AlterPath™ Manager E2000 and 2500 Installation, Configuration, and User's Guide

Software Version 1.3.1

Cyclades Corporation
3541 Gateway Boulevard
Fremont, CA 94538 USA
1.888.CYCLADES (292.5233)
1.510.771.6100
1.510.771.6200 (fax)
http://www.cyclades.com

Release Date: September 2005
Part Number: PAC0344

Contents

Tables

Figures

Procedures

Before You Begin

The AlterPath Manager serves as the command and control center for the AlterPath system of products. It provides consolidation of control, added security, and flexibility to very large server and server management configurations.

This manual provides the information needed for you or your system administrator to install, configure, administer, and operate the AlterPath E2000 and 2500 as well as to guide you in the operation of these products.

Note: This manual frequently refers to the AlterPath Manager E2000 2500 as “AlterPath Manager” or as “APM**.”** If a reference is being made to a specific model of AlterPath Manager, references such as “AlterPath Manager E2000”and **“**AlterPath Manager 2500” are used.

Audience

This document is designed for system administrators and regular users of the AlterPath Manager E2000 and 2500. Users are expected to have basic knowledge of using a graphical user interface such as MicroSoft™ Windows.

Document Organization

The document contains the following chapters:

Chapter Number and Title	Description
1: Introduction	Provides an overview of the features of the AlterPath Manager along with necessary prerequisite information for understanding the rest of the information in this guide.
2: AlterPath Manager Installation	Explains the procedure for installing the AlterPath Manager and preparing it for web configuration and access.
3: User Level Web Access	Explains the standard user interface. This chapter is particularly designed for regular users (as distinguished from system administrators) of the AlterPath Manager. It highlights such procedures as connecting to a console, dealing with alarms, and other system tracking and management procedures
4: Configuration and 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.

Chapter Number and Title	Description
5: Advanced Configuration	Covers first time configuration. Explains the serial console interface (Linux shell) and the command line interface (CLI) functionality, as well as some advanced setup procedures.
Appendix A: Technical Specifications	Lists hardware, software, electrical, and environmental specifications and requirements.
Appendix B: ACS Modem Configuration	Covers special considerations for setting up a modem on an ACS for communication between an ACS and the AlterPath Manager.
Appendix C: DLS Activation	Covers special considerations for adding DLS activation.
Glossary	Defines terms used in this book.

Typographic and Other Conventions

The following table describes the typographic conventions used in Cyclades manuals.

Table P-1: Typographic Conventions

Typeface	Meaning	Example
Links	Hypertext links or URLs	Go to: http://www.cyclades.com
Emphasis	Titles, emphasized or new words or terms	See the *AlterPath Manager Quick Start.*

Table P-1: Typographic Conventions

Typeface	Meaning	Example
`Filename or Command`	Names of commands, files, and directories; onscreen computer output.	Edit the `pslave.conf` file.
`User input`	What you type in an example, compared to what the computer displays	[APM #] **`ifconfig eth0`**

The following table describes other terms and conventions.

Table P-2: Other Terms and Conventions

Term or Convention	Meaning	Examples
Hot keys	• When hot keys are shown, a plus (+) appears between two keys that must be pressed at the same time, and a space appears between two keys that must be pressed sequentially.	• `Ctrl+k p` entered while the user is connected to a KVM port brings up an IPDU power management screen. `Ctrl` and `k` must be pressed at the same time followed by `p`. • `Ctrl+Shift+i` entered while the user is connected to a serial port brings up the IPMI power management utility. The `Ctrl` key and the `Shift` and `i` keys must be pressed at the same time.

Table P-2: Other Terms and Conventions

Term or Convention	Meaning	Examples
Navigation shortcuts	Shortcuts use the “greater than” symbol (>) to indicate how to navigate to Web Manager forms.	Go to Configuration>KVM> General >IP Users in Expert mode.

Table P-3: Naming conventions

Name	Convention
Administrator	Also referred to as the *Admin User*. The system administrator of the AlterPath Manager who has the authority to configure and manage the AlterPath Manager.
APM	AlterPath Manager. Synonymous with E2000 and 2500 “APM” is often used in the Command Line Interface.
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.

Table P-3: Naming conventions

Name	Convention
Form Names	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. The most commonly used form names are List forms and Detail forms. The configuration forms of the AlterPath Manager (*i.e.*, Devices, Consoles, Users, Alarm Trigger) use the two types of forms. Examples: Console List form; Console Detail form.
Regular User	Refers to one who uses the AlterPath Manager application as a regular user (*i.e.*, the web management interface is on "Access" mode, not "Admin" mode) even though the user may be a system administrator
Select	To *select* is the same as to *click your mouse*.

Linux Shell Syntax

While this manual is primarily designd for using the E2000 and 2500 web interface, some special features show you how to configure the AlterPath Manager using the *Serial Console Interface* . The Serial Console 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.

Table P-4: Linux Shell Syntax

Typeface	Meaning	Example
Brackets ([])	Indicate that the parameter inside them is optional. The command will still 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.	`iptables [-ADC] chain rule-specification [options]`
Ellipses (. . .)	Indicate that the latest parameter can be repeated as many times as needed. Usually this is used to describe a list of subjects.	`ls [OPTION]... [FILE]...`
Vertical Line, or Pipe (|)	One of the parameters separated by this character should be used in the command.	`netstat {--statistics|-s} [--tcp|-t] [--udp|-u] [--raw|-w]`

Table P-4: Linux Shell Syntax

Typeface	Meaning	Example
`<text>`	Text enclosed in greater than or less than symbols (or angle brackets) is variable text that is to be substituted in a specific command line.	`add user <username>`

`Spacing and Separators`	Lists will not normally have spaces between the items, but will have commas, hyphens, or semicolons as separators.	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>]...`

Additional Resources

Cyclades Technical Training Available

Cyclades offers a suite of technical courses to increase your knowledge of the AlterPath Manager.

- AlterPath Manager I: Accessing and Monitoring Your out-of-band Infrastructure.
- AlterPath Manager II: Configuring and Administering Your out-of-band infrastructure.

To learn more about Cyclades Technical Training Center and offerings, please visit our website at www.cyclades.com/training, call us at 1-888-292-5233, or send an email to training@cyclades.com.

Cyclades Firmware Upgrades

Cyclades offers periodic firmware upgrades for the AlterPath Manager E2000 and AlterPath Manager 2500. These upgrades are available free of charge to current Cyclades customers. Visit http://www.cyclades.com/support/downloads to download the latest firmware. See “Firmware Upgrade” on page 341 for instructions on upgrading the firmware on your AlterPath Manager.

Chapter 1
Introduction

The AlterPath Manager E2000 and 2500are feature-rich, out-of-band (OOB) managers 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 regular user of the APM E2000 and APM 2500 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 APM 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 APM 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 APM and its users.

Connectivity and Capacity

The E2000 allows you to configure 2048 devices, 4096 console ports and maintain 256 Data Logging Sessions (DLS) or simultaneous connections to consoles and devices. You can perform firmware upgrades on 256 separate console management devices. The E2000 supports up to 256 simultaneously connected users, and it allows multi-user access to each port.

Figure 1-1: APM E2000, Front View

The port connections, power connection, and power switch of the E2000 are shown in Figure 1-2.

Note: On some APM hardware, Eth0 is labeled “Eth1,” and Eth1 is labeled as “Eth2.”

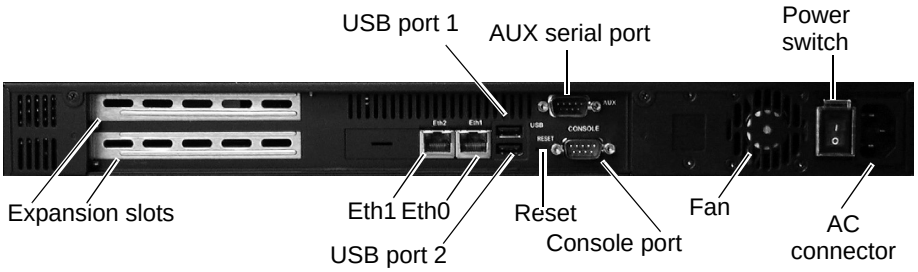

Figure 1-2: APM E2000, Back View

The AlterPath 2500 has a base DLS or simultaneous connection capacity of 64. This can be upgraded to up to 512 DLS connections. The APM 2500 is also available with additional DLS connection capacity at the time of initial purchase. For details abourt DLS capacity, refer to *Appendix C, “DLS Activation.”*

The LCD control panel, power on/reset, and power off buttons are shown in Figure 1-3.

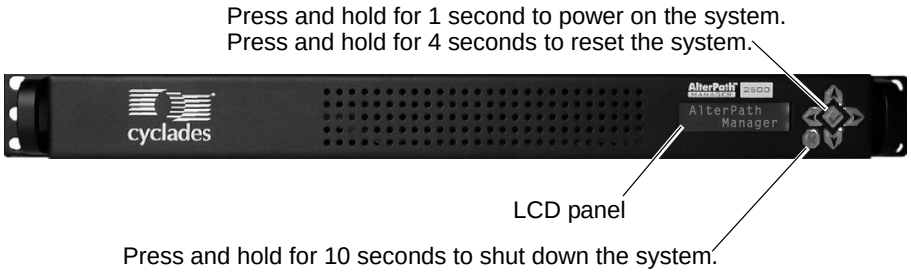

Figure 1-3: APM 2500, Front View

The port connections, power switch and power connector of the APM 2500 are shown in Figure 1-4.

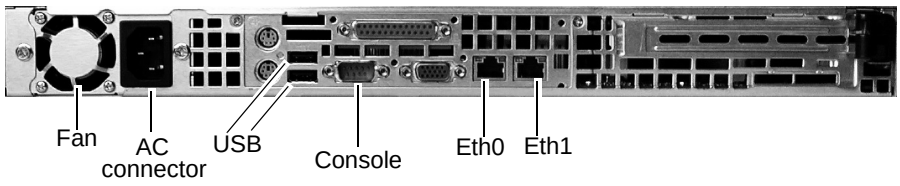

Figure 1-4: APM 2500, Back View

Key Features

The key features of AlterPath Manager E2000 and 2500 are:

Single Point Security Gateway

The AlterPath Manager has been designed such that communication between users and the management network must pass through a single point of access (the AlterPath Manager) 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 AlterPath Manager. For all users who access the console ports, the AlterPath Manager provides the following authentication methods: local database, RADIUS, TACACS+, LDAP, Kerberos, NIS, and Active Directory.

Consolidated Views and Console Access

From the AlterPath Manager 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.

Centralized Data Logging System

The APM E2000/2500 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. Data logging will work with permanently connected devices on Console Servers, Terminal Servers, and OnSite serial ports.

The console log capacity is 20GB, which is about 80MB for each of the APM E2000's 256 maximum possible concurrent data logging sessions. The secure online/offline storage ensures availability of all important console messages.

The APM 2500 has a base Data Logging Session (DLS) capacity of 64. This capacity can be expanded (through a DLS feature activation option from Cyclades) to up to 512 DLSs for the APM 2500. The APM 2500 is also available at the time of purchase, with additional, installable DLS activation.

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

Log File Compression and Rotation

The system logger automatically saves the current log file after a certain point in time, 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.

The administrator has the option to move the saved log file(s) to another server for archiving.

Prioritized Triggers & Alarms

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

The APM E2000/2500 event handling feature enables the system to identify possible issues and alert the user. As the APM 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 APM 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 AlterPath Manager 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 AlterPath Manager 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.

Note: Modems are not supported on the APM 2500.

Dial Back Support

The AlterPath Manager 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 AlterPath Manager to initiate a call to a remote AlterPath ACS unit, and then have the ACS dial back the connection using a predefined number.

Multiport Ethernet

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

Note: Additional Ethernet cards are not supported on the APM 2500.

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

The Ethernet hardware has commands to control the link speed and duplex supported on each interface.

Enhanced Ethernet Port Configuration

There is a script named setethernet that is invoked automatically along with the other initial APM configuration the first time the APM is run.The setethernet script can also be run by the administrator manually from the console at any time.

The *setethernet* script allows the configuration of the Ethernet interface. The following parameters can be set:

- Auto-negotiation mode
- 10MBps full duplex
- 10MBps half duplex
- 100MBps full duplex
- 100MBps half duplex

- 1000MBps full duplex
- 1000MBps half duplex

Health Monitoring

This feature allows enables the AlterPath Manager 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 its 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 AlterPath Manager to recognize the current configuration of a Cyclades TS, ACS, or KVM/net and, through the use of a wizard, auto populate the console parameters based on the values used by the Cyclades TS, ACS, or KVM/net.

For users who already have TS/ACS and/or KVM/net 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 AlterPath Manager 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 AlterPath Manager.

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

Support for OnSite

The AlterPath OnSite is a compact device that has serial console ports like an ACS and KVM ports like a KVM/net. The AlterPath Manager supports viewing of ACS-based consoles as well as Keyboard-Video-Mouse-based consoles through the use of an AlterPath OnSite installed in the network.

Support for IPMI

The AlterPath Manager 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 AlterPath Manager users information that allow power control of servers, recovery, and asset tracking.

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

Note: IPMI is a paid-for option for AlterPath Manager users. The feature is enabled only for users who have purchased the option.

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.

Backup, Restore, and Replicate User Data

This feature allows users to create a backup of the AlterPath Manager configuration, data, and log 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 AlterPath Manager is designed such that any number of change management procedures can be configured through the AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager can provide you with a command line interface by making a regular Secure Shell connection to the AlterPath Manager.

CLI is one of two user interfaces (the other is the web interface) available to AlterPath Manager users. The CLI is also used for First Time Configuration and system recovery procedures.

Interoperability, Integration, and Compatibility

APM E2000 and 2500 Database Compatibility

Each AlterPath Manager model can migrate, backup, and restore its database to or from any other AlterPath Manager model.

Interoperability with Routers and Ethernet Switches

The built-in Ethernet ports on the AlterPath 2500 is fully compatible with the following leading manufacturer's routers and Ethernet switches:

- Cisco®
- Juniper®
- Nortel®

The following features are supported by the built-in Ethernet ports:

- 10/100 Base T Ethernet full and half duplex
- Gigabit Ethernet full and half duplex
- Autosensing
- Fully compatible configurability
  - 10/100/1000 Megabit auto sense
  - Fixed 10 Megabit
  - Fixed 100 Megabit
  - Fixed 1000 Megabit (Gigabit)

Note: Gigabit Ethernet is available on the APM 2500 only.

Interoperability with Cyclades Devices

The APM firmware 1.3.1 interoperates with the latest versions of the AlterPath Console Server, the AlterPath KVM/net (configuration only), the AlterPath Terminal Server, and the AlterPath OnSite.

Interoperability and Compatibility with Modem Vendors

The AlterPath Manager's serial port(s) work with the following external modem manufacture's products that provide encryption within the modem setup process:

- Hayes™
- Motorola®
- US Robotics®

The AlterPath Manager supports dial in, dial out, and dial back capability through the following:

- PCI modem
- built-in serial card (required to connect external modems supporting encryption)

The APM E2000's serial port, Ethernet card, and modem card are all supported in the APM 2500.

Deploying the AlterPath Manager

There are two typical ways (or topologies) in which the AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager user who needs to access console ports in the TS and ACS boxes must pass through the AlterPath Manager, this is the most secure way to deploy the AlterPath Manager (see Figure 1-5).

Single Network Topology

In a single network topology, the AlterPath Manager is connected to only one network, and the AlterPath Manager 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 AlterPath Manager is already controlling access to the ports. In a single network configuration, a Virtual Local Area Network (VLAN) configuration is recommended (see Figure 1-6).

Private Network Diagram

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

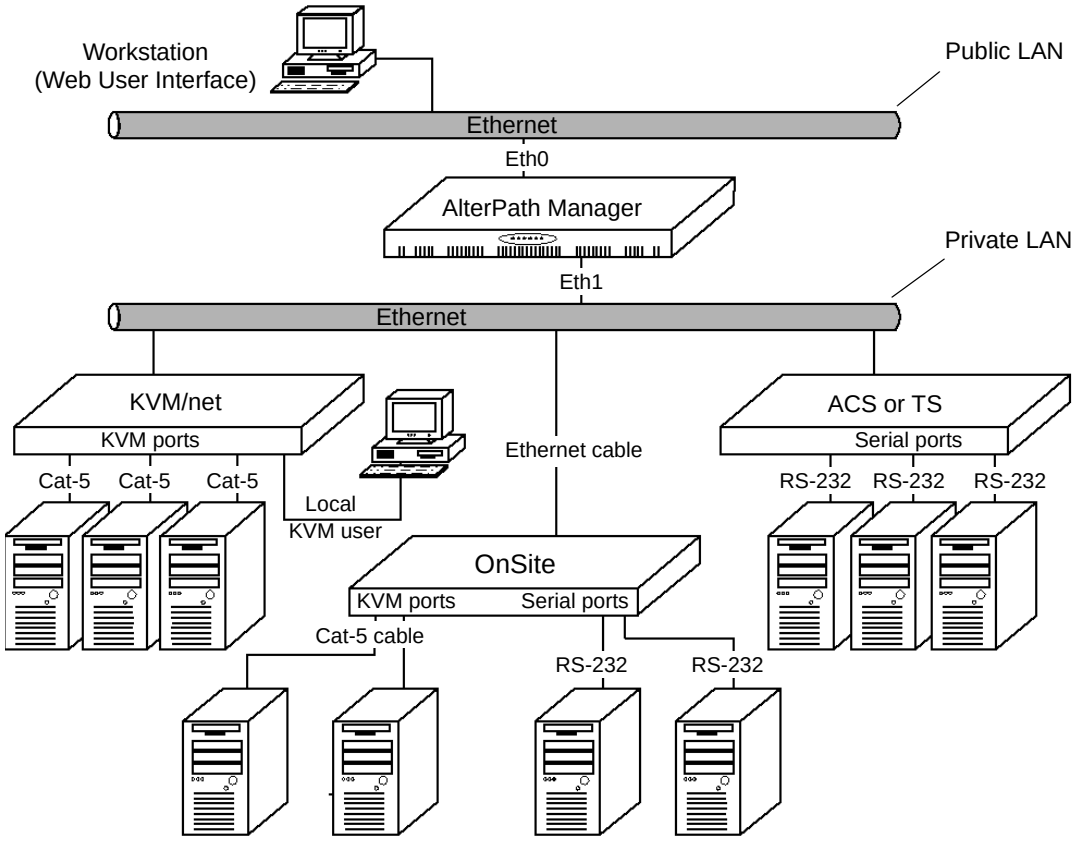

Figure 1-5: Private Network Diagram

Single Network Diagram

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

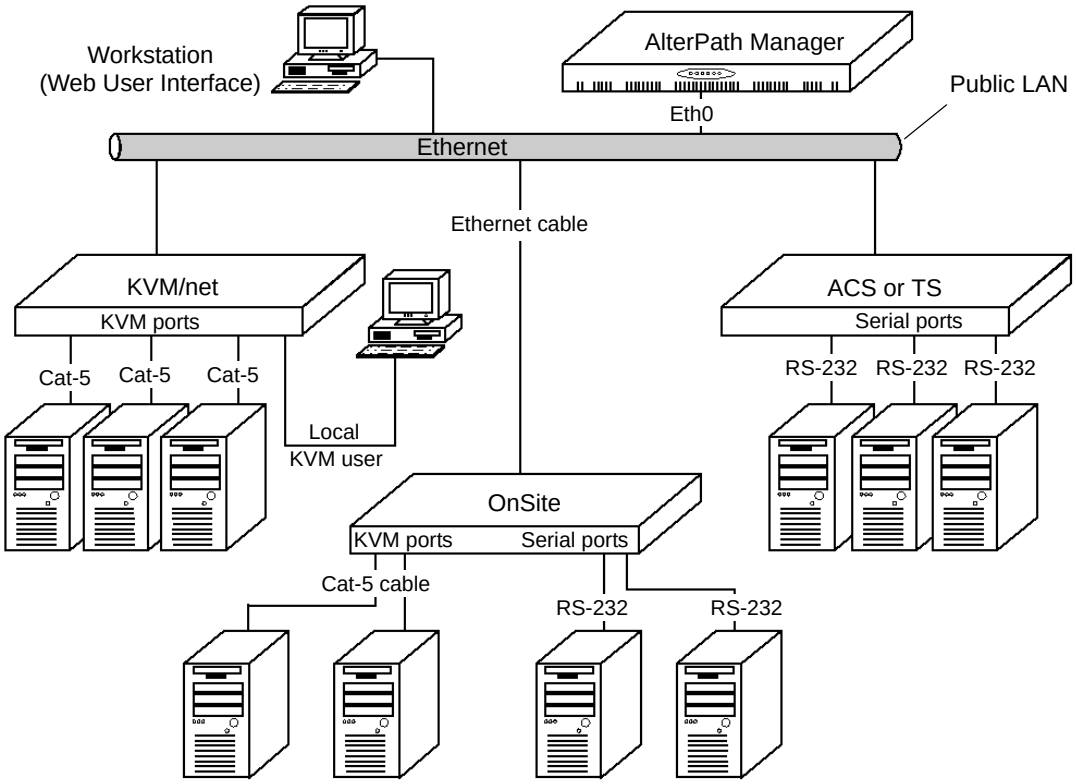

Figure 1-6: Single Network Diagram

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. In the network, you can install a KVM/net with 16 or 32 KVM ports (i.e., AlterPath KVM/net 16 or AlterPath KVM/net 32).

Typical Configuration of AlterPath Manager and KVM

The configuration below shows the AlterPath Manager 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.

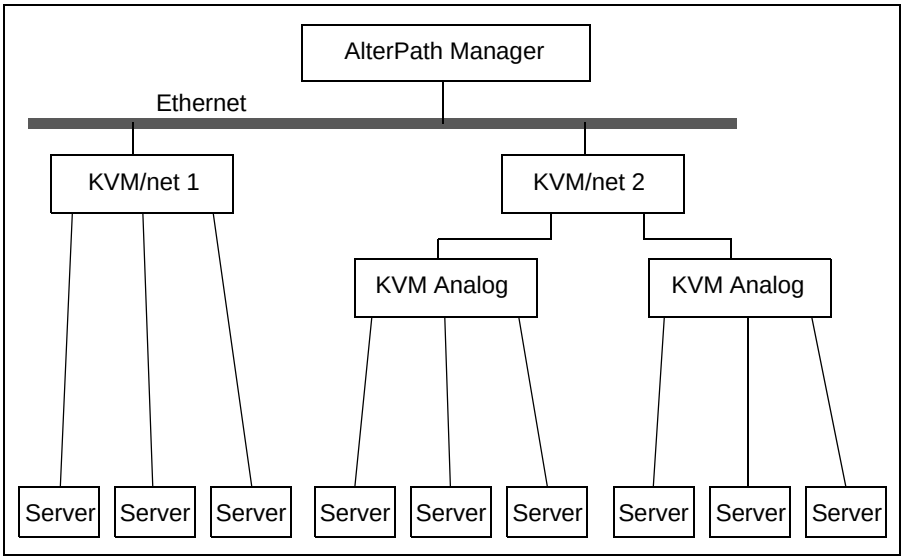

Figure 1-7: Configuration Example of APM and KVM/net

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 KVM/net 2 is a 16-port device and the two analog switches are also 16-port devices, then KVM/net 2 will have 44 ports available to the user; 32 ports from the two analog switches and 12 ports from KVM/net 2. The four ports in 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) function in the same manner as they do for serial console ports. Health Monitoring consists 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.

AlterPath Manager 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.

OnSite Support

Starting with Software version 1.3.1, the AlterPath Manager supports the AlterPath OnSite. The OnSite is a single, compact, and powerful AlterPath product that has both serial and KVM ports. The OnSite can be accessed through a terminal, through the ethernet, through a modem, or through your AlterPath Manager.

The AlterPath Manager allows you serial port console access to any computer whose serial port is connected to and configured on an associated OnSite. The AlterPath Manager also allows you KVM port access to any computer whose KVM port is connected to and configured on an associated OnSite. The AlterPath Manager can even provide both types of access to a single computer if both types of access are configured on the associated OnSite.

Example Configuration of an APM and an OnSite

The following configuration diagram shows an example of an APM connected to an OnSite with KVM servers and console servers. One server can be accessed through both types of connection.

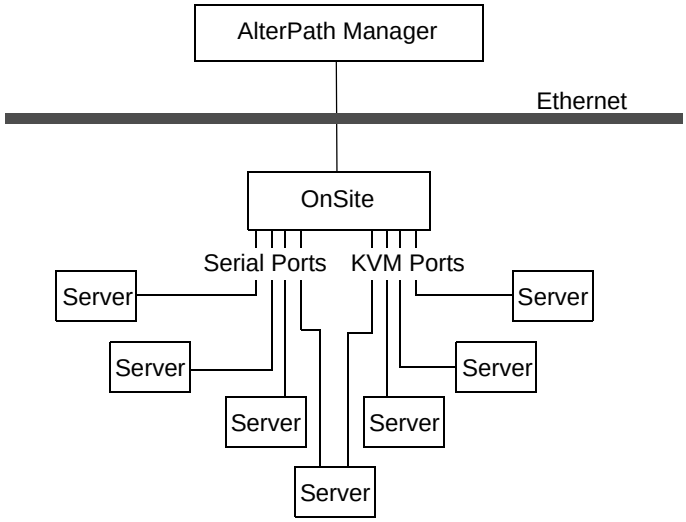

Figure 1-8: Example of an OnSite accessed by an APM

Chapter 2
AlterPath Manager Installation

This section discusses the procedures and requirements for installing the AlterPath Manager E2000 and 2500. The section is organized as follows:

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

Product Installation Checklist

Your AlterPath Manager E2000 and 2500 are shipped with the components as described by the following table:

Check	Item	Part Number	Description	Purpose
☐		PAC0266	Documentation CD	CD with complete documentation for all AlterPathManager models, as well as documentation for other products that can be used with the APM

Check	Item	Part Number	Description	Purpose
☐		PAC0255	Quick Start Guide	A quick installation and configuration guide to get you started with your APM right away
☐		See below for country-specific part numbers.	Power cable	Main power cable for AlterPath Manager E2000 and 2500
		CAB0010	Power cable, USA	
		CAB0037	Power cable, Europe	
		CAB0056	Power cable, UK	
		CAB0055	Power cable, Australia	
		CAB0278	Power cable, Japan	
☐		CAB0036	Cable, crossover DB-9 female to RJ-45 6 ft.	Can be used with AUX port, ACS and TS serial ports.

Check	Item	Part Number	Description	Purpose
☐		HAR0550	Mounting Kit Mounting brackets, necessary screws for APM E2000	Hardware for rack mounting the AlterPath Manager E2000.
☐		HAR0017 HAR0018	Mounting rail kit Mounting brackets, screws for APM 2500	Hardware for rack mounting the AlterPath Manager 2500. Note: The APM 2500 is furnished with the mounting brackets (ears) already attached to it.
☐		CAB0041	Cable, 4-foot DB-9 female to DB-9 female null modem cable for APM E2000	Cable for connection from the APM console port to a serial terminal
☐		CAB0286	Cable, 6-foot DB-9 female to DB-9 female null modem, for APM 2500	Cable for connection from the APM console port to a serial terminal

▼ *To Rack Mount and Connect the AlterPath Manager*

To rack-mount and connect the AlterPath Manager 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 AlterPath Manager in a secure position.
3. Refer to “Safety Considerations When Rack Mounting” on page 22 of this chapter to ensure safety.
4. Plug the power cable into the AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager; and connect the other end to your PC’s available COM port.

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

Note: See “To Configure the COM Port Connection and Log In” on page 23.

You can obtain the latest update to HyperTerminal from:

http://www.hilgraeve.com/htpe/download.html

7. Connect Switch or Hub to PC and the AlterPath Manager.

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

Safety Considerations When Rack Mounting

When rack-mounting the AlterPath Manager, consider the following:

Operating temperature

The manufacturer’s recommended operating temperature for the AlterPath Manager is 50° to 95°F (10°C to 35°C).

Elevated operating ambient temperature

If you install the AlterPath Manager 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.

▼ *To Configure the COM Port Connection and Log In*

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

First Time Configuration establishes the superusers for the Console Interface (hardware configuration) and the web interface. AlterPath Manager connectivity and system settings is also set up during First Time Configuration. Configuration through the web interface is discussed in the chapter, "Configuration and Administration."

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

1. Select an available COM port.

   In HyperTerminal (Start > Program > Accessories > Communications > Hyper Terminal), select File > Properties, and click the “Connect To” tab. Select the available COM port number from the Connection dropdown.

2. Configure COM port.

   Click the Configure button.

   Your PC, considered here to be a “dumb terminal,” should be configured as follows:

   - Serial Speed: 9600 bps
   - Data Length: 8 bits
   - Parity: None
   - Stop Bits: 1 stop bit
   - Flow Control: none
   - ANSI emulation

3. Power on the AlterPath Manager

4. Click OK on the Properties window.

   You will see the AlterPath Manager booting on your screen. After it finishes booting, you should see the configuration screen.

Pre-Configuration Requirements

Before configuring AlterPath Manager, ensure that you have a local system with 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.

Requirement	Description
IP Addresses	Have the IP/Mask addresses of the following ready: - All console servers - Gateway - DNS Optional addresses: - 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 “First Time Configuration Wizard” on page 68, in Chapter 4.

Note: Chapter 3, “User Level Web Access” is designed for regular users who will use or operate the application after the AlterPath Manager 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 AlterPath Manager, refer to Appendix A, “Technical Specifications.”

Web Browser Requirements

You will need a local Windows workstation running a web browser that supports the following:

- ActiveX
- Java plug-ins

To view KVM console ports on your local Windows workstation, you will need to run a web browser that has ActiveX enabled. Windows browsers that support ActiveX include Microsoft Internet Explorer, and Netscape 7.x.

Caution: Microsoft Internet Explorer update version SP2, does not have ActiveX enabled by default. If you update Internet Explorer, or if you implement a new installation of Internet Explorer, you must be sure to enable ActiveX.

To view serial console ports, you will need to install Java plug-ins. Java plug-ins are located at:

```
http://www.sun.com
```

▼ *To Enable ActiveX on Internet Explorer*

1. Open an Internet Explorer session.
2. Click on Tools > Internet Options > “Security” tab > “Custom Level” button.
3. Make sure you enable the selections shown as enabled in Figure 2-1, “Options to Enable for ActiveX.”

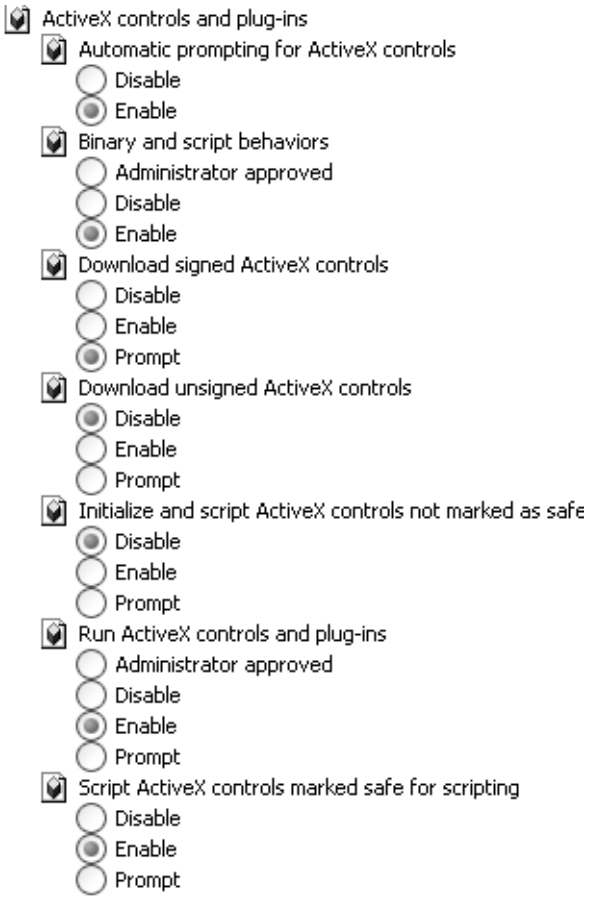

Figure 2-1: Options to Enable for ActiveX

▼ *To Enable ActiveX on Netscape 7.x*

Note: This applies to Netscape 7.x where x ≥ 1.

1. Go to the following path, using Windows Explorer:

   `C:\Program Files\Netscape\Netscape\defaults\pref`

Note: This path can vary if Netscape 7.x was installed in a directory other than the default.

2. Locate the file named “activex.js” and edit it.
3. In the editor, change the following line from:

```
pref("security.classID.allowByDefault", false);
```

to:

```
pref("security.classID.allowByDefault", true);
```

4. Save the file and exit the editor.
5. Restart Netscape 7.x

▼ *To Enable ActiveX on Netscape 8.x*

1. Open the Netscape 8.x Browser.
2. On the pull-down menu bar, go to the Tools > Options.

   An “Options” window appears.

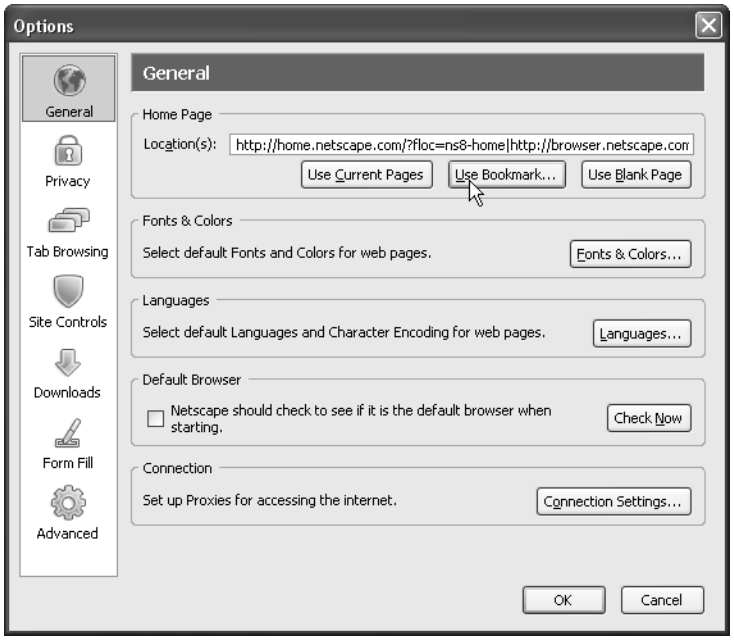

Figure 2-2: Netscape 8 Options Window

3. Click on “Site Controls” in the left column of the window.

The window that appears has the button to enable ActiveX.

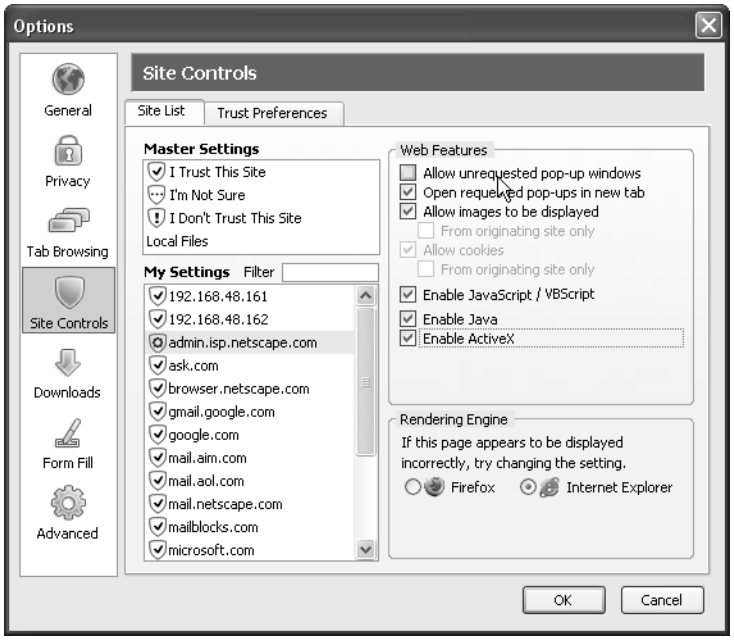

Figure 2-3: "Site Controls" Option Selection

4. Select "Internet Explorer" in the "Rendering Engine" box in the lower right of the window.
5. Select "Enable ActiveX" in the "Web Features" box.
6. Click the "OK" button.
7. Enter the IP address of your APM in the URL entry field of your Netscape browser.

   Notice the shield icon shown in Figure 2-4:

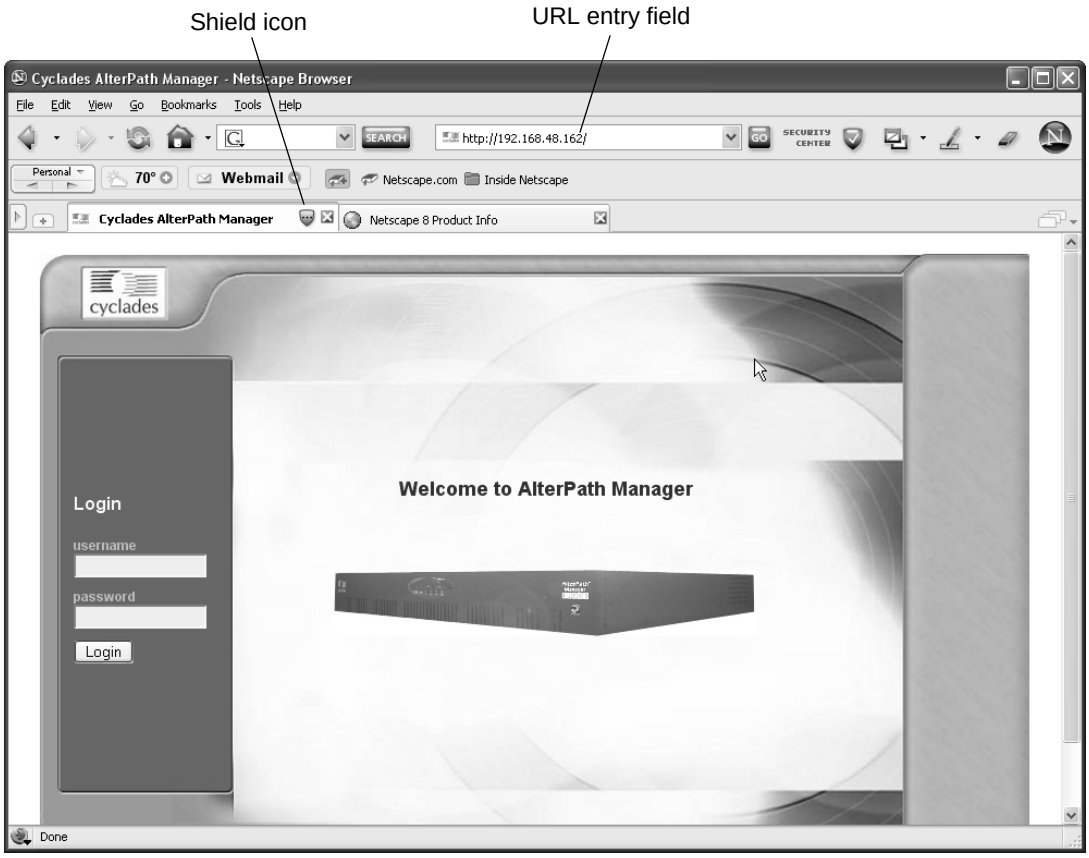

Figure 2-4: Location of Shield Icon and URL Entry Field

8. Click on the Shield Icon.

A “Trust Settings” dialog box appears.

Figure 2-5: Trust Settings Dialog Box

9. Click on the “I Trust This Site” button.

ActiveX is enabled, and you have marked your APM’s IP address as a trusted site.

IPMI Option

You can purchase the IPMI option from your Cyclades sales team, or Cyclades partners.

Cyclades customer service will need the MAC (Ethernet hardware) address of Eth0 (the first Ethernet controller in your APM) to generate the license file which will activate your new features. To find your MAC address, see “Verifying your MAC Address” on page 32

Verifying your Current IPMI Capability

Log on to the Web User Interface and click on the “About” link in the lower left corner of the display. A window similar to the following will appear:

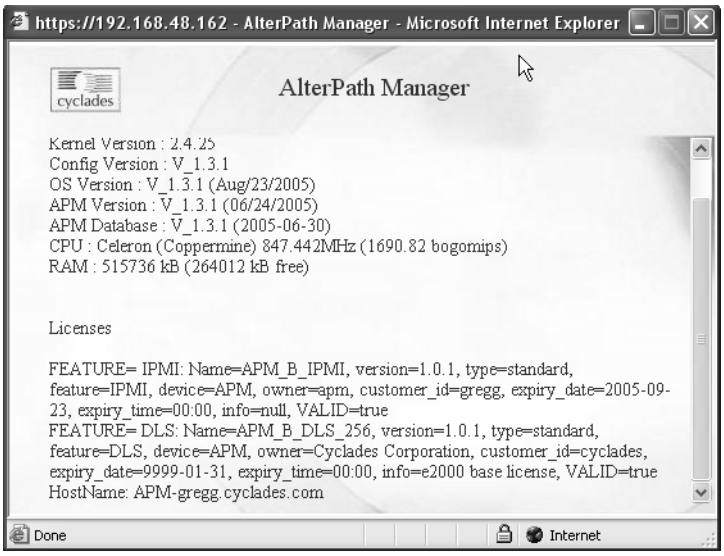

Figure 2-6: Feature Window

You can also log on to the CLI (on the serial console port) as root or as admin and run the following command:

```
# ls /var/apm/licenses/data
```

If IPMI is activated, the screen will display a file name similar to this:

```
APM_B_IPMI.enc
```

Verifying your MAC Address

Log on to the CLI (on the serial console port) as root or as admin and run the following Linux system command:

```
# ifconfig
```

A display similar to the following will appear:

```
eth0      Link encap:Ethernet  HWaddr 00:90:FB:81:57:17
          inet addr:192.168.48.162  Bcast:192.168.51.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9691587 errors:133 dropped:0 overruns:0 frame:133
          TX packets:5726282 errors:0 dropped:0 overruns:0 carrier:0
          collisions:1038728 txqueuelen:1000
          RX bytes:685270715 (653.5 Mb)  TX bytes:548308906 (522.9 Mb)
          Interrupt:10 Base address:0xc000 Memory:e5020000-e5020038

eth1      Link encap:Ethernet  HWaddr 00:90:FB:01:8C:D7
          inet addr:10.10.10.2  Bcast:10.10.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:632 errors:0 dropped:0 overruns:0 frame:0
          TX packets:622 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:38288 (37.3 Kb)  TX bytes:42288 (41.2 Kb)
          Interrupt:11 Base address:0xc400 Memory:e5021000-e5021038

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113528 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113528 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:15268713 (14.5 Mb)  TX bytes:15268713 (14.5 Mb)
```

The numbers following the “HWaddr” subheading for each Ethernet controller installed (eth0 and eth1 by default) is the MAC address for the controller.

Chapter 3
User Level Web Access

The web interface provides two modes for using the AlterPath Manager E2000 and 2500 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 AlterPath Manager web interface in *Access* mode.

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

Note: If you are an AlterPath Manager system administrator, refer to Chapter 4, "Configuration and Administration."

User Interface Overview

The AlterPath Manager user interface provides you with four main menu options

Note: With browsers other than Internet Explorer, there are limitations with multiple users accessing the AlterPath Manager via the Web Management Interface on a single workstation. If you plan to have more than one user simultaneously open APM Web access sessions from a single workstation, you should use Internet Explorer.:

Table 3-1: User Interface Main Menu

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
Consoles	Use the Consoles list form to view a list of consoles assigned to you. From the list, click on the console you wish to access. For IPMI users, the Consoles List form provides access to the IPMI SOL.
Logs	Use the Logs form to view the "Access" logs, "Events" logs, and "Data Buffer" logs for a particular console or device.
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 view your own security profile.

▼ *To Access the APM Web Application*

To open the AlterPath Manager 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 AlterPath Manager administrator.

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

Note: See "To Disable HTTP to Use Only HTTPS" on page 219 (Chapter 5) 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.

Figure 3-1: APM Login Screen

3. Select the “Login” button.

   Upon successful login, the Alarms List form appears.

Note: When the AlterPath Manager 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 AlterPath Manager 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.

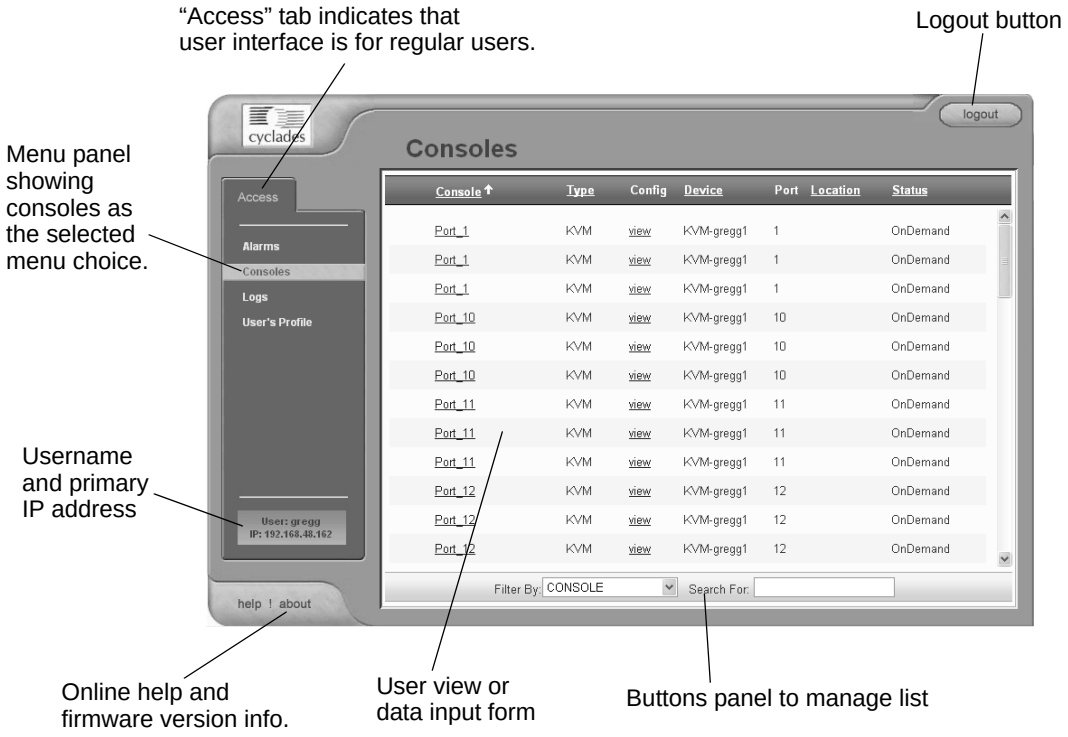

Figure 3-2: Console Menu

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 only to 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 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 “Filter By” and “Search For” fields at the bottom of a 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 and filling in the “Search” field.

The “Search” function has been improved in SW version 1.3.1. You can now type the first critical characters of a search string and press “Enter” to view all items in a list that start with those characters. The input field is retained until you click a menu item.

The view generated from the “Filter By” field is automatically saved.

Alarms

The Alarms List form is the default form of the AlterPath Manager Web Interface in “Access” mode. An alarm is a brief message alerting you of a possible problem that requires an action.

When AlterPath Manager detects an alarm, it sends the alarm along with a ticket number to the user’s Alarms 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 AlterPath Manager 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 > (select console) > Event Logs

▼ To Respond 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:

1. Accept the ticket or assignment.
2. 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 the 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.

Alarms List Form

When you first log in to the AlterPath Manager as a regular user or select “Alarms” from the menu, the Alarms 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 re-assign the current ticket, change the ticket status, and add notes or comments, use the “Alarms Detail (or Ticket Info) Form” on page 43.

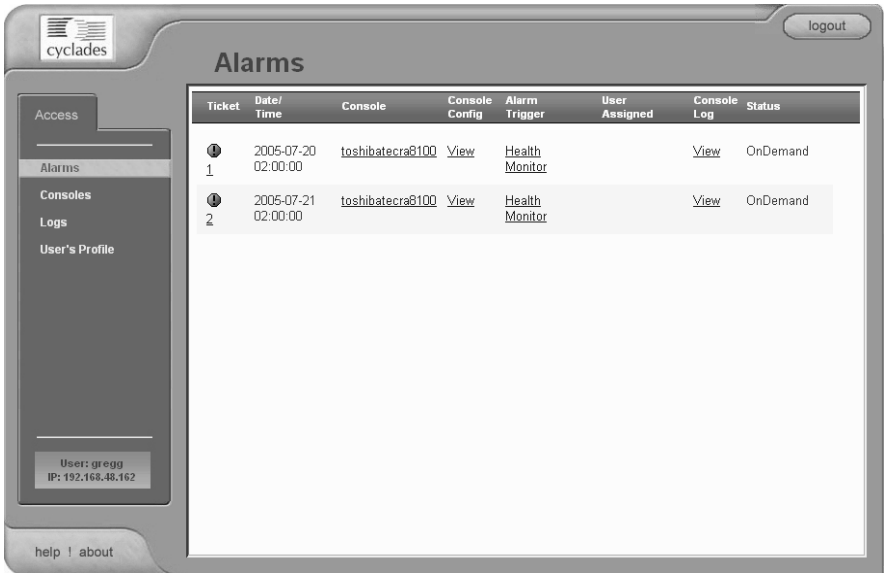

Figure 3-3: Alarms List Form

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.

▼ *To View the Alarms Detail Form*

The Alarms 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. Click on the ticket number shown in Figure 3-3, “Alarms List Form.”

   The form brings up the Alarms Detail form.

Figure 3-4: Alarms Detail (or Ticket Info) 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 Alarms List form.
Save	Button to save your entries.
Reset	Button to reset the form to its original or default values.

▼ *To View Alarm or Console Logs*

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

1. From the Alarms 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:

Figure 3-5: Logs Form

▼ *To Assign or Re-assign a Ticket to a User*

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

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

   The system opens the Alarms Detail form.

2. From the Ticket Information form, select a 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, ACS, or OnSite).
- Launch the KVM Viewer and connect you to a KVM port (for KVM/net or OnSite).

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.

▼ *To View the Consoles List*

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

To view the Consoles 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 Consoles List form appears.

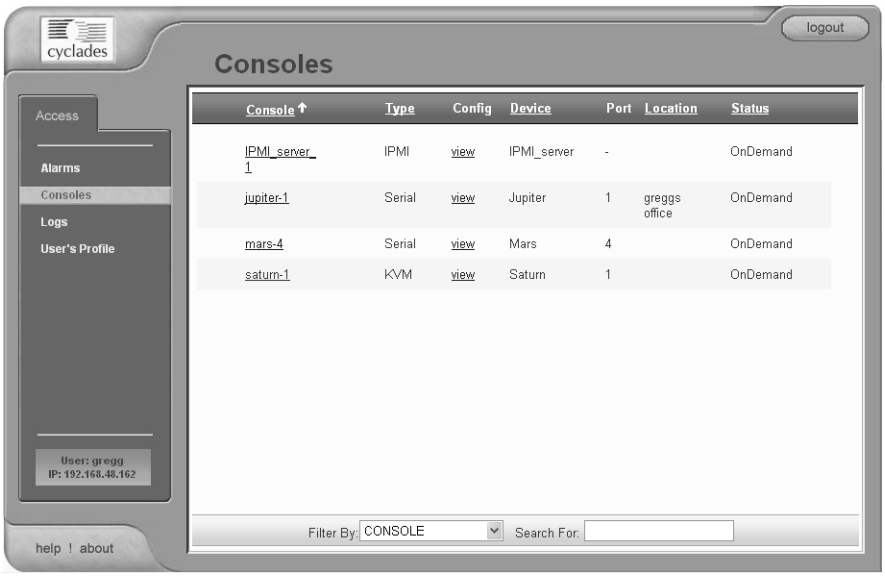

Figure 3-6: Consoles List Form

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	Drop-down to filter your search by Console Group Name which you select from the dropdown box.
Search	Field in which to type a search string used to search for a console name.

▼ *To Connect 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 AlterPath Manager handles the authentication.

Multiple Users and Read/Write Access

Because the AlterPath Manager 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.

Consoles Detail Form

Use the Consoles Detail form to view specific information about a particular console. You can invoke this form from either the Alarms List form or the Consoles 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 use an IPMI console as an example.

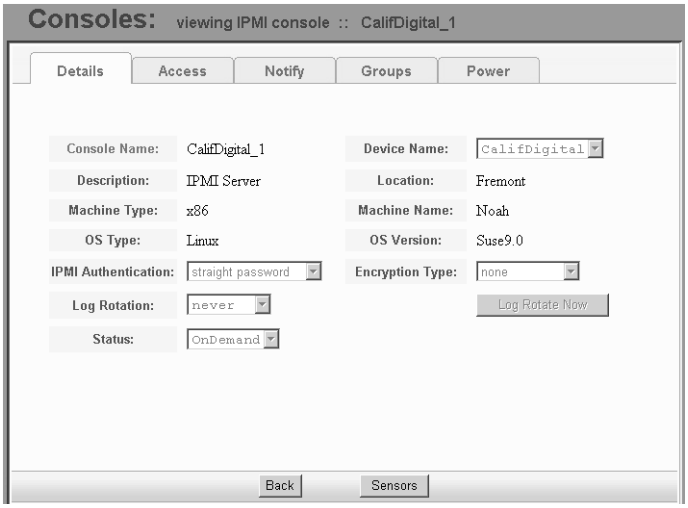

Figure 3-7: Consoles Detail Form

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

Field Name	Definition
Details	Tab to display the Console Detail form.
Access	Tab to view users who are authorized to access the current console.
Notify	Tab to view users who can be notified of an alarm pertaining to the current console.
Groups	Tab to view the group(s) to which the current console belongs.

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

Field Name	Definition
Power	Tab 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 (Enable, Disable, On Demand).
Back	Button to return to the previous page or form.

▼ *To View the Consoles Access Form*

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

To view the Consoles Access form:

1. From the Consoles Detail form, click on the “Access” tab.

   The system displays the Consoles Access form:

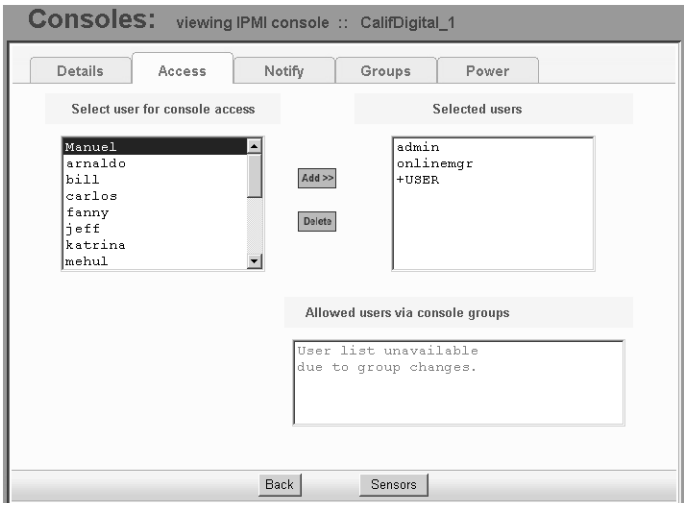

Figure 3-8: Consoles Access Form

▼ *To View the Consoles Notify Form*

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

To view the Consoles Notify form:

1. From the Consoles Detail form, click on the “Notify” tab.

   The system displays the Consoles Notify form:

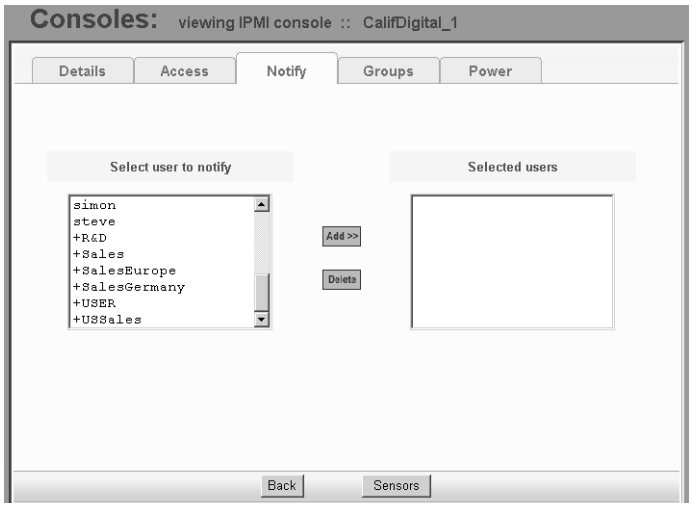

Figure 3-9: Consoles Notify Form

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

▼ *To View the Consoles Groups Form*

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

To view the Consoles Group form:

1. From the Consoles Detail form, click on the “Groups” tab.

   The system displays the Consoles Group form:

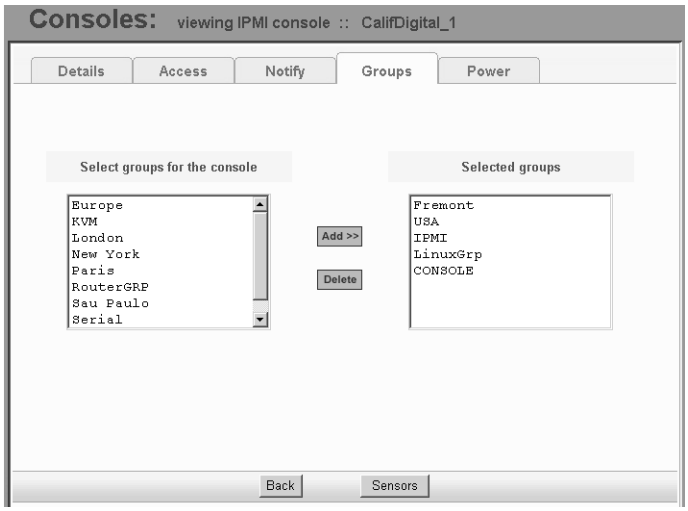

Figure 3-10: Consoles Group Form

▼ *To View IPMI Sensors*

Note: IPMI is a paid-for added feature of AlterPath Manager, 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:

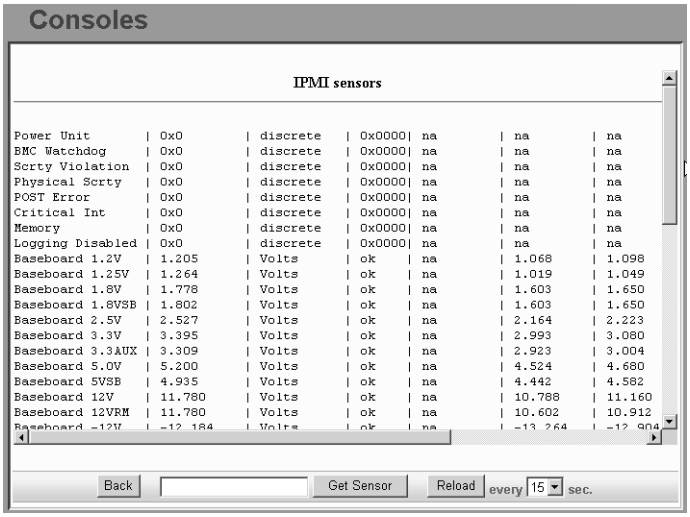

Figure 3-11: IPMI Sensors form

Logs

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

Table 3-6: Log Types

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

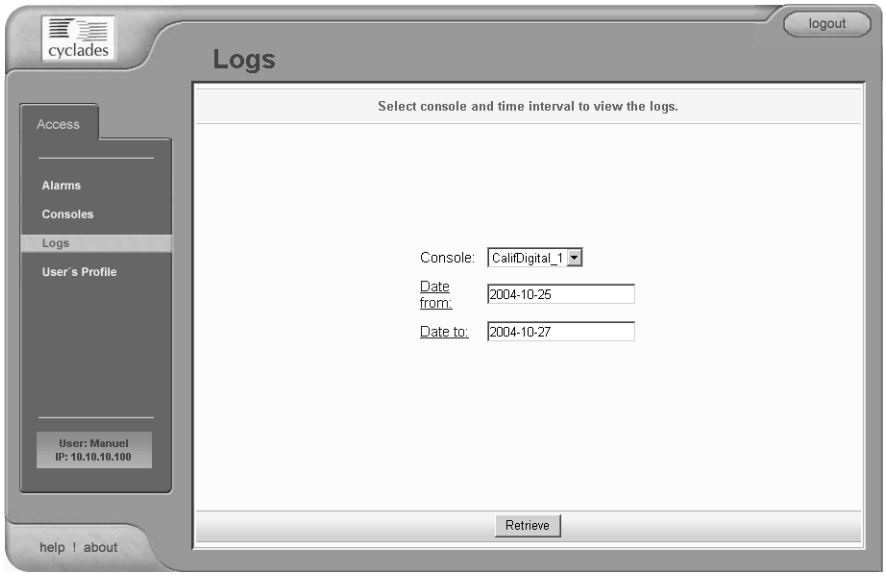

Figure 3-12: Logs Form

Table 3-7: 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.

▼ *To View 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.

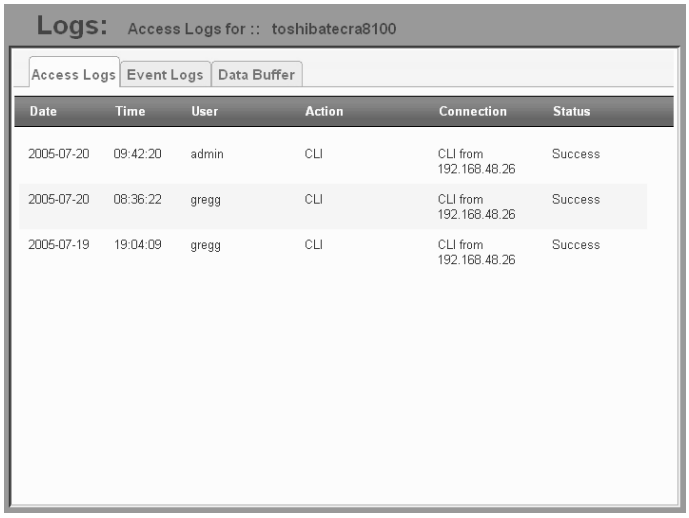

Figure 3-13: Access Logs Form

Table 3-8: 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.

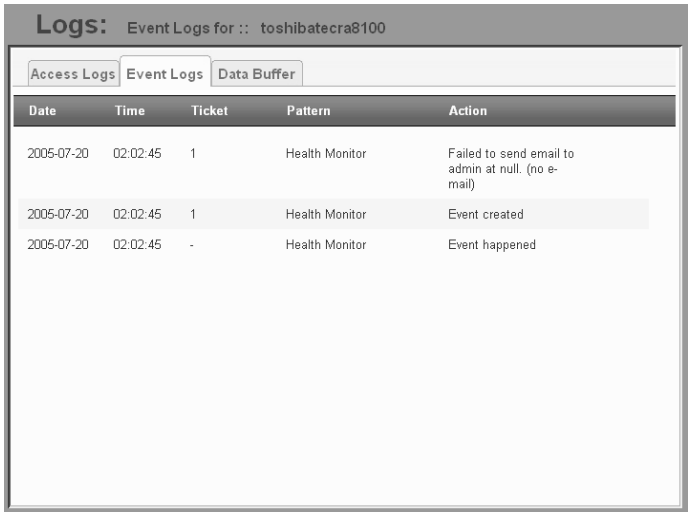

Figure 3-14: Event Logs Form

Table 3-9: 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.

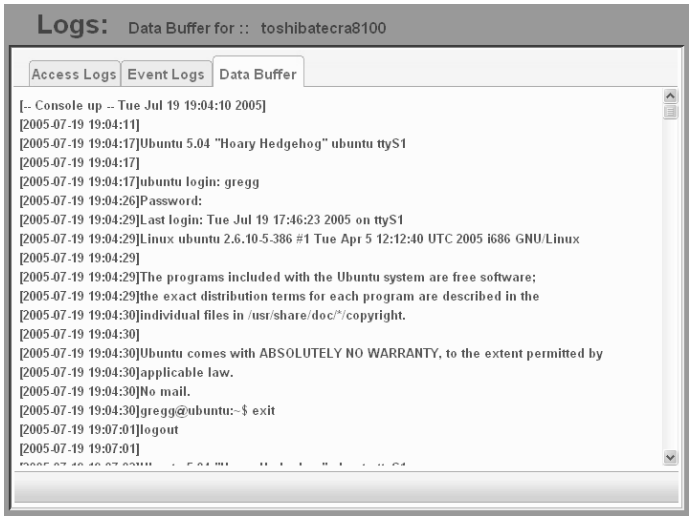

Figure 3-15: Data Buffer Log Form

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

User’s Profile

The User’s Profile forms allow 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.

Figure 3-16: User’s Profile Details Form

Table 3-10: User’s Profile Details Form - Fieldnames and Elements

Field Name	Definition
Details	Tab to display the User’s Profile Detail form. This is also the primary form of User’s Profile.
Access	Tab to display the User’s Profile Access form which shows all consoles assigned to the current user.
Groups	Tab to display the User’s Profile Group form which shows all groups to which the current user belongs.

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

Field Name	Definition
Security	Tab to display the security level (admin or regular user) of the current user.
User Name	The user name used to log into the AlterPath Manager.
Admin User	Check box to indicate that the user has Admin privileges, and also belongs to the Admin user group.
Security Profile (*For Admin use only*)	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: `/var/apm/bin/apm_unlock_admin.sh` from the Linux shell through the Serial Console Interface.
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.

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

Field Name	Definition
Status	Indicates whether the user is *enabled* or *disabled*.

▼ *To Change Your Password*

To change your password, perform the following steps:

1. From the User's Profile Details form, click on the "Set Password" button.

   A password dialog box will be launched.

2. From the password dialog box, enter the new password twice.
3. Click on the dialog box's internal "Set Password" button.

▼ *To View the User's Profile Access Form*

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

To view the User's Profile Access form:

1. From the User's Profile Detail form, click on the "Access" tab.

   The system displays the User's Profile Access form:

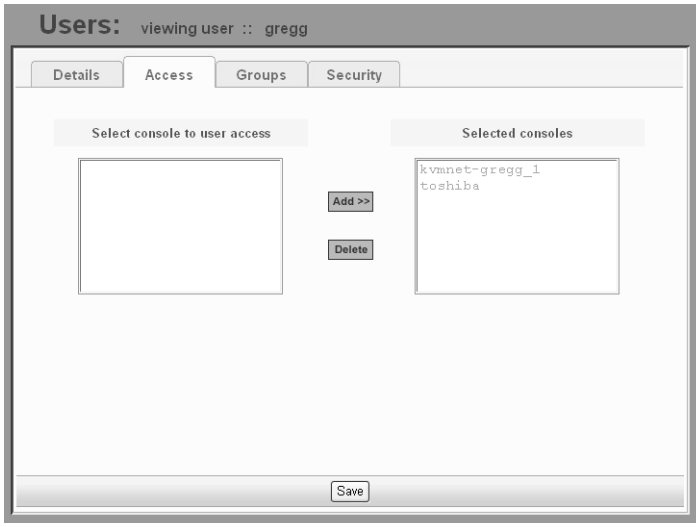

Figure 3-17: User's Profile Access Form

▼ *To View the User's Profile Groups Form*

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

To view the User's Profile Groups form:

1. From the User's Profile Detail form, click on the "Groups" tab.

   The system displays the User's Profile Groups form:

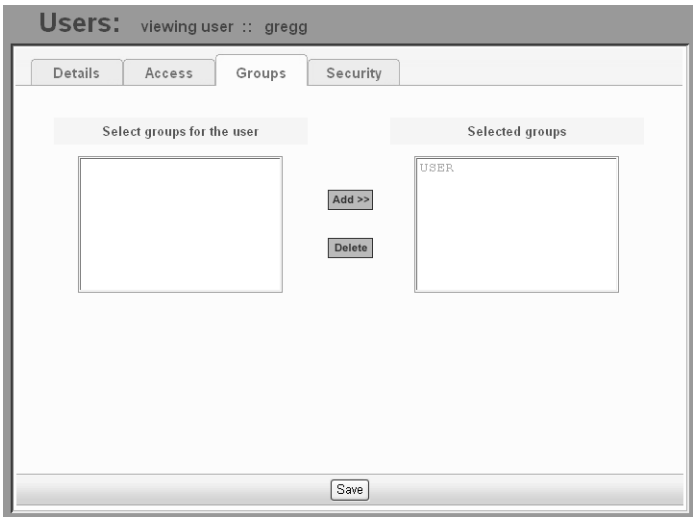

Figure 3-18: User's Profile Groups Form

Table 3-11: 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.

▼ *To View the User's Profile 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.

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 User's Profile Security form:

Figure 3-19: User's Profile Security Form

Table 3-12: 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.
Add	Button to add a selected security profile (left list box) to the "Selected security profile" list box.

Table 3-12: User’s Profile Security Form - Fieldnames and Elements

Field Name	Definition
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
Configuration and Administration

This chapter presents the procedures for configuring the AlterPath Manager E2000 and 2500 through the web interface. Addressed to the E2000/2500 administrator who must use the AlterPath Manager web interface in *Admin* Mode, the chapter is organized as follows:

Operational Modes

The AlterPath Manager provides two operating modes for configuration:

- First Time Configuration (Linux shell on the *serial console*)
- Admin Mode (GUI-based)

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

The admin user, by default, is the system administrator of the AlterPath Manager 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 Chapter 3, “User Level Web Access” on page 35

Note: Certain configuration procedures (e.g., System Recovery, Modem Card Configuration) require the use of the Linux shell on the serial console by advanced users. These procedures are discussed in Chapter 5, “Advanced Configuration” on page 185

Configuration Process Flow

The entire configuration process through the serial console and through the WMI is as follows:

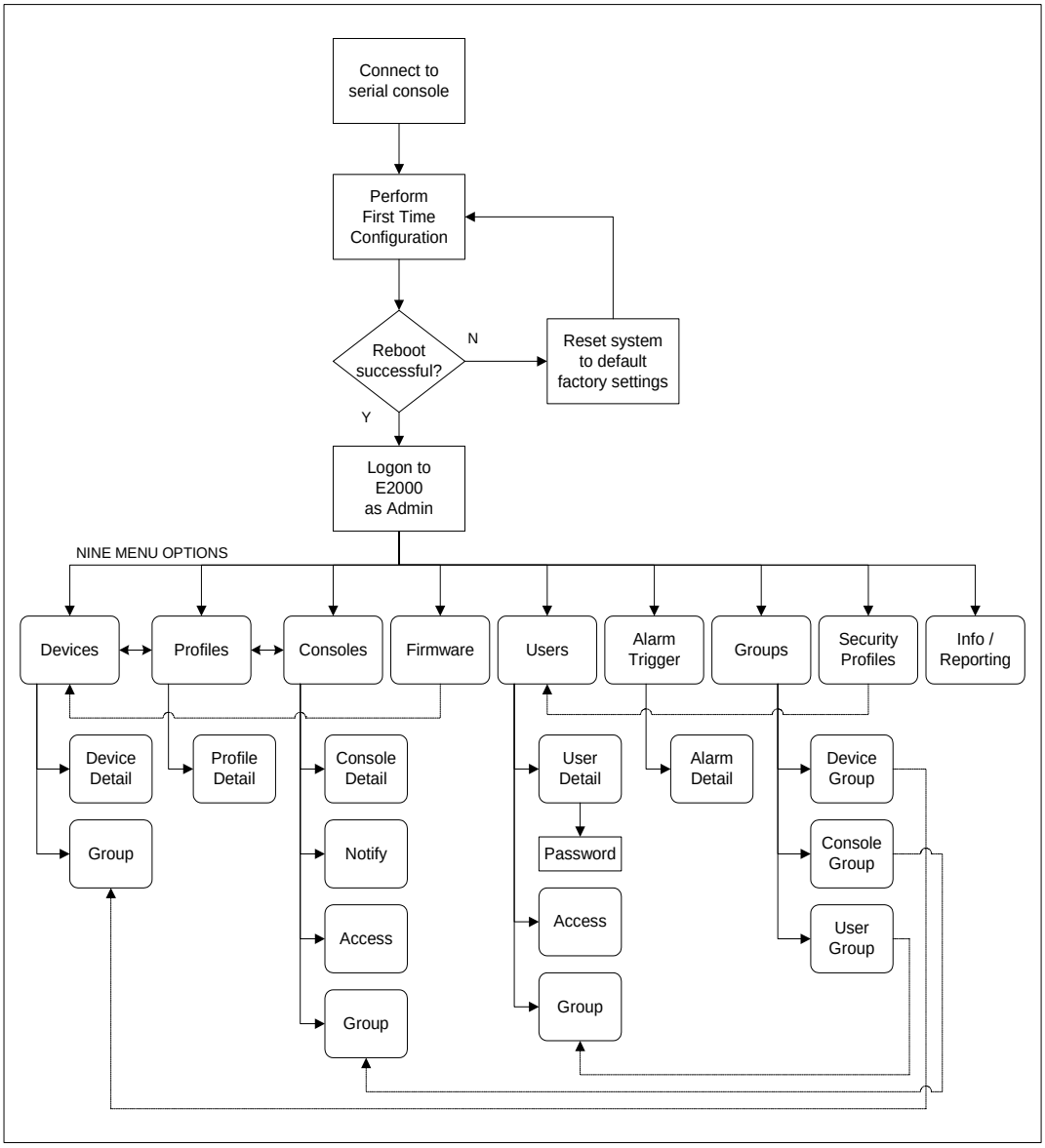

Figure 4-1: AlterPath Manager Configuration Process Flow

You must perform the First Time Configuration process (see Configuration Flow Diagram) using the Linux shell through the serial console interface. Once completed, you may perform the rest of the configuration process and all daily administration procedures through the AlterPath Manager web interface.

To configure all your devices with the AlterPath Manager (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, “AlterPath Manager 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 serial console interface.
- Establish user as Admin, the superuser for the AlterPath Manager web user interface and the command line interface (CLI).
- Initialize your system and user settings to ensure full connectivity and functionality of the AlterPath Manager.

First Time Configuration requires that you:

- Connect to the serial console
- Log in as “root”.

▼ *To Use the First Time Configuration Wizard*

1. Before you power on the AlterPath Manager, connect one end of a DB-9 to DB-9 Null Modem cable (or equivalent) to the console port of the AlterPath Manager.
2. Connect the other end of the cable to a terminal or a computer’s serial port.
3. Using the terminal or a terminal emulation program installed on a computer, start a session with the following settings:
   - 9600 BPS
   - 8 data bits
   - No parity
   - 1 stop bit
   - ANSI emulation
4. Power on the APM

   Boot information will scroll up on the screen for a short time until the system is ready for initial configuration input data.

```
                    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.
```

5. Press any key to run the First Time Configuration Wizard.

   You will be asked to enter the following parameters:
   - Enter a password for root (and re type the password)
   - Enter a password for admin (and re type the password)

- Select a time zone
- Enter a new system date and time (format is MM/DD/YY)

Note: You must type a date, even if it is the same as the date displayed, in order to change the time.

- Enter the time (if you did not select the default date: format is HH:MM)
- Select static or none (for DHCP) for the primary IP address
- Enter the primary Ethernet IP address (if you selected static)

Note: When you are connecting to a public network (see Figure 1-6, “Single Network Diagram” on page 15), Eth0 can be configured with 2 IP addresses as long as the addresses both conform to the subnet and address range of the public LAN.

- Enter the primary Ethernet subnet mask address
- Select static or none for the secondary IP address
- Enter the secondary Ethernet IP address (if you selected static)

Note: When you are connecting to a private network (see Figure 1-5, “Private Network Diagram” on page 14), Eth0 (the primary Ethernet port) is connected to the public LAN. The Eth0 address and subnet must conform to the public LAN’s subnet and address range. Eth1 (the secondary Ethernet port) is connected to the private LAN with its own subnet and address range.

- Enter the secondary Ethernet subnet mask address
- Configure Ethernet subinterfaces (Y)es, (N)o, or (L)ist
- Configure Ethernet VLANs (Y)es, (N)o, or (L)ist
- Enter Ethernet default gateway
- Set Ethernet eth0 speed/duplex
- Choose the correct operation mode from the following:

    1) Auto-negotiation

2) 10 Mbps, full duplex

3) 10 Mbps, half duplex

4) 100 Mbps, full duplex

5) 100 Mbps, half duplex

6) 1000 Mbps, full duplex

7) 1000 Mbps, half duplex

Note: Gigabit Ethernet is available on the APM 2500 only.

- Set Ethernet eth1 speed/duplex
- Enter the system's hostname (max 30 characters)
- Enter the system's domain name (max 60 chars)
- Enter the primary nameserver's IP address
- Enter the secondary nameserver's IP address
- Enter the NTP server
- Enter the E-mail (SMTP) server
- Enter an authentication method (local, RADIUS, TACACS+, LDAP, Kerberos, NIS, Active Directory)

Note: After you select an authentication service type, you will be prompted with questions that are specific to that type of authentication. For example, if you select RADIUS, you will be prompted for the RADIUS server name and the RADIUS secret.

Once you have finished with the last parameter, the configuration will automatically be saved to flash memory.

▼ *To Correct Configuration Mistakes*

Note: If you have made a mistake in any of the foregoing configuration steps, you can adjust most configuration parameters by running one of the following commands as required.

---

1. Choose the appropriate command from the list belos
   - setauth
   - setboot
   - setdatetime
   - setdhcp
   - setethernet
   - sethosts
   - setnames
   - setnetwork
   - setntp
   - setserial
   - setsmtp
   - date

   When you are finished updating any of the configurations that use the preceding commands, enter the command: **`saveconf`**

▼ *To Reset 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.

An Example follows:

:

```
APM_gregg login: root
Password:

************************************************************************
* WARNING: changing system files directly is dangerous and may adversely *
*          affect your system's functionality. Proceed with caution, and *
*          only if you know what you are doing!                          *
************************************************************************

[root@APM_gregg 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@APM_gregg root]# reboot
```

Refer to the sample First Time Configuration Wizard example in the following section, to view how the parameters are entered into the system.

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!”

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

Caution: Be sure you answer “n” to the following questions.

Note: In the following examples, items shown in bold type represent user input.:

```
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]
```

The screen scrolls to the Welcome heading.

```
                    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.
```

Press any key to get to the password entry prompts.

Note: Passwords are not displayed on the console screen when they are typed.

```
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
```

After configuring your root and admin passwords, you are prompted to enter your time zone.

```
Please choose the time zone where this machine is located.
 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) SystemV
 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
```

Since this is the first time you are booting your APM, you need to configure the date, the time, the Ethernet settings, and the authentication protocol.

```
Current system date and time is:
    Thu Aug 18 08:21:56 PDT 2005
Press ENTER to accept it or specify new ones.
Enter date in MM/DD/YYYY format: 08/18/2005
Enter time in HH:MM format: 15:23
Thu Aug 18 15:23:00 PDT 2005
Ethernet eth0 IP address: (S)tatic or (N)one ? [S]: s
Enter Ethernet eth0 IP address: 192.168.48.162
Enter Ethernet eth0 Subnet Mask: 255.255.252.0
Ethernet eth1 IP address: (S)tatic or (N)one ? [S]: s
Enter Ethernet eth1 IP address: 10.10.10.2
Enter Ethernet eth1 Subnet Mask: 255.255.0.0
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]: 192.168.48.1
Current Ethernet eth0 speed/duplex settings: AUTO
Change Ethernet eth0 speed/duplex: (Y)es or (N)o ? [N]: n
Current Ethernet eth1 speed/duplex settings: AUTO
Change Ethernet eth1 speed/duplex: (Y)es or (N)o ? [N]: n
Enter the System's Hostname
    (max 30 characters) [APM]: APM-gregg
Enter the System's Domain Name
    (max 60 chars) [localdomain]: cyclades.com
Enter the Primary Nameserver's IP address [none]: 192.168.44.21
Enter the Secondary Nameserver's IP address [none]:
Enter the NTP server:
Enter the email (SMTP) server: smtp.cyclades.com
Choose the desirable authentication method
    (local/radius/tacacs+/ldap/kerberos/nis/active_directory) [local]:
Saving configuration files to flash (/flash/config/config.tgz)... done.
Removing init_config flag... done.
```

At this point, the First Time Configuration Wizard has completed its job. Some system and configuration status messages scroll up the screen until the “login” prompt appears.

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 214 of Chapter 5, "Advanced Configuration."

Configuring Active Directory

To use Active Directory as your authentication method, select `active_directory`. See "To Configure Active Directory" on page 218 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
- Alphabetical (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 AlterPath Manager web application.

Multiport Ethernet Card Configuration

The AlterPath Manager supports up to two multiport Ethernet cards to allow connection to network segments. The First Time Configuration Wizard will detect any multiport Ethernet card that is installed in the AlterPath Manager 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 “Modem Card Configuration” on page 207 of Chapter 5, “Advanced Configuration.”

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

▼ *To Begin Web Configuration*

1. Type the URL in the one of the following formats in your web browser
   - non-encrypted:

     `http://nnn.nnn.nnn.nnn`
   - encrypted.

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

   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 then enter the admin password (as specified during the First Time Configuration).

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

Disabling HTTP to Use Only HTTPS

The AlterPath Manager is configured to allow both HTTP and HTTPS access. You can, however disable HTTP access by commenting out its configuration in the AlterPath Manager unit by using the command line.

Note: See “To Disable HTTP to Use Only HTTPS” on page 219 of Chapter 5, “Advanced Configuration**”** for the procedure on how to configure the encrypted version.

AlterPath Manager Web Interface: Admin Mode

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

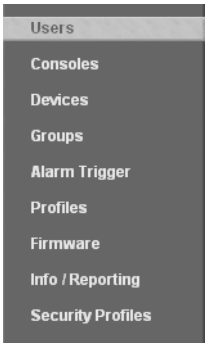

Figure 4-2: Admin Menu Panel Selections

Configuring the AlterPath Manager 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

▼ *To Log Into the APM Web Interface*

1. Type “admin” or the name of another user with administrator privileges in the “username” field.
2. Type the password for the admin user in the “password” field.
3. Press Enter.

Figure 4-3: Logging in as Admin

4. Select the “Login” button.

   Upon successful login, the Users List form appears.

Note: *When the AlterPath Manager 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 AlterPath Manager. Once the screens are stored, retrieving them should be fast.*

Note: *The rest of the procedures in this chapter assume 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 AlterPath Manager Web Management Interface in *Admin Mode*. The form example shows the Users List form, the first form to appear in the web interface. Basic features are similar in all WMI forms.

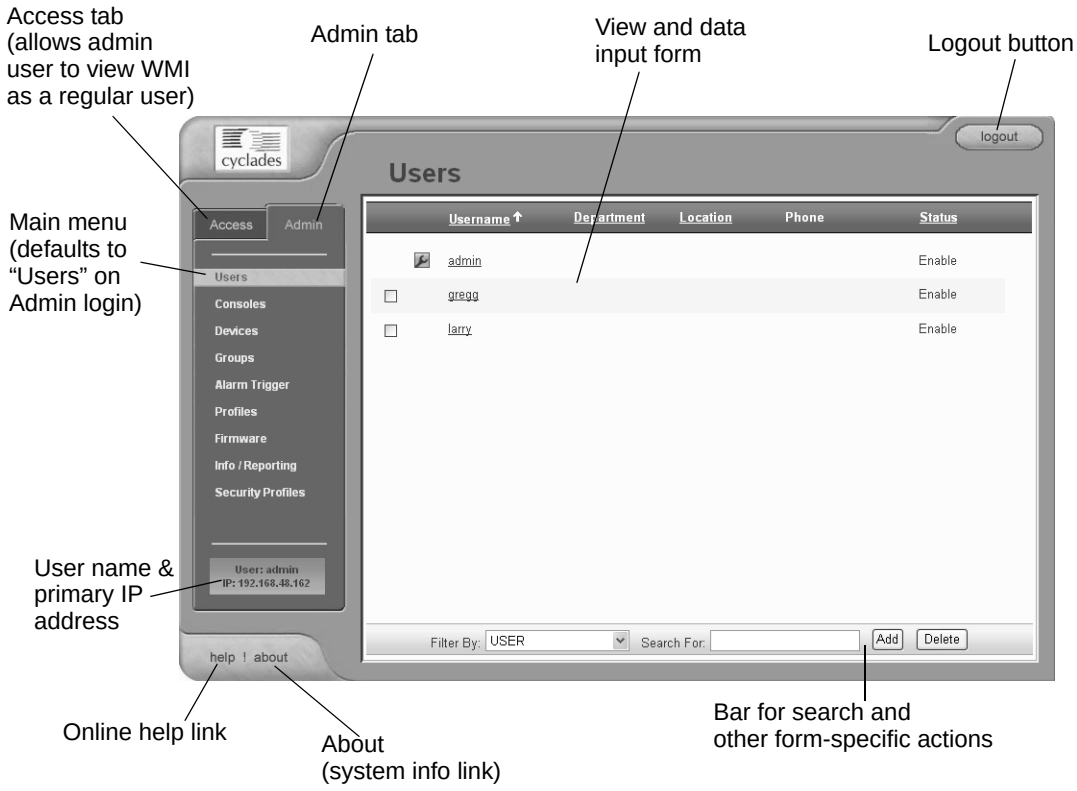

Figure 4-4: Basic Functional Fields of a Typical Form

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.

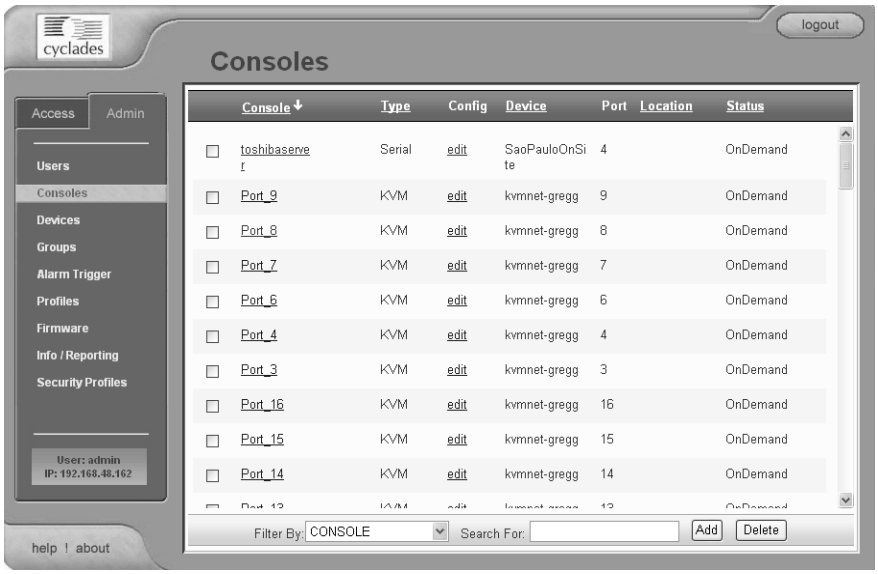

Figure 4-5: Console List Form Sorted by Console

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

To filter your list by group, use the “Filter by” pull-down. The list generated by selecting the “Filter by” pull-down is automatically saved.

To search for a particular console, use the “Search for” field.

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.

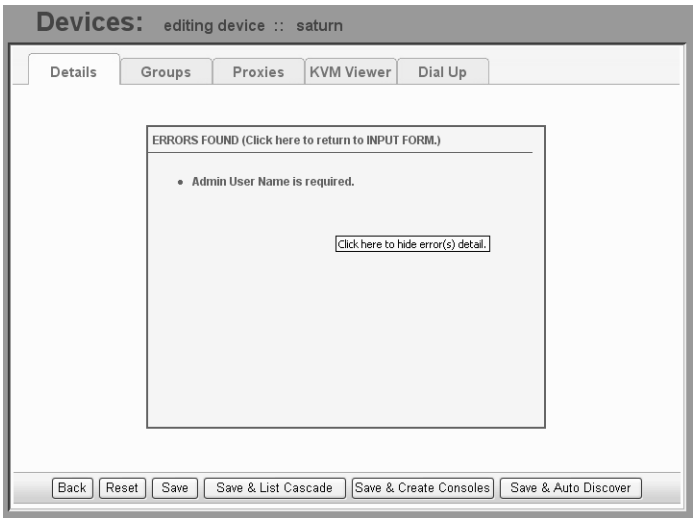

Figure 4-6: Device Configuration Error Message

Clicking the error message, generates the form in error:

Figure 4-7: Form in Error

Devices

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.e.*, ACS, TS, KVM/net, OnSite, 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).
Configure device health monitor.	Device detail form (Health Monitor input field).

Table 4-1: Summary of Devices Forms

Form Function	Form(s) Used
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: Devices List form.

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

- Consoles 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 device firmware.

When a new ACS or TS firmware is imported through the AlterPath Manager, the new firmware is added to the database and is reflected in the Firmware List form and in the Firmware/Boot dropdown list in the lower left region of the ACS or TS Device Details form.

Device List Form

The Devices List form, which is the default devices form, allows you to view a list of devices that are configured in the AlterPath Manager. From this form, you can add, modify, or delete devices. .

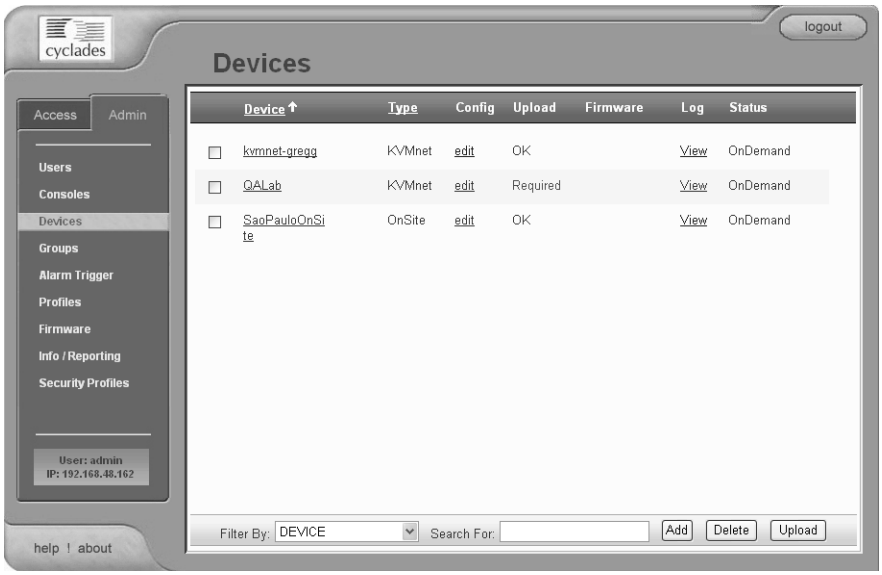

Figure 4-8: Devices List Form

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 AlterPath Manager supports firmware and configuration upgrades for the following products: - ACS and TS: Firmware and configuration - KVM: Configuration only - OnSite: Configuration only
Firmware	The firmware version for this device.
Log	Device log buffer. Click on “Log” to view the logs for this device.

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

Fieldname / Element	Definition
Status	Status of the device: Enabled, Disabled or OnDemand. OnDemand means that the device is enabled only upon user connection.
Filter By	A dropdown box that lets you select a filter element from a list of one or more. After you select the filter element, press Enter, and all items that match the filter element will be displayed.
Search For	A field box that accepts a string. After you enter the string into the field, press Enter, and all items that match the filter selection and the field entry, will be displayed.
Add	Button used to add new devices.
Delete	Button used to delete any devices selected for deletion.
Upload	Button used to upload the configuration or firmware to the selected device.

Supported Devices

The AlterPath Manager supports the following types of devices:

- ACS
- TS
- KVM/net
- OnSite
- IPMI (Optional)

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

Copy the IPMI license file that you purchased from Cyclades into the following directory on your APM:

`/var/apm/licenses/data/APM_B_IPMI.enc`

▼ *To Add 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.

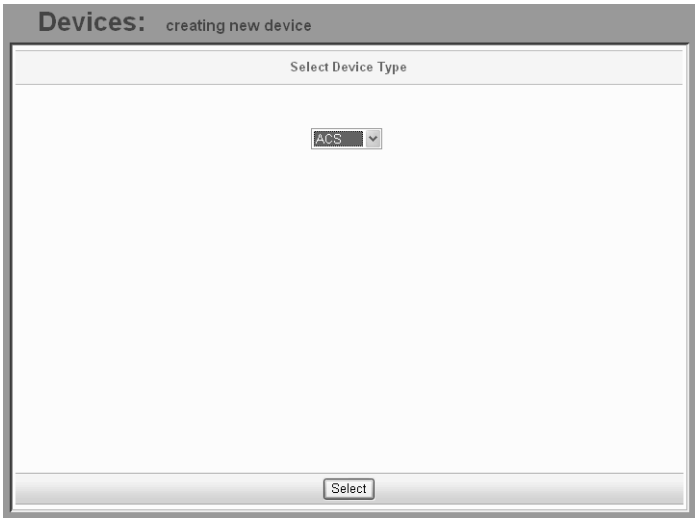

Figure 4-9: Select Device Type Form

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

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

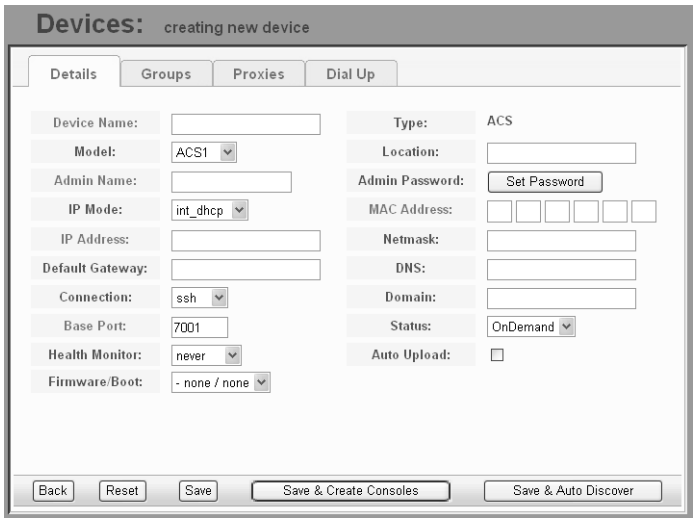

Figure 4-10: Device Detail Form

4. 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.

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 the AlterPath Manager is the DHCP server for this device, or "ext_dhcp" if DHCP is served by another server, or "Static" if you are using a static IP address. *See "Configuring Your DHCP Server" on page 104*.
MAC Address	The MAC address is required if the selected IP mode is "int_dhcp."
IP Address	The IP address of the device is required if the IP mode is "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 AlterPath Manager 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 AlterPath Manager 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. *See "Difference between Auto Upload and Manual Upload" on page 106.*
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 Device Discovery Wizard and save the resulting settings for the ACS, TS, or KVM/net.

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.

Note: For Health Monitoring to work with alarms, you must create the alarm triggers. See “Configuring Alarms for Device Health Monitoring” on page 133.

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

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

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 AlterPath Manager; 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 without ARP	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.
Forward Proxy using ARP (Address Resolution Protocol)	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.

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 AlterPath Manager 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 AlterPath Manager web interface cannot support the following connections:

- Serial console connection to the ACS/TS.
- Use the KVM viewer to access KVM/net console.

▼ *To Configure 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 Device Proxies form.

Figure 4-11: Device Proxies Form

4. From the Device Proxies 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 AlterPath Manager if your PC and the device are in different networks.

---

5. Click on “Save” to complete the procedure.

▼ *To Verify your Proxy Setting*

1. To verify your configuration, return to the Devices List form.

2. Place the mouse pointer over a device for which you configured a proxy setting.

   A small box with the choices “CLI” and “WEB” will appear.

3. Select “WEB.”

   This will launch a browser window that displays the web pages of the selected device.

Disabling the Proxy

Setting “Proxy type” to “none enabled” will prevent any admin user from accessing the selected device’s 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 214.

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 AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager.

When the AlterPath Manager 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.

▼ *To Configure 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 Device Dial Up form.

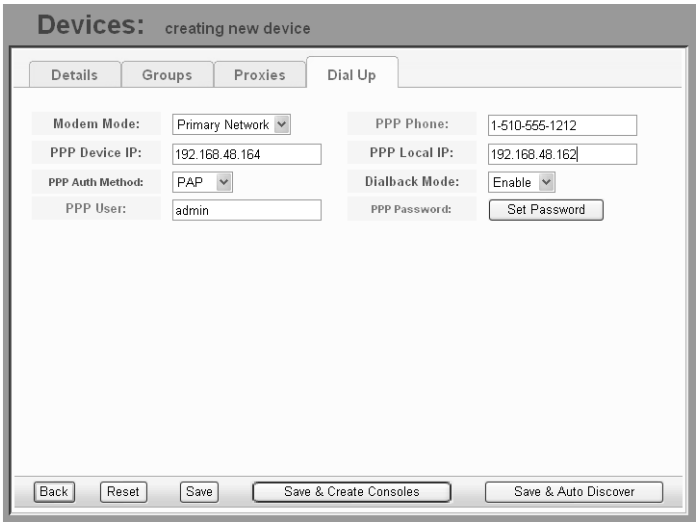

Figure 4-12: Device Dial Up Form

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.

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

Field Name	Definition
PPP Phone	*If Modem Mode is enabled (either as Primary or Network Backup), then this field is required for PPP connection*. 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 AlterPath Manager 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 AlterPath Manager:

1. Go to the web interface: “Console” 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:

1. Using a serial console or a telnet or ssh connection, create a new user and password for the ACS using the commands:
   - **adduser** <ppp_user>
   - **passwd** <ppp_user>

Note: See the section, “Changing the Ports to be Proxied” on page 214 in Chapter 5, “Advanced Configuration.”

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 AlterPath Manager:

1. Using the serial console interface, edit the file:
   `/var/apm/apm.properties`
2. Add the AlterPath Manager dial back 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:

Figure 4-13: KVM/net Device Detail Form

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:

Table 4-6: Features Unique to the KVM/net Device Configuration

GUI Element	Definition
KVM Viewer	Tab 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.

▼ *To Configure 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 the “Add” button.
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 122, this chapter.

OnSite Device Detail Form

The example that follows shows the device detail form that is used to configure the OnSite.

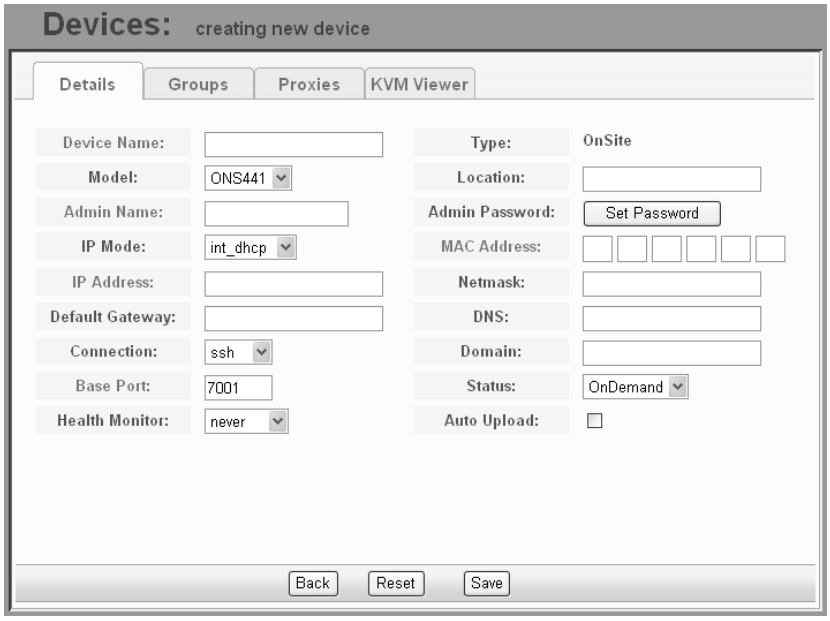

Figure 4-14: Device Detail Form for the AlterPath OnSite

Be sure to select the model you select matches the model number of your OnSite. OnSite model numbers and their meanings are shown in Table 4-7:

Table 4-7: OnSite Model Number Designations

Model Number	No. Serial Ports	No. KVM Ports	Users
ONS441	4	4	1
ONS481	4	8	1
ONS841	8	4	1
ONS881	8	8	1
ONS442	4	4	2
ONS482	4	8	2
ONS842	8	4	2
ONS882	8	8	2

Since the OnSite has both KVM ports and Serial ports, you can choose either type of port to configure and then direct the configuration to the OnSite device.

▼ *To Configure OnSite Ports*

1. Go to Consoles > Console List.
2. From the Console List form, select the “Add” button.
3. From the Add Console form, choose either “KVM,” or “Serial.”
4. From the Console Detail form, click “Device Name” and choose your OnSite device.

   See the “Consoles” section of this chapter for more details.

IPMI Device Detail Form

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

Copy the IPMI license file that you purchased from Cyclades into the following directory on your APM:

`/var/apm/licenses/data/APM_B_IPMI.enc`

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 4-8: 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.
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 AlterPath Manager 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.

▼ *To Use 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 "To Add an IPMI Console from Console Detail Form" on page 151 of this chapter.

▼ *To View 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 built into the AlterPath Manager. You can use your company's DHCP server or the AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager through the Device Definition form.

Function of the Status Field

The "Status" field of the Device Detail form indicates whether the connection between the AlterPath Manager and the device/console is "Enabled" (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 AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager and entering the username as follows:

  ```
  <username>:<console name>
  ```

- Uploading device configuration

Modem Mode

There are three modes of PPP connection:

Table 4-9: PPP Connection Modes

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 AlterPath Manager establishes a PPP connection as a backup network whenever a device/console access is requested.

Health Monitoring and PPP Settings

The AlterPath Manager 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 prevent your upload from being saved.

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:

Table 4-10: Modem Mode 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:

Table 4-11: PPP Settings

PPP Setting	Definition
PPP Device IP	*Optional*. IP address for the current device.
PPP Local IP	*Optional*. Local IP address for using PPP.
PPP Phone	*Required*. 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."*

▼ *To Configure the Health Monitoring System*

The Device Health Monitoring feature enables the AlterPath Manager 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" pull-down list box. Your choices are:

Table 4-12: Health Monitor Pull-down List Options

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 at 4 am 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 "Alarm Trigger" on page 129 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 4-13: 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.
Upload Progress	Indicates the percentage complete and displays any messages or errors. This page is shown if you did not check “Auto Upload” in the Device Details form.

Table 4-13: Summary of Console Wizard Forms

Wizard Form	Function
Console Creation Finish	This page is shown if you did not select “Auto Upload” from the Device Details form.

▼ *To Run 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.
   a. If you are configuring a new device (you selected “Add”), the system displays a pull down box that lets you select device types. Select the type of device that you want.
   b. Click the “Select” button.

   The system displays the Device Details form.

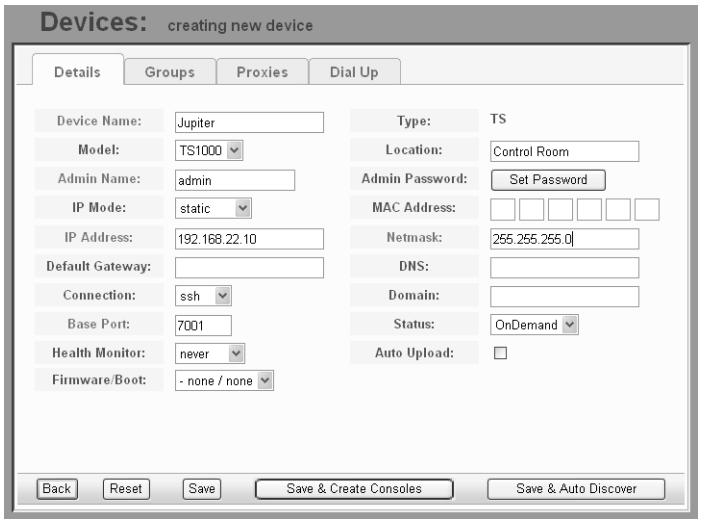

Figure 4-15: Device Details Form

2. From the Device Details 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.

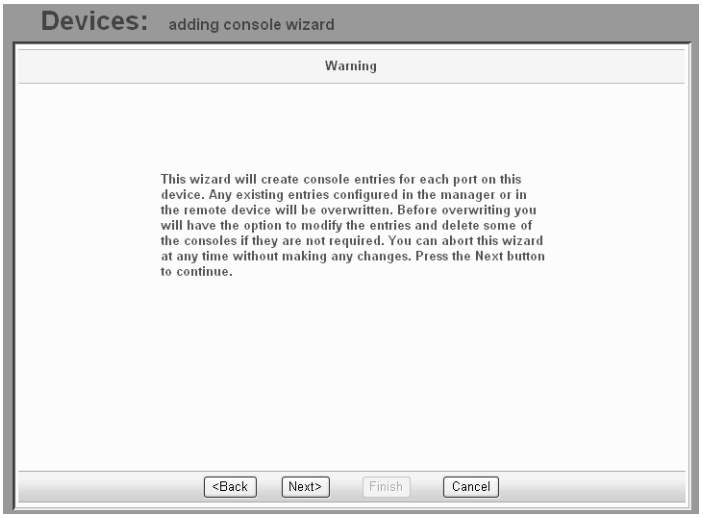

Figure 4-16: Console Wizard Warning Message

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.

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.

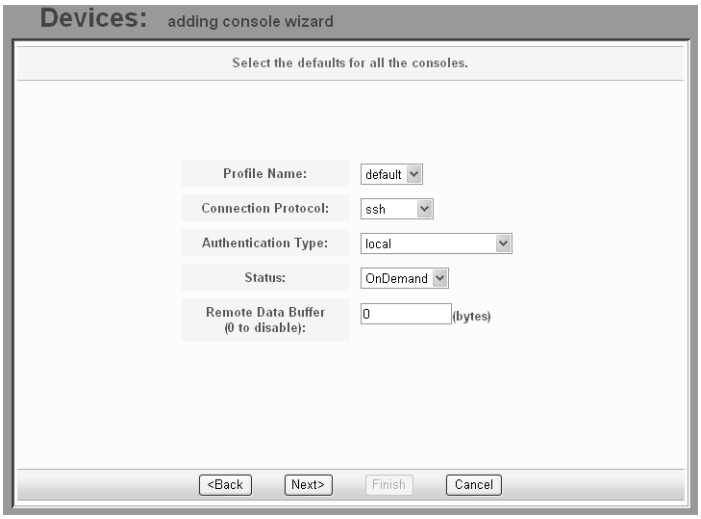

Figure 4-17: Console Wizard Defaults Form

5. Complete the above fields, and then select the "Next" button when done.

The system brings up the User Access form:

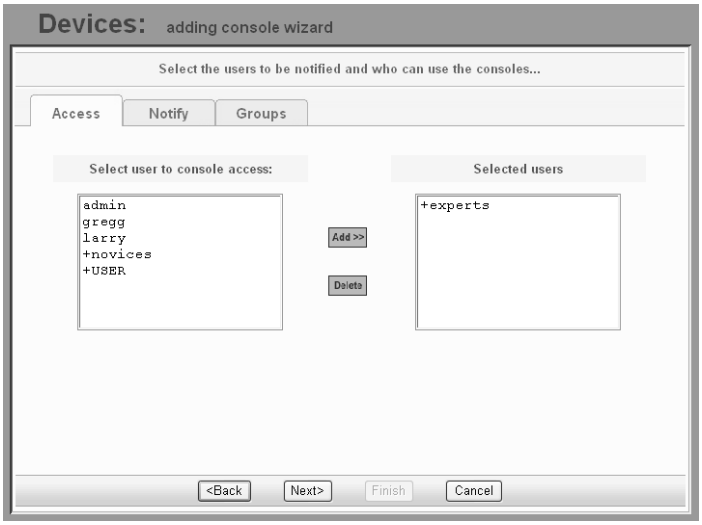

Figure 4-18: Console Wizard Access Form

"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:

Figure 4-19: Console Wizard Notification Form

7. Click the “Groups” tab and complete the Console Wizard Groups form, as necessary.

8. Select the “Next” button to display the Unconfigured Consoles form:

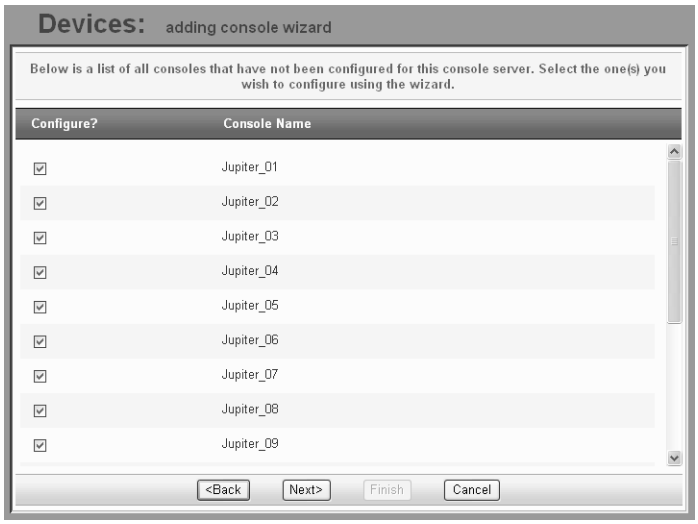

Figure 4-20: Unconfigured Consoles List

9. Select the unconfigured console(s) that you wish to configure, and then select the “Next” button to display the Edit Console Settings form.

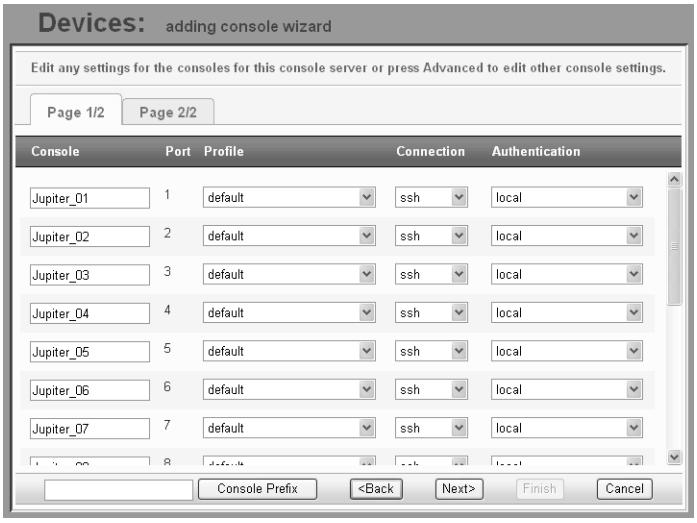

Figure 4-21: Edit Console Settings Form - Page 1

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.

10. From the resulting form, modify any settings as needed, and then click on the “Page 2/2” tab to continue the same form:

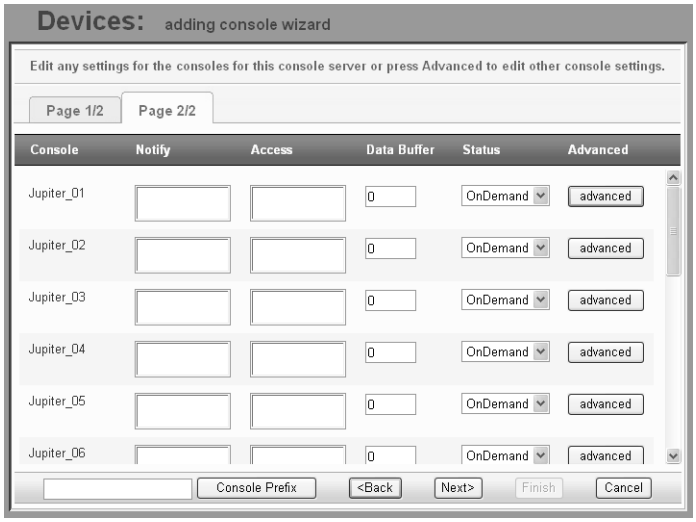

Figure 4-22: Edit Console Settings Form - Page 2

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

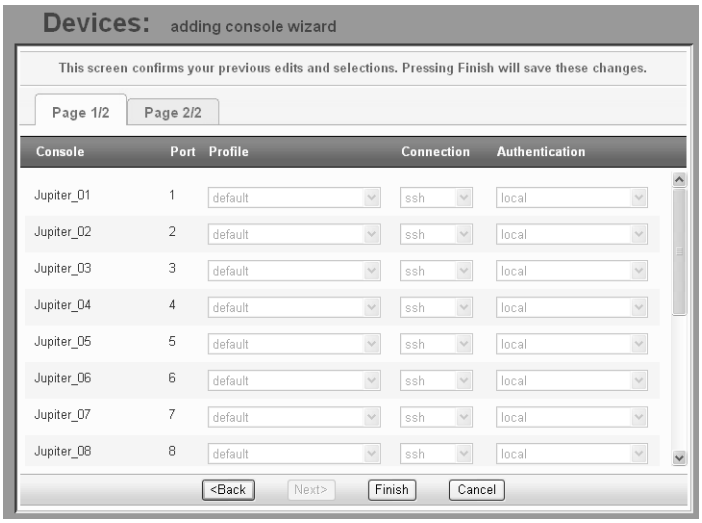

Figure 4-23: Confirm Console Edits Form - Page 1

12. Check your console settings from the Confirm Edits form (the "Page 2/2" tab included). If information is incorrect, select the "Back" button and repeat steps 10. and 11. Otherwise select the "Finish" button.

Device Discovery (Auto Discovery)

The Device Discovery feature enables the AlterPath Manager to recognize the current configuration of a Cyclades AlterPath TS, ACS, or KVM/net and, through the use of a wizard, autopopulate the console parameters based on the existing device configuration settings.

Note: Auto Discovery is not supported for the OnSite.

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

▼ *To Run the Device Discovery Wizard*

To run the Device Discovery Wizard follow the steps below:

1. Log in as *admin* (or as a user with an admin profile) to the AlterPath Manager
2. From the menu, select “Devices.”
3. From the Devices List form, select the “Add” button to configure the ACS, TS or KVM/net.
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 Name and Admin Password from the configured device.
   - IP Address and Netmask from the configured device.
   - Select “Static” from the “IP Mode” pull down box.
   - Place a check mark in 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 (shown in Figure 4-16, “Console Wizard Warning Message”) which alerts you to the fact that existing consoles will be overwritten if you follow through with the configuration.

Note: The ACS with SW version 2.3.1 and later is shipped with all ports disabled by default. Auto Discovery will not find ports that are disabled, and

therefore will not find any ports on a new ACS as shipped from the factory. If this is the case, and you are configuring an ACS using the “Save & Auto Discover” button, you will see the message:

```
No Console Found
```

You will need to do one of the following:

Manually enable some console ports by directly logging on to the ACS you are configuring in order to allow the auto discovery feature to discover those console ports.

Or:

Select the “Save & Create Consoles” button on the APM device configuration wizard.

---

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

▼ *To Connect 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 following example, the selected device is a KVM/net switch and the configured connection type is SSH.

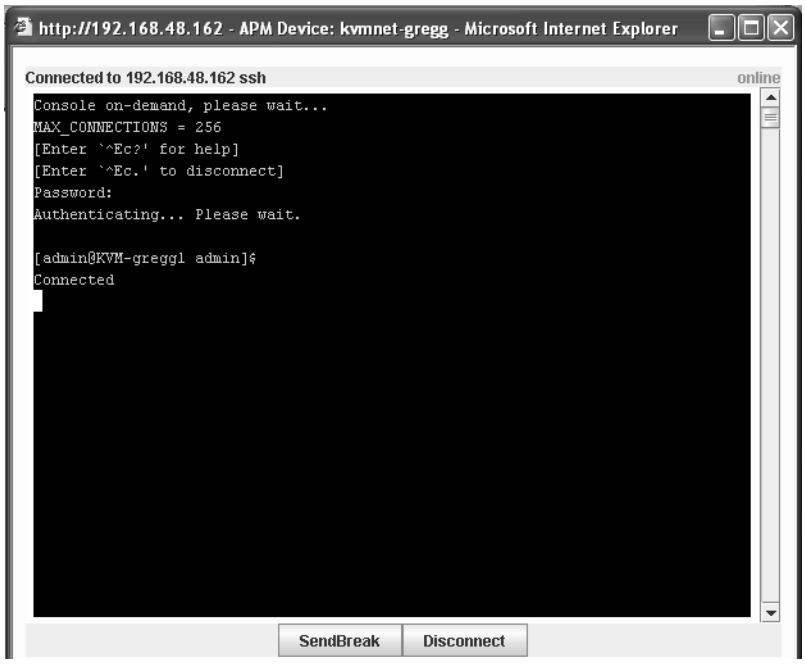

Figure 4-24: Connection to a Device

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

▼ *To Delete a Device*

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

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

▼ *To Delete a Device from a Group*

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

1. From the menu panel, select “Devices.”

   The system displays the Devices List form.
2. Under the “Config” column of the Devices 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 “Groups” on page 161 in this chapter.

▼ *To Upload Firmware to a Console Device*

Using the Device Detail form, you can configure the AlterPath Manager to upload firmware from its firmware repository to any ACS or TS 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.

Note: The Firmware/Boot drop down list only appears in the Device Detail forms of the ACS and the TS.

---

2. Click on the “Save” button.
3. Go back to the Device List form and select the device(s) that need to be uploaded by clicking the corresponding checkbox, and then click “Upload.”

Figure 4-25: Device Firmware Upload

4. Select “Upload firmware/bootcode” and/or “Upload configuration” to select either a firmware upload, a configuration upload, or both.
5. Click on the “Submit” button.

Note: The “Upload firmware/bootcode” option appears even if the AlterPath Manager 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 4-14: 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 4-14: 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

▼ *To Configure 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 DeviceDetails form.

Figure 4-26: KVM Device Details Form

3. From the Device Detail form, click on the “KVM Viewer” tab.

The system displays the KVM Device Viewer form.

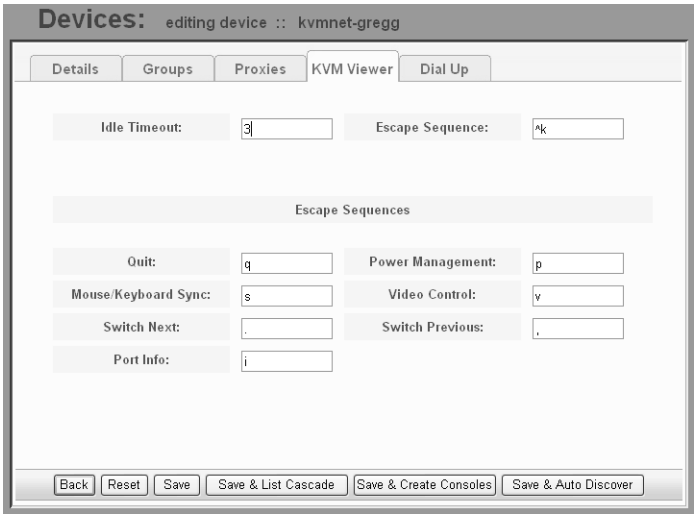

Figure 4-27: KVM Device Viewer Form

Table 4-15: Device 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 4-15: Device 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**.

▼ *To Cascade 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.

3. From the Console Detail form, click on the “Save & List Cascade” button.

The system displays the Device Cascade List form.

Figure 4-28: Device Cascade List Form

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

4. To configure a new device for cascading, click the “Add” button.

Or, to edit an existing cascaded device, click on the “edit” link that corresponds to that device .

The system displays the Device Cascade Detail form:

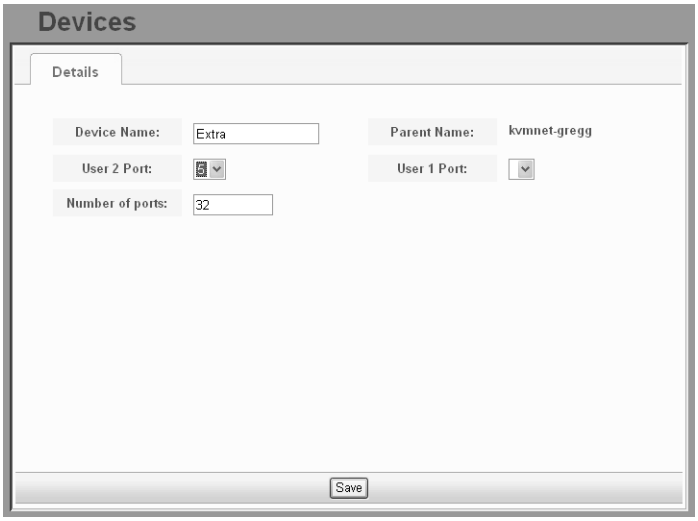

Figure 4-29: Device Cascade Detail Form

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 AlterPath Manager, 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 4-16: 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”).

Table 4-16: Forms Used to Configure Alarms

Form Function	Form(s) Used
Create notification events (email list).	Alarm Trigger detail form (input field: “Notify”).
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’s Profile form.

▼ *To View the Alarm Trigger List Form*

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

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

1. From the menu, select “Alarm Trigger.”

   The system displays the Alarm Trigger List form.

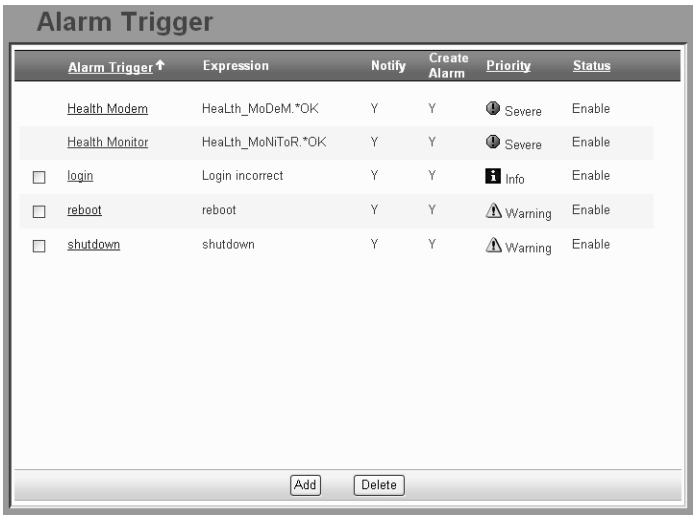

Figure 4-30: Alarm Trigger List Form

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.

▼ *To Create 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.

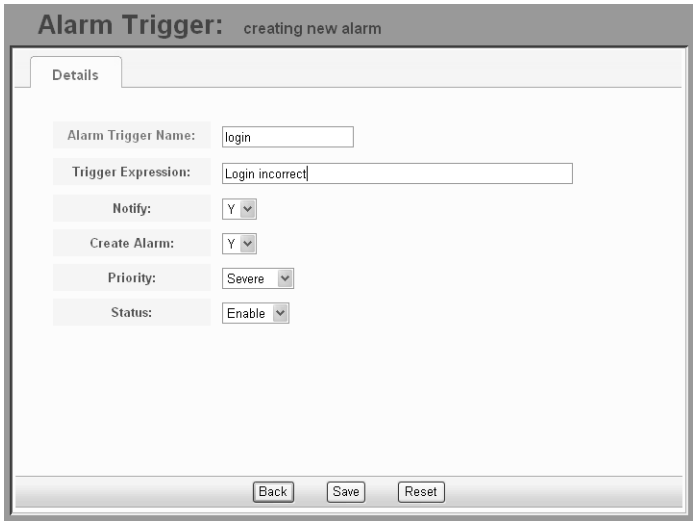

Figure 4-31: Alarm Trigger Detail Form

Table 4-17: 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.e.*, send an email to) the user.
Create Alarm	Yes or No. Indicates if system needs to send an alarm to the user.
Priority	Indicates the priority or severity level of the alarm.
Status	Enable or disable a trigger.
Back	Button to return to the previous page or form.
Save	Button to save your trigger entry.

Table 4-17: Alarm Trigger Detail Form - Fieldnames and Elements

Field Name	Definition
Reset	Button to reset the form to create a new trigger entry.

3. Complete the fields, as necessary.
4. Click the “Save” button to complete the procedure.

▼ *To Delete 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 the “Delete” button.

Configuring Alarms for Device Health Monitoring

To enable the Device Health Monitoring feature of the AlterPath Manager, 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:

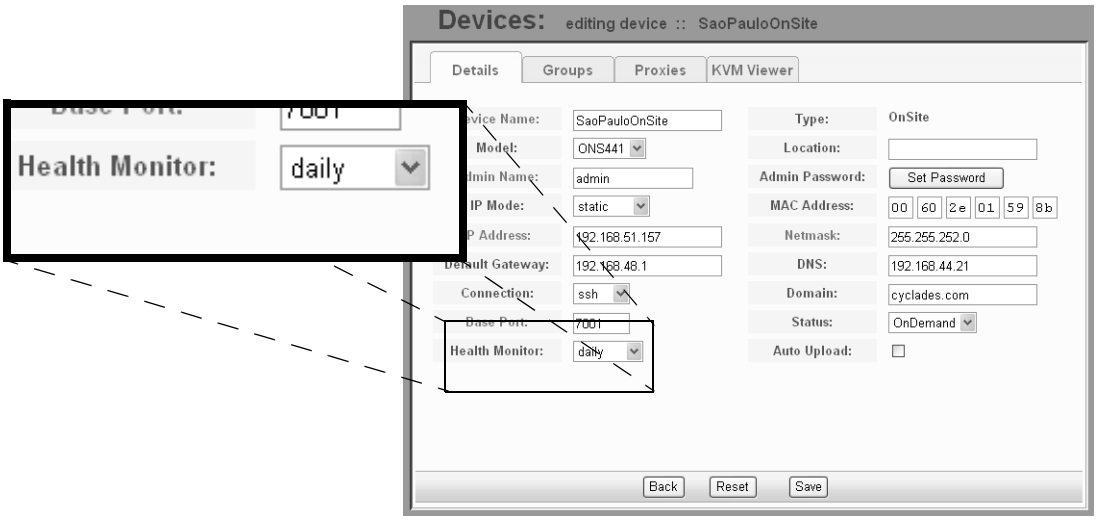

Figure 4-32: Health Monitor User Entry Field

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 at 4 am 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.

▼ *To Define 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).

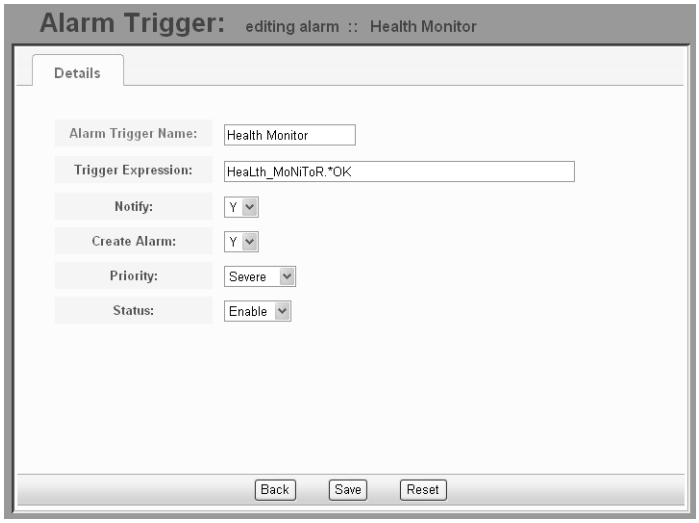

Figure 4-33: Health Monitoring Alarm Trigger Detail Form

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

Table 4-18: Alarm Trigger Setup Fields

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).

Table 4-18: Alarm Trigger Setup Fields

Input Fieldname	Definition
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.

Note: 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 4-19: 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.

Figure 4-34: Profiles List Form

▼ *To Add 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:

Figure 4-35: Profile Detail Form

Table 4-20: 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).
DCD Sensitive	How the console server responds to changes to DCD signal.
Port Break Sequence	As indicated.

Table 4-20: Profiles Detail Form - Fieldnames and Elements

Field Name	Definition
Back / Save / Reset	Buttons for the indicated actions.

2. Enter your port settings and other profile information in the provided fields
3. Click “Save” to complete the configuration.

▼ *To Modify 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. Click “Save” to complete the configuration.

Consoles

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

Table 4-21: Summary of Console Forms

Action	Form(s) Used
Add a new console to connect to the AlterPath Manager and for user access.	Consoles List (“Add” button) > Select Console Type > Console detail.
Select or change the authentication method for console access.	Console Detail form (“Authentication” drop down list) NOTE: The AlterPath Manager authenticates users from the console or terminal server.
Assign the current console to any number of users.	Console Detail form (“Access” tab) > Console Access form.

Table 4-21: Summary of Console Forms

Action	Form(s) Used
Select the users to be notified of any alarms from the current console.	Console Detail form (“Notify” tab) > Console Notify form.
Edit a console.	Consoles List form (“edit” link under the Config column) > Console detail form.
Delete console.	Consoles List form (“Delete” button).
Assign or remove console(s) from the console group.	Console Detail form (“Groups” tab) > Console Groups.
Search, sort, and save list.	Consoles 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 Consoles 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 106 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.

▼ *To View the Console List*

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

1. From the menu panel, select “Consoles.”

The system displays the Consoles List form:

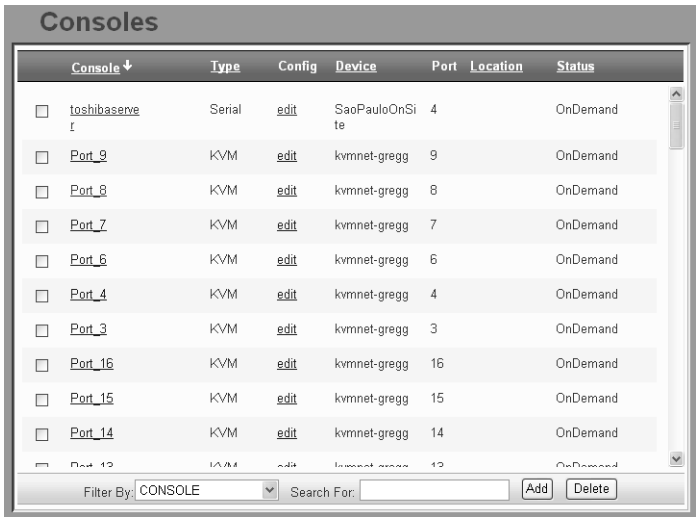

Figure 4-36: Consoles List Form

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

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 “To Change the Number of Consoles per Page” on page 205.

▼ *To Add 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 Consoles List form.

2. From the Consoles List form, click on the “Add” button.

   The system displays the Creating New Console form:

Figure 4-37: Creating New Console Form

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

   The system displays the Console Detail form:

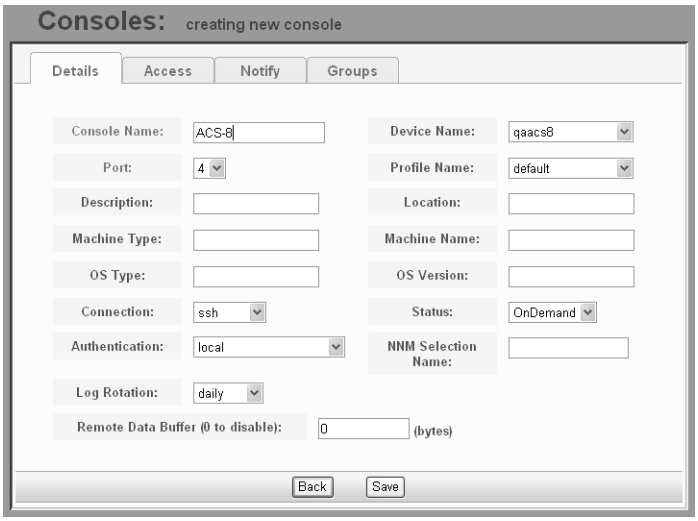

Figure 4-38: Console Detail Form

Table 4-22: Consoles, Details Form - Fieldnames and Elements

Fieldname	Definition
Details	Tab to display the Console Detail form which is the currently displayed form.
Notify	Tab 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	Tab to display the Console Access form used to assign or authorize users to access the current console.
Groups	Tab to display the Select Console Group form used to assign the current console to one or more console groups.
Console Name	*Required*. Name of the console
Device Name	Drop down list. Console server to which the current console is connected.

Table 4-22: Consoles, Details Form - Fieldnames and Elements

Fieldname	Definition
Port	Port on the console server when the console is connected.
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 AlterPath Manager 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 4-22: Consoles, Details Form - Fieldnames and Elements

Fieldname	Definition
Logrotate Now	This field appears only if you selected the "Edit" link instead of the "New" button from the Consoles 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 ports for a KVM/net switch or KVM ports for an OnSite switch.

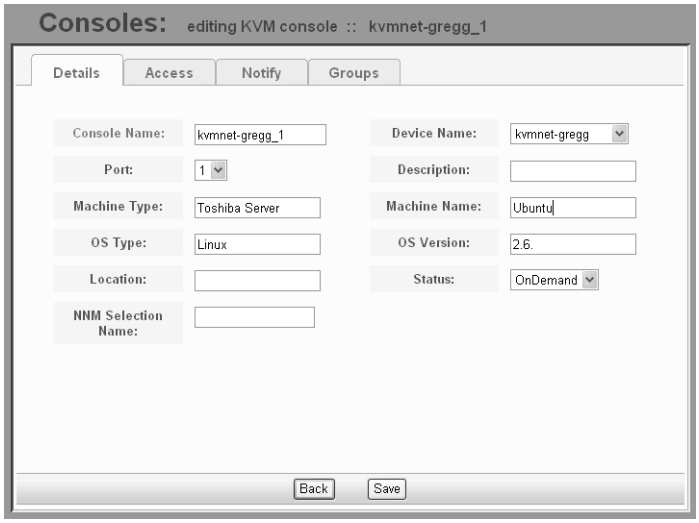

Figure 4-39: KVM/net or OnSite KVM Console Detail Form

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

▼ *To Select 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” tab.

   The system displays the Console Access form:

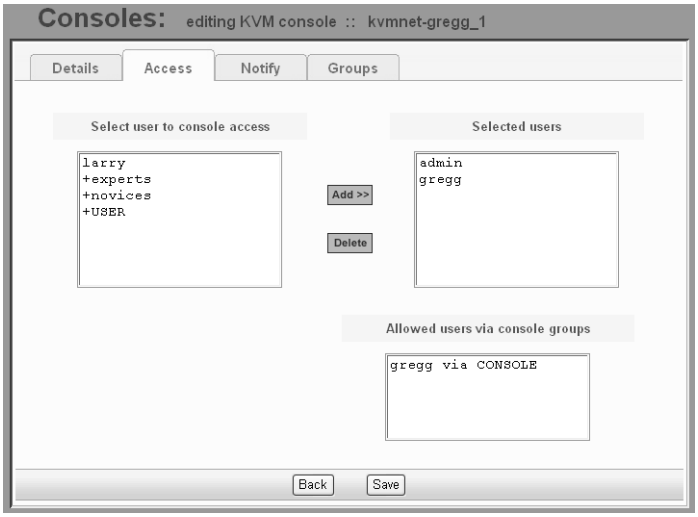

Figure 4-40: KVM Console Access Form

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.

▼ *To Select 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” tab.

   The system displays the KVM Console Notify form:

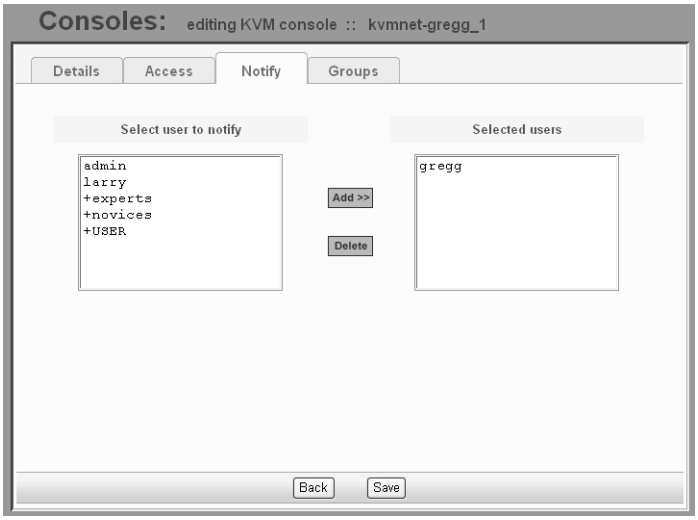

Figure 4-41: KVM Console Notify Form

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.

▼ *To Assign 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:

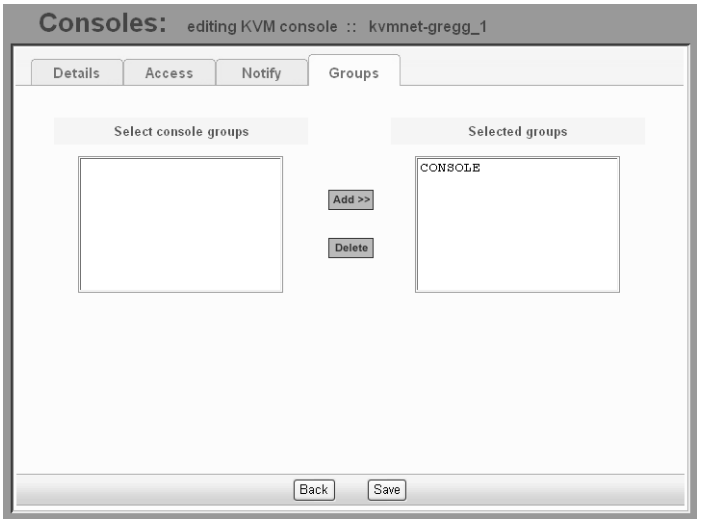

Figure 4-42: KVM Console Groups Form

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.

▼ *To Delete a Console from a Group*

To delete a Console from one or more groups, follow 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.

1. From the Console Detail form, click on the “Groups” tab.
   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 Admin menu.

See “Groups” on page 161 in this chapter.

▼ *To Connect to a Console*

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

Note: This does not apply to KVM consoles.

---

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.

▼ *To Initiate Log Rotate (Manual Operation)*

To initiate the logrotation perform the following steps:

1. From the Console List form, click on the “edit” link for the console whose log you wish to rotate.

   The system displays the Console Detail form.
2. From the Console Detail form, click “Logrotate Now.”

▼ *To Set 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 “edit” link of 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 the “Save” button.

Note: There is a known limitation when log rotation by size is enabled. If the size of the log file is equal to or has exceed the trigger size, the size will not be checked until the time of log rotation has occured (e.g., 2AM for the daily setting, 3AM on Sunday for the weekly setting, and 4AM on the first of the month for the monthly setting).

▼ *To Add an IPMI Console from Console Detail Form*

1. Open the Console List form (Consoles: Console List).
2. From the Console List form, click on the “Add” button.
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 is a paid-for option for AlterPath Manager users. The feature is hidden from users who do not need it.

▼ *To Activate IPMI*

Copy the IPMI license file that you purchased from Cyclades into the following directory on your APM:

`/var/apm/licenses/data/APM_B_IPMI.enc`

Caution: Licenses (except for factory default licenses) must be reinstalled after you recreate the system partition or after you run the "installimg" command.

If you want to preserve your licenses before you recreate a system partition or before you run "installimg," you can edit the file "/etc/files.list" and add your license file name to the list of files. Be sure to use the full path of each license file name you enter into this file. For example if the name of the license file you are adding is "APM_B_IPMI.enc" you should enter the full path name:
`/var/apm/licenses/data/APM_B_IPMI.enc`
Be sure to follow up with the "saveconf" command. It is also a good idea to save a copy of each license file on a server that can be accessed by your APM, just to be extra safe.

If at any time you run "defconf" the file, "/etc/files.list" will revert back to its original state, and you will need to reinstall your license.

Users

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

Table 4-23: 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” tab) > 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” tab) > 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 AlterPath Manager application MUST be entered in the AlterPath Manager database in order to access the application.

User List form

Use the User List form to view all AlterPath Manager 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 AlterPath Manager application *must* be entered in the AlterPath Manager database in order to have access to the application,

regardless of whether you are using any other authentication services or not. RADIUS users, for example, must still be registered in the AlterPath Manager database through the User Detail form:

Below is the Users List form.

Figure 4-43: Users List Form

For an explanation of field column, refer to Table 4-24.

▼ *To Add 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.

Figure 4-44: User Deatil Form

3. Complete the User Detail form, as necessary.

Table 4-24: Users Detail 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 *admin* mode.

Table 4-24: Users Detail 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. 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.
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.

▼ *To Select 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 Users List form.

2. From the Users 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” tab.

   The system displays the User Access form:

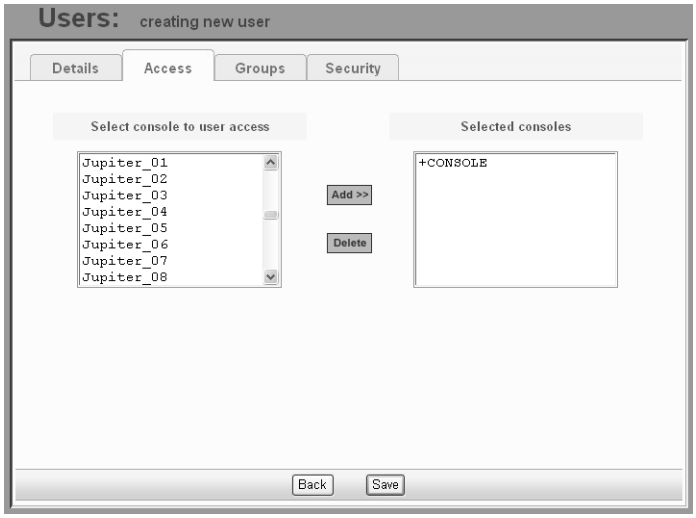

Figure 4-45: User Access Form

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. Click on 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.

▼ *To Select 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 Users List form.

2. From the Users 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 the “Groups” tab.

   The system displays the User Groups form.

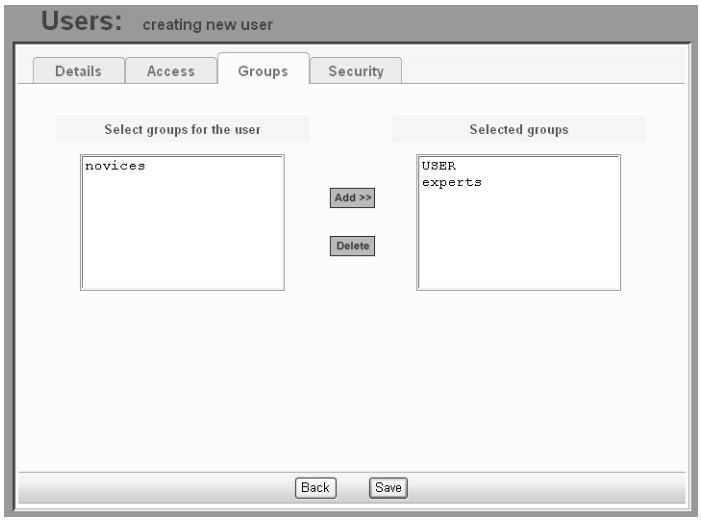

Figure 4-46: User Groups Form

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.

▼ *To Set a User’s Security Profile*

The “Security” tab selects the User’s Security Profile, which allows you to assign or delete a security profile of a user group to which the current user belongs. You can assign a security profile to a user or a user group.

Figure 4-47: User Security Profile Form

▼ *To Delete 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 the “Delete” button.

▼ *To Delete a User from a Group*

1. From the menu panel, select “Users.”

   The system displays the Users List form.

2. From the Users 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 the “Groups” tab.

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

▼ *To Configure the Local Password*

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

1. From the Users List form, select the user for whom you will set a password.

   The system will bring up the definition form for that user.

2. If a password has not been set up, from the User Details form, select set password.

   System brings up the Password dialog box.

3. From the password dialog box, enter the password twice, and then click the “Submit” button.

4. From the User Details form, click on the “Local Password” check box.

5. From the User Details form, click the “Save” button.

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 AlterPath Manager 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.

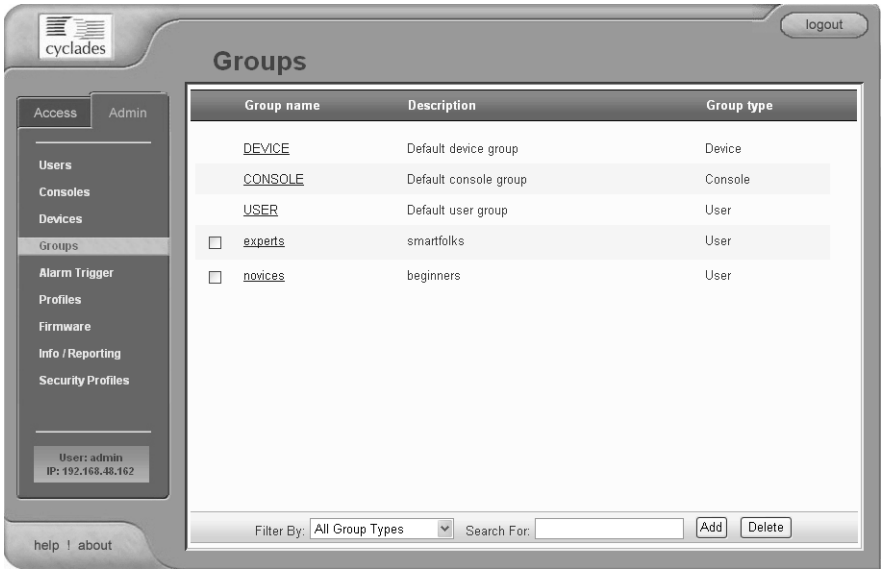

Figure 4-48: Groups List Form

▼ *To Create a Group*

To create a new group, follows the steps below:

1. From the menu, select “Groups.”

   The system displays the Groups List form (Figure 4-48).

2. From the Groups List form, click on the “Add” button.

   The system displays the Adding Group form:

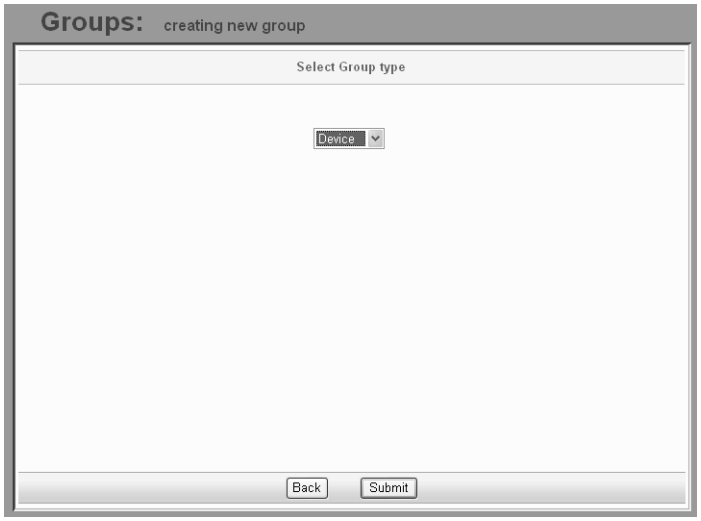

Figure 4-49: Adding Group Form

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 General form for the Group Type, User.

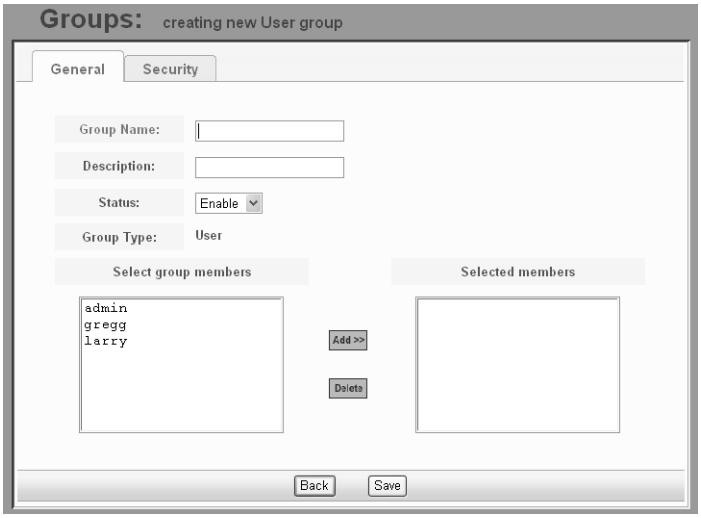

Figure 4-50: New User Group General Form

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

5. Select desired members from the “Select group members” list box.
6. Click on the “Add” button.
7. Click on the “Save” button to complete the procedure.

▼ *To Add Members to a Group*

To add members to an existing group, follow the steps below:

1. From the menu, select “Groups.”
2. From the resulting Groups List form, select the type of group you want to configure.
3. From the resulting Group Details form, choose from the left list box the members you wish to add to the group.
4. Click on the “Save” button.

▼ *To Delete 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 Groups List form.
2. From the Groups List form, click on the checkbox of the group that you wish to delete.
3. Click on the “Delete” button.

▼ *To Assign a Security Profile to a User Group*

Note: The “User” group includes an additional tab, “Security,” which allows you to assign one or more security profiles to the current user group.

1. Select the security profile from the “Select security profile” box and then click on the “Add” tab.
2. Click on the “Save” button.

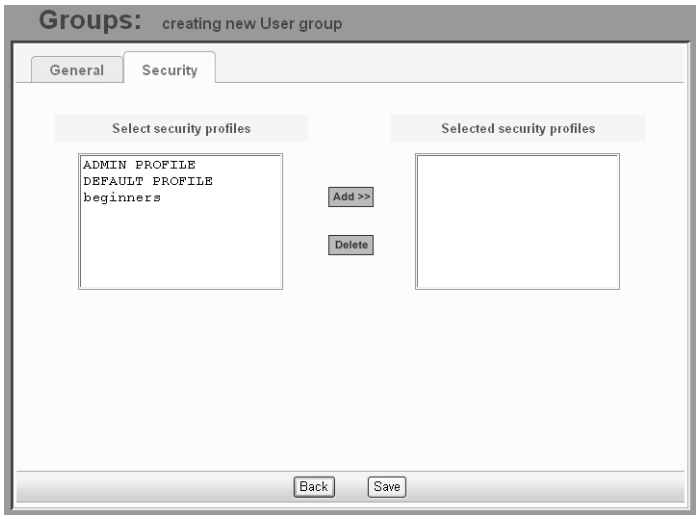

Figure 4-51: New User Group Security Form

Firmware

AlterPath Manager 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 AlterPath Manager 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 “Firmware/Boot” pull-down list that appears in the Device Detail form. 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 AlterPath Manager firmware.

Firmware List Form

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

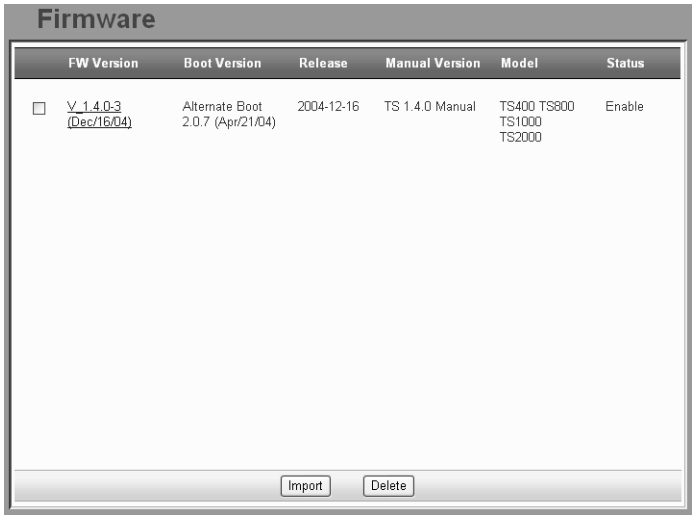

Figure 4-52: Firmware List Form

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

▼ To Add Firmware

Note: Firmware files (.tgz) are normally downloaded from the web and copied into the AlterPath Manager 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 Linux shell on the serial console interface, use the SSH **scp** command to copy the firmware to AlterPath Manager.

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 to the Firmware List form. The system also updates the “Firmware/Boot” pull-down list in the Device Details form.

▼ *To Delete Firmware*

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.

▼ *To Upload Firmware to Console Devices*

1. From the Device Details form (Device List > “edit” link), select the firmware you wish to upload from the “Firmware/Boot” pull-down list.
2. Click the “Save” button.
3. Go back to the Device List form and select the device(s) that need to be uploaded, and then click the “Upload” button.
4. Select “Upload firmware/bootcode” and/or “Upload configuration” (you have the choice to select either firmware, or configuration, or both).
5. Click the “Submit” button.

Note: The “Upload firmware/bootcode” option appears even if the AlterPath Manager 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 4-25: 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.

▼ *To View and Access Firmware Information*

1. From the Firmware List form, select the particular Firmware Version you wish to view.

   The form brings up the Firmware Details form. From the Firmware Details form, you can do any of the following:

2. To access firmware documentation, select "Manual."
3. To access Release Notes for the current firmware, select "Release Notes."
4. Type in notes in the "Comments" input text box and then select "Save" to enter notes and comments about the current firmware.
5. If needed, enter the status (Enable or Disable) of the firmware installation or update.

▼ *To Upgrade the AlterPath Manager Firmware*

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

1. From the Cyclades website (www.cyclades.com), download and copy the firmware to the AlterPath Manager via Secure Copy (SCP).

   The firmware is composed of two files:

   - AlterPath Manager_v110.tgz
   - AlterPath Manager_v110.md5sum.tgz

   Copy the two files to the AlterPath Manager /tmp directory as follows:

   `scp E2000_v131.tgz root@E2000_IP:/tmp` Enter
   `scp E2000_v131.md5sum.tgz` Enter

2. Login to the AlterPath Manager as *root*, and then change the directory to `/tmp` as follows:

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

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

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

Backing Up User Data

Using the serial console interface, you can back up and restore the configuration and data files of the AlterPath Manager 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 AlterPath Manager 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 Type	Definition
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 AlterPath Manager unit. This method enables you to keep the network identity of each AlterPath Manager unit, but maintain the same configuration for both units. The second unit serves as a spare system.
- Replacing the existing AlterPath Manager - You back up ALL data to an external server. The AlterPath Manager 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 the serial console interface, please refer to Chapter 5, “Advanced Configuration.”

System Recovery Guidelines

In the event that the AlterPath Manager 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 AlterPath Manager goes down, you will still have direct access to ports and consoles, but you will need to redefine the devices.

APM Database Transaction Support

The AlterPath Manager commits all successful database transactions to the AlterPath Manager database. To ensure data integrity, the AlterPath Manager 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.

Figure 4-53: Database Error Warning Message

▼ To Respond 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.

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 the “Save” button.

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 accidently 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 AlterPath Manager, please refer to Chapter 5, “Advanced Configuration.”

Info / Reporting

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

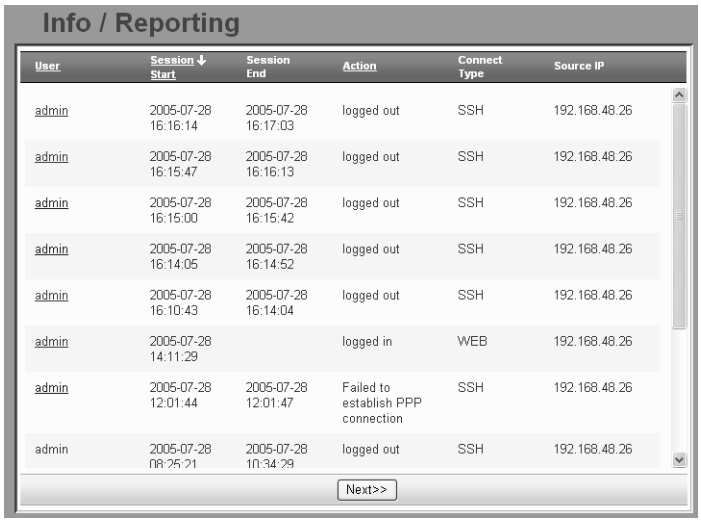

Figure 4-54: Info / Reporting List Form

Table 4-26: Info / Reporting List Form - Fieldnames and Elements

Field Name	Definition
User	Name of session user. To sort by User, click on the “User” column heading.
Session Start	Date and time when the session started. To sort by Session Start, click on the “Session Start” column heading. Down arrow indicates that the list is in descending order; up arrow, in ascending order.
Session End	Date and time when the session ended.

Table 4-26: Info / Reporting List Form - Fieldnames and Elements

Field Name	Definition
Action	The user's action or the system action generated by the user. To sort by Action, click on the "Action" column heading.
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:

Figure 4-55: Info / Reporting Detail List

Security Profiles

A security profile defines a set of rules or conditions regarding a user's access permissions and limits for accessing the AlterPath Manager 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." The conditions you configure in the "Default" profile, are 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 4-27: 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.
LAN ITF	Enter the LAN interfaces and subnets to which you may allow a user to connect.

Table 4-27: Summary of Security Profile Forms

Form Title	Use this form to:
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:

Table 4-28: Security Profile List Column Descriptions

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 appicable, lists all authorized actions for the current profile.
Rule	States whether the rule is to “allow” or “deny.”

Figure 4-56: Security Profiles List Form

▼ *To Add or Edit 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” form.

Figure 4-57: Security Profile General Form

3. From the Security Profile General 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 the “Save” button.

▼ *To Configure Conditions for Accepting Source Pages*

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

   The system displays the Security Profile Source IP form.

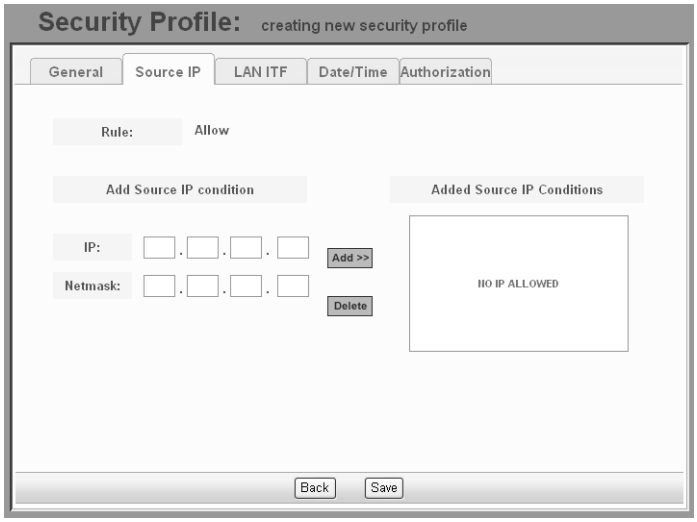

Figure 4-58: Security Profile Source IP Form

2. Complete or modify the form, as needed.

Table 4-29: 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.
Add	Button to add to the conditions list the address you just entered in the IP or Netmask field.

Table 4-29: Security Profiles, Source IP - Fieldnames and Elements

Field Name	Function
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 the “Save” button.

Security Profiles: LAN ITF

The LAN ITF (Local Area Network Interfaces) 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.

Figure 4-59: Security Profile LAN Inerfaces Form

Table 4-30: Security Profiles, LAN ITF - Fieldnames & Elements

Field Name	*Function*
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” list box and add to the “Selected LAN ITF Conditions” list 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.

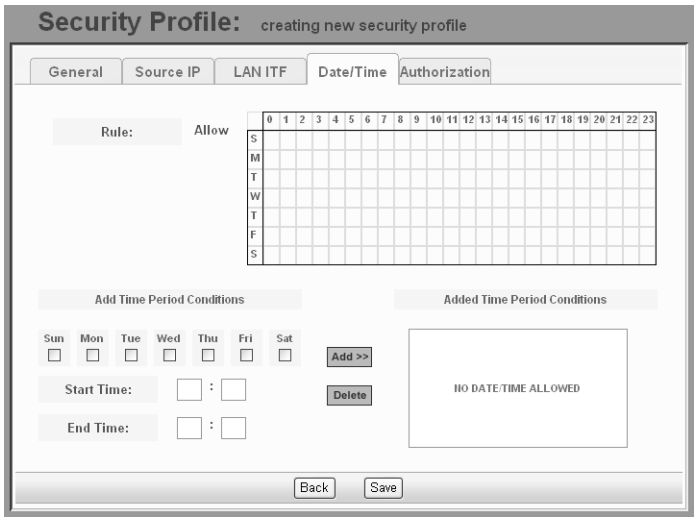

Figure 4-60: Security Profile Date / Time Form

Table 4-31: 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.
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.

Table 4-31: Security Profiles Date/Time Form - Fieldnames and Elements

Field Name	Function
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.

Figure 4-61: Security Profile Authorization Form

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.

▼ *To Delete 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 the “Delete” button.

Chapter 5
Advanced Configuration

This chapter presents some procedures for configuring the AlterPath Manager E2000 and 2500 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 AlterPath Manager.

This chapter is organized as follows:

Working from a CLI

The AlterPath Manager allows you to use a command line interface (CLI) as an alternative to the web interface. You can use a terminal or terminal emulator on a local workstation to connect to the APM's console port. You may also use a Linux or Windows-based secure shell (SSH) client. The same restrictions to the web management interface apply to the CLI.

Note: Throughout this manual, the term "CLI" refers to the command line interface provided by the APM's console port. This interface can also be accessed through an ssh connection to the APM's IP address. There is also a CLI shell that provides access to ACS/TS type consoles.

▼ *To Log Into the Serial Console Port*

1. Connect a terminal or a computer with a terminal emulator to the APM's serial console port, using a null modem cable.
2. Power on the APM and start the terminal or terminal emulator.
3. When prompted, log in.

▼ *To Do a Windows SSH Login*

1. Using an IP connection client such as PuTTY, select “SSH” for the protocol setting.
2. In the client’s IP address window, type the IP address of the APM.

   A CLI screen will be launched.
3. When prompted, log onto the APM.

▼ *To Do a Linux or UNIX SSH Login*

To connect to the AlterPath Manager, from a Linux or UNIX shell prompt, enter the following shell commands:

```
# ssh -l <username> <IP_address_of_APM>
# <password>
```

Note: The “**l**” in **ssh-1** is the alphabetical character “l” as in *lemon*.

If you are an admin user, the system will display a menu.

You can either run the “CLI” shell from the menu, or you can go directly to a Linux system prompt.

If you log in to the CLI as root, you will only have access to the Linux system prompt, but you will have all the normal privileges as any root user on any Linux system.

If you are a regular user, you will get the “CLI” shell alone, without a menu or system prompt. This will give you access primarily to serial (ACS/TS) consoles configured on the APM.

If you are an admin user, you will get a menu that gives you the following choices:

```
Please choose from one of the following options:

1.      CLI
2.      Shell Prompt
3.      Quit


Option ==>
```

Shell Commands

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

Table 5-1: CLI Specific Commands

Command	Use this command to:
man list	list the available commands.
man <command name>	get a definition of and syntax help for 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:

Table 5-2: Console Applet Window Menu 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..

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 AlterPath Manager as a security proxy.

▼ To Connect from a Windows SSH Client

1. Using a Windows SSH client, such as Putty, select “SSH” for the protocol.
2. In the “Host Name (or IP address)” field, type the connection parameters in the following format:

   ```
   <user name>:<console name>@<IP address of APM>
   ```

   Figure 5-1 shows a PuTTY configuration window with a sample SSH configuration setup that uses the APM as a security proxy.

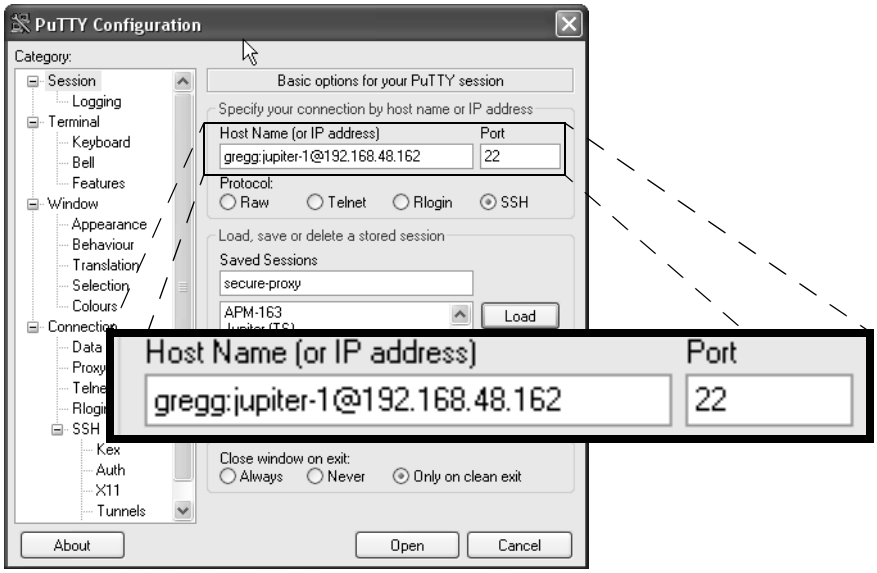

Figure 5-1: PuTTY Configuration of APM as a Security Proxy

▼ *To Connect SSH from a Linux or UNIX System*

Using SSH on a Linux or UNIX system, type in:

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

This command opens a SSH connection to the AlterPath Manager, checks the username and password, checks the access control list to verify user access, and then establishes the connection to the appropriate console. After the connection is established, you will be prompted to log in to the system connected to the console port.

Sample Command Line Interface

An example of a command line interface as accessed by an admin follows:

```
Cyclades-APM V_1.3.1 (Aug/03/2005) - Console (kernel 2.4.25)

APM_Gregg login: admin
Password:

************************************************************************
* WARNING: changing system files directly is dangerous and may adversely *
*          affect your system's functionality. Proceed with caution, and *
*          only if you know what you are doing!                          *
************************************************************************


               --------------------------------------------------
                                 AlterPath Manager
               --------------------------------------------------



Please choose from one of the following options:

1.      CLI
2.      Shell Prompt
3.      Quit

Option ==> 1
User: admin
AlterPath Manager @(#)V_1.3.1 (06/24/2005) - CLI
admin@Mgr> man list
console        - connects to a console
consolelist    - lists all consoles you are allowed to access
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> consolelist
Jupiter_01 - port 1
Jupiter_02 - port 2
Jupiter_03 - port 3
Jupiter_04 - port 4
toshibaserver - port 4
admin@Mgr> console toshibaserver
Console on-demand, please wait...
MAX_CONNECTIONS = 256
[Enter `^Ec?' for help]
[Enter `^Ec.' to disconnect]
admin:7004@192.168.48.199's password:
Authenticating... Please wait.


Connected
```

Console Session Hot Keys

For your convenience, the console session hot key commands (viewable by pressing Ctrl+Shift+e c ?) are summarized in the table below. Each command must be preceded by Ctrl+Shift+e c (abbreviated in the menu as ^Ec).

For example, to send a broadcast message, you must press: Ctrl+Shift+e and then c and then b

Table 5-3: Console Applet ^Ec Command Set.

Command	Action	Command	Action
.	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?** (letter “el” ?)	break sequence list
l0	send break per config file	**l1-9** (letter “el” one - nine)	send specific break sequence
o	(re)open the tty and log file	**p**	replay the last 60 lines
r	replay the last 20 lines	**s**	spy read only
u	show host status	**v**	show version info
w	who is on this console	**x**	show console baud info
z	suspend the connection	**<cr>**	ignore/abort command
?	print this message	**^R**	replay the last line
\ooo	send character by octal code	**Off**	power off
On	power on	**Os**	power status

To exit from the CLI, press: Ctrl+*underscore*

Set Commands

The following set commands are available to enable you to manually and individually configure specific AlterPath Manager settings from the Linux shell:

Example sessions of each of the set commands follow:

SETAUTH - Set Authentication

```
[root@APM-gregg data]# 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.
*** WARNING: It may be required to restart the sshd daemon.
[root@APM-gregg data]#
```

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 - Set the Network Boot Utility

```
[root@APM-gregg root]# setboot

Manager Network Boot Configuration Utility
----------------------------------------
Current Status:         DISABLED

Press <ENTER> if you wish to change it, or [Q<ENTER>] to quit:

Enter Local IP Address []: <IP_of_APM>

Enter Server IP Address []: <IP_of_tftpboot>

Enter Kernel Filename []: <kernel_filename>

Enter InitRD Filename []: <initRD_filename>

WARNING: make sure you're setting valid values for the network boot
         parameters, or the network boot may not work!

Current Status:         ENABLED
- Local IP Address:     <IP_of_APM>
- Server IP Address:    <IP_of_tftpboot>
- Kernel Filename:      <kernel_filename>
- InitRD Filename:      <initRD_filename>
Do you wish to save these parameters? (y/N) y
Saving network boot configuration ... done.
NOTE: the new network boot parameters will be effective after the next reboot.
```

SETCONS - Set Console Connection

```
[root@APM-gregg 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) y
Saving console configuration ... done.
NOTE: the new console parameters will be effective after the next reboot.
```

SETDATETIME - Set System Date and Time

```
[root@APM-gregg root]# setdatetime
Please choose the time zone where this machine is located.
 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) SystemV
 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:
    Wed Aug 31 20:03:15 PDT 2005
Press ENTER to accept it or specify new ones.
Enter date in MM/DD/YYYY format: 08/31/2005
Enter time in HH:MM format: 20:07
Wed Aug 31 20:07:00 PDT 2005

*** Configuration changed!
*** Execute saveconf to save the new values in flash.
[root@APM-gregg root]# saveconf
Saving configuration files to flash (/flash/config/config.tgz)... done.
```

SETDHCP - View Dynamic IP Addressing

```
[root@APM-gregg root]# setdhcp
        ddns-update-style ad-hoc;
#subnet 192.168.44.0 netmask 255.255.252.0 {
        #eth0
#}

#subnet 192.168.160.0 netmask 255.255.255.0 {
        #eth1
        #option routers                 192.168.160.1;
        #option subnet-mask             255.255.255.0;
        #option broadcastAddr           192.168.160.255;
        #option dhcpT1value             21610;
        #option dhcpT2value             37800;
        #option nis-domain              "cyclades.com";
        #option domain-name             "cyclades.com";
        #option domain-name-servers     192.168.160.1;
        #option time-offset              -8;
        #option ntp-servers             192.168.1.1;
        #range                          192.168.160.100, 192.168.160.200;
        #default-lease-time             21600;
        #max-lease-time                 43200;
        #default-lease-time             600;
        #max-lease-time                 7200;
#}

subnet 192.168.48.0 netmask 255.255.252.0 {
        #eth0
}

subnet 10.10.0.0 netmask 255.255.0.0 {
        #eth1
}
```

SETETHERNET - Set Ethernet Speed and Duplex

Note: Gigabit Ethernet is available on the APM 2500 only.

Note: Ethernet and other expansion cards are not supported on the APM 2500.

```
[root@APM-gregg root]# setethernet
Current Ethernet eth0 speed/duplex settings: AUTO
Change Ethernet eth0 speed/duplex: (Y)es or (N)o ? [N]: y
Choose the correct operation mode:
  1) Auto-negotiation
  2) 10 Mbps, full duplex
  3) 10 Mbps, half duplex
  4) 100 Mbps, full duplex
  5) 100 Mbps, half duplex
  6) 1000 Mbps, full duplex
  7) 1000 Mbps, half duplex
Enter the number corresponding to your choice [1]: 1
Enabling auto-negotiation for eth0.
Current Ethernet eth1 speed/duplex settings: AUTO
Change Ethernet eth1 speed/duplex: (Y)es or (N)o ? [N]: y
Choose the correct operation mode:
  1) Auto-negotiation
  2) 10 Mbps, full duplex
  3) 10 Mbps, half duplex
  4) 100 Mbps, full duplex
  5) 100 Mbps, half duplex
  6) 1000 Mbps, full duplex
  7) 1000 Mbps, half duplex
Enter the number corresponding to your choice [1]: 1
Enabling auto-negotiation for eth1.

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

Configuring eth0 speed/duplex...
Configuring eth1 speed/duplex...
```

SETHOSTS - Synchronize Host Names

```
[root@APM-gregg root]# sethosts

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

SETNAMES - Set Host, Domain Names, Nameserver

```
[root@APM-gregg root]# setnames
Enter the System's Hostname
    (max 30 characters) [APM-gregg]: Accounting-APM
Enter the System's Domain Name
    (max 60 chars) [localdomain]: <domain_name>
Enter the Primary Nameserver's IP address [none]: 192.168.44.21
Enter the Secondary Nameserver's IP address [none]:

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

SETNETWORK - Set Ethernet Subinterfaces

```
[root@APM-gregg root]# setnetwork
Ethernet eth0 IP address: (S)tatic, (N)one or (K)eep current ? [K]: s
Enter Ethernet eth0 IP address: 192.168.48.162
Enter Ethernet eth0 Subnet Mask: 255.255.252.0
Ethernet eth1 IP address: (S)tatic, (N)one or (K)eep current ? [K]: s
Enter Ethernet eth1 IP address: 10.10.10.2
Enter Ethernet eth1 Subnet Mask: 255.255.0.0
Configure  Ethernet Subinterfaces: (Y)es, (N)o or (L)ist ? [N]: l
Number of Subinterfaces already configured: 0
Configure  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]: 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]: y
Enter the Ethernet number [0-1]: 1
Enter the Subinterface index [0-9999]: 9999
Subinterface eth1:9999 IP address: (S)tatic or (N)one ? [S]: s
Enter Subinterface eth1:9999 IP address: 2.2.2.2
Enter Subinterface eth1:9999 Subnet Mask: 255.0.0.0
Configure more Ethernet Subinterfaces: (Y)es, (N)o or (L)ist ? [N]: l
eth0:1, 1.1.1.1, 255.0.0.0
eth1:9999, 2.2.2.2, 255.0.0.0
Number of Subinterfaces already configured: 2
Configure more Ethernet Subinterfaces: (Y)es, (N)o or (L)ist ? [N]: n
Configure  Ethernet VLANs: (Y)es, (N)o or (L)ist ? [N]: y
Enter the Ethernet number [0-1]: 0
Enter the VLAN index [0-4094]: 1
VLAN eth0.1 IP address: (S)tatic or (N)one ? [S]: s
Enter VLAN eth0.1 IP address: 3.3.3.3
Enter VLAN eth0.1 Subnet Mask: 255.0.0.0
Configure more Ethernet VLANs: (Y)es, (N)o or (L)ist ? [N]: n
Enter Ethernet Default Gateway [none]: 192.168.48.1

*** Configuration changed!
*** Execute saveconf to save the new values in flash.
Do you want to make these changes effective now (y/n)? y
Reconfiguring network interfaces: Added VLAN with VID == 1 to IF -:eth0:-
WARNING:  VLAN 1 does not work with many switches,
consider another number if you have problems.
```

```
Configuring eth0 speed/duplex...
Configuring eth1 speed/duplex...
done.
Shutting down dhcpd: OK
Starting dhcpd: OK
Stopping Tomcat... OK.
Stopping sniff_port daemon: sniff_port.
Starting sniff_port daemon: sniff_port.
Starting Tomcat... OK.
```

Note: 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, and 0:9999.

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 Ctrl+c to stop changing interfaces and keep all changes made. If you do not exit with Ctrl+c at the end, the script will ask if you want to make the changes effective now. If you answer “y” the script automatically runs `/etc/init.d/networking restart`.

SETNTP - Set Network Time ProtSocol Server

```
[root@APM-gregg root]# setntp
Enter the NTP server: 192.168.48.164

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

SETSERIAL - Examine the Serial Port Parameters

```
[root@APM-gregg root]# setserial /dev/ttyS0
/dev/ttyS0, UART: 16550A, Port: 0x03f8, IRQ: 4
```

SETSMTP - Set the Email Server's IP Address.

```
[root@APM-gregg root]# setsmtp
Enter the email (SMTP) server: smtp.<your_domain.com

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

DATE - Set the Date and Time

Note: Date format is: [MMDDhhmm[[CC]YY].SS]

```
[root@APM-gregg root]# date 083122552005
Wed Aug 31 22:55:00 PDT 2005
```

Changing the Escape Sequence

There are two ways to change the escape sequence:

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

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

```
#modify this line to have -e <escape seq>.
```

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+Shift+hyphen* (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 `/var/apm/bin/apmrun.sh` file, below the commented line shown:

```
# Redefine CTRL+C here. Customize it as you wish.
stty intr ^_
```

▼ To Change the Number of Lines in the SSH Applet

Note: 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.

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.

▼ To Change 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
```

▼ To Change the Number of Consoles per Page

The default number of consoles that you can view from the Consoles List form is set to 512. Edit the `/var/apm/apm.properties` file.

4. Go to the `apm.consolesperpage=512` line.
5. Change the “512” in the line to the value desired.

▼ To Enable Telnet

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

1. Edit `/etc/services and` add the following line:

```
telnet          23/udp
```

2. Edit `/etc/xinetd.conf` by removing the # symbols from the beginning of the following lines so they appear as shown below:

```
#service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/kerberos/sbin/
        telnetdlog_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 restart
```

Note: xinetd services will be available after reboot, since this script is already included in the startup procedure.

▼ To Change 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
 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 AlterPath Manager.

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

The Ethernet hardware has commands to control the link speed and duplex supported on each interface.

There is a script named “setethernet” that is invoked automatically along with the other initial APM configuration the first time the APM is run (see “First Time Configuration Wizard” on page 68).The setethernet script can also be run by the administrator manually from the console at any time.

Refer to “SETETHERNET - Set Ethernet Speed and Duplex” on page 199 for details on configuring the Ethernet port.

Note: Gigabit Ethernet is available on the APM 2500 only.

Modem Card Configuration

Note: Modems are not supported on the APM 2500.

The AlterPath Manager 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 AlterPath Manager, 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@APM root]# check_modem -s
ttyPS0 Available
ttyPS1 Available
ttyPS2 Available
ttyPS3 Available
```

▼ To Exclude Modems from the Modem Pool

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

1. Using VI, edit the following file: **`vi /var/apm/apm.properties`** <ENTER>
2. Type in: **`modem.pool.exclude=ttyPS`**

   For example, to exclude ttyPS2 and ttyPS3, type in: **`modem.pool.exclude=ttyPS2 ttyPS3`**
3. Once a modem has been excluded, you must initialize the configuration by typing in: **`/etc/init.d/modem_pool restart`**

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

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

Viewing the Latest Status 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@APM 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 Manager supports the use of a PCI-based multi-port serial cards. The cards are used to connect the AlterPath Manager 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 AlterPath Manager. If one or more

modems are connected after the AlterPath Manager 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

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 AlterPath Manager, 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@APM 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@APM 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
```

▼ *To Define Different Scripts for Each tty Device*

The modem chat scripts are located in "/etc/ppp", and are used by "pppd" to initialize the modem and to dial out.

The file, "/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. Enter **`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 96, Chapter 4: AlterPath Manager 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 AlterPath Manager 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 AlterPath Manager "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 AlterPath Manager "Dial Up" form.

- From the AlterPath Manager, go to "/var/apm/apm.properties" file and add the APM phone number in the parameter: "dial.apm_phone_number=<phone number>"

Note: The AlterPath Manager 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 AlterPath Manager, 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 AlterPath Manager will wait for 60 seconds.

- Define the time (in seconds) in which the AlterPath Manager should wait before allocating the modems for dial-in after receiving a confirmation from an ACS that it will call the AlterPath Manager 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.ttySn”

to:

“/etc/ppp/options.ttyS*(n+1)*”

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:
<actions>	this syntax has this format: [<status>=<action>] WHERE: <status> = SUCCESS, NOTFOUND, UNAVAIL, or TRYAGAIN <action> = 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 *return*.
NOT FOUND	The lookup process works, but the needed value was not found. The default action for this status is *continue*.
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 AlterPath Manager 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 AlterPath Manager 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
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 AlterPath Manager 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 AlterPath Manager

The AlterPath Manager automatically creates “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 “/etc/krb5.keytab” file into the AlterPath Manager.

Method 1:

Using SCP, copy the “/etc/krb5.keytab” file from the Kerberos Key Distribution Center (KDC), also known as the Kerberos Server.

Method 2:

Connect to the Kerberos database by executing the command:
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
```

▼ *To Configure Active Directory*

1. Choose the “active_directory” authentication method at the following prompt:

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

2. Enter the Active Directory server: **<active_directory_server_name>**
3. Enter the distinguished name of the search base:

   ```
   (ex: 'dc=cyclades,dc=com'):
   dc=<first_part_of_domain_mame>,dc=<second_part_of_domain_name>
   ```

Note: The second part of the domain name is usually ".com," ".net," ".org," etc.

4. Enter the common name to bind to the server:

```
(ex: 'cn=Administrator,cn=Users,dc=cyclades,dc=com'):
dc=<first_part_of_domain_mame>,dc=<second_part_of_domain_name>
```

5. Enter the password to bind with:
6. Re-enter the password:

   The following messages will be displayed:

```
*** Configuration changed!

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

*** WARNING: It may be required to restart the sshd daemon.

[root@APM_2500 root]#
```

▼ *To Disable HTTP to Use Only HTTPS*

The AlterPath Manager 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 out 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

▼ *To Add Firmware*

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

1. From the web (www.cyclades.com), download the firmware to the server you use to store your firmware.
2. Connect to the AlterPath Manager from your server using SSH.
3. Use the “scp” command to copy the firmware to the AlterPath Manager from your server.

   Example: **`scp v214.tgz root@<ip_address>:/usr/fw`**
4. 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.

▼ *To Upgrade the APM Firmware*

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

1. From the Cyclades website (www.cyclades.com), download and copy the firmware to the server you want to use to store firmware for the AlterPath Manager.

   The firmware is composed of two files:

   - APM_v131.tgz
   - APM_v131.md5sum.tgz
2. From your firmware server, copy the two files to the AlterPath Manager / tmp directory as follows:

```
scp APM_v131.tgz root@APM_IP:/tmp
scp APM_v131.md5sum.tgz
```

3. Login to the AlterPath Manager as “root”, and then change the directory to “/tmp” as follows:

```
ssh root@APM_IP
cd /tmp
```

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

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

Caution: Licenses (except for factory default licenses) must be reinstalled after you recreate the system partition or after you run the “installimg” command.

If you want to preserve your licenses before you recreate a system partition or before you run “installimg,” you can edit the file “/etc/files.list” and add your license file name to the list of files. Be sure to use the full path of each license file name you enter into this file. For example if the name of the license file you are adding is “APM_B_IPMI.enc” you should enter the full path name: **`/var/apm/licenses/data/APM_B_IPMI.enc`**
Be sure to follow up with the “saveconf” command. It is also a good idea to save a copy of each license file on a server that can be accessed by your APM, just to be extra safe.

If at any time you run “defconf” the file, “/etc/files.list” will revert back to its original state, and you will need to reinstall your license.

Backing Up User Data

Using CLI, you can back up and restore the configuration and data files of the AlterPath Manager to a local or a remote destination. This feature allows you

to backup and restore (either independently or altogether) the following data types:

Table 5-4: Data Types You Can Backup and Restore

Data Type	Definition
System Configuration	Data related to the AlterPath Manager 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 AlterPath Manager unit. This method enables you to keep the network identity of each AlterPath Manager unit, but maintain the same configuration for both units. The second unit serves as a spare system.
- Replacing the existing AlterPath Manager - You back up ALL data to an external server. The AlterPath Manager 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

From the CLI at the Linux shell prompt, the command lines 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 on the local host, or executes a restore from the local host.

The backup/restore operations use secure copy (scp). The file is saved as a tar file (*.tgz).

Note: You must reboot after you execute either the “restore sys” command or the “restore all” command.

Managing Log Files

Where Log Files are Archived

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

```
/var/log/consoles/rotated
```

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

Backing Up Log Files to a Remote Server

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

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

Where:

-flush deletes the current rotated logs

-now forces an immediate log rotation

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

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

For remote destination, ensure that the remote machine is prepared to accept connections to ssh service on port 22. If only the file name is supplied, the

system will copy the logs locally. You can include path names as part of the file name.

System Recovery Guidelines

In the event that the AlterPath Manager 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 AlterPath Manager 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".

Table 5-5: Default Configuration Values from the "apm.properties" File

Property Name	Default Property Value	If you change the default property value, ensure that . . .
db.apm	apmdb	The system creates a corresponding database.
db.apm.user	apm	The system creates a corresponding database user.

Table 5-5: Default Configuration Values from the "apm.properties" File

Property Name	Default Property Value	If you change the default property value, ensure that . . .
db.apm.pw	apmdb	The system creates a corresponding database.
db.apm.max_connections	20	"max_connections" in my.cnf file is set to greater or equal to "db.apm.max_connections" value.
db.apm.min_connections	10	
db.apm.host	localhost	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
```

▼ *To Install SSL Certificates*

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

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

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

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:

Table 5-6: Information for the "openssl" Command

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.*, jcertfile.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" subcommand:

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

The certification becomes effective in the next reboot.

More About Importing Certificates

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

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

You import a certificate for two reasons:

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

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

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

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

```
keytool -printcert -file /tmp/cert
  Owner: CN=ll, OU=ll, O=ll, L=ll, S=ll, C=ll
```

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

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

Note: It is not required that you execute a "-printcert" subcommand prior to importing a certificate, since before adding a certificate to the list of trusted certificates in the keystore, the "-import" subcommand prints out the certificate information and prompts you to verify it. You then have the option of aborting the import operation. 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
Technical Specifications

Hardware Specifications

Feature	AlterPath E2000	AlterPath 2500
CPU	Intel® Celeron® 850MHz	Intel Celeron 3.06GHz
Memory	512MB RAM 256MB compact flash	2GB RAM 256MB compact flash
HDD	80GB SATA	160GB SATA
Interfaces	2 x 10/100 MB auto sense Ethernet	2 x 10/100/1000 auto sense Ethernet
Dimensions (W x D x H)	1U @ 17 x 14.5 x 1.75 in (43.18 x 36.25 x 4.45 cm)	1U @ 16.8 x 14 x 1.75 in (42.67 x 35.56 x 4.45 cm)
PCI slots	2	1
LCD front panel	No	Yes
Power Supply	150W, single, 115 - 230V~, autoranging	260W, single, 115 - 230V~, autoranging
Operating Temperature	50°F to 112°F (10°C to 44°C)	50°F to 95°F (10°C to 35°C)
Operating Humidity	20% to 90% relative, non-condensing	5% to 90% relative, non-condensing
Storage Temperature	32°F to 158°F (0°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Storage Humidity	5% to 95% relative, non-condensing	5% to 95% relative, non-condensing

Software Specifications

Feature	AlterPath E2000	AlterPath 2500
Operating system	Linux 2.4.x (embedded)	Linux 2.4.x (embedded)
Users and administrators	Unlimited	Unlimited
Managed devices	2048	2048
Managed consoles	4096 (fixed)	1024 to 8192 (licensed)
Data logging	256 (fixed)	64 to 512 (licensed)
Concurrent serial console sessions	256 (fixed)	64 to 512 (licensed)
Support for KVM/net	Yes (SW 1.1.0 and above)	Yes (SW 1.1.0 and above)
Support for OnSite	Yes	Yes
Support for TS	Yes	Yes
Support for ACS	Yes	Yes
Supported web browsers	Internet Explorer 6.0 Mozilla 1.02 Netscape 7.1	Internet Explorer 6.0 Mozilla 1.02 Netscape 7.1
Java runtime plug-ins	1.4.2 or greater	1.4.2 or greater

Appendix B
ACS Modem Configuration

The AlterPath Manager allows you to automatically dial out to remote console servers such as the AlterPath Consolde 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.

▼ *To Configure the PCMCIA Modem*

1. Edit the file `/etc/ppp/pap-secrets`.

   When the file is opened for the first time, it should look something like this:

```
# Secrets for authentication using PAP
# client        server  secret           IP addresses
#"mary"         *       "marypasswd"            *
```

2. Add the following line:

   ```
   *               *           ""                   *
   ```

   The file should now look something like this:

```
# Secrets for authentication using PAP
# client        server  secret           IP addresses
#"mary"         *       "marypasswd"            *
*               *           ""                  *
```

This configures the modem to accept any password.

▼ *To Configure the External Modem*

To configure your external modem, perform the following steps:

Caution: Ensure that you do not configure the console where the modem is attached otherwise any upload process on the console will overwrite your configuration.

1. Open the file, `/etc/portslave/pslave.conf` in an editor such as VI.
2. Go to the "all.initchat" section of the file.

   The "all.initchat" section of the `/etc/portslave/pslave.conf` file appears as follows the first time the file is opened:

```
#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
```

3. Modify the "all.initchat" section by removing all the "#" symbols from the beginning of each line in the section.
4. Change the first line of "all.initchat" to"sxx.initchat" (where *xx* is the number of the serial port to which the external modem is attached).

The section should now appear as follows:

```
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
```

5. Go to the “all.autoppp” section of the `/etc/portslave/pslave.conf` file.

   The “all.autoppp” section will appear as follows when the file is first opened:

```
#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
```

6. Remove the “#” symbols from the beginning of the first 4 lines in this section.

   Optionally, you can remove the two remaining lines that begin with “#” (“ms-dns 192.168.160.5 ms-dns 0.0.0.0 \” and “plugin /usr/lib/libpsr.so”).

Note: If you do not remove these two lines, leave the “#” symbol in front of each one.

7. Change “all.autoppp” to “sxx.autoppp” (where *xx* is the number of the serial port to which the external modem is attached).

8. In the first line of this section, change "%i:%j" to "0.0.0.0:0.0.0.0".

9. Remove the backslash from end of the line that reads: "mtu %t mru %t \" .

   The section should now appear as follows:

```
sxx.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
#               ms-dns 192.168.160.5 ms-dns 0.0.0.0 \
#               plugin /usr/lib/libpsr.so
```

10. Go to the “all.pppopt” section of the */etc/portslave/pslave.conf* file.

    The “all.pppopt” section will appear as follows when the file is first opened

```
#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
```

11. Remove the “#” symbols from the beginning of the first 4 lines in this section.

    Optionally, you can remove the two remaining lines that begin with “#” (“ms-dns 192.168.160.5 ms-dns 0.0.0.0 \” and “plugin /usr/lib/libpsr.so”).

Note: If you do not remove these two lines, leave the “#” symbol in front of each one.

---

12. Change “all.pppopt” to “sxx.pppopt” (where *xx* is the number of the serial port to which the external modem is attached).

13. In the first line of this section, change "%i:%j" to "0.0.0.0:0.0.0.0".

14. Remove the backslash from the end of the line that reads: “idle %I maxconnect %T \”.

The section should now appear as follows:

```
sxx.pppopt      0.0.0.0:0.0.0.0 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
```

15. Edit the file “/etc/ppp/pap-secrets”.

When the file is opened for the first time, it should look something like this:

```
# Secrets for authentication using PAP
# client        server  secret           IP addresses
#"mary"         *       "marypasswd"           *
```

16. Add the following line:

```
*               *           ""                  *
```

The file should now look something like this:

```
# Secrets for authentication using PAP
# client        server  secret           IP addresses
#"mary"         *       "marypasswd"           *
*               *           ""                 *
```

This configures the modem to accept any password.

17. Ensure that the filename “/etc/ppp/ pap-secrets” is listed in “/etc/config_files”. If not, edit “/etc/config_files” and add the following line to the end of the file.

```
/etc/ppp/pap-secrets
```

18. 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 whose name will be the APM Admin Username for that device.

19. 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 changed to 0 is as follows:

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

20. Change the ownership of the user's home directory to root as follows:

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

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

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

Appendix C
DLS Activation

Data Logging Session Activation

The AlterPath Manager E2000 is available with a fixed capability of 256 activated Data Logging Sessions (DLSs). This is also equal to the maximum number of concurrent console connections. The maximum number of managed consoles, or the total number of configurable console connections for the APM E2000 is 4096.

The APM 2500 comes with a standard base capacity of 64 activated DLSs and a capacity of 1024 managed consoles.

Caution: Licenses (except for factory default licenses) must be reinstalled after you recreate the system partition or after you run the "installimg" command.

If you want to preserve your licenses before you recreate a system partition or before you run "installimg," you can edit the file "/etc/files.list" and add your license file name to the list of files. Be sure to use the full path of each license file name you enter into this file. For example if the name of the license file you are adding is "APM_FA_DLS_64_128.enc" you should enter the full path name:
`/var/apm/licenses/data/APM_FA_DLS_64_128.enc`
Be sure to follow up with the "saveconf" command. It is also a good idea to save a copy of each license file on a server that can be accessed by your APM, just to be extra safe.

If at any time you run "defconf" the file, "/etc/files.list" will revert back to its original state, and you will need to reinstall your license.

Additional DLS at Time of Purchase

Additional DLS activation can be included at the time of initial purchase, or it can be added as a feature activation conversion. Cyclades recommends you

purchase the additional DLS activation with your APM. There is a price benefit when you buy the DLS activation this way.

Initial purchase part numbers for the DLS activation options along with their corresponding managed console capacities are shown in the table that follows:

Table C-1: DLS Activations Available at Initial Purchase

Part Number	DLSs	Max. Number of Managed Consoles
APM 2500		
APM 2500 Base System	64	1024
APM B-DLS 128	128	2048
APM B-DLS 256	256	4096
APM B-DLS 512	512	8192

DLS Activation Conversion

For the APM 2500, DLS capacity can be expanded and additional capacity can be purchased from Cyclades. This is an activation conversion. Activation conversion options are shown in the following table:

Table C-2: Activation Conversion Options

Conversion Number	From	To
AlterPath 2500		
APM FA-DLS 64-128	64	128
APM FA-DLS 64-256	64	256
APM FA-DLS 64-512	64	512
APM FA-DLS 128-256	128	256
APM FA-DLS 128-512	128	512
APM FA-DLS 256-512	256	512

Each DLS activation is assigned to a single MAC (Ethernet hardware) address, and cannot be transferred to another AlterPath Manager.

Obtaining Expanded DLS Activation

You can purchase expanded DLS activation from your Cyclades sales team or from Cyclades partners.

Cyclades customer service will need the MAC (Ethernet hardware) address of Eth0 (the first Ethernet controller in your APM) to generate the license file which will activate your new features.

▼ To Install Expanded DLS Activation

1. Log onto your APM as root, using the serial console interface.
2. Examine the contents of the following the "/var/apm/licenses/data" directory.

Note: At least one file should already be in this directory. This file should be named "APM_B_DLS.enc". This is a *base* license file (indicated by the "B" in the file name). Only *one* base file is allowed in the "/var/apm/licenses/data" directory.

---

3. Copy any new license files into this directory.

Note: If you have more than one feature activation (FA) license file for DLS activation, you must be sure all the license files are included in the "/var/apm/licenses/data" directory.

For example, if you purchase a license to expand from 128 to 512 DLSs, you directory will contain the following files prior to the new expansion:

```
APM_B_DLS_64.enc
APM_FA_DLS_64_128.enc
```

When you copy your new license file into the "/var/apm/licenses/data" directory, it must contain all of the following:

```
APM_B_DLS_64.enc
APM_FA_DLS_64_128.enc
APM_FA_DLS_128_256.enc
```

Note: Multiple FA (feature activation) license files must be named with sequential number ranges, as shown in the foregoing example.

4. Enable your license immediately, by entering the command:

   # **/etc/init.d/tomcat restart**

Verifying Your Current DLS Activation

Log on to the Web User Interface and click on the “About” link in the lower left corner of the display. A window similar to the following will appear:

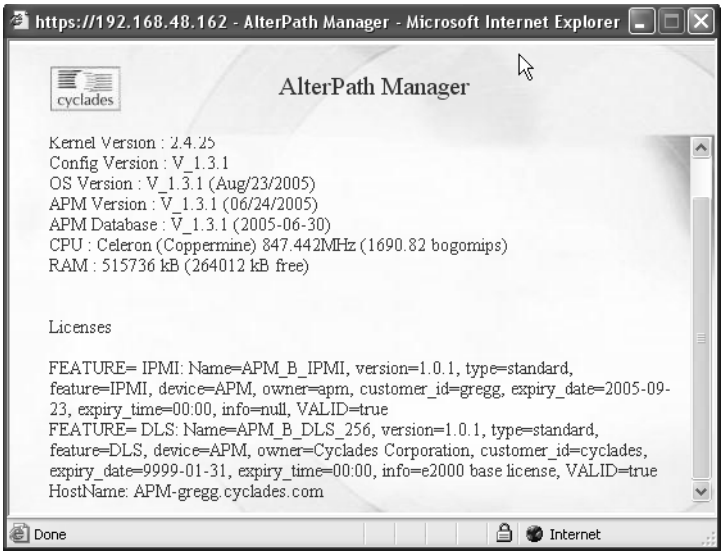

Figure C-1: Feature Window

You can also verify your current DLS Activation by logging onto your APM CLI as root and running the following command:

ls /var/apm/licenses/data

If DLS is activated, the screen will display a file name similar to this:

```
APM_B_DLS_256.enc
```

The foregoing file name indicates a DLS capacity of 256 logging sessions.

Verifying your MAC addresses

Log on to the CLI (on the serial console port) as root or as admin and run the following command:

```
# ifconfig
```

A display similar to the following will appear:

```
eth0      Link encap:Ethernet  HWaddr 00:90:FB:81:57:17
          inet addr:192.168.48.162  Bcast:192.168.51.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9691587 errors:133 dropped:0 overruns:0 frame:133
          TX packets:5726282 errors:0 dropped:0 overruns:0 carrier:0
          collisions:1038728 txqueuelen:1000
          RX bytes:685270715 (653.5 Mb)  TX bytes:548308906 (522.9 Mb)
          Interrupt:10 Base address:0xc000 Memory:e5020000-e5020038

eth1      Link encap:Ethernet  HWaddr 00:90:FB:01:8C:D7
          inet addr:10.10.10.2  Bcast:10.10.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:632 errors:0 dropped:0 overruns:0 frame:0
          TX packets:622 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:38288 (37.3 Kb)  TX bytes:42288 (41.2 Kb)
          Interrupt:11 Base address:0xc400 Memory:e5021000-e5021038

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113528 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113528 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:15268713 (14.5 Mb)  TX bytes:15268713 (14.5 Mb)
```

The numbers following the “HWaddr” subheading for each Ethernet controller installed (eth0 and eth1 by default) is the MAC address for the controller.

Glossary

3DES

Triple Data Encryption Standard, an encrypting algorithm (cipher) that encrypts data three times, using a unique key each time, to prevent unauthorized viewers from viewing or changing it. 3DES encryption is one of the security features provided by Cyclades products to support data center security policies.

authentication

Controlling access by requiring users to enter names and passwords. Anyone accessing Cyclades products and connected devices must log in by entering a username and password. The usernames and passwords entered during login attempts are checked against a database that lists all the valid usernames along with the encrypted passwords. Access is denied if the username or password is not valid. The password database being checked can reside either locally (on the device being accessed) or on an authentication server on the network. If an authentication method is selected that relies on a server, the corresponding authentication server must be already installed and configured in order for authentication to work. Using one or more of the many types of popular authentication methods can reduce administrator workload when an administrator needs to add, modify, of delete user accounts.

ALOM (Advanced Lights Out Manager)

Remote out-of-band management technology on certain Sun servers that includes an independent system controller (service processor) and firmware. Provides remote monitoring, logging, alerting, and basic control of the server in a “lights out” environment.

ASIC

Application-Specific Integrated Circuit. Pronounced “ay-sik.” A type of chip used for applications that provide a specific function, such as an ASIC chips that serves as a BMC.

Baseboard Management Controller (BMC)

On some servers, an internal processor separate from the main system that operates even if the main processor is not operable, sits on the server's motherboard. Monitors on-board instrumentation. Provides remote reset or power-cycle capabilities. Enables remote access to BIOS configuration or operating system console information, and in some cases provides KVM control of the server. Includes a communication protocol that brings the information and control to administrators.

BIOS (basic input/output system

Pronounced "bye-ose." Instructions in the onboard flash memory that start up (boot) a computer without the need to access programs from a disk. Sometimes used for the name of the memory chip where the start-up instructions reside. BIOS access is available even during disk failures. Administrators often need to access the BIOS while troubleshooting, for example to temporarily change the location from which the system boots. How to access the BIOS varies from one manufacturer to the other.

baud rate

Pronounced "bawd rate." When configuring terminal or modem settings on serial ports and console port connections on AlterPath devices, the specified baud rate must match the baud rate of the connected devices.

Options range from 2400–921600 Kbps. 9600 is the most-common baud rate for devices.

CAT5

An Ethernet cable standard defined by the Electronic Industries Association and Telecommunications Industry Association (commonly known as EIA/TIA). CAT5 is the fifth generation of twisted pair Ethernet cabling and the most popular of all twisted pair cables in use today. The support for CAT5 cabling in many Cyclades products allows the use of existing cabling infrastructure in the data center.

CLI

A means of operating a computer by typing a text command at an on-screen prompt and hitting the Enter or Return key to issue the command. The computer then processes the command, displays

whatever output is appropriate, and presents another prompt for the next command. Typical commands are to run a program, enter a text editor, list files, and change directories. This mode of interaction is common, for instance, in the traditional DOS and UNIX operating systems.

Command line interface. An interface that allows users to use text commands that tell computers to perform actions (compared to using a GUI). Through a CLI, individual commands can be given to the computer one at a time using a keyboard. Alternately, users can save a series of frequently-used commands in a file called a script. Being able to create and run scripts to automate repetitive tasks is one of the reasons many administrators prefer using a CLI.

Most computer operating systems have both GUI and CLI modes. Cyclades products run the Linux operating system, and most Cyclades products provide CLI access. CLI access is achieved through several different means. For one example, if a remote administrator uses Telnet to access an AlterPath OnSite, the administrator can then tell the OnSite to perform actions using the CLI by typing commands on the Linux shell's command line.

Do not be confused by the fact that some Cyclades products offer a management tool called the CLI, which has the same name as the term used in general for any command line interface. The Admin user can select “CLI” at a prompt after logging into the APM console (a regular user logging into the APM console gets the “CLI” prompt by default). The Cyclades CLI tool provides many commands and nested parameters in a format called the CLI parameter tree.

Client-side management software—See Management software

Console

This term is used to mean the serial console interface that is present on most Cyclades devices. It is a physical serial port that interfaces with a serial terminal that can be used to interface with the device. The serial console interface allows an administrator to have shell access to the device. The administrator can use this interface for advanced configurations.

On the AlterPath Manager, “Console” also is used to describe any of the ports on a device, such as KVM ports on a KVM/net device or an OnSite device; or any of the serial ports on an ACS device, a TS device, or an OnSite device.

Checksum

An algorithm, usually generated by a program, to check the integrity of a target file or target packet of data that has been transferred across a network. A very common checksum program is “md5sum” that is run after a target file has been downloaded. The checksum file generated by “md5sum” is compared with a checksum file that was generated on the original target file and stored with it prior to the target file’s transmission. If the two checksum files match, it is nearly a certainty that the target file was transferred correctly.

Consolidation

Provides controlled access to basic management features on multiple Ethernet-based servers that have embedded service processors, using only one Internet address. When managed separately, each service processor needs its own IP address. Managing multiple servers with multiple IP address is both expensive and time consuming without consolidation.

Decryption

Decoding of data that has been encrypted using an encryption method.

Device

From the AlterPath Manager’s point of view, a device is a product that the APM is designed to control directly through an Ethernet port. This includes the KVM/net, ACS, TS, and the OnSite. Any of the individual ports on one of these devices, which is designed to connect to a server or workstation, is a console.

Encryption

Translation of data into a secret format using a series of mathematical functions so that only the recipient can decode it. Designed to protect unauthorized viewing or modification of data, even when the encrypted data is travelling over unsecure media (such as the Internet). See 3DES and SSH. As an example, a remote terminal session using secure shell SSH usually encrypts data using 3DES or better algorithms.

DRAC (Dell Remote Assistant Cards)

Dell’s solution

GUI

Graphical user interface (pronounced GOO-ee). A computer interface that allows users to tell computers to perform actions by clicking on graphical elements such as icons, choosing options from menus, and typing in text fields on forms displayed on the computer screen. Many Cyclades products provide GUI access through the Web Manager.

iLO (Integrated Lights Out)

HP's proprietary service processor. Even though HP is a major supporter of IPMI, HP also provides iLO because it provides many more functions than IPMI. The iLO processor resides on the motherboard. As long as power is available to the server, even if the server is off, iLO is active. When the dedicated Ethernet port is plugged into the network, iLO uses DHCP. iLO has a web interface and a telnet interface. When the server is off, only the web interface works.

IPDU

Intelligent power distribution unit. Cyclades supports a family of AlterPath PM IPDUs.

IPMI (Intelligent Platform Management Interface)

An open standards service processor currently adopted by every major server platform vendor. Its main benefit over other service processors is that it is installed on servers from many vendors, providing one interface and protocol for all servers. Its main disadvantage is that it doe not always provide as much functionality as the proprietary service processors.

Kerberos

Network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

KVM switch

Enables use of only one keyboard, video monitor, and mouse to run multiple servers. Reduces expenses by eliminating the cost of acquiring, powering, cabling, cooling, managing, and finding data-center space for one keyboard, monitor, and mouse for every server. Servers are connected to KVM ports on Cyclades AlterPath KVM switches using AlterPath KVM terminators on the

server end and up to 500 feet of CAT5 cable. AlterPath KVM switches provide authentication and other security features and allow only authorized users to access a restricted set of connected servers. See also KVM analog switch and KVM Over IP switch.

KVM analog switch

A KVM switch that requires a local user connection to gain access to the servers that are connected to the switch.

KVM over IP

Supports remote access over a LAN or WAN or telephone line using the TCP/IP protocols and a web browser. Enables operations over long distances. Cyclades AlterPath KVM/IP switches are one component of the out-of-band infrastructure,

LDAP

Lightweight Directory Access Protocol. A set of open protocols for accessing directories of information.

Management console—See service processor

Management software

Each server company that offers a service processor produces its own client side software to access the servers' management features through the service processor. In some cases, management software is imbedded in the service processor and is presented either as a web interface or as a command line interface accessed using SSH or Telnet, or as both a web interface and command line interface. In other cases, the management software is installed in a client workstation and accesses the management features of the service processor using an IP-based protocol, such as IPMI. Each type of software only manages one server, does not scale, does not address the need for consolidated access-control, multi-user access, data logging, and event detection, encyrption and other needs. The <ProductName> (Change variable definition) addresses these needs and provides a single interface to access basic features of multiple-vendors' service processors.

NEBS (Network Equipment Building Systems) Compliance

Means that equipment has been tested and proven to meet the NEBS requirements commonly adhered to by several telecommunications carriers. The requirements are in place to ensure that telecommunications equipment poses no risk or safety hazard to people, nearby equipment, or to the physical location where the equipment operates, and that equipment is reliable and dependable during both normal and abnormal conditions. Tests address heat release, surface temperature, fire resistance, electomagnetic capability, electrical safety, and manufacturing component characteristics, among other attributes.

NIS (Network Information Service)

An industry-standard directory protocol used for authentication, specifically in Sun "legacy" systems.

OOBI (Out-of-band Infrastructure)

Provides secure, alternate paths to connect to and manage IP production infrastructure remotely. Components include console servers, KVM switches, IPDUs, and service processor managers. Enables lights out data centers where computers can be monitored, preventively maintained, and restored to operation without site visits by technicians.

Out of band

A type of access to assets that is either separate from or independent of the normal production network. Used for remote monitoring and control even when the managed assets lose connection to the production network. Typically out-of-band access is through an RS-233 or Ethernet console, a power/reset circuit, or a KVM port.

RSC (Remote System Control)

Sun’s remote out-of-band management technology on certain Sun servers that includes an independent RSC card and software. Enables the remote administrator to run diagnostic tests, view diagnostic and error messages, reboot the server, and display environmental status information from a remote console even if the server’s operating system goes offline. The RSC firmware runs independently of the host server, and uses standby power drawn from it. The RSC card on some servers include a battery

that provides approximately 30 minutes of power to RSC in case of a power failure.

RSA (Remote Supervisor Adapter)

IBM's

Security

Service processor

Ethernet-based management console on a server, which provides out of band management through an interface between the server's administrator and an internal BMC that enables the management features. Management features include serial console emulation (using telnet or IPMI), KVM over IP, power control, sensor and log information from the server hardware, and virtual media. Examples of vendors and the service processor technologies they support are shown in the following table.

Table G-1: Service Processor Technology by Vendor

Vendor	Protocol
HP	iLO (Integrated Lights Out), Riloe, PCMCIA
Sun	RSC (Remote System Control), ALOM
Dell	DRAC, PCMCIA
Intel	PCMCIA

Shell

A command interpreter on UNIX-based operating systems (like the Linux operating system that controls most Cyclades products). At the time this is being written, Microsoft has announced an upcoming release of a Microsoft shell. A shell typically is accessed in a terminal window where the shell presents a prompt. For example: [admin@OnSite /home/admin]# is the prompt that appears when a user logs into an OnSite as admin and is in the /home/admin directory. Users tell the operating system to perform actions by typing commands in the shell, which interprets the commands and performs the specified actions.

Web Manager

Cyclades' web management interface (WMI), which runs in supported browsers.

Index

E

F

H

I

K

L

M

N

O

P

R

S

T

U

W