Time Period Conditions box and apply them to the rule.
Delete	Button to delete the day and time settings from the Added Time Period Conditions box.
Added Time Period Conditions	Title of the list entry box for applying the day and time conditions.

Security Profile: Authorization Configuration

The Authorization tabbed form allows you to define the authorized actions for the current profile. If the rule chosen for a security profile is Allow, then you must select at least one action from the Authorization form. The left hand box

lists all the possible actions. The selected action(s), by selecting the **Add** button, are listed in the right hand box.



The list of valid actions to select from are as follows:

Authorized Action	Use this action to:
ConnectToDeviceCLI	Allow user access to CLI configuration interface.
ConnectToDeviceGUI	Allow user access to web configuration interface.
ConsoleGUI	Allow web access to console.
ConsoleReadWrite	Allow Read and Write access to console.
KVMReadWrite	Allow READ/WRITE access to a KVM/IP interface.
PowerControl	Allow user to perform power control operations.
System	Allow system access.

Authorized Action

Use this action to:

UserVirtualMedia

Allow user access to blades.

>> ***Deleting a Security Profile***

To delete a security profile, perform the following steps:

1. From the main menu, select **Security Profiles**.
2. From the Security Profiles list form, check mark the Security Profile that you wish to delete.
3. Click on **Delete**.

Chapter 5

Advanced Configuration

This chapter presents some procedures for configuring the E2000 through the Command Line Interface (CLI).

First Time Configuration aside, Cyclades recommends the use of the CLI only for advanced *admin* users who are proficient with CLI, and would like more control over the configuration features of the E2000.

This chapter is organized as follows:

- Working from a CLI
 - Logging In
 - Shell Commands
 - Copying and Pasting Text within the Console Applet Window
 - Connecting Directly to Ports
 - CLI Commands
 - Set Commands
- Changing the Escape Sequence
- Re-defining the Escape Key
- Changing the Number of Lines in the SSH Applet
- Changing the Session Timeout
- Changing the Number of Consoles Per Page
- Enabling Telnet
- Changing the ASC/TS Admin Name
- Ethernet Port Configuration
- Modem Card Configuration
- Serial Card Configuration
- Configuring Dial Out and Dial Back
- Modem Dial Back for ACS
- Changing the Ports to be Proxied
- NIS Authentication
- Disabling HTTP to Use only HTTPS

5: Advanced Configuration

- Adding/Upgrading Firmware
- Backing Up User Data
- Enabling the Restore Script
- Managing Log Files
- Changing the Database Configuration
- Restoring Your Configuration
- Installing SSL Certificates

Working from a 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 management 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>
```

Note: The “**l**” in **ssh-l** is the alphabet “l” as in *lemon*.

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 the 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:

Command	Use this command to:
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:

Menu Option	Use this option to . . .
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..

5: Advanced Configuration

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.

Note: Linux browsers do not support the Copy and Paste feature.

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>
```


Working from a CLI

```
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. For example, to send a broadcast message, you must press: <Ctrl>**Ecb**

Key(s)	Command	Key(s)	Command
.	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

Key(s)	Command	Key(s)	Command
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: <^> <shift>_
(i.e., <Ctrl> <Shift> <underscore>)

Set Commands

The following set commands are available to enable you to manually and individually configure specific E2000 settings through CLI:

- setauth
- setboot
- setcons
- setdatetime
- date
- setnames
- setnetwork
- setntp
- setsntp

SETAUTH - sets the authentication method. For example:

```
[root@APM_Paulo root]# setauth
Your configuration will be overwritten by the default files!!
Are you sure you want to continue? (y/n)[n] y
Continuing setauth...
Choose the desirable authentication method local/radius/
tacacs+/ldap/kerberos/nis/active_directory) [local]:
*** Configuration changed!
*** Execute saveconf to save the new values in flash.
```

Note: If you select Radius as the authentication method, the system will prompt you for other Radius servers to be configured, thus allowing you to configure more than one Radius Server.

SETBOOT - sets the network boot utility. For example:

```
[root@APM_Paulo root]# setboot
NL4000 Network Boot Configuration Utility
-----
Current Status:          DISABLED
Press <ENTER> if you wish to change it, or [Q<ENTER>] to
quit:
Enter Local IP Address []:
Current Status:          DISABLED
Do you wish to save these parameters? (y/N) n
*** Network boot parameters NOT saved
```

SETCONS - sets console connection. For example:

```
[root@APM_Paulo root]# setcons
APM Console Configuration Utility
-----
Current Parameters: 9600, 8n1, vt100
Press <ENTER> if you wish to change it, or [Q<ENTER>]
to quit:
Enter Baud Rate (in bps) [9600]:
Enter Word Length (5, 6, 7 or 8) [8]:
Enter Parity (even, odd or no) [no]:
Enter Stop Bits (1 or 2) [1]:
Enter Terminal Type [vt100]:
WARNING: make sure you're setting valid values for the
console parameters, or you may make your console
inaccessible!
Current Parameters: 9600, 8n1, vt100
Do you wish to save these parameters? (y/N)
```

SETDATETIME - sets the system date and time based on the selected time zone. For example:

```
[root@APM_Paulo root]# setdatetime
Please choose the time zone where this machine is located.
```

5: Advanced Configuration

1) Africa	18) Eire	35) Jamaica	52) ROC
2) America	19) Etc	36) Japan	53) ROK
3) Antarctica	20) Europe	37) Kwajalein	54) Singapore
4) Arctic	21) Factory	38) Libya	55) System
5) Asia	22) GB	39) MET	56) Turkey
6) Atlantic	23) GB-Eire	40) MST	57) UCT
7) Australia	24) GMT	41) MST7MDT	58) US
8) Brazil	25) GMT+0	42) Mexico	59) UTC
9) CET	26) GMT-0	43) Mideast	60) Universal
10) CST6CDT	27) GMT0	44) NZ	61) W-SU
11) Canada	28) Greenwich	45) NZ-CHAT	62) WET
12) Chile	29) HST	46) Navajo	63) Zulu
13) Cuba	30) Hongkong	47) PRC	64) iso3166.tab
14) EET	31) Iceland	48) PST8PDT	65) posix
15) EST	32) Indian	49) Pacific	66) posixrules
16) EST5EDT	33) Iran	50) Poland	67) right
17) Egypt	34) Israel	51) Portugal	68) zone.tab

Enter the number corresponding to your choice: **48**

Current system date and time is:

Tue Jan 25 15:40:35 PST 2005

Press ENTER to accept it or specify new ones.

Enter date in MM/DD/YYYY format:

Tue Jan 25 15:40:00 PST 2005

*** Configuration changed!

*** Execute saveconf to save the new values in flash.

DATE - sets the date and date format. For example:

```
[root@APM_Paulo root]# date 012515402005
```

```
Tue Jan 25 15:40:00 PST 2005
```

SETNAMES - sets the hostname, domain name, and primary nameserver's IP address. For example:

```
[root@APM_Paulo root]# setnames
```

Enter the System's Hostname

(max 30 characters) [E2000]: APM_Paulo

Enter the System's Domain Name

(max 60 chars) [localdomain]:

Enter the Primary Nameserver's IP address [none]:

Working from a CLI

```
*** Configuration changed!  
*** Execute saveconf to save the new values in flash.
```

SETNETWORK - sets the Ethernet subinterfaces and VLANs. The example below configures the following devices as follows:

```
eth0  
eth0:1  
eth0:9999  
eth0.2
```

```
[root@APM network]# setnetwork  
Primary Ethernet IP address: (S)tatic, (N)one or  
  (K)eeP current ? [K]: s  
Enter Primary Ethernet IP address: 192.168.48.48  
Enter Primary Ethernet Subnet Mask: 255.255.255.0  
Secondary Ethernet IP address: (S)tatic, (N)one or  
  (K)eeP current ? [K]:  
Subinterface eth0:1 IP address: (S)tatic, (N)one or  
  (K)eeP current ? [K]:  
Subinterface eth0:9999 IP address: (S)tatic, (N)one or  
  (K)eeP current ? [K]:  
Configure more Ethernet Subinterfaces: (Y)es, (N)o or  
  (L)ist ? [N]: 1  
eth0:9999, 199.199.199.199, 255.255.255.252  
Number of Subinterfaces already configured: 1  
Configure more Ethernet Subinterfaces: (Y)es, (N)o or (L)ist ? [N]: y  
Enter the Ethernet number [0-1]: 0  
Enter the Subinterface index [0-9999]: 1  
Subinterface eth0:1 IP address: (S)tatic or (N)one ? [S]:  
Enter Subinterface eth0:1 IP address: 1.1.1.1  
Enter Subinterface eth0:1 Subnet Mask: 255.0.0.0  
Configure more Ethernet Subinterfaces: (Y)es, (N)o or  
  (L)ist ? [N]:  
VLAN eth0.2 IP address: (S)tatic, (N)one or  
  (K)eeP current ? [K]:  
Configure more Ethernet VLANs: (Y)es, (N)o or  
  (L)ist ? [N]: 1  
eth0.2, 2.2.2.2, 255.255.0.0
```

5: Advanced Configuration

```
Number of VLANs already configured: 1
Configure more Ethernet VLANs: (Y)es, (N)o or (L)ist ? [N]:
Enter Ethernet Default Gateway [none]:
```

```
*** Configuration changed!
*** Execute saveconf to save the new values in flash.
Do you want to make these changes effective now (y/n)? y
```

This script creates the configuration file `/etc/network/ifcfg-eth<index>`, which has the same format as `ifcfg-eth0` and `ifcfg-eth1`.

OBS: In this example, index = 0, 0:1, 0:9999 and 0.2

The third option, **(K)eep command**, gives you the option to skip to the next Ethernet interface without changing the configuration of the current interface.

Use **^C** to stop changing interfaces and keep all changes made. If you do not exit with **^C** at the end, the script will ask if you want to make the changes effective now, in which case the script automatically runs `/etc/init.d/networking restart`.

SETNTP - sets the NTP server's IP address. For example:

```
root@APM_Paulo root]# setntp
Enter the NTP server:
*** Configuration changed!
*** Execute saveconf to save the new values in flash.
```

SETSMTP - sets the email server's IP address. For example:

```
[root@APM_Paulo root]# setsmtp
Enter the email (SMTP) server:
*** Configuration changed!
*** Execute saveconf to save the new values in flash.
```

Changing the Escape Sequence

There are two ways to change the escape sequence:

- Locally: From the console session, use option `^E` (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>.
```

Note: 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 ^_
```

Changing the Number of Lines in the SSH Applet

By default, the number of lines used by the memory buffer when a user scrolls the window is set to 1000 lines (Terminal buffer = 1000). You may change this value to suit your needs. Be aware, however, that specifying values greater than 1000 can degrade scroll performance.

To configure the number of lines:

1. Edit the file: **/opt/tomcat/apm/applet.conf**
2. Locate the line and edit as follows:

```
Terminal.buffer = [number of lines]
```
3. Type in **saveconf** to save your configuration.
4. Close and reopen the applet window to make the change effective.

Changing the Session Timeout

The default session timeout value is 60 minutes. To change this value, follow the steps below:

1. Edit the file: **/opt/tomcat/apm/WEB-INF/web.xml**
2. Locate and edit the line:

```
<session-timeout>60</session-timeout>
```
3. To make the change effective, reboot or restart tomcat as follows:

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

Changing the Number of Consoles per Page

The default number of consoles that you can view from the Consoles List form is set to 512. To change this value, edit the **consolesperpage** parameter from the **/var/apm/apm.properties** file, and then restart tomcat.

Enabling Telnet

Telnet is available in the E2000, but disabled by default to avoid security problems. To enable Telnet, follow the steps below:

Changing the ACS/TS Admin Name

1. From **/etc/services**, add the following line:

```
telnet          23/udp
```

2. Edit **/etc/xinetd.conf** as follows:

```
service telnet
{
    flags          = REUSE
    socket_type    = stream
    wait          = no
    user           = root
    server         = /usr/kerberos/sbin/telnetd
    log_on_failure += USERID
}
```

3. Create **/etc/protocols** with the following content:

```
tcp    6    TCP      # transmission control protocol
udp    17   UDP      # user datagram protocol
```

4. To complete the procedure, restart **xinetd** with the following command:

```
/etc/init.d/xinetd.conf restart
```

Note: xinetd services will be available after reboot, since this script is already included in the startup procedure.

Changing the ACS/TS Admin Name

If you want to use another admin name other than root for ACS or TS devices, perform the following steps:

1. Create a new user in the device

Example:

```
adduser myadmin
```

2. Edit the files **/etc/passwd** and **/etc/group** by setting the userid and groupid of the new user to zero (0) and setting the home directory to **/root**.

Example:

```
/etc/passwd
```

5: Advanced Configuration

```
myadmin:.dm7VcWSPBOGI:0:0:Embedix User,,,:/root:/bin/sh
/etc/group
teste:x:0:
```

Each time a connection is made to the ACS or TS device or any of its consoles, the system uses the admin user name and password that is set in the device page. This is true regardless whether the connection is for an upload or for a console session, or which user is logged into the E2000.

If you configure any of the consoles of a device to do remote authentication, ensure that the admin user name and password configured for the device can be authenticated by the remote service.

Setting any of the consoles of a device to do remote authentication does not mean that the device itself will do remote authentication. If you need to (for example when the device needs a configuration upload or when the device console is opened), change the **/etc/pam.conf** file of the device accordingly.

Ethernet Port Configuration

Ethernet port configuration through CLI allows you to set the following modes:

- **0** sets Auto Negotiation
- **0x10** sets Full Duplex
- **0x20** sets 100Mb
- **0x40** sets 10Mb

Therefore:

0x30 sets 100Mb Full Duplex (0x20 + 0x10)

0x50 sets 10Mb Full Duplex (0x40 + 0x10)

To change the speed/duplex settings, follow these steps:

1. `ifconfig ethx down` (once for each interface)
2. `rmmmod eepr100`
3. `insmod eepr100 [debug=1] options=0xXX, 0xYY` (where X=eth0 setting, Y=eth1 setting)
4. `ifconfig ethx <IP> netmask <netmask> up`

To make your settings permanent:

1. Edit the file `/etc/modules.conf` and add the options for the Ethernet driver.

Example:

```
alias eth0 eepro100
options eepro100 options='0x40, 0x30'
```

The first option (0x40) relates to eth0; the second option (0x30) relates to eth1.

2. Execute `saveconf` to save your configuration.

Modem Card Configuration

The AlterPath E2000 is equipped with modem dialing capability, allowing complete out-of-band access to remote console server devices. This section provides basic procedures for configuring the card through a command line interface.

Checking Your Modems

The four modems are detected during bootup. 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 the E2000, 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@E2000 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>**).

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

Viewing the Latest Status for 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@E2000 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
```

Serial Card Configuration

The AlterPath E2000 supports the use of a PCI-based multi-port serial cards. The cards are used to connect the E2000 to external modems. Up to eight serial devices are created if modems are connected to serial ports and the devices are names ttyPS0-ttyPS7

This section provides basic procedures for configuring the card through a command line interface.

How to Detect Modems Connected to the Ports

To detect modem connected to the serial ports, ensure that the modem is powered ON during system boot of the E2000. If one or more modems are connected after the E2000 is running, you must use the following command:

```
/etc/init.d/modem_pool restart
```

Warning: *This command will disconnect all modems that are in use.*

Checking Your Modems

Connect to the E2000 using SSH and login as **root**.

All modems that are powered ON are included automatically in the modem pool. To view which modems are in use or which ones are available, use SSH to connect to the E2000, 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@E2000 root]# check_modem -s  
ttyPS0 Available  
ttyPS1 Available  
ttyPS2 Available  
ttyPS3 Available
```

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@E2000 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
```

How to Define Different Scripts for Each tty Device

The modem chat scripts are located in **/etc/ppp**, and used by **pppd** to initialize the modem and to dial out.

The **/etc/ppp/chat-init** is the default script used for modem initialization and **/etc/ppp/chat-connect** is the default script for modem dial out.

1. To define an init script for a specific port, copy **/etc/ppp/chat-init** as **/etc/ppp/chat-init-*<tty device>***.

Where: *<tty device>* is the port where you want to apply the script.

For example, if **/etc/ppp/chat-init-ttyPS0** is present, then the system uses this file instead of **/etc/ppp/chat-init** to initialize ttyPS0.

2. To define a connect script for a specific port, copy **/etc/ppp/chat-connect** as: **/etc/ppp/chat-connect-*<tty device>***.

For example, if **/etc/ppp/chat-connect-ttyPS0** is present, then the system uses this file instead of **/etc/ppp/chat-connect** to dial out through ttyPS0.

3. Add the new file names in **/etc/files.list**
4. Type in **saveconf** to save your configuration.

Configuring Dial Out and Dial Back

To enable device or console access through dial out or dial back, you must configure the following:

Note: For a complete list of all configuration requirements for Dial Out and Dial Back, see “Dial Up and Dial Back” on page 4-27, Chapter 4: E2000 Web Administration.

For ACS Devices:

Using CLI, create a new user and password from the ACS using the commands:

- **adduser** <ppp_user>
- **passwd** <ppp_user>

Modem Dial Back for ACS

The dial back feature, which is configurable from the web interface, is designed to enable the E2000 to automatically dial to a remote ACS unit should the network fail, and enable the ACS to dial back the connection.

Required CLI configuration

This dial back feature is configured mostly from the web interface (Admin Mode, **Devices > Dial Up**). There are, however, three parameters that you must configure from the CLI:

- From the ACS, create a user by using the Linux command and syntax:
adduser <ppp_user>

Note: This must be the same PPP user configured in the E2000 **Dial Up** form.

- Also from the ACS, set the password for the ppp_user in the ACS using the command and syntax: **passwd** <ppp_user>

Note: This must be the same PPP password configured in the E2000 **Dial Up** form.

- From the E2000, go to `/var/apm/apm.properties` file and add the APM phone number in the parameter: **dial.apm_phone_number**=<phone number>.

Note: The E2000 allows only one phone number for this parameter so that there is a hunt group configured to point to only one phone number.

Optional CLI Configuration

The following parameters (with examples) are OPTIONAL:

From the E2000, edit the file: **/var/apm/apm.properties** to:

- Define the PPP idle timeout (in seconds).
`ppp.idle=600`
- Exclude modems from the modem pool by listing the modems to be excluded.

`modem.pool.exclude=ttypS2 ttypS3`

- Select modems that will never be used for dial-in by listing them as follows:

`modem.pool.out_only=ttypS1 ttypS3`

- Configure timeout to wait for a dial-back call from an ACS:

`modem.pool.dial_in_timeout=30`

If a timeout value is not provided, the E2000 will wait for 60 seconds.

- Define the time (in seconds) in which the E2000 should wait before allocating the modems for dial-in after receiving a confirmation from an ACS that it will call the E2000 back.

`modem.pool.on_hook_time=4`

For external modems:

From the ACS, edit the file **/etc/inittab** and **/etc/pslave.conf** to:

- Remove the control of Portslave over it, and add **mgetty**.

For PCMCIA modem:

From the ACS, copy the file:

/etc/ppp/options.ttyXX

to:

/etc/ppp/options.ttyS(n+1)

Changing the Ports to be Proxied

Where: "n" is the number of the last serial interface of your ACS (*i.e.*, 1 for ACS1, 8 for ACS8, etc).

For PCMCIA modems, no further configuration is required; just insert the modem card and mgetty will open the modem port and wait for the ring.

Changing the Ports to be Proxied

When Forward Proxy (with or without ARP) is enabled for a device, the default proxied ports are 80 and 443. To change the opened ports, perform the following steps:

1. Edit the **property proxyserver.ports** in the **/var/apm/apm.properties** file.
2. Separate the port numbers using commas. There should be no spaces in this line.

Example:

```
proxyserver.ports=80,443,8080
```

NIS Configuration

To use NIS authentication, NIS is selected from the First Time Configuration script. To further control NIS authentication, edit the following configuration file as follows:

File to edit: **/etc/nsswitch.conf**

Format: <database>:<service>[<actions><service>]

Where:	Parameter Definition:
<database>	Available: aliases, ethers, group, hosts, netgroup, network, passwd, protocols, publickey, rpc, services, and shadow.
<service>	Available: nis (use NIS version 2), dns (use Domain Name Service), and files (use the local files).

Where:	Parameter Definition:
<code><actions></code>	this syntax has this format: [<code><status>=<action></code>] WHERE: <code><status></code> = SUCCESS, NOTFOUND, UNAVAIL, or TRYAGAIN <code><action></code> = RETURN or CONTINUE

What the status messages mean:

Status:	Meaning:
SUCCESS	No error occurred and the desired value is returned. The default action for this status is <i>return</i> .
NOT FOUND	The lookup process works, but the needed value was not found. The default action for this status is <i>continue</i> .
UNAVAIL	The service is permanently unavailable.
TRYAGAIN	The service is temporarily unavailable.

User Authentication

To use NIS only to authenticate users, change the lines about `passwd`, `shadow` and `group` in the configuration file (`/etc/nsswitch.conf`) as described below.

The E2000 does not support user authentication against a NIS map and the local file (`/etc/passwd`) at the same time. Either the user is present in the NIS map or in the `passwd` file, but not both. The E2000 will not even allow you to add a user in the local database if the user is already present in the NIS server.

The configuration below enables the system to authenticate NIS users and local users.

Authenticate the user first through the local database and if the user is not found, use NIS.

```
passwd: files compat
shadow: files compat
```

Creating the krb5.keytab for Kerberos Authentication

```
group: files compat

passwd_compat: nis
shadow_compat: nis
group_compat: nis
```

Authenticate the user first through NIS and if the user is not found, use the local database.

```
passwd: compat files
shadow: compat files
group: compat files

passwd_compat: nis
shadow_compat: nis
group_compat: nis
```

Authenticate the user first through NIS, and if the user is not found or the NIS server is down, use the local database.

```
passwd: compat [UNAVAIL=continue TRYAGAIN=continue] files
shadow: compat [UNAVAIL=continue TRYAGAIN=continue] files
group: compat [UNAVAIL=continue TRYAGAIN=coninue] file

passwd_compat: nis
shadow_compat: nis
group_compat: nis
```

Creating the krb5.keytab for Kerberos Authentication

The E2000 supports kerberized networks. Kerberos is a computer network authentication protocol designed for insecure networks based on the key distribution model. It allows individuals communicating over a network to prove their identity to each other while also preventing eavesdropping or replay attacks. It also detects modifications and prevents unauthorized reading.

How Kerberos Works

On a kerberized network, the Kerberos database contains principals and their keys (for users, their keys are derived from their passwords). The Kerberos database also contains keys for all of the network services.

When a user on a kerberized network logs in to their workstation, their *principal* is sent to the Key Distribution Center (*KDC*) as a request for a Ticket Granting Ticket (*TGT*). The login program sends the request (so that it is transparent to the user) or the *kinit* program sends it after the user logs in.

The KDC checks for the *principal* in its database. If the principal is found, the KDC creates a TGT, encrypts it using the user's key, and sends it back to the user. The login program or *kinit* decrypts the *TGT* using the user's key (which it computes from the user's password). The *TGT*, which is set to expire after a certain period of time, is stored in your credentials cache.

An expiration time is set so that a compromised *TGT* can only be used for a certain period of time, usually eight hours (unlike a compromised password, which could be used until changed). The user will not have to re-enter their password until the *TGT* expires or they logout and login again.

When the user needs access to a network service, the client uses the *TGT* to request a ticket from the Ticket Granting Service (*TGS*) which runs on the *KDC*. The *TGS* issues a ticket for the desired service which is then used to authenticate the user.

Creating the *krb5.keytab* in the E2000

The E2000 automatically creates the **krb5.conf**, the file that holds information about KDC addresses and port numbers. The user, however, must create the **/etc/krb5.keytab** file, a binary file that holds the cryptographic keys to validate the Kerberos tickets received.

There are two different ways to get the **krb5.keytab** file into the E2000.

Method 1:

Using SCP, copy the **/etc/krb5.keytab** from the Kerberos Key Distribution Center (KDC), also known as the Kerberos Server.

Method 2:

Connect to the Kerberos database by executing the **kadmin -p <principal>**.

This is an interactive program; it will ask for the password for the principal used to connect to the Kerberos database.

After successful connection, run `ktadd` command for each principal required in order to add its respective cryptographic keys of that principal to the keytab file. Both the client host and the users supposed to be authenticated must have entries in the keytab file.

You can explicitly indicate which file to be used as keytab by using the option `-k`.

For example:

```
ktadd -k /etc/krb5.keytab host/apm.somedomain
ktadd -k /etc/krb5.keytab nestor
ktadd -k /etc/krb5.keytab guest
```

If the desirable principal was not yet added to the Kerberos database, they should be added with `addprinc` command before executing `ktadd`.

For example:

```
addprinc -randkey host/apm.somedomain
addprinc nestor
addprinc guest
```

Active Directory Configuration

To configure the E2000 to use Active Directory for authentication, follow the steps below:

1. During First Time Configuration (see **Chapter 4: Web Configuration**), select **ldap** when prompted for the desired authentication method.
2. Connect to the E2000 using SSH and login as **root**.
3. Configure `/etc/ldap.conf` as follows:

```
host 172.20.98.150
base dc=qalab,dc=cyclades,dc=com,dc=br
binddn cn=Administrator,cn=Users,dc=qalab,
      dc=cyclades,dc=com,dc=br
bindpw qa
pam_login_attribute sAMAccountName
pam_password ad
```

5: Advanced Configuration

- a. On line 3 (see example above), add the lines as shown in **boldface**, using your own values.
 - b. Delete the **uri** statement (already deleted from line 3 in the example) which is used in traditional LDAP, but not needed in Active Directory.
4. Type in **saveconf** to save your configuration.
 5. Reboot the E2000.

Regarding **/etc/ldap.conf**, the host and base items are exactly the same when configuring traditional LDAP.

binddn is the distinguished name (dn) to bind with, and is composed by the common name (cn) plus the distinguished name of the search base, and **bindpw** is the password in the active directory server which corresponds to the common name given in the binddn statement.

pam_login_attribute and **pam_password** must be set to exactly the values shown above, thus informing the active directory server what kind of authentication is taking place.

Disabling HTTP to Use Only HTTPS

The E2000 is configured to allow both HTTP and HTTPS access. To disable HTTP access to allow only HTTPS, perform the steps below:

1. Edit the file: **/usr/conf/httpd-std.conf**
2. Comment the listen directive: **#Listen 80**
3. To make the configuration effective, restart tomcat and apache by first stopping tomcat followed by apache, and then starting apache followed by tomcat:

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

4. Use the **saveconf** command to save the configuration.

Firmware

Adding Firmware

Firmware files (.tgz) are normally downloaded from the web and copied into the E2000 using 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.

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:

Data Type	Definition
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 database.
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 system uses the current username.

If you do not specify a host, then the system creates a backup of the local file.

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

Enabling the Restore Script

Sometimes, the system may not restore a backup database because the restore script is unable to compare the restored version number with the previous version number. When this happens, the database restore is aborted and the system generates an error message.

To enable the restore script, run the following commands::

```
/var/apm/bin/apm_db_cleanup.sh  
/etc/init.d/mysqld restart
```

Managing Log Files

Where Log Files are Archived

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

```
/var/log/containers/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:

5: Advanced Configuration

```
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 path names as part of the file name.

System Recovery Guidelines

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

When performing a recovery procedure, 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.

Changing the Database Configuration

Note: *This configuration procedure is for advanced users only.*

You can change the default configuration values from the properties file (`/var/apm/apm.properties`).

Property Name	Default Property Value	If you change the default property value, ensure that . . .
<code>db.apm</code>	<code>apmdb</code>	The system creates a corresponding database.
<code>db.apm.user</code>	<code>apm</code>	The system creates a corresponding database user.
<code>db.apm.pw</code>	<code>apmdb</code>	
<code>db.apm.max_connections</code>	<code>10</code>	max_connections in <code>my.cnf</code> file is set to greater or equal to db.apm.maxconnectiuons value.
<code>db.apm.host</code>	<code>localhost</code>	the new host is available on the network.

Restoring Your Configuration

If during a configuration upgrade, the system displays an error or failed message, you can check the log file (`/var/log/conf-V_[version number].log`) and decide whether to restore the original configuration.

For example, if you are upgrading your configuration from `V_1.2.1` to `1.3.0`, then the log file to check is: `/var/log/conf-V_1.3.0.log`

To restore the previous configuration:

```
restconf config.tgz.old
```

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.

5: Advanced Configuration

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:

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:

Parameter	Description
Country Name (2-letter code) [AU]:	The 2-letter country code.
State or Province Name (full name) [Some-State]:	The full name (not the code) of the state.
Locality Name (e.g., city) []:	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.

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.

3. Upon receipt, install the certificate

Once the CSR is approved, the CA sends a certificate (*e.g.*, `jcrtfile.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 jcrtfile.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

5: Advanced Configuration

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. 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.

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, TACACS+, Kerberos, LDAP, Active Directory, 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/>

Supported AlterPath KVM/net Version: 1.1.0 and above.

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
```

Glossary

Authentication	The process by which a user's identity is checked within the network to ensure that the user has access to the requested resources.
ARP	Address Resolution Protocol. An ARP protocol in which a router masks its identity and sends routing packets to the requesting host. A proxy ARP can minimize the bandwidth on slower WAN links. See also Proxy ARP .
Basic In/Out System (BIOS)	Chips on the motherboard of a computer contain read only memory instructions that are used to start up a computer. The operating system of a PC also makes use of BIOS instructions and settings to access hardware components such as a disk drive. Some BIOS/CMOS settings can be set to scan for viruses, causing problems for some installation programs.
Baud Rate	The baud rate is a measure of the number of symbols (characters) transmitted per unit of time. Each symbol will normally consist of a number of bits, so the baud rate will only be the same as the bit rate when there is one bit per symbol. The term originated as a measure for the transmission of telegraph characters. It has little application today except in terms of modem operation. It is recommended that all data rates are referred to in bps, rather than baud (which is easy to misunderstand). Additionally, baud rate cannot be equated to bandwidth unless the number of bits per symbol is known.
Boot	To start a computer so that it is ready to run programs for the user. A PC can be booted either by turning its power on, (Cold Boot) or by pressing Ctrl+Alt+Del (Warm Boot).
Break Signal	A break signal is generated in an RS-232 serial line by keeping the line in zero for longer than a character time. Breaks at a serial console port are interpreted by Sun servers as a signal to suspend operation and switch to monitor mode.

Checksum	A computed value which depends on the contents of a block of data and which is transmitted or stored along with the data in order to detect corruption of the data. The receiving system recomputes the checksum based upon the received data and compares this value with the one sent with the data. If the two values are the same, the receiver has some confidence that the data was received correctly.
Cluster	A cluster is a group of one or more computers working as a group to execute a certain task. From the user standpoint, a cluster acts as a large computer system.
Console	Terminal used to configure network devices at boot (start-up) time. Also used to refer to the keyboard, video and mouse user interface to a server.
Console Port	Most of the equipment in a data center (servers, routers, switches, UPS, PBX, etc.) has a serial console port for out-of-band management purposes.
DHCP	<p><i>Dynamic Host Configuration Protocol.</i> A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.</p> <p>DHCP enables individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.</p>
DNS Server	<p><i>Domain Name Server.</i> The computer you use to access the DNS to allow you to contact other computers on the Internet. The server keeps a database of host computers and their IP addresses.</p>

Domain Name

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. A given machine may have more than one Domain Name but a given Domain Name points to only one machine. For example, the domain names: matisse.net, mail.matisse.net, workshop.matisse.net can all refer to the same machine, but each domain name can refer to no more than one machine. Usually, all of the machines on a given Network will have the same thing as the right-hand portion of their Domain Names (matisse.net in the examples above). It is also possible for a Domain Name to exist but not be connected to an actual machine. This is often done so that a group or business can have an Internet e-mail address without having to establish a real Internet site. In these cases, some real Internet machine must handle the mail on behalf of the listed Domain Name.

Escape Sequence

A sequence of special characters that sends a command to a device or program. Typically, an escape sequence begins with an escape character, but this is not universally true.

An escape sequence is commonly used when the computer and the peripheral have only a single channel in which to send information back and forth. If the device in question is "dumb" and can only do one thing with the information being sent to it (for instance, print it) then there is no need for an escape sequence. However most devices have more than one capability, and thus need some way to tell data from commands.

Ethernet

A LAN cable-and-access protocol that uses twisted-pair or coaxial cables and CSMA/CD (Carrier Sense Multiple Access with Collision Detection), a method for sharing devices over a common medium. Ethernet runs at 10 Mbps; Fast Ethernet runs at 100 Mbps. Ethernet is the most common type of LAN.

Flash

Flash refers to a type of memory that can be erased and reprogrammed in units of memory known as blocks rather than one byte at a time; thus, making updating to memory easier.

Flow Control

A method of controlling the amount of data that two devices exchange. In data communications, flow control prevents one modem from "flooding" the other with data. If data comes in faster than it can be processed, the receiving side stores the data in a buffer. When the buffer is nearly full, the receiving side signals the sending side to stop until the buffer has space again. Between hardware (such as your modem and your computer), hardware flow control is used; between modems, software flow control is used.

GRUB

Grand Unified Boot Loader. GRUB is a boot loader that is capable of booting different OS types, some of them via network. (A boot loader is a program that resides in the starting sectors of a disk, for example, the MBR (Master Boot Record) of the hard disk. After testing the system during bootup, the BIOS (Basic Input/Output System) transfers control to the MBR if the system is set to be booted from there. Then the program residing in the MBR gets executed. This program is called the boot loader. Its duty is to transfer control to the operating system, which will then proceed with the boot process.)

Hot-Swap

Ability to remove and add hardware to a computer system without powering off the system.

ICMP

Internet Control Message Protocol is an Internet protocol sent in response to errors in TCP/IP messages. It is an error reporting protocol between a host and a gateway. ICMP uses Internet Protocol (IP) datagrams (or *packets*), but the messages are processed by the IP software and are not directly apparent to the application user.

In-band Network

In a computer network, when the management data is

Management	accessed using the same network that carries the data, this is called “in-band management.”
IP Address	<p>A 32-bit address assigned to hosts using TCP/IP. It belongs to one of five classes (A-E) and is expressed as 4 octets separated by periods formatted as dotted decimals.</p> <p>Each address has a network number, an optional sub network number and a host number. The first two numbers are used for routing, while the host number addresses an individual host within the network or sub network. A subnet mask is used to extract network and sub network information from the IP address.</p>
ISDN	A set of communications standards allowing a single wire or optical fibre to carry voice, digital network services and video. ISDN is intended to eventually replace the plain old telephone system.
Kerberos	<p>Kerberos was created by MIT as a solution to network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection.</p> <p>After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.</p>
KVM	Keyboard, video and mouse interface to a server.
LDAP	<p><i>Lightweight Directory Access Protocol.</i> A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet.</p> <p>LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.</p>

MAC *Medium Access Control*. Internationally unique hardware identification address that is assigned to the NIC (Network Interface Card) which interfaces the node to the LAN.

MTU Short for *Maximum Transmission Unit*, the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent.

Every network has a different MTU, which is set by the network administrator. On Windows, you can set the MTU of your machine. This defines the maximum size of the packets sent from your computer onto the network. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

Trial and error is the only sure way of finding the optimal MTU, but there are some guidelines that can help. For example, the MTU of many PPP connections is 576, so if you connect to the Internet via PPP, you might want to set your machine's MTU to 576 too. Most Ethernet networks, on the other hand, have an MTU of 1500.

Network Mask A 32-bit number used to group IP addresses together or to indicate the range of IP addresses on a single IP network/subnet/supernet. There is a group of addresses assigned to each network segment. For example, the mask 255.255.255.0 groups together 254 IP addresses. If we have, as another example, a sub-network 192.168.16.64 with mask 255.255.255.224, the addresses we may assign to computers on the sub-network are 192.168.16.65 to 192.168.16.94, with a broadcast address of 192.168.16.95.

A number used by software to separate the local subnet address from the rest of a given Internet protocol address

Network masks divide IP addresses into two parts (network address and address of a particular host within the network). Mask have the same form as IP addresses (i.e. 255.255.255.0), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. The primary function of a subnet mask is to define the number of IP hosts that participate in an IP subnet. Computers in the same IP subnet should not require a router for network communication.

NTP

Network Time Protocol. A standard for synchronizing your system clock with the "true time", defined as the average of many high-accuracy clocks around the world.

Parity

In serial communications, the parity bit is used in a simple error detection algorithm. As a stream of data bits is formed, an extra bit, called the parity bit, is added. This bit is set on (1) or off (0), depending on the serial communications parameters set in the UART chip.

The following lists the available parity parameters and their meanings:

Odd - Parity bit set so that there is an odd number of 1 bits

Even - Parity bit set so that there is an even number of 1 bits

None - Parity bit is ignored, value is indeterminate

PCMCIA

Personal Computer Memory Card International Association. An organization consisting of some 500 companies that has developed a standard for small, credit card-sized devices, called PC Cards. Originally designed for adding memory to portable computers, the PCMCIA standard has been expanded several times and is now suitable for many types of devices including network cards (NICs).

The PCMCIA 2.1 Standard was published in 1993. As a result, PC users can be assured of standard attachments for any peripheral device that follows the standard.

Port

A port is a 16-bit number (the allowed range being 1 through 65535) used by the TCP and UDP protocols at the transport layer. Ports are used to address applications (services) that run on a computer. If there was only a single network application running on the computer, there would be no need for port numbers and the IP address only would suffice for addressing services. However, several applications may run at once on a particular computer and we need to differentiate among them. This is what port numbers are used for. Thus, a port number may be seen as an address of an application within the computer.

PPP

Point-to-Point Protocol. This protocol is a way to connect your computer to the Internet over telephone lines. PPP is replacing an older protocol, SLIP, as it is more stable and has more error-checking features.

PPP has been a widely-used Internet standard for sending datagrams over a communications link. The PPP standard is described in RFC 1661 by the Point-to-Point Working Group of the Internet Engineering Task Force (IETF). PPP is commonly used when remote computers call an Internet service provider (ISP) or a corporate server that is configured to receive incoming calls.

Profile

Usage setup of the ACS either as a Console Access Server (CAS), a Terminal Server, or a Remote Access Server.

Proxy ARP

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway.

RADIUS	<i>Remote Authentication Dial-In User Service</i> is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.
RFC	A document that defines the accepted or proposed Internet standards or standards of practice. The acceptance of a document as an RFC is governed by the IETF (Internet Engineering Task Force). RFCs begin life as Internet-Drafts, which may be written by anyone. The IETF decides which Internet-Drafts become RFCs.
Root Access	<i>Root</i> is the term for a very highly privileged administrative user (particularly in unix environments). When an ISP grants you root access, it means you will have full control of the server. With full control, you will be able to install any software and access any file on that server.
Routing Table	The Routing Table defines which interface should transmit an IP packet based on destination IP information.
Secure Shell (SSH)	SSH has the same functionality as Telnet (see definition for Telnet), but adds security by encrypting data before sending it through the network.
Server Farm	A collection of servers running in the same location (see Cluster).
SMTP	Simple Mail Transfer Protocol. Specifies the format of messages that an SMTP client on one computer can use to send electronic mail to an SMTP server on another computer.
SSH (Secure Shell)	A protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server.

- Stop Bit** A bit which signals the end of a unit of transmission on a serial line. A stop bit may be transmitted after the end of each byte or character.
- Subnet Mask** A bit mask used to select bits from an Internet address for subnet addressing. Also known as Address Mask.
- STTY** Set the options for a terminal device interface.
- This command prints information about your terminal settings. The information printed is the same as if you had typed stty while interacting with a shell.
- The stty utility sets or reports on terminal I/O characteristics for the device that is its standard input. Without options or operands specified, it reports the settings of certain characteristics, usually those that differ from implementation-dependent defaults. Otherwise, it modifies the terminal state according to the specified operands.
- TACACS** *Terminal Access Controller Access Control System.* Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.
- TACACS+** *Terminal Access Controller Access Control System Plus.* A protocol that provides remote access authentication, authorization, and related accounting and logging services, used by Cisco Systems.
- TCP Keep-Alive Interval** The time interval between the periodic polling of all inactive TCP/IP connections, checking that the client processes really are still there. After a certain period of inactivity on an established connection, the server's TCP/IP software will begin to send test packets to the client, which must be acknowledged. After a preset number of 'probe' packets has

been ignored by the client, the server assumes the worst and the connection is closed.

The keepalive timer provides the capability to know if the client's host has either crashed and is down or crashed and rebooted.

Telnet

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console

Terminal Server

A terminal server has one Ethernet LAN port and many RS-232 serial ports. It is used to connect many terminals to the network. Because they have the same physical interfaces, terminal servers are sometimes used as console access servers.

TTY

1. In Unix, refers to any terminal; sometimes used to refer to the particular terminal controlling a given job (it is also the name of a Unix command which outputs the name of the current controlling terminal). 2. Also in Unix, any serial port, whether or not the device connected to it is a terminal; so called because under Unix such devices have names of the form **tty**.

TFTP

Abbreviation of Trivial File Transfer Protocol, a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features. Servers often use it to boot diskless workstations, X-terminals, and routers.

UDP

User Datagram Protocol uses a special type of packet called a datagram. Datagrams do not require a response; they are one way only (connectionless). Datagrams are usually used for streaming media because an occasional packet loss will not affect the final product of the transmission.

U Rack Height Unit

A standard computer rack has an internal width of 17 inches. Rack space on a standard rack is measured in units of height (U). One U is 1.75 inches. A device that has a height of 3.5 inches takes 2U of rack space.

This page has been intentionally left blank.