AlterPath™ OnBoard
User's Guide

Software Version 1.1.0

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: April 2006
Part Number: PAC0392

Contents

##

##

##

Figures

Tables

Procedures

Before You Begin

This *AlterPath OnBoard User's Guide* provides background information and procedures for using the Cyclades™ AlterPath™ OnBoard to access server-management services that are provided by service processors and to gain console access to devices that allow access to their consoles through Ethernet ports.

Audience

This manual is intended for users who are authorized to connect to service processors or to the consoles of connected servers or other types of devices and to manage power through the OnBoard. The user's guide is also prerequisite reading for the administrator, who needs to understand what the user can do on the OnBoard and how to connect to the OnBoard before being able to perform the procedures in the *AlterPath OnBoard Administrator's Guide*.

Note: This manual describes use of the OnBoard only. It does not describe how to set up and administer other external services or servers that the OnBoard may access for authentication, system logging, IPMI control, SNMP notifications, data buffering, file sharing, or other purposes. This manual assumes that users who are authorized to connect to service processors and other devices through the OnBoard already know how to use the management functions provided by the connected devices.

Document Organization

The document contains the chapters listed in the following table.

Table P-1: Document Organization

Chapter Number and Title	Description
1: Introduction	Provides an overview of the features of the AlterPath OnBoard for the regular user, along with necessary prerequisite information for understanding the rest of the information in this guide and in the administrator's guide.
2: Web Manager Introduction	Describes how authorized users use the Web Manager to do the following: • Access management features of service processors • Access the console of other types of devices that are connected to the private Ethernet ports on the OnBoard • Manage power • Change their own passwords

Table P-1: Document Organization (Continued)

Chapter Number and Title	Description
3: Accessing the OnBoard and Connected Devices	Describes options other than using the Web Manager, which a user can use to do the following: • Access management features of service processors • Access the console of other types of devices that are connected to the private Ethernet ports on the OnBoard • Manage power • Change the user's passwords Options include the following: • Connecting to the OnBoard console and choose options from a menu • Using `ssh` with device management commands to access and manage devices directly through the OnBoard.
A. "MindTerm Applet Reference	Describes using and customizing the MindTerm applets that appear when the console of the OnBoard or a connected device is accessed through the Web Manager. Also describes the special keys and commands the user can use once connected to the web interface or console of a service processor or device.
Glossary	Defines terms needed for understanding how to use Cyclades products.

Table P-1: Document Organization (Continued)

Chapter Number and Title	Description
Index	Provides a way to look up information and procedures. In the online version of this manual, clicking the terms in the index brings you to where they are used in the manual.

Related Documents

Before installing or using this product, refer to the release notes for important information about supported hardware and software, known problems, and outstanding bugs. You can download the release notes by going to `http://www.cyclades.com/support/downloads.php` and searching for the product name "AlterPath OnBoard."

The following table lists the AlterPath OnBoard documents. As indicated, the QuickStart Guide is printed, and it is also included with the other AlterPath OnBoard documents in PDF format on the Documentation CD that is also shipped with the product. The documents are also at http://www.cyclades.com/support/downloads.php under "AlterPath OnBoard."

Table P-2: Related Documentation

Guide Title	Printed and Shipped?	PDFs on DocCD?	Part Number
AlterPath OnBoard QuickStart Guide	Y	Y	PAC0389
AlterPath OnBoard Installation Guide	N (orderable)	Y	PAC0390
AlterPath OnBoard Administrator's Guide	N (orderable)	Y	PAC0391

Printed versions of this document and all the above listed documents can be ordered from your Cyclades sales representative.

Documents for the AlterPath PM mentioned in this guide are also on the Documentation CD shipped with the product, and they are also available at: http://www.cyclades.com/downloads under the product's name.

Updated versions of this document will be posted on the downloads section of the Cyclades website when Cyclades releases new versions of the software. See "Additional Resources" on page xix for information about free software upgrades.

Typographic and Other Conventions

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

Table P-3: 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 OnBoard Quick Start.*
`Filename or Command`	Names of commands, files, and directories; onscreen computer output.	Edit the `pslave.conf` file.
`User type`	What you type in an example, compared to what the computer displays	`#` **`ifconfig eth0`**

The following table describes other terms and conventions.

Table P-4: 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` pressed by itself. • `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-4: Other Terms and Conventions (Continued)

Term or Convention	Meaning	Examples
Navigation shortcuts	Shortcuts use the –> symbol to indicate how to navigate to Web Manager or OSD screens.	Go to Configuration –> KVM –> General –> IP Users in Expert mode.

\ in a command line example	Used in screen examples when a command does not fit in the space available. Indicates that the whole command should be entered in either of the two following ways:
	• On one line without the backslash
	• On multiple lines with a backslash at the end of each line to tell the shell that the command continues on the following line.
		`# openssl req -new \ -nodes -key \`
		`private_key.pem \`
		`-out cert.csr`

Additional Resources

The following sections describe how to get technical support, training, and software upgrades.

Cyclades Technical Support

Cyclades offers free technical support. To find out how to contact the support center in your region, go to: http://www.cyclades.com/support/technical_support.php.

Cyclades Technical Training

To learn about the Cyclades Technical Training Center and the courses offered, visit http:www.cyclades.com/training, call 1-888-292-5233, or send an email to training@cyclades.com.

Cyclades Software Upgrades

Cyclades offers periodic software upgrades for the AlterPath products free of charge to current Cyclades customers. You may want to check http://www.cyclades.com/support/downloads.php from time to time to see if upgrades are available for the OnBoard or for an AlterPath PM that you may also be using with this product.

See the *AlterPath OnBoard Administrator's Guide* for instructions on upgrading the software on your AlterPath OnBoard and on an optionally-connected AlterPath PM IPDUs.

Chapter 1
Introduction

The AlterPath OnBoard controls which users have access to connected devices and creates a secure path between a remote user’s computer and a connected device.

Note: This introduction describes what users need to know in order to perform management actions on connected devices. The information in this introduction is needed for understanding the information and procedures in the rest of this guide and in the AlterPath OnBoard Administrator’s Guide.

The following table lists the topics in this chapter.

OnBoard Advantages for Server Management

The OnBoard provides access to server-management services that are provided by *service processors*. Service processors are *out-of-band* management controllers that many vendors include in their servers. The OnBoard provides a single source for authentication, authorization, and management for multiple types of service processors. Using the OnBoard, users can access and manage multiple servers from a single point without having to learn how to use multiple service processor-management interfaces.

For example, the ability to manage power is provided by most service processors, but each service processor has its own interface and its own commands for power management. The OnBoard allows an authorized user to manage power on multiple servers from multiple vendors using a single interface and a single set of commands.

The security features provided by the OnBoard work together to create a *secure path* between a user and a server that is being managed.

Figure 1-1 is a conceptual illustration of a secure path between a remote user and a service processor through the OnBoard. (Users can also be on the same LAN as the OnBoard and the connected devices.)

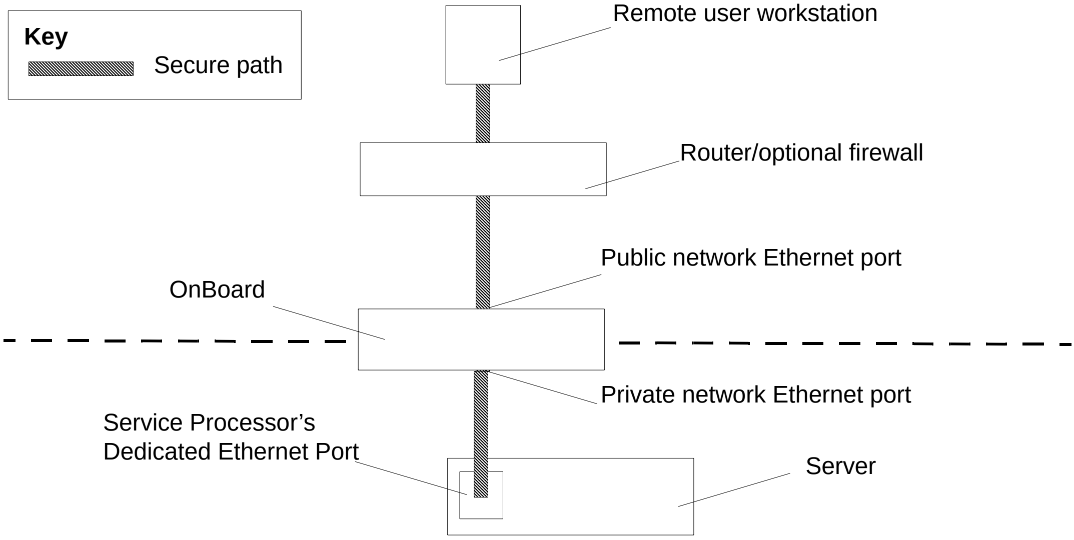


Figure 1-1: Secure Path to a Connected Service Processor

In Figure 1-1, the public network is above the dashed line, and the private network is below the dashed line. The dedicated Ethernet port of a service processor is connected to one of the OnBoard’s private Ethernet ports. The IP address of the public Ethernet port is the only publicly-defined IP address.

To allow management of the connected device, each device has a privately-designated IP address and at the administrator’s discretion, each device may also have a virtual IP address. If virtual addresses are defined, users may be allowed to see a connected device’s virtual IP address but not to see the device’s privately-defined IP address.

In the example, the remote user accesses the OnBoard through a network connection to the public Ethernet port and then selects a service processor management action that user is authorized to perform on a specific service processor. (Users may also dial into the OnBoard through an optional external modem or PCMCIA modem card.)

After the user selects the desired management action, the OnBoard then creates a secure connection between the user and the service processor, acting as a proxy on behalf of the user when communicating with the service processor. While the user is performing any of the service processor management actions for which the user is authorized, the connection between the OnBoard and the service processor is kept separate and protected from the connection between the user and the OnBoard. Nothing that happens on the private network is exposed to the public network. Depending on the mode of access, HTTPS or SSH can be used to protect communications that are transported on the public network between the user and the OnBoard.

Security Features Used in Access Control

The OnBoard allows administrators to enforce an organization's security policies by providing *security features* that control who can access management features on connected devices. The access-related security features are shown in the following table with links to where the features are described in more detail.

Table 1-1: Access-related Security Features

Security Features	Where Described
User types and authorizations	"Types of Users" on page 5 "Types of User Authorizations" on page 7
The security profile in effect on the OnBoard and which services are turned on or off	"Security Profiles' Effects on Users' Actions" on page 8
Separate authentications for accessing the OnBoard and connected devices	"Authentication" on page 8

Types of Users

The OnBoard supports two main types of users:

- Users authorized to administer the OnBoard and to administer connected devices, called *administrative users*
- Users authorized to perform one or more management functions on one or more connected devices, called *authorized users*

Two predefined administrators are `root` and `admin`, and they cannot be deleted.

The `admin` user can do the following:

- Access the Web Manager and use any of its functions
- Access the OnBoard's console and use the unrestricted shell
- Invoke the OnBoard configuration utility, `cycli`
- Invoke any Linux commands available to the non-root user
- Invoke any Linux commands available to the root user by using the `sudo` command

The `root` user can do the following:

- Access the OnBoard's console and use the unrestricted shell.
- Invoke the OnBoard configuration utility, `cycli`
- Invoke any Linux commands available to the root user

The root user cannot access the Web Manager.

Either `root` or `admin` can add regular user accounts and authorize them to access management features on connected devices. Optionally, adding regular users to the "`admin`" group makes them administrative users able to perform OnBoard administration.

The following table summarizes the responsibilities of each type of user and provides the default password for each type of user.

Table 1-2: User Types, Responsibilities, and Default Password

User Name	Responsibilities	Default Password
`root`	Cannot be deleted. Only direct logins to the OnBoard command line are allowed. Runs the `cycli` utility to do initial network configuration, as described in the *AlterPath OnBoard Installation Guide*. Also can run other OnBoard-specific commands and Linux commands on the command line of the Linux shell.	cyclades
`admin`	Cannot be deleted. Has full access to every function of the Web Manager. Also can run the `cycli` utility on the command line of the Linux shell and can use any Linux commands available to the non-root user.	cyclades

Table 1-2: User Types, Responsibilities, and Default Password (Continued)

User Name	Responsibilities	Default Password
administrator-assigned	User account optionally configured by an administrator to be able to perform management functions on devices connected to the OnBoard. Users' access to devices and to device-management features is controlled by authorizations. Users with permission to access management features on connected devices are referred to as "authorized users." **Note:** If a regular user is assigned to the "admin" group, that user can also perform the same administrative functions on the Web Manager as the "admin" user, as described above. Regular users added to the admin group are referred to as *administrative users*.	*administrator-assigned*

Types of User Authorizations

Users can be authorized for the following:

- Access to connected service processors or other types of connected devices
- Access to management features available on the devices that users are authorized to access:
  - Service Processor Console
  - Device Console
  - Sensors
  - Power
  - Event Log
  - Native IP

  For details, see "Management Features Available to Authorized Users" on page 14.

Note: The administrator may create and enable a custom security profile that has the “override authorization” feature set, which causes all authenticated users to have all access to all connected devices. For details, see “Security Profiles’ Effects on Users’ Actions” on page 8.

Authentication

Anyone accessing the OnBoard must log in by entering a username and password. Controlling access by requiring users to enter names and passwords is called *authentication*. The usernames and passwords entered during login attempts are checked against a database. Access is denied if the username or password is not valid.

The password database being checked can reside either locally (on the OnBoard) or on an authentication server on the network.

The OnBoard user is required to enter a username and password in the following cases:

- When logging into the OnBoard

  The authentication method chosen for the OnBoard is used for all access through `telnet`, `ssh`, or the Web Manager. By default, logins to the OnBoard use Local authentication.

- When accessing a service processor or other connected device.

Users may be required to enter different username and password pairs when accessing the OnBoard than when accessing a connected device.

Security Profiles’ Effects on Users’ Actions

The administrator selects a security profile for the OnBoard based on the security requirements of the organization. The security profile may limit which services are available to users and which functions may be allowed or disallowed.

Note: All of the features and procedures described in this guide work when the Moderate security profile is in effect.

Each OnBoard has a security profile, which controls the following:

- Which services are turned on
- Whether authorizations are being checked

Services and other functions controlled by security profiles are listed in the following table:

Table 1-3: Services and Other Functions Controlled by Security Profiles

Service	Other Functions That Can Be Allowed/Disallowed
FTP	
HTTP, HTTPS	Redirect HTTP automatically to HTTPS
ICMP	
IPSec	
PPTP	
RPC	
SNMP v1, v2c, v3	
SSH v1, SSH v2	Allow root login using SSH Assign an alternate port to SSH
Telnet	Allow Telnet to OnBoard
Override authorization—enable access based on authentication only	
Specify a default authentication type to apply by default to all subsequently-configured devices.	

Services can also be turned on and off independently from the security profile. For more details, see “Understanding Services” in the AlterPath OnBoard Administrator’s Guide.

Note: If you are prevented from using a service you need to use, such as FTP or SNMP, talk with the OnBoard’s administrator to find out if the service can be enabled or if another way of performing a necessary task is available that is consistent with your site’s security policies.

Types of Managed Devices

The connected device can be one of the following types:

- A *service processor*.
- A server or other type of device that does not have a service processor but that provides access to its command line through a dedicated Ethernet port

  This type of device includes servers that redirect their serial console output to dedicated Ethernet ports (which provide a type of access generally referred to as serial over LAN or *SoL*).
- A device with a dedicated Ethernet port that supports management access via Telnet, SSH, SNMP, or the OnBoard's native IP access capability

Note: The term “device” is used in this guide when referring to a service processor, server, or other connected device, unless the type of device must be clearly stated in the context.

Options for Accessing the OnBoard, Managing User Passwords, IPDU Power, and Devices

Authorized users can access the OnBoard through the local network, the Internet, and through dial-ins to an optional modem or phone card for the following purposes:

- Performing device management actions on connected devices
- Managing outlets on optionally-connected AlterPath PM IPDUs
- Managing the user’s own password.

For details about modem access, see “Management Features Provided on Supported Device Types” on page 19.

The following means are available for logging into the OnBoard and performing the above-listed actions:

- Using the Web Manager and choosing from a list of menu options.

  For more details, see “Cyclades Web Manager” on page 23.

- Using an SSH application or the `ssh` command on the command line of the user's workstation to connect to the OnBoard's command line, and then choosing from a list of menu options.

  See "Accessing the OnBoard's Console" on page 12, "User Shell (rmenush)" on page 13, and "OnBoard Shell (onbdshell)" on page 14.

Users can also use `ssh` on the command line to execute a service processor management command directly on the service processor. For details, see "Using SSH with the OnBoard" on page 20. The device management features are described under "Management Features Available to Authorized Users" on page 14.

The OnBoard provides device management commands for `ssh` that are not provided for `telnet`. Because ssh is encrypted, and therefore more secure, by default `ssh` is the only supported means of performing device management actions directly on a device, as summarized in the following list:

- Users cannot use `telnet` to connect directly to a device and perform management actions through the OnBoard.
- Users can use `ssh` to connect directly to a device and perform management actions through the OnBoard.

Command Line Access Through Console Logins

Administrators and authorized users can access the command line of the OnBoard and of service processors, servers, and other connected devices by accessing the device's console. Users of any type can log into a console of any of the above listed types using either the Web Manager, menus available through the OnBoard console, or `ssh`. The following table provides links to where console access is defined.

Table P-2: Console Login Types

Console Type	Where Documented
OnBoard	• "Accessing the OnBoard's Console" on page 12 • "To Access the OnBoard's Console" on page 76
Device or service processor console	• "To Use OnBoard's Console Menus to Access the Device Management Options" on page 81 • "To Use a SSH Command to Connect Directly to a Device's or Service Processor's Console" on page 80"

When a user connects to any console using the Web Manager, a window running a MindTerm applet appears with an encrypted SSH connection between the user’s computer and the console. MindTerm is an SSH client that includes an integrated xterm/vt100 terminal emulator and that runs as a Java applet within a browser window.

To use MindTerm, the user’s browser must have a Java plug-in enabled, as described in “Requirements for Java Plug-In Availability” on page 38.

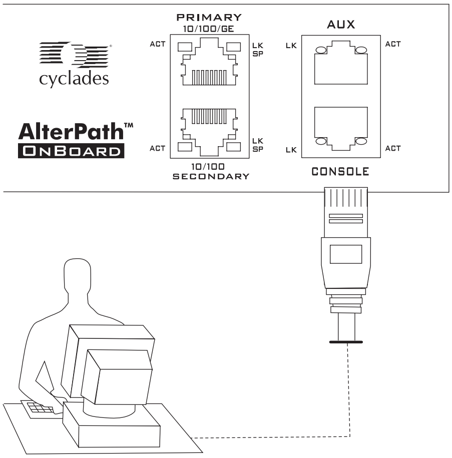
See Appendix A, “MindTerm Applet Reference” for details about using and configuring the applets and about hot keys that can be used during console sessions through the Web Manager.

Accessing the OnBoard’s Console

Administrators and authorized users can access the OnBoard’s console, in the following three ways.

- By local logins through the console port

  Local OnBoard administrators or authorized users can access the command line by logging in through the console port. This requires the user or administrator to have physical access to a terminal or computer that is connected to the OnBoard’s console port as shown in the following figure. The user or administrator logs in through a terminal or through a terminal emulation program on the connected computer.



- By using SSH

  Remote administrators and authorized users can access the OnBoard’s command line through a SSH connection between the user’s computer and the OnBoard. See “Using SSH with the OnBoard” on page 20.

- By clicking “Connect to OnBoard” on the Web Manager.

  After logging into the Web Manager, any type of user can access the console by clicking “OnBoard” in the left menu and then clicking the “Connect to OnBoard” button.

User Shell (`rmenush`)

The default login shell for OnBoard non-administrative users is `/usr/bin/rmenush`. After logging in as described in “Accessing the OnBoard’s Console” on page 75, users see the menu options described in the following table.

Table P-3: User Shell Default Menu Options

Menu Option	Function
Access Devices	Executes the `onbdshell` to display a list of devices the user can access. See “OnBoard Shell (onbdshell)” on page 14.
Change Password	Allows the user to set a new password.
Logout	Logs the user out of the OnBoard’s console

The OnBoard administrator may modify the menu options and commands shown in Table 3 on page 13 so that users may be presented with a different menu of choices.

A user moves from one item to another on the menu and submenus by using the keyboard’s arrow keys. A line (-) appears next to the selected item.

After an option is selected, pressing the “Enter” or “Return” key brings up a submenu or runs the selected command. The following section describes the submenu that appears when “Access Devices” is selected.

OnBoard Shell (onbdshell)

The OnBoard shell, `/usr/bin/onbdshell`, displays a list of devices an authorized user can access. A submenu lists the device management actions available to the user. See “Accessing Device Management Features From the OnBoard’s Console Menu” on page 77 for more details.

Management Features Available to Authorized Users

The following table describes the management features for the different types of managed devices. These features are available a user through the Web Manager, through the `onbdshell` menu, and through the `ssh` utility on the command line. The first column shows the following:

- The option name for the feature in the Web Manager
- The option name for the feature in the `onbdshell` action menu
- The command name used with `ssh` on the command line to access the feature.

The “Device” column shows the type of device that supports each feature (“dev” for device without a service processor and “SP” for a service processor).

Table 1-1: Options and Command Names for Device Management (Sheet 1 of 3)

Web Manager Option / `onbdshell` **Option /** `ssh` **Command**	**Device**	**Description**
Service Processor Console / `Access the service processor's console` / `spconsole`	SP	Gives access to the service processor’s console (sometimes called the native command interface or NCI).
Device Console / Access the device’s console / `devconsole`	dev/SP	Gives access to the console of one of the following: • A server that allows console access through its service processor • A device without a service processor that presents a command line interface through its Ethernet port
Power / `Manage power` / `power`	SP	In the Web Manager, brings up a screen with the power management options. When access to the service processor goes through the OnBoard’s console, brings up a list of power management options. When the user performs power management directly on the service processor using the `ssh` command, power management options are performed using power management commands. Some types of service processors offer multiple options for powering off and power cycling a server. For details, see “What the Power Commands Do on Different Servers” on page 18. The following rows show the Web Manager and OnBoard shell menu options and the name of the power management commands that can be executed directly on the service processor using the `ssh` command from the user’s computer.

Table 1-1: Options and Command Names for Device Management (Sheet 2 of 3)

Web Manager Option / `onbdshell` **Option /** `ssh` **Command**	**Device**	**Description**	
		Web Manager / onbdshell Option	`ssh` **Command**
		Turn power on / `Turn power on`	`poweron`
		Turn power off / `Turn power off`	`poweroff`
		Power cycle / `Turn power off then on`	`powercycle`
		Check power status / `Get power status`	`powerstatus`
Reset / `reset`	SP	Resets the server where the service processor resides. Various type of resets are available on service processors. See “What the Reset Command Does on Different Servers” on page 18.	
Sensors / `sensors`	SP	Displays unformatted sensor data collected from the server by its service processor. The page provides a button that displays graphs of data from individual sensors.	

Table 1-1: Options and Command Names for Device Management (Sheet 3 of 3)

<table>
<tr><th>Web Manager Option /
onbdshell Option /
ssh Command</th><th>Device</th><th>Description</th></tr>
<tr><td>Event Log /
Manage the event log /
sel</td><td>SP</td><td>Displays the system event log (SEL) menu from the server where the service processor resides. Events are messages logged when system management events are detected. The events can be logged by the service processor or by the server. The user can view or clear event logs directly on the service processor using the ssh command.
<table>
<tr><th>Web Manager / onbdshell Option.</th><th>ssh Command.</th></tr>
<tr><td>View event log</td><td>sel</td></tr>
<tr><td>Clear event log</td><td>clearsel</td></tr>
</table></td></tr>
<tr><td>Native IP /
Enable native IP/
nativeipon
Disable native IP /
nativeipoff</td><td>SP</td><td>Used when a service processor supports access to a native web application or provides a management application that runs on the user’s computer. For “Native IP” to be available, a VPN connection must be active between the remote computer and the OnBoard. When the option to enable native IP is chosen, the user can then do one of the following:
• Launch a browser on the remote computer to bring up the native web application
• Launch the management application on the remote computer
<b>Note:</b> Instead of using a VPN tunnel, a user may use a ssh tunnel to access a device’s native web application without going through the Web Manager or the OnBoard’s console. For more details, see “Accessing a Device’s Native Management Features” on page 24.</td></tr>
</table>

Note: When a connected device does not have a service processor., “Device Console” and “Native IP” are the only management features available by default. The OnBoard command templates and device management Expect scripts can be customized to make other management features available.

What the Power Commands Do on Different Servers

The effects of the service processor power management commands differ from one vendor’s service processor to another. The possible options are described in the following table. If a service processor provides more than one of the options shown, the hard option is performed.

Table P-2: Possible Power Management Command Effects

Power Command	Option
Power off	• Hard power off: remove the power • Soft power off: shut down the operating system before removing the power
Power cycle (turn power off, then on again, to reboot the server)	• Hard power cycle: remove the power, wait several seconds, and then turn the power on again (to reboot the server) • Soft power cycle: shut down the operating system, wait several seconds, and then turn power on again

What the Reset Command Does on Different Servers

The effects of the “Reset” command differ from one vendor’s service processor to another, and sometimes the types of resets available on service processors of the same type from the same vendor differ from one firmware version to another. In addition, sometimes service processors have more than one type of reset, as described in the following list:

- Warm reset (or warm boot): only the server’s operating system is restarted
- Cold boot: the server is fully restarted (the same effect as issuing a “Power cycle” command)

If n service processor has more than one type of reset option, the OnBoard "Reset" command performs the highest level of reset: the cold boot option if available.

If the OnBoard administrator is configuring a service processor that provides multiple reset options, the administrator can customize an associated service processor management script to cause the "Reset" command to perform one of the lower levels of reset that are available on the service processor. Customizing service processor management scripts in described in the AlterPath OnBoard Administrator's Guide.

Management Features Provided on Supported Device Types

The following table shows the management features available on the supported service processors and on devices without service processors that present a command line interface through a dedicated Ethernet port.

Table 1-1: Supported Device Types and Management Features

Supported Service Processors/ Devices	SP Console	Device Console	Power	Event Log	Sensors	Native IP
RSA II	Y	Y	Y	Y	Y	Y
IPMI 1.5	Y	N	Y	Y	Y	Y
DRAC	Y	Y	Y	Y	N	Y
ILO	Y	Y	Y	Y	N	Y
Device	N	Y	N	N	N	Y

Using SSH with the OnBoard

Both SSH v1 and SSH v2 services are supported on the OnBoard. The OnBoard administrator may disable either version; if only one version is enabled, authorized users can use only a client running the same version that is enabled.

If SSH is enabled, authorized users can use `ssh` in the following ways.

- Access the OnBoard console using `ssh` and then connect through the OnBoard to perform device management actions.

  See “Accessing the OnBoard Using SSH” on page 21.

- Using `ssh` with special device management commands to perform device management actions without having to log into the OnBoard first.

  See “Device Management Commands for Use With SSH” on page 21.

  The format of the `ssh` command line is shown in the following screen example.

```
ssh -t username:devicename@onboard_IP_or_DNS_name [command]
```

  where:

  `-t` is required to launch an interactive session.

  username is the name of the authorized user.

  devicename is the name/alias that was assigned to the device by the OnBoard administrator.

  onboard_IP_or_DNS_name is the IP address of the OnBoard or its DNS name.

  `command` is one of the OnBoard-specific device management commands.

- Create an SSH tunnel to get access to a native web application on a device.

  See “Accessing a Device’s Native Management Features” on page 24 and “Information Users Need” on page 27.

Accessing the OnBoard Using SSH

As described under “User Shell (rmenush)” on page 13 and “OnBoard Shell (onbdshell)” on page 14, authorized users who connect to the OnBoard’s console are presented with a menu of choices. From the initial menu, users can bring up a list of devices that they are authorized to access and then access a submenu of management actions they can perform on the selected device. Users can use `ssh` to connect to OnBoard’s console and to access the `rmenush` menu in the following ways:

- `ssh` *username*`:@`*onboard_IP_or_DNS_name*
- `ssh -t` *username*`:@`*onboard_IP_or_DNS_name* `rmenush`

Both of the above commands give the non-administrative user access to the same menu. If an administrative user enters the first command line without the `rmenush` command, the user gets a shell prompt.

Users can use `ssh` to access the submenu of device management actions for a specific device in the following ways:

- `ssh` *username*`:`*device_alias*`@`*onboard_IP_or_DNS_name*
- `ssh -t` *username*`:`*device_alias*`@`*onboard_IP_or_DNS_name* `rmenush`

Both of the above commands give the user access to the same menu.

Device Management Commands for Use With SSH

Users can perform device management actions directly on a service processor by using the `ssh` command along with one of the following OnBoard-specific device management commands:

- `spconsole`
- `devconsole`
- `poweron`, `poweroff`, `powercycle`, `powerstatus`
- `reset`
- `sensors`
- `sel, clearsel`
- `native_ip_on`, `native_ip_off`

The `-t` option is required to launch an interactive session.

For details about the management actions performed by the commands, see “Management Features Available to Authorized Users” on page 14.

The format of the `ssh` command line is shown in the following screen example.

```
ssh -t username:devicename@onboard_IP_or_DNS_name command
```

where:

username is the name of the authorized user.

devicename is the name/alias that was assigned to the device by the OnBoard administrator.

onboard_IP_or_DNS_name is the IP address of the OnBoard or its DNS name.

`command` is one of the OnBoard-specific device management `ssh` commands.

For example, for authorized user `fred` to turn on the power for a server whose name is configured on the OnBoard as `drac`, when the IP address of the OnBoard is `192.168.29.22`, the `poweron` command would be entered as shown in the following screen example:

```
ssh -t fred:drac@192.168.29.22 poweron
```

Dial-in Access

Authorized users can dial into the OnBoard through either of the following types of optional modems and phone cards:

- An external modem connected to the AUX port
- A modem, GSM, or CDMA PCMCIA card inserted into one of the front PCMCIA slots

The OnBoard can be accessed using PPP when the following prerequisites are completed:

- The modem or phone card has been configured on the OnBoard for PPP or Autodetect and for optional callback

- The PPP application at the remote caller’s end has been configured for dialing into the OnBoard and optionally for callback from the OnBoard.
- The user account has been configured for PPP access, and the user knows the PPP username and password configured by the OnBoard administrator.

The OnBoard can be accessed from a terminal emulation program on the user’s computer if the modem or phone card is configured for Login or autodetect. The one-time password authentication method can be configured for login access to PCMCIA modem or phone cards.

Cyclades Web Manager

Both authorized users and administrative users can access the Web Manager from a supported browser using HTTP or HTTPS. Authorized users can use the Web Manager to log into devices, manage power on devices plugged into optional AlterPath PM IPDU power units, and change their own passwords. Only administrative users have access to the OnBoard screens for configuring users or ports.

See Chapter 2, “Web Manager Introduction” for information about using the Web Manager that is needed by authorized users and administrative users.

Browser access to the Web Manager is through one of the following ways:

- Through the Ethernet
- Through one of the modem types described in “Management Features Provided on Supported Device Types” on page 19.

Power Management Options on the OnBoard

Authorized users and OnBoard administrators can turn power off, turn power on, and turn power off and on again quickly (cycle power) to reboot devices.

The OnBoard provides the following two types of power management options for administrators and authorized users:

- IPDU power management

  Allows the user to manage power for any type of AC device that may be plugged into an AlterPath PM intelligent power distribution unit (IPDU), when the IPDU is connected to the OnBoard’s AUX port.

For details about the Web Manager –> IPDU screen that is used to manage power outlets and for links to procedures, see “Managing Power Outlets on a Connected IPDU” on page 65.

- Service processor power management

  Allows the user to manage power for a server whose service processor is connected to the OnBoard when the service processor provides power management capabilities. See “Management Features Available to Authorized Users” on page 14 for details about power management of connected servers with service processors.

  For links to sections that describe how to access a service processor’s power management capabilities using the Web Manager or `ssh`, see Table 3 on page 31.

Accessing a Device’s Native Management Features

Native IP access gives an authorized user authenticated access to a device’s native features such as integrated web servers and other proprietary interfaces that are available over IP.

Native Web

Access to native functions on some service processors is through a proprietary web interface on the service processor. HP iLO, Dell DRAC, and IBM RSA II service processors have a local web server running and provide a web interface that allows administrators remote access for provisioning, monitoring, and managing the server. The web interface is accessed through a specific port number.

The monitoring and management features supported by some service processors through their native web interfaces include access to the server’s serial or graphical user interface, power control, access to sensor data and server event logs, SNMP agents, and virtual media.

Native Management Applications

Native applications are proprietary service processor management applications provided by some server vendors, such as HP InSight Manager, IBM Director, and Dell Open Manage. Access to a native application usually requires the user to have the application installed on the user’s computer. Some management applications reside on the service processor itself.

After an authenticated and authorized user establishes a VPN connection and chooses the “Native IP” option, the user can bring up the management application from where it resides on the user's computer or from the service processor’s console.

Native IP Access Requirements

Native IP access depends on the following being true:

- The service processor must provide the desired native management functionality.

  For example, service processors using IPMI protocols do not provide native web access.
- The user can be trusted to use the native IP access appropriately.
- The OnBoard administrator has authorized the user to access the “Native IP” option on a service processor
- The user has created a secure tunnel to the OnBoard:
  - An SSH tunnel gives access to native web applications only
  - A VPN tunnel gives access to both native web and native management applications

Tasks for Creating Secure Tunnels and Obtaining Native IP Access

The following table lists the tasks for creating secure tunnels and obtaining native IP access and where the tasks are documented.

Table 1-2: Tasks for Creating Tunnels and Obtaining Native IP Access

Task	Where Documented
Create an SSH tunnel, and bring up a browser to access a native web application	• "Creating an SSH Tunnel" on page 82 • "To Use OpenSSH on Linux to Create an SSH Tunnel" on page 83 • "To Use PuTTY on a Windows PC to Create an SSH Tunnel" on page 83 • "To Bring Up a Native Web Application When an SSH Tunnel Exists" on page 85
Create a VPN tunnel using either IPSec or PPTP, and do one of the following: • Bring up a browser to access a native web application • Launch a native management application from the device or from a remote workstation.	• "Creating a VPN Tunnel" on page 86 • "Routing Requirements for VPN Connections" on page 88 • "Summary of VPN-related Requirements for Native IP Access" on page 90 • "VPN Through IPSec Connections" on page 91 • "To Create an IPSec VPN Tunnel" on page 92 • "To Enable Native IP Access Through an IPSec VPN Tunnel" on page 92 • "PPTP VPN Connections" on page 93 • "To Create a PPTP VPN Tunnel" on page 93 • "To Enable Native IP Access Through a PPTP VPN Tunnel" on page 94 • "To Access a Native Web Application When a VPN Tunnel Exists" on page 94 • "To Access a Native Management Application" on page 95

Information Users Need

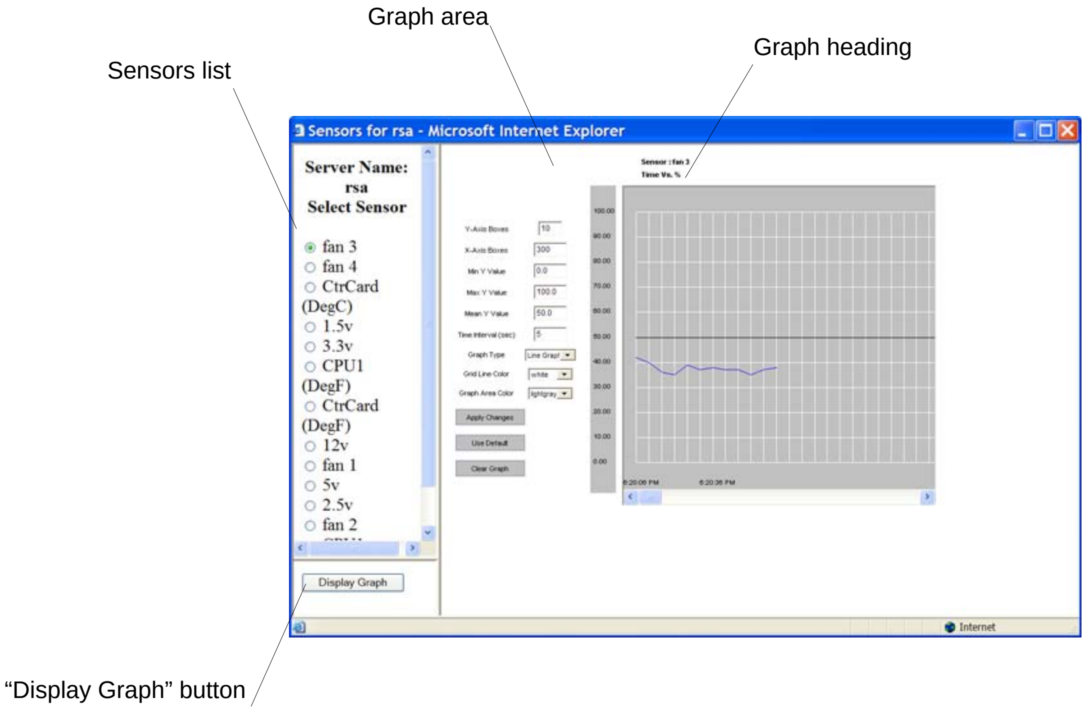
Users need to obtain the following information from the OnBoard administrator.

- The user’s name and password
- The names of devices that the user is authorized to manage and the device management actions that the user is authorized to perform
- Information about services that are enabled or disabled on the OnBoard. For example, the administrator may have configured the OnBoard so that HTTP or SSH v1 are disabled.
- A list of IPDU power outlets the user may be authorized to manage.
- For native IP users using PPTP VPN connections, the PPTP password, which may be different from the password used to access the OnBoard.
- For native IP users using IPSec VPN connections, authentication information for either shared secret or RSA key authentication.

Sensor Plotting

An authorized user or administrative user can view graphical displays of sensor data collected from servers by their service processors and can also modify graph display settings, either through the Web Manager, the user shell menu, by using `ssh` with the sensor commands.

The following figure shows an example graph.



Server Name: rsa

Select Sensor

● fan 3
○ fan 4
○ CtrCard (DegC)
○ 1.5v
○ 3.3v
○ CPU1 (DegF)
○ CtrCard (DegF)
○ 12v
○ fan 1
○ 5v
○ 2.5v
○ fan 2

Sensor : fan 3
Time Vs. %

Y-Axis Boxes 10
X-Axis Boxes 300
Min Y Value 0.0
Max Y Value 100.0
Mean Y Value 50.0
Time Interval (sec) 5
Graph Type Line Graph
Grid Line Color white
Graph Area Color lightgray

Figure 1-2: Example Graph for Readings From a Fan Sensor

The graph heading reads: “Time Vs. *sensor_value*.” *sensor_value* varies with the type of data being measured. The example fan sensor reading in Figure 1-2 has a heading “Time Vs. %” because the value being sensed is the percentage of total possible fan speed. Examples of other possible values for *sensor_value* (which vary from one vendor’s service processor to the next) are “*Volts*,” “*Degrees Centigrade*,” and “*Degrees Farenheit*.”

The following table shows graph features that can be modified. An error message appears if you enter a value that is greater than or lower than the supported range of values.

Table P-2: Sensor Graph Parameters

Field/Menu	Use	Default	Allowed Values
y-Axis Boxes	Specify a different number of rows.	10	1-55

Table P-2: Sensor Graph Parameters (Continued)

Field/Menu	Use	Default	Allowed Values
x-Axis Boxes	Specify a different number of columns. Each graph cell represents the interval between readings.	300	1-999
Min Y Value	Specify a different minimum sensor value to be plotted on the x axis. The only valid keys are numeric keys, period (.), and hyphen (-).	Varies with the type of sensor	Varies with the type of sensor
Max Y Value	Specify a different maximum sensor value to be plotted on the y axis. The only valid keys are numeric keys, period (.), and hyphen (-).	Varies with the type of sensor	Varies with the type of sensor
Mean Y Value	Specify a different mean value to use as a basis for comparison with the actual detected value. The only valid keys are numeric keys, period (.), and hyphen (-). In line graphs, the Mean Temp is indicated by a black horizontal line. In bar graphs, the colors of the bars indicate the following: • Blue – Less than the mean Y value. • Red – Greater than mean Y value. • Black – Equal to the mean Y value.	Varies with the type of sensor	Varies with the type of sensor
Time Interval	Specify a different frequency in seconds for fetching sensor data. The only valid keys are numeric keys.##	5	5-300
Graph Type	Chose another graph type.	• Line Graph	• Line Graph • Bar Graph

Table P-2: Sensor Graph Parameters (Continued)

Field/Menu	Use	Default	Allowed Values
Grid Line Color	Choose another color for the lines.	• white	• yellow green cyan gray darkgray lightgray magenta orange pink white
Graph BG Color	Select the background color.	• light gray	• yellow green cyan gray darkgray lightgray magenta orange pink white

For procedures for monitoring sensors, see “To View a Server’s Sensor Data from a Service Processor [Web Manager]” on page 54.

Common Tasks for Device Management

The following table shows the tasks related to accessing and managing devices and lists the options the OnBoard user and administrator have for performing those tasks.

Table P-3: Tasks for Managing Devices

Task	Options and Where Described
Connect to a device's console	• Using the Web Manager See "Accessing a Device's Console" on page 48. • Using an SSH utility or `ssh` on the command line to connect to the OnBoard's console before accessing the device's console through a menu. See "To Access the OnBoard's Console" on page 76. • Using ssh on the command line to connect directly from the user's computer to the device's console. See "To Use a SSH Command to Connect Directly to a Device's or Service Processor's Console" on page 80.
Connect to a service processor's console	• Using the Web Manager See "Accessing a Service Processor's Console" on page 47 • Using an SSH utility or `ssh` on the command line to connect to the OnBoard's console before accessing the service processor's console through a menu. See "To Access the OnBoard's Console" on page 76 • Using `ssh` on the command line to connect directly from the user's computer to the service processor's console with OnBoard-specific spconsole command. See "To Use a SSH Command to Connect Directly to a Device's or Service Processor's Console" on page 80.

Table P-3: Tasks for Managing Devices (Continued)

Task	Options and Where Described
Manage a server’s power through its service processor	• Using the Web Manager See “To Manage a Server’s Power Through a Service Processor [Web Manager]” on page 50 • Using ssh to connect to the OnBoard and then manage power See “Accessing the OnBoard Using SSH” on page 21. • Using ssh on the command line with power commands See “Device Management Commands for Use With SSH” on page 21.
Manage a system’s event logs through its service processor	• Using the Web Manager See “To View or Clear a Server’s Event Log Through a Service Processor [Web Manager]” on page 56 • Using `ssh` to connect to the OnBoard and then view or clear event logs. See “Accessing the OnBoard Using SSH” on page 21. Using `ssh` on the command line with event log commands. See “Device Management Commands for Use With SSH” on page 21.

Table P-3: Tasks for Managing Devices (Continued)

Task	Options and Where Described
View server sensor data through the server’s service processor	• Using the Web Manager See “To View a Server’s Sensor Data from a Service Processor [Web Manager]” on page 54 • Using ssh to connect to the OnBoard and then view or clear event logs. See “Accessing the OnBoard Using SSH” on page 21. • Using ssh on the command line with event log commands. See “Device Management Commands for Use With SSH” on page 21.

Chapter 2
Web Manager Introduction

This chapter describes how authorized users and administrative users use the Web Manager to access the OnBoard, to manage connected service processors and other devices, to manage power outlets on any connected AlterPath PM IPDUs, and to manage their own passwords.

This chapter provides background information listed in the following table.

The procedures in this chapter are listed in the following table.

Prerequisites for Using the Web Manager

This section describes the required browsers, preparation, and browser plug-ins needed for different types of access.The prerequisites described in this section must be complete before anyone can access the Web Manager. If you have questions about any of the following prerequisites, contact your site's system or network administrator.

- The IP address of the OnBoard must be known.

  Entering the IP address of the OnBoard in the address field of one of the supported browsers listed in Table 2-1 on page 37 is the first step required to access the Web Manager.

  When DHCP is enabled, a device's IP address may or may not be fixed,. When the address is not fixed, anyone wanting to access the OnBoard must find out the currently-assigned IP address each time. If DHCP is enabled and you do not know how to find out the current IP address of the OnBoard, contact your system administrator for help.

- A user account must be defined on the Web Manager.

  By default, the "admin" has an account on the Web Manager. An administrator can add regular user accounts to access connected devices using the Web Manager.

For accessing the Web Manager, you can use any type of modern computer that has access to the network where the AlterPath OnBoard is installed and any modern browser (such as Internet Explorer 5.5 or above, Netscape 6.0 or above, Mozilla, or Firefox) with a Java 2 plug-in.

The browser and JRE versions in the following tables have been tested and proven to work.

Table 2-1: Supported Browser and JRE Versions

Browser	Version	JRE Version
Firefox	1.0.7	JRE 1.5.0_01
Internet Explorer	6.0	JRE 1.5.0_02
Mozilla	1.7	JRE 1.5.0_01
Netscape	7.1	JRE 1.5.0_02

Requirements for Java Plug-In Availability

The Web Manager launches Java applets in the following situations:

- When establishing console access to the OnBoard and to SPs and other connected devices
- When displaying sensor data.

The Java applets rely on the Java plug-in being installed on the computer and registered with the browser being used.

Installing Java 2 Runtime Environment (J2RE) software, Standard Edition, automatically installs the needed Java plug-in. After you download and install the JRE software, you then must make sure the Java plug-in is registered with the browser. The following table provides links to the related procedures.

To Check Browsers for Java Plug-in Support	Page 38
To Install JRE2 Software and Register the Java Plug-in	Page 39

Note: The Java Runtime Environment is also called Java 2 Platform, Standard Edition (J2SE) at the java.sun.com website, and in the IE browser, it is called Java 2.

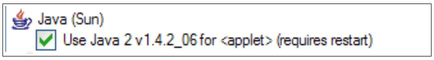
▼ *To Check Browsers for Java Plug-in Support*

1. To check Internet Explorer on Windows, do the following steps.

a. Go to Tools –> Internet Options –> Advanced.

b. Scroll down to find the Java section.

A line with an adjacent checkbox should appear with the wording "Use JRE 1.5.0_*NN*" as shown in the following figure.



Java (Sun)

☑ Use Java 2 v1.4.2_06 for <applet> (requires restart)

i. If the line appears and the checkbox is not checked, check the checkbox to register the plug-in with the browser.

   ii. If the line does not appear, install the JRE 2 software as described under “To Install JRE2 Software and Register the Java Plug-in” on page 39.

2. To check Netscape or Mozilla on Windows, do the following steps.

   a. Go to Edit –> Preferences –> Advanced.

   b. Check the “Enable Java” checkbox.

   c. To see what version of the Java plug-in is registered, do the following steps.

      i. Go to Help –> About Plug-ins.

      ii. Scroll to the Java Plug-in section.

      iii. Check whether the registered Java plug-in is the same as the version you installed.

3. If needed, go to “To Install JRE2 Software and Register the Java Plug-in” on page 39.

▼ *To Install JRE2 Software and Register the Java Plug-in*

1. Make sure the Java 2 Runtime Environment (JRE 2) software, version 1.4.2 or 1.5 is installed on the computer.

2. If needed, download the JRE 2 software from:

   `http://java.sun.com/j2se/1.4.2/download.html`

   OR

   `http://java.sun.com/j2se/1.5.0/download.jsp`

3. If needed, follow the instructions at:

   http://java.sun.com/j2se/1.4.2/jre/install.html

   OR

   http://java.sun.com/j2se/1.5.0/install.html

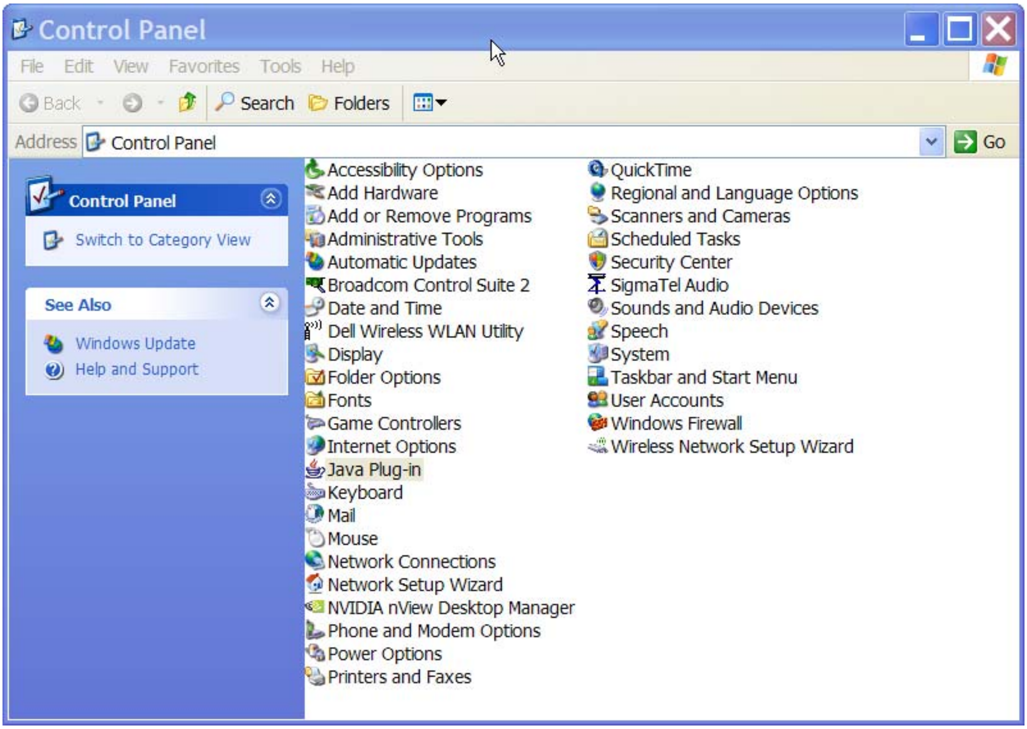
4. Register the plug-in.

   Installing JRE2 1.5 gives you an option to register the Java plug-in for the browsers on your computer during installation. Follow the prompts to register the plug-in. If you install JRE2 1.4.2, you need to manually register the Java plug-in afterwards, as described in Step 5

5. To enable the Java plug-in, do the following steps.

   a. Go to the Control Panel on the start menu on the Windows computer.

      The Control Panel appears.

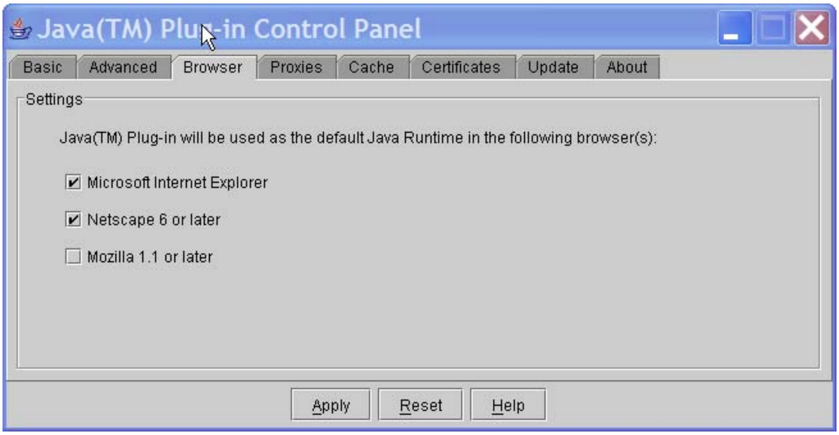


   b. If the Java Plug-in icon appears, click it.

      The Java Plug-in Control Panel appears.

   c. Click the Browser tab.

      The Browser form appears.



Settings

Java(TM) Plug-in will be used as the default Java Runtime in the following browser(s):

☑ Microsoft Internet Explorer

☑ Netscape 6 or later

□ Mozilla 1.1 or later

d. Check a checkbox next to the name of each browser in which to enable the Java plug-in.

e. Click “Apply.”

6. Verify that the browser is successfully registered with the browser by performing this procedure: “To Check Browsers for Java Plug-in Support” on page 38.

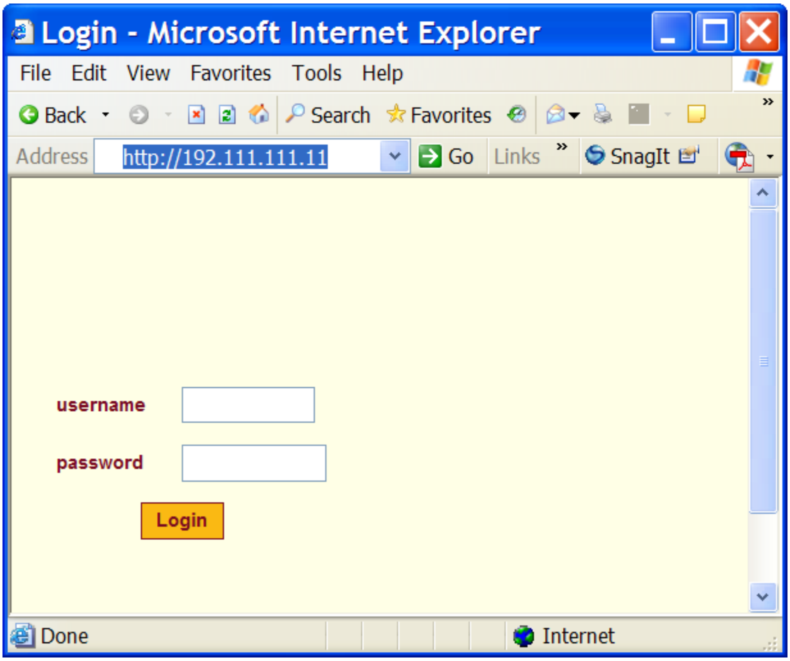
Logging Into the Web Manager for Regular Users

Both authorized users and OnBoard administrators can access the Web Manager from a browser using HTTP or HTTPS over the Internet or through a dial-in or callback PPP connection.

After being authenticated during login, authorized users can use the Web Manager to log into devices, manage power, and change their own passwords, but they cannot use the Web Manager for configuring users or devices. Any number of regular users can connect to the Web Manager at the same time.

OnBoard administrators can perform additional user and device configuration tasks through the Web Manager. See the *AlterPath OnBoard Administrator's Guide* for details.

The following figure shows the login screen for the Web Manager that appears when the OnBoard's IP address is entered in a Microsoft Internet Explorer browser.


Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
SnagIt
Login
Done
Internet

Address: http://192.111.111.11

username

password

Figure 2-1: Web Manager Login Screen

Any number of regular users can connect to the Web Manager at the same time.

See “Cyclades Web Manager” on page 23 for more about how to use the Web Manager and “Prerequisites for Using the Web Manager” on page 37 for the required browsers, preparation, and browser plug-ins needed for different types of access.

▼ *To Log Into the Web Manager*

This procedure assumes you have a valid username and password for an account authorized to perform device management and that your computer has one of the following types of access to the OnBoard:

- A network connection
- A PPP connection

1. Enter the IP address of the OnBoard in a supported browser.

   See Table 2-1 on page 37 for a list of supported browsers, if needed.

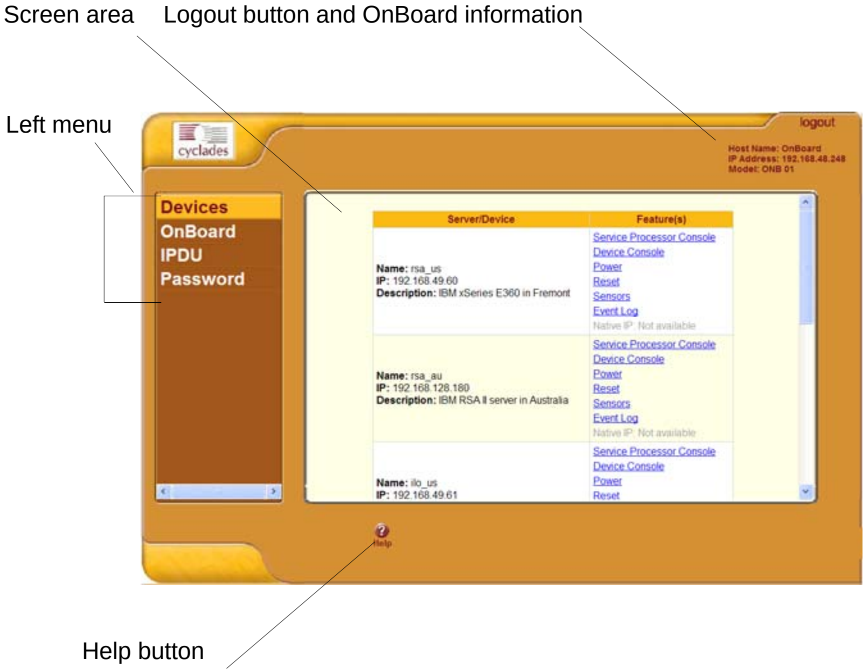
   The Web Manager login screen appears.

2. Enter your username and password.

3. Click the “Login” button.

Features of Regular Users’ Windows

The following figure shows features of the Web Manager that appear when regular users log in.



Host Name: OnBoard
IP Address: 192.168.48.248
Model: ONB 01

Server/Device	Feature(s)
Name: rsa_us **IP:** 192.168.49.60 **Description:** IBM xSeries E360 in Fremont	Service Processor Console Device Console Power Reset Sensors Event Log Native IP: Not available
Name: rsa_au **IP:** 192.168.128.180 **Description:** IBM RSA II server in Australia	Service Processor Console Device Console Power Reset Sensors Event Log Native IP: Not available
Name: ilo_us **IP:** 192.168.49.61	Service Processor Console Device Console Power Reset

Figure 2-2: User Options on the Web Manager

A menu of options appears on the left. When you select an option, the fields, buttons, and menus that appear in the screen in the middle change according to which option is selected.

Web Manager Menu Options for Regular Users

The user can select from the options shown in Figure 2-2 to do the tasks shown in the following table, which gives links to where the tasks are described.

Table 2-2: Device Access Menu Options

Task	Where Described
Connect to a device	“Using the Devices Screen” on page 45
Connect to the OnBoard	“Accessing the OnBoard Console [Web Manager]” on page 63
Manage outlets on an IPDU	“Managing Power Outlets on a Connected IPDU” on page 65
Change your password	“Configuring Your Password” on page 72

OnBoard administrators see the same list of options shown in Table 2-2 under the administrator’s “Access” tab. The “Access” tab is one of multiple tabs that are available on the Web Manager whenever an administrator logs in. Administrators can refer to the *AlterPath OnBoard Administrator’s Guide* for more details.

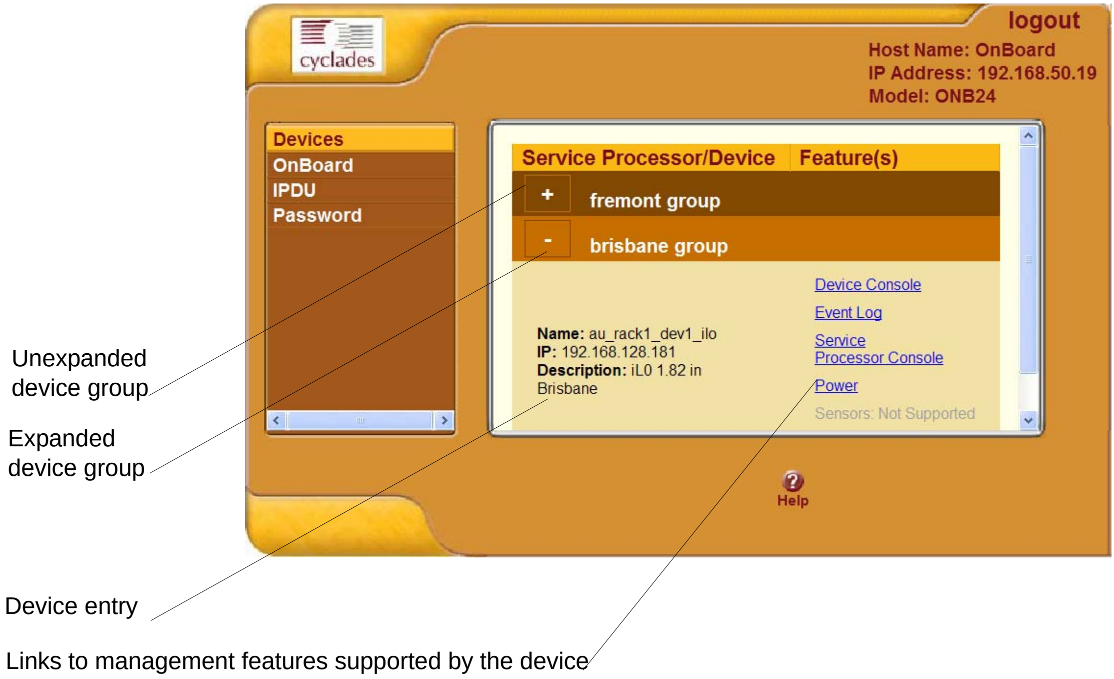
Using the Devices Screen

The Devices screen lists device groups and individual devices that are not in groups for every device the user is authorized to access. Clicking the plus (+) sign next to the name of a group expands the list of device entries. Clicking a minus (-) sign hides the list of device entries.

The entry for each device has the following:

- Links to the management features the user is allowed to access on that device
- The name (alias) assigned to the device
- A real IP address (if a virtual IP address is not assigned to the device)
- A virtual IP address (if one is assigned to the device)
- A description of the device

The Devices screen is shown in the following figure.



Host Name: OnBoard
IP Address: 192.168.50.19
Model: ONB24

Name: au_rack1_dev1_ilo
IP: 192.168.128.181
Description: iL0 1.82 in Brisbane

Figure 2-3: Devices Web Manager Screen

Links to device management features are active only when they are supported for a particular device. The following table lists the management features, which are introduced in Table 1-1, “Options and Command Names for Device Management,” on page 15. The following table provides links to more information about accessing these features using the Web Manager.

Table 2-3: Management Features Accessed Through the Web Manager

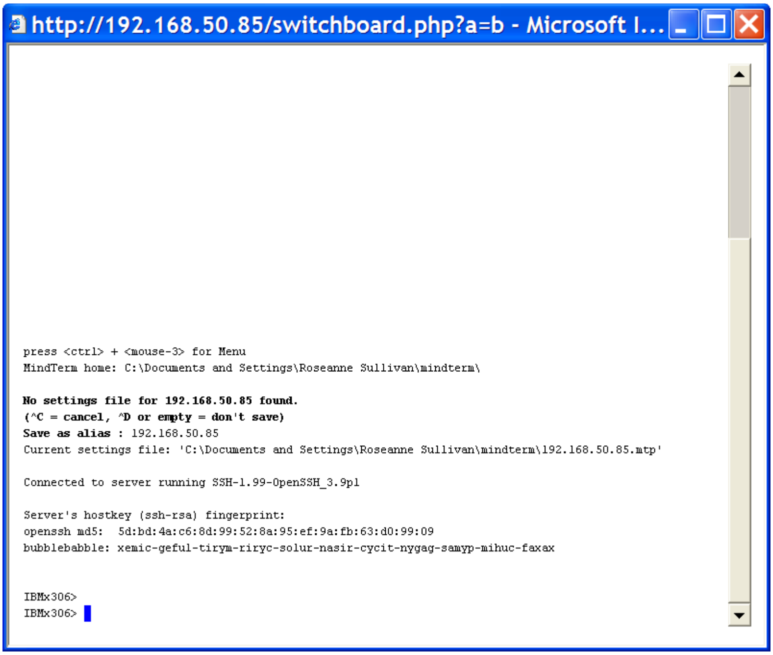
Feature	Where Described
Service Processor Console	“Accessing a Service Processor’s Console” on page 47
Device Console	“Accessing a Device’s Console” on page 48
Power	“Viewing and Clearing Event Logs” on page 55
Reset	“Running Reset on a Service Processor” on page 51

Table 2-3: Management Features Accessed Through the Web Manager (Continued)

Feature	Where Described
Sensors	“Viewing Sensor Data” on page 51
Event Log	“Viewing and Clearing Event Logs” on page 55
Native IP	“Accessing Native Features on a Service Processor” on page 57

Accessing a Service Processor’s Console

Clicking the “Service Processor Console” link on the Devices screen gives you access to the command line of the service processor. A window running a MindTerm Java applet appears, as shown in the following screen example.



```
press <ctrl> + <mouse-3> for Menu
MindTerm home: C:\Documents and Settings\Roseanne Sullivan\mindterm\

No settings file for 192.168.50.85 found.
(^C = cancel, ^D or empty = don't save)
Save as alias : 192.168.50.85
Current settings file: 'C:\Documents and Settings\Roseanne Sullivan\mindterm\192.168.50.85.mtp'

Connected to server running SSH-1.99-OpenSSH_3.9p1

Server's hostkey (ssh-rsa) fingerprint:
openssh md5:  5d:bd:4a:c6:8d:99:52:8a:95:ef:9a:fb:63:d0:99:09
bubblebabble: xemic-geful-tirym-riryc-solur-nasir-cycit-nygag-samyp-mihuc-faxax


IBMx306>
IBMx306>
```

Figure 2-4: Service Processor Console Example

▼ *To Connect to a Service Processor’s Console [Web Manager]*

1. Bring up the Web Manager and log in.

   See “To Log Into the Web Manager” on page 43, if needed.

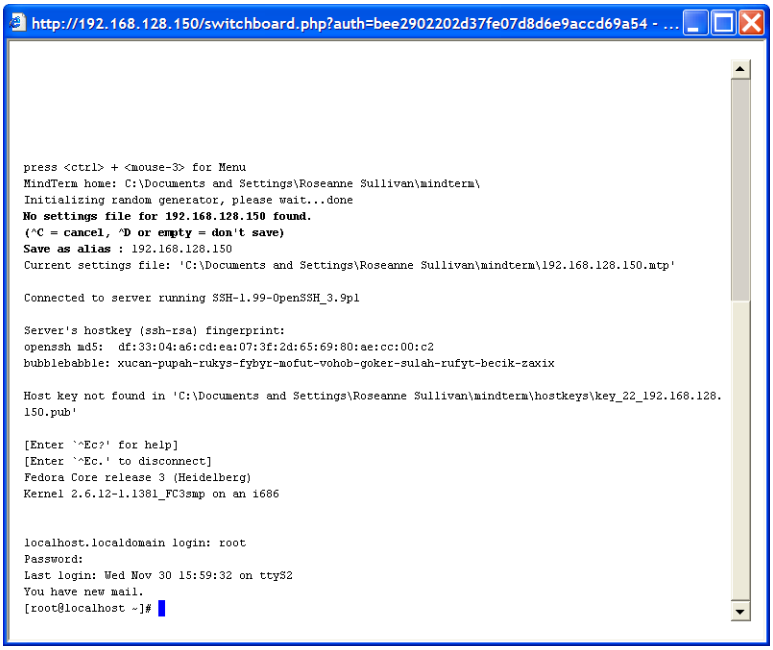
2. From the list of devices that displays on the “Devices” screen, click the “Service Processor Console” link that is associated with the server whose console you want to access.

   A MindTerm window displays with an `ssh` connection to the device.

3. If authentication is enabled for the service processor, log in as prompted.

Accessing a Device’s Console

Clicking the “Device Console” button on the Devices screen launches a terminal window running a Java applet and creates a console connection with the device. The following figure shows an example terminal window with a connection to a device console on a Compaq Proliant server with an iLO type service processor.


http://192.168.128.150/switchboard.php?auth=bee2902202d37fe07d8d6e9accd69a54 - ...

```
press <ctrl> + <mouse-3> for Menu
MindTerm home: C:\Documents and Settings\Roseanne Sullivan\mindterm\
Initializing random generator, please wait...done
No settings file for 192.168.128.150 found.
(^C = cancel, ^D or empty = don't save)
Save as alias : 192.168.128.150
Current settings file: 'C:\Documents and Settings\Roseanne Sullivan\mindterm\192.168.128.150.mtp'

Connected to server running SSH-1.99-OpenSSH_3.9p1

Server's hostkey (ssh-rsa) fingerprint:
openssh md5:  df:33:04:a6:cd:ea:07:3f:2d:65:69:80:ae:cc:00:c2
bubblebabble: xucan-pupah-rukys-fybyr-mofut-vohob-goker-sulah-rufyt-becik-zaxix

Host key not found in 'C:\Documents and Settings\Roseanne Sullivan\mindterm\hostkeys\key_22_192.168.128.
150.pub'

[Enter `^Ec?' for help]
[Enter `^Ec.' to disconnect]
Fedora Core release 3 (Heidelberg)
Kernel 2.6.12-1.1381_FC3smp on an i686


localhost.localdomain login: root
Password:
Last login: Wed Nov 30 15:59:32 on ttyS2
You have new mail.
[root@localhost ~]#
```

Figure 2-5: Device Console Example

▼ *To Connect to a Device's Console [Web Manager]*

1. Bring up the Web Manager and log in.

See “To Log Into the Web Manager” on page 43.

2. From the list of devices that displays on the “Devices” screen, click the “Device Console” link for the server or device whose console you want to access.

A MindTerm window displays with an `ssh` connection to the device.

3. If authentication is enabled for the device, lo gin as prompted.

Managing Power Through a Service Processor

Clicking the “Power” button on the Devices screen gives you access to a menu of power management options that are available on the service processor, as shown in the following screen example.

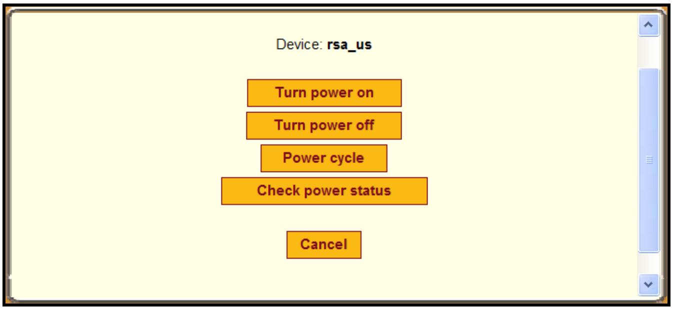
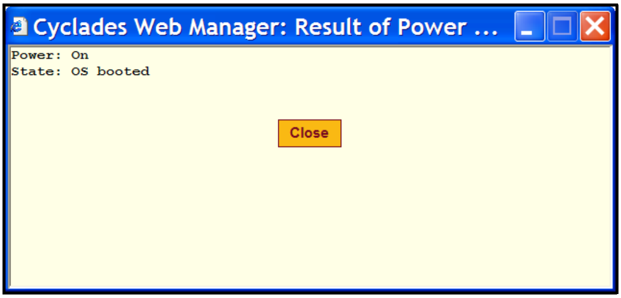

Device: rsa_us

Figure 2-6: Power Web Manager Screen

Clicking the “Check power status” button brings up a dialog box that shows the server’s power status. The following screen example shows the power is on and the operating system (OS) is booted on the server.



```
Power: On
State: OS booted
```

Figure 2-7: Example Power Status Dialog

▼ *To Manage a Server’s Power Through a Service Processor [Web Manager]*

1. Bring up the Web Manager and log in.

   See “To Log Into the Web Manager” on page 43, if needed.

2. From the list of devices that displays on the “Devices” screen, click the “Power” link that is associated with the server whose power you want to manage.

3. To turn power on for the server, click the “Turn power on” button.

4. To turn power off for the server, click the “Turn power off” button.

5. To turn power off and then on for the server (to reboot the server), click the “Power cycle” button.
6. To check the power status of the server, click the “Check power status” button.

Running Reset on a Service Processor

If a service processor has more than one type of reset option, the OnBoard “Reset” command on the Devices screen performs the highest level of reset: the cold boot option if available. See “What the Reset Command Does on Different Servers” on page 18 for details.

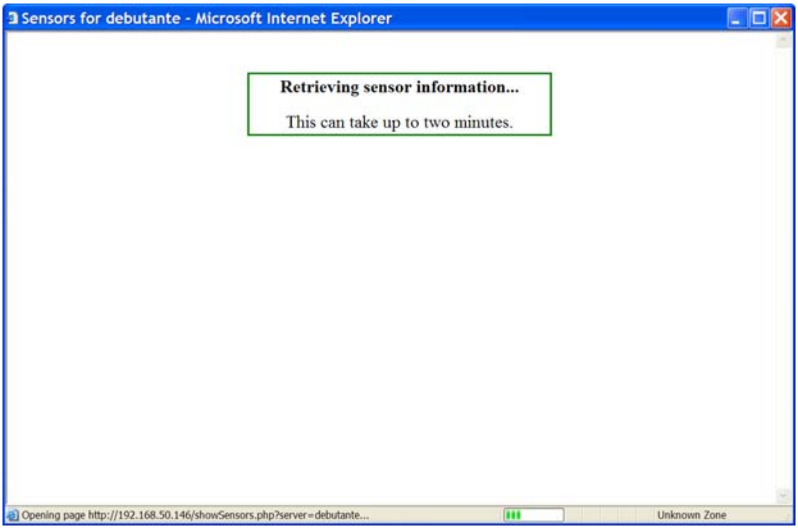
▼ *To Reset a Server from a Service Processor [Web Manager]*

1. Bring up the Web Manager and log in.

   See “To Log Into the Web Manager” on page 43, if needed.
2. From the list of devices that displays on the “Devices” screen, click the “Reset” link associated with the server.

Viewing Sensor Data

Clicking the “Sensors” button on the Devices screen displays the service processor’s sensor plotting page. The following screen example shows the message that comes up while the sensor information is being loaded. For details about the “Sensor Plotting” on page 27.



Sensors for debutante - Microsoft Internet Explorer

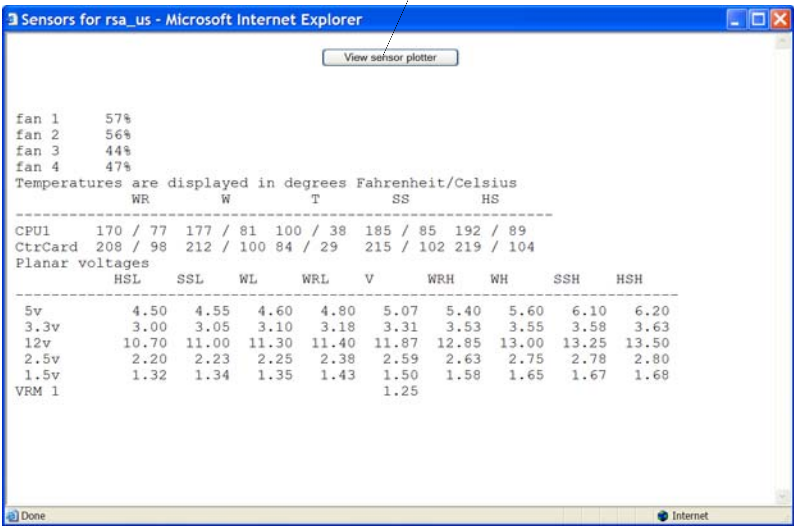
Retrieving sensor information...

This can take up to two minutes.

Opening page http://192.168.50.146/showSensors.php?server=debutante...
Unknown Zone

Figure 2-8: Sensors Data Loading Message

The following screen example shows the Sensors screen that displays unformatted data.



View sensor plotter button

```
fan 1     57%
fan 2     56%
fan 3     44%
fan 4     47%
Temperatures are displayed in degrees Fahrenheit/Celsius
             WR        W         T        SS        HS
------------------------------------------------------------
CPU1     170 / 77  177 / 81  100 / 38  185 / 85  192 / 89
CtrCard  208 / 98  212 / 100 84 / 29   215 / 102 219 / 104
Planar voltages
           HSL    SSL    WL     WRL    V      WRH    WH     SSH    HSH
--------------------------------------------------------------------------
 5v          4.50   4.55   4.60   4.80   5.07   5.40   5.60   6.10   6.20
 3.3v        3.00   3.05   3.10   3.18   3.31   3.53   3.55   3.58   3.63
 12v        10.70  11.00  11.30  11.40  11.87  12.85  13.00  13.25  13.50
 2.5v        2.20   2.23   2.25   2.38   2.59   2.63   2.75   2.78   2.80
 1.5v        1.32   1.34   1.35   1.43   1.50   1.58   1.65   1.67   1.68
VRM 1                                    1.25
```

Figure 2-9: Example of Unformatted Sensor Data

Clicking the “View sensor plotter” button shown in Figure 2-6 brings up a screen that allows you to view data from individual sensors on the server.

The sensor plotter page is shown in the following screen example. Callouts indicate the list of sensors in the left column with a radio button next to each item; the graph area; and the “Display Graph” button. After the radio button next to the desired sensor is clicked, clicking “Display Graph” displays the data from the selected sensor in the graph area.

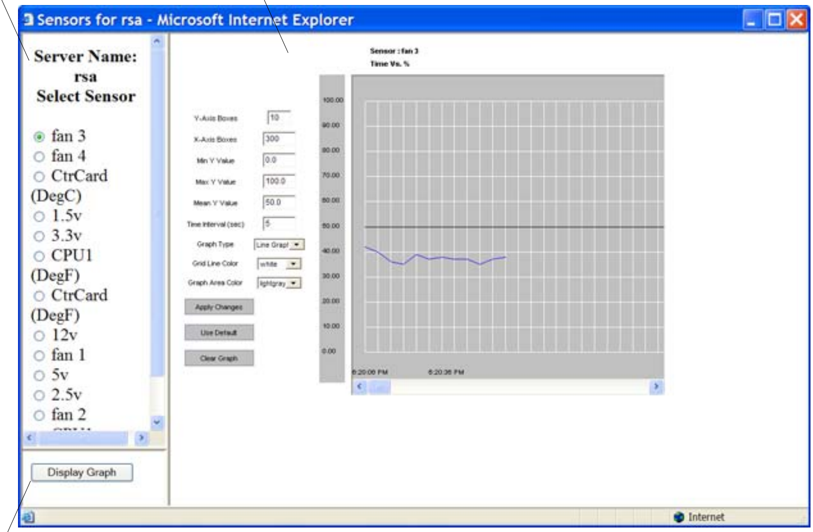
Users can bring up multiple instances of the sensor plotter page and view different sensors in different graphs at the same time.The graph displays a new reading at a specified interval. The default is five seconds. You can change the interval.

See Table 2, “Sensor Graph Parameters,” on page 28 for descriptions of the defaults and allowed values you can specify to change the display.

The following figure shows the default graph format.

Sensors list

Graph area



Y-Axis Boxes 10

X-Axis Boxes 300

Min Y Value 0.0

Max Y Value 100.0

Mean Y Value 50.0

Time Interval (sec) 5

Graph Type Line Graph

Grid Line Color white

Graph Area Color lightgray

“Display Graph” button

Figure 2-10: Graph Example

▼ *To View a Server’s Sensor Data from a Service Processor [Web Manager]*

1. Bring up the Web Manager and log in.

See “To Log Into the Web Manager” on page 43, if needed.

2. From the list of devices that displays on the “Devices” screen, click the “Sensors” link associated with the server whose sensors you want to view.

A MindTerm Java applet appears showing unformatted sensor data.

3. Click the “View sensor plotter” button.

A list of sensors appears on the left with the main graph area empty.

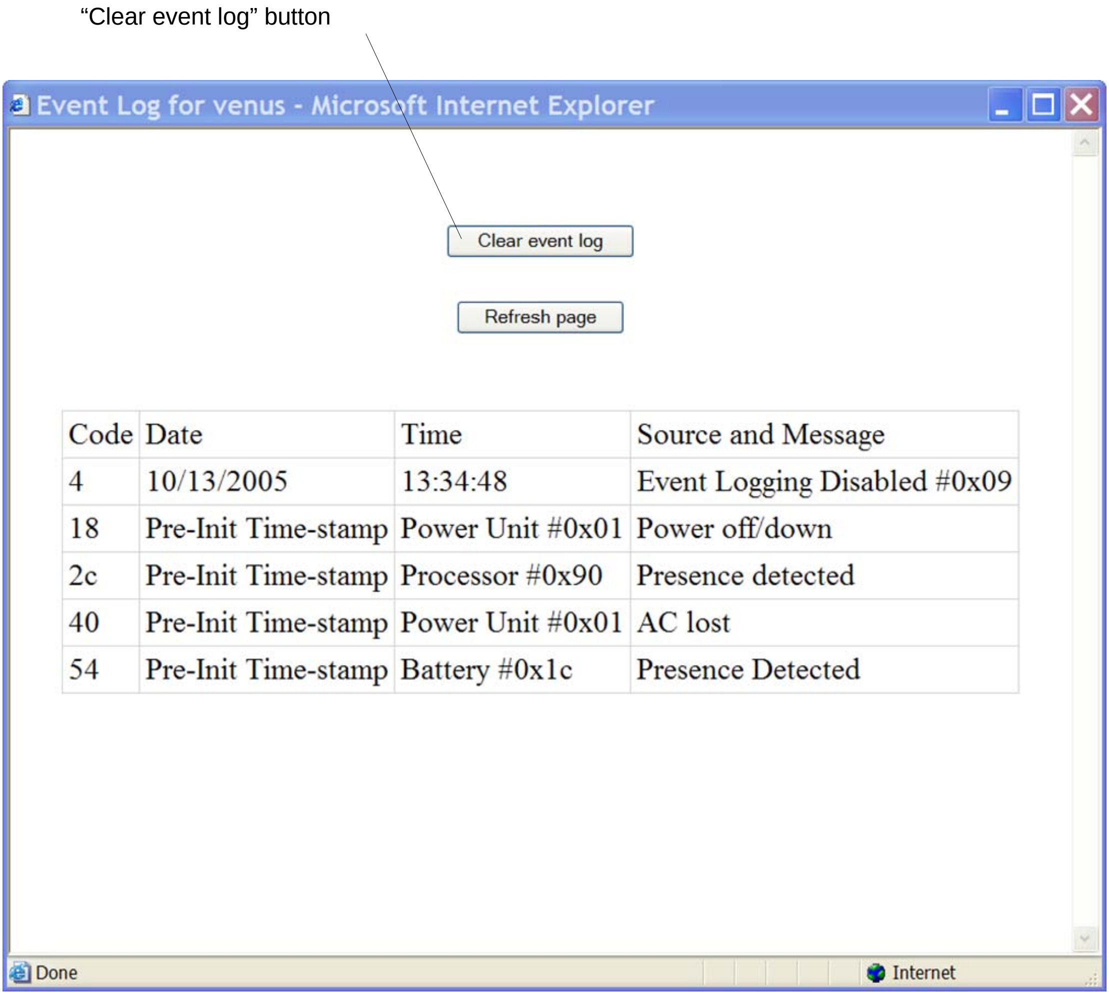
4. Click the radio button next to the name of the sensor you want to view.

5. Click the “Display Graph” button.

A graph of data from the selected sensor displays in the default graph format.

Viewing and Clearing Event Logs

Clicking the “Event Log” button on the Devices screen displays the system event log (SEL) menu from the server where the service processor resides. Event messages are sent by the service processor when system management events are detected. The events may be being logged either by the service processor or by the server. The “Clear event log” button appears at the top of the screen, as shown in the following screen example.



Code	Date	Time	Source and Message
4	10/13/2005	13:34:48	Event Logging Disabled #0x09
18	Pre-Init Time-stamp	Power Unit #0x01	Power off/down
2c	Pre-Init Time-stamp	Processor #0x90	Presence detected
40	Pre-Init Time-stamp	Power Unit #0x01	AC lost
54	Pre-Init Time-stamp	Battery #0x1c	Presence Detected

Figure 2-11: Example Event Log Web Manager Screen

Clicking the “Clear event log” button clears the log.

▼ *To View or Clear a Server’s Event Log Through a Service Processor [Web Manager]*

1. Log into the Web Manager.

See “To Log Into the Web Manager” on page 43, if needed.

2. From the list of devices that displays on the “Devices” screen, click the “Event log” link associated with the server whose power you want to manage.

   The Event log displays for your review.

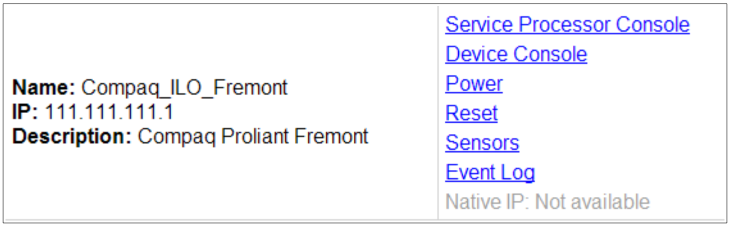
3. To clear the event log click the “Clear event log” button.

Accessing Native Features on a Service Processor

The Web Manager Access –> Device screen displays the “Enable Native IP” option for a service processor only if the following are all true:

- The user is authorized for native IP access to the service processor,
- The device supports native IP access, and
- A VPN connection (tunnel) exists between the user and the OnBoard.

If a VPN connection is not already up, the Access –> Device screen displays a “Native IP: Not available” message, as shown in the following screen example.



Name: Compaq_ILO_Fremont
IP: 111.111.111.1
Description: Compaq Proliant Fremont

Figure 2-12: Native IP: Not Available Status

By clicking the “Enable” link next to “Native IP” on the Devices screen, an authorized user enables access to several native features that may be available on a service processor or device, including:

- A native web application
- A native management application

For more details, see “Accessing a Device’s Native Management Features” on page 24.

The rules for how the user brings up the Web Manager to access the Devices screen differs between IPSec and PPTP VPN connections as indicated here:

- If the VPN connection is being made using IPSec, the authorized user may use the OnBoard’s IP address to bring up the Web Manager first and go to the Device screen before making the VPN connection. After subsequently making the VPN connection, the user can reload the form to see the Enable Native IP link active.
- If the VPN connection is made using PPTP, the VPN connection must be made before the Web Manager can be launched, because the Web Manager must be launched using the PPTP IP address.

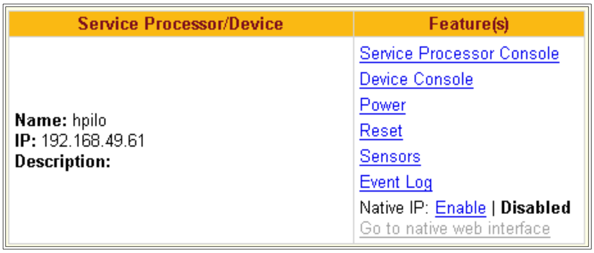
  The user obtains the IP address assigned to the PPTP interface by entering the `ifconfig` or `ipconfig` command on the computer’s command line (which command to use depends on the operating system). In the command output, the IP address assigned to the connection appears next to the words “PPP adapter.”.

```
C:\> ipconfig
...
PPP adapter OnBoard_PPTP_VPN
...
      IP Address. . . . . . . . . . : 172.0.0.0.100
...
```

  The user then enters the PPTP IP address in a browser to bring up the Web Manager and enable Native IP access.

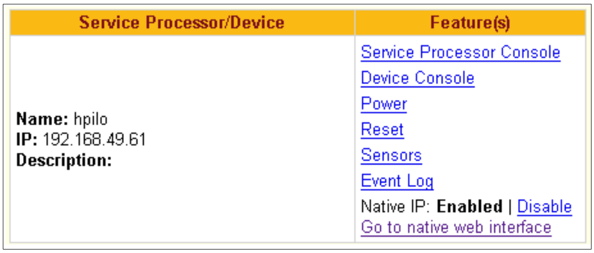
See “Tasks for Creating Secure Tunnels and Obtaining Native IP Access” on page 26 for more details.

As shown in the following screen example, the words Enable | Disabled appear appears next to the Native IP option if a VPN connection exists, with the Enable link active.



Service Processor/Device	Feature(s)
Name: hpilo **IP:** 192.168.49.61 **Description:**	Service Processor Console Device Console Power Reset Sensors Event Log Native IP: Enable | **Disabled** Go to native web interface

Clicking the Enable link enables native IP and makes the Disable link active and the “Go to native web interface” link appears, as shown in the following screen example.

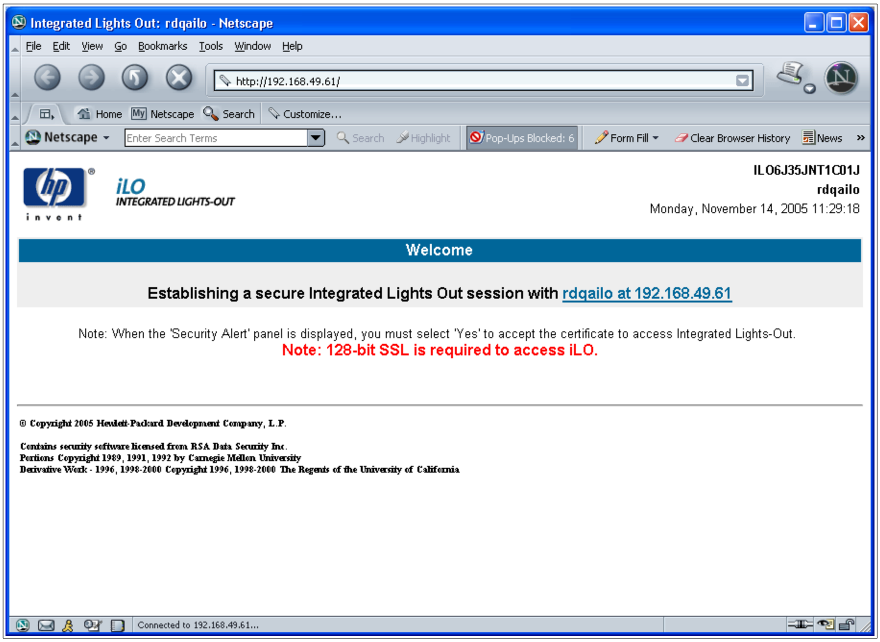


Service Processor/Device	Feature(s)
Name: hpilo **IP:** 192.168.49.61 **Description:**	Service Processor Console Device Console Power Reset Sensors Event Log Native IP: **Enabled** | Disable Go to native web interface

The authorized user can then do one of the following:

- Click the “Go to native web interface” link to launch a browser that brings up the native web application on the service processor.
- Launch a service processor management application from the user’s remote computer.

The following figure shows an example of a HP iLO web interface that appeared after an authorized user clicked the “Go to native web interface” link shown in the previous figure.



ILO6J35JNT1C01J
rdqailo
Monday, November 14, 2005 11:29:18

Welcome

Establishing a secure Integrated Lights Out session with rdqailo at 192.168.49.61

Note: When the 'Security Alert' panel is displayed, you must select 'Yes' to accept the certificate to access Integrated Lights-Out.
Note: 128-bit SSL is required to access iLO.

© Copyright 2005 Hewlett-Packard Development Company, L.P.

Contains security software licensed from RSA Data Security Inc.
Portions Copyright 1989, 1991, 1992 by Carnegie Mellon University
Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California

Figure 2-13: Example HP iLO Native Web Interface

Caution! When finished with service processor management tasks performed using native IP, the authorized user should always click the "Disabled" link before closing the VPN connection. Leaving native IP enabled creates a security risk.

▼ *To Create a PPTP VPN Connection Profile on Windows—Example*

This procedure assumes the following prerequisites:

- You are running Windows NT on your remote computer.

  If you are running any other Windows operating system, follow these steps as an example.

- The OnBoard administrator has done all of the following:
  - Authorized your OnBoard user account for PPTP access.

- Provided you with the PPTP password if it is different from your OnBoard password.
- Enabled the PPTP service.
- Configured the OnBoard for VPN PPTP connections
- Provided you with an IP address that was assigned while configuring VPN PPTP access on the OnBoard.

1. Login in as an administrator on Windows NT.

2. From the start menu, go to My Network Places –> view network connections –> Create a new connection.

The “New Connection Wizard” appears.

3. Click the “Next” button.

4. On the next dialog that appears, click the radio button next to “Connect to the network at my workplace.”

5. Click the “Next” button.

6. On the next dialog that appears, click the radio button next to “Virtual Private Network connection.”

7. Click the “Next” button.

8. On the next dialog that appears, enter a name for the connection.

9. Click the “Next” button.

10. If the “Public Network” dialog appears, click the radio button next to “Do not dial the initial connection.”

11. On the next dialog that appears, for the “VPN Server Selection,” enter an IP address.

Note: The IP address is the one assigned to the public interface of the OnBoard.

12. Click the “Next” button.

13. Click the “Finish” button.

▼ *To Enable Access to Native Features on a Device [Web Manager]*

1. Create a VPN tunnel between your computer to the OnBoard.

   If you created a VPN connection profile, click the name of the connection profile to create the connection.

2. If the VPN connection was made using IPSec, bring up the Web Manager by entering in a browser the IP address that is assigned to the OnBoard's public interface.

3. If the VPN connection was made using PPTP, obtain and use the IP address that is assigned on your computer to the PPTP interface.

   a. If your computer has a Windows operating system, enter the `ipconfig` command on the computer's command line.

   b. If your computer has a UNIX-based operating system, enter the `ifconfig` command on the computer's command line.

   c. In the command output, locate the IP address assigned to the connection.

   The following screen example shows the PPTP interface IP address output from the `ipconfig` command on an Windows NT operating system.

```
C:\> ipconfig
...
PPP adapter OnBoardPPTPVPN
...
      IP Address. . . . . . . . . . . : 172.0.0.0.100
...
```

   d. Enter the PPTP IP address in a browser to bring up the Web Manager.

4. Log into the Web Manager and go to Devices screen.

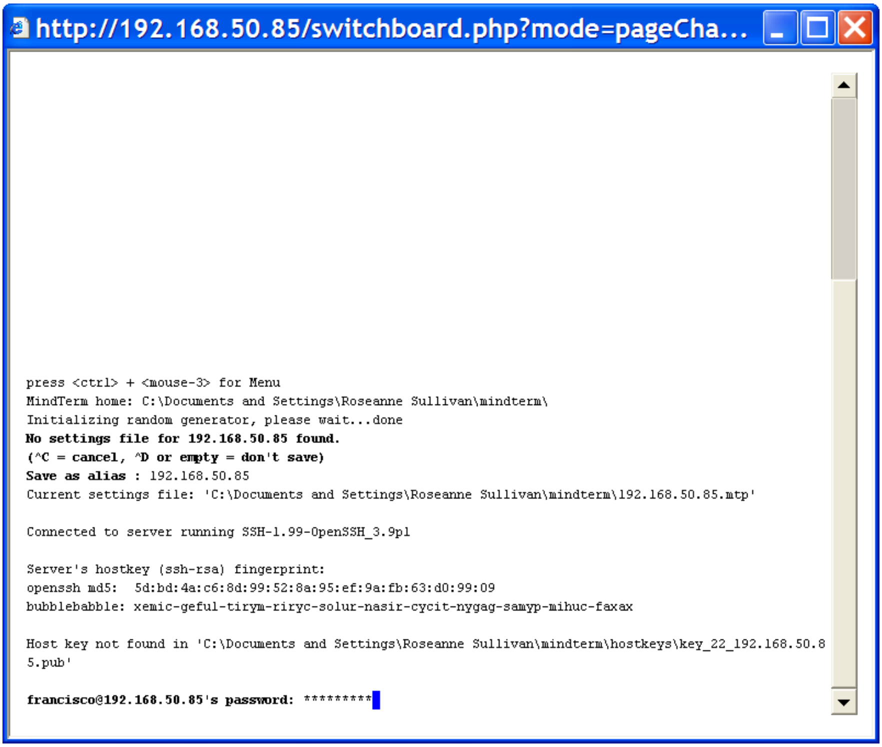
5. From the list of devices that displays on the “Devices” screen, click “Enable” next to the “Native IP” link for the device on which you want native IP access.

   The “Go to native web interface” link becomes active.

6. Click the “Go to native web interface” link to launch a browser that brings up the native web application on the service processor.
7. From your local computer, launch a previously-installed service processor management application for the server, if desired.
8. Essential security precaution: When you are done, click the Disable link.

Accessing the OnBoard Console [Web Manager]

Clicking the OnBoard option on the Web Manager menu and clicking the “Connect to OnBoard” button brings up a window running a MindTerm Java applet with an `ssh` connection to the OnBoard, as shown in the following screen example.



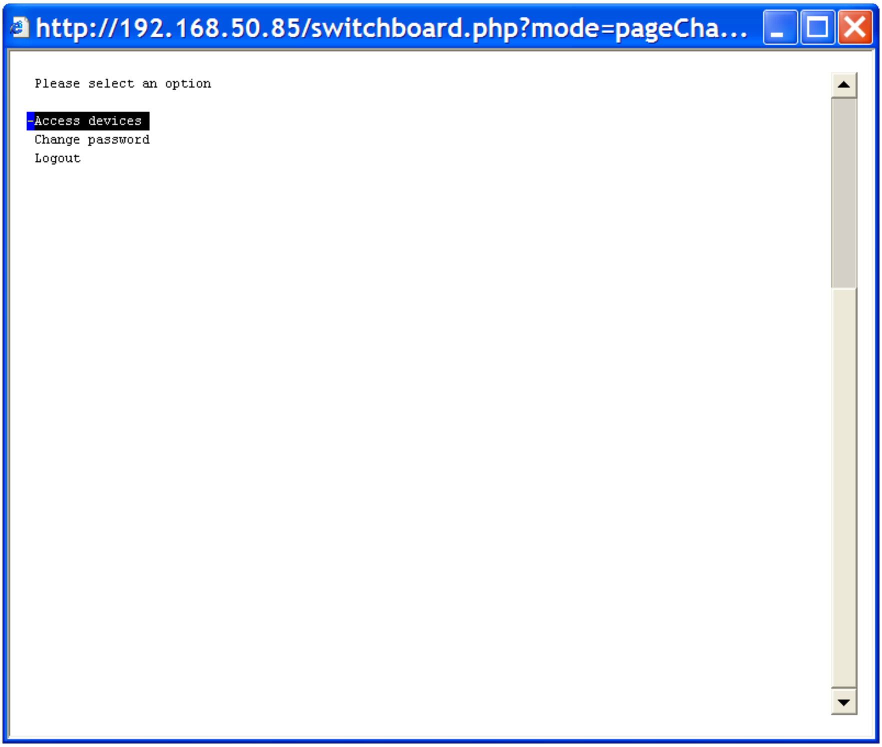
```
press <ctrl> + <mouse-3> for Menu
MindTerm home: C:\Documents and Settings\Roseanne Sullivan\mindterm\
Initializing random generator, please wait...done
No settings file for 192.168.50.85 found.
(^C = cancel, ^D or empty = don't save)
Save as alias : 192.168.50.85
Current settings file: 'C:\Documents and Settings\Roseanne Sullivan\mindterm\192.168.50.85.mtp'

Connected to server running SSH-1.99-OpenSSH_3.9p1

Server's hostkey (ssh-rsa) fingerprint:
openssh md5:  5d:bd:4a:c6:8d:99:52:8a:95:ef:9a:fb:63:d0:99:09
bubblebabble: xemic-geful-tirym-riryc-solur-nasir-cycit-nygag-samyp-mihuc-faxax

Host key not found in 'C:\Documents and Settings\Roseanne Sullivan\mindterm\hostkeys\key_22_192.168.50.8
5.pub'

francisco@192.168.50.85's password: *********
```

Figure 2-14: OnBoard Console Login Screen

Regular users by default are not able to access the OnBoard’s shell, and they cannot do anything on the OnBoard’s console that they could not do from the

Web Manager menu options. Users are encouraged to use the Web Manager instead of going through it and using the console.

After authentication, the regular user sees the two following choices to access devices or change the user’s password, which are similar to the Web Manager menu options.



```
Please select an option

Access devices
Change password
Logout
```

Figure 2-15: User Menu When Connected to the OnBoard’s Console

For information about what the administrative user can do on the OnBoard console, see *AlterPath OnBoard Administrator’s Guide*.

▼ To Access the OnBoard’s Console [Web Manager]

1. Bring up the Web Manager and log in.

See “To Log Into the Web Manager” on page 43, if needed.

2. Click the “OnBoard” option in the left menu.

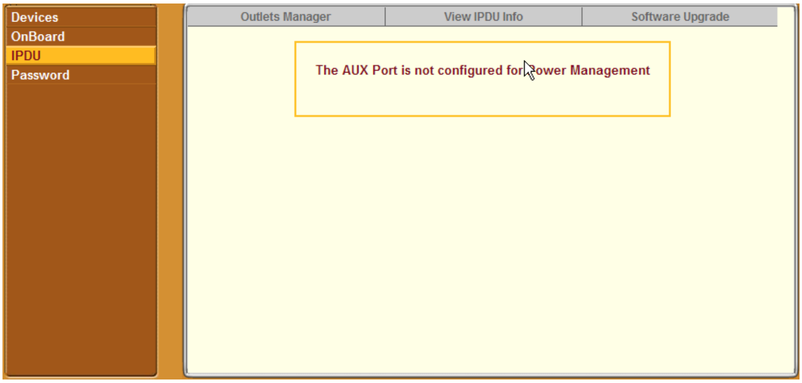
   A terminal window displays and establishes a console connection to the OnBoard.

3. Enter the password, if prompted.

   A menu of options displays for the regular user. For an administrative user a shell prompt appears.

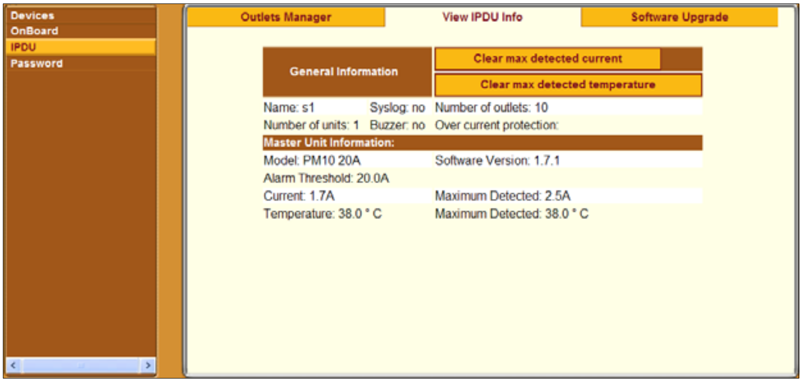
Managing Power Outlets on a Connected IPDU

Clicking the IPDU option on the Access menu brings up the message shown below if the AUX port has not been configured for IPDU power management. Contact the OnBoard administrator for help if you see this message.



The AUX Port is not configured for Power Management

Clicking the IPDU option on the Access menu when the AUX port has been configured for IPDU power management brings up three tabs, as shown in the following screen example.



Name: s1 Syslog: no Number of outlets: 10
Number of units: 1 Buzzer: no Over current protection:

Master Unit Information:

Model: PM10 20A Software Version: 1.7.1
Alarm Threshold: 20.0A
Current: 1.7A Maximum Detected: 2.5A
Temperature: 38.0 ° C Maximum Detected: 38.0 ° C

Figure 2-16: IPDU Tabs

Authorized users can access the screens under the three tabs to manage power on the outlets and to view information about the IPDUs. Administrative users can additionally assign names and set the power up interval for outlets and can upgrade software on the IPDU as described in the *AlterPath OnBoard Administrator's Guide*.

The three tabs are listed below with links to where they are described:

- Outlets Manager

  See "Using the Outlets Manager Tab to Turn Power On and Off and Check Power Status" on page 66.

- View IPDUs Info

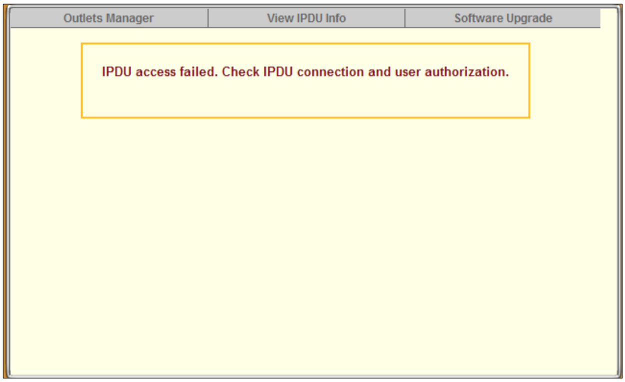
  See "Viewing IPDU Information" on page 69.

- Software Upgrade

  The regular user can only view this screen.

Using the Outlets Manager Tab to Turn Power On and Off and Check Power Status

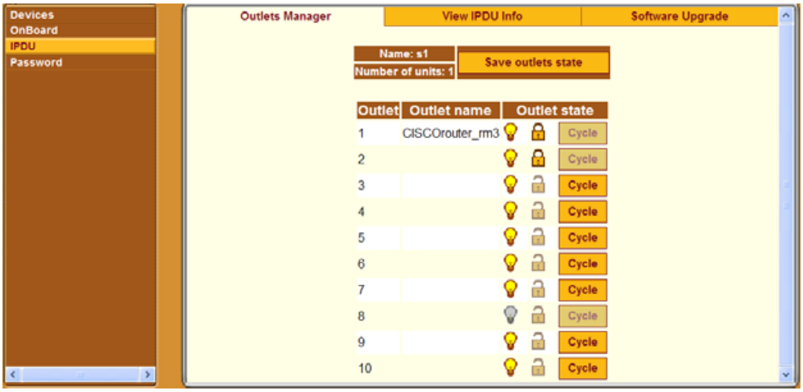
If a regular user clicks the "Outlets Manager" tab under Access –> IPDU, the message shown in the following figure appears if the user is not authorized to manage power on any outlets, or if the OnBoard cannot detect an AlterPath PM connected to the AUX port. Contact the OnBoard administrator for help if you see this message.



IPDU access failed. Check IPDU connection and user authorization.

Figure 2-17: IPDU Access Failed Message from “Outlets Manager”

If a regular user clicks the “Outlets Manager” tab under Access –> IPDU, the screen displays a list of all the outlets the user is authorized to manage. If an administrative user clicks on Outlets Manager under Access –> IPDU, all the power outlets on all connected IPDUs are listed, as shown in the following figure.



Name: s1
Number of units: 1

Outlet	Outlet name	Outlet state		
1	CISCOrouter_rm3	●	🔒	Cycle
2		●	🔒	Cycle
3		●	🔓	Cycle
4		●	🔓	Cycle
5		●	🔓	Cycle
6		●	🔓	Cycle
7		●	🔓	Cycle
8		○	🔓	Cycle
9		●	🔓	Cycle
10		●	🔓	Cycle

[

Figure 2-18: Access –> IPDU –> Outlets Manager Screen

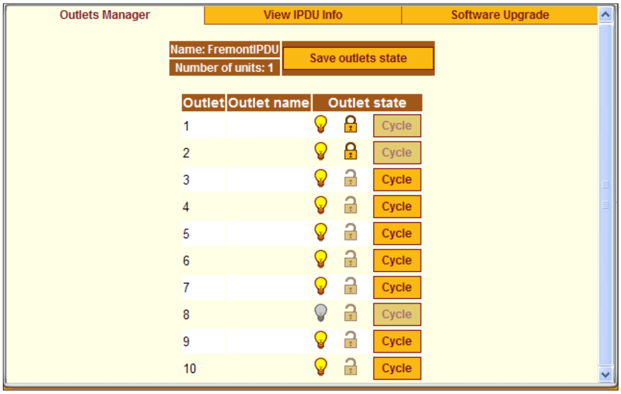
Both regular users who are authorized for IPDU power management and administrative users can do the following for any of the listed outlets:

- Cycle (turn power briefly off and then on again to reboot the server).
- Lock outlets in the on or off state to prevent accidental changes
- Unlock the outlets
- Turn power off

- Turn power on
- Save any changes made to the outlets state

The Name that appears on the screen is either the default “s1,” which is the port number of the AUX port; or an administrator-specified name. A yellow bulb indicates that the outlet’s power is on. A gray bulb indicates that the outlet’s power is off. An open padlock indicates that the outlet is unlocked. A closed padlock indicates that the outlet is locked. An orange “Cycle” button is active next to each outlet that is on; the “Cycle” button is grayed when the outlet is off. The “Save outlets state” button allows the user to save any changes made on this screen.

In the example below, all outlets are switched on except outlet 8, outlets 1 and 2 are locked and outlets 3 through 8 are unlocked.



Name: FremontIPDU
Number of units: 1

Outlet	Outlet name	Outlet state		
1		●	🔒	Cycle
2		●	🔒	Cycle
3		●	🔓	Cycle
4		●	🔓	Cycle
5		●	🔓	Cycle
6		●	🔓	Cycle
7		●	🔓	Cycle
8		○	🔓	Cycle
9		●	🔓	Cycle
10		●	🔓	Cycle

Figure 2-19: Outlets Manager Outlets State Close-up

▼ *To Manage Power Outlets on a Connected IPDU*

1. Bring up the Web Manager and log in.

See “To Log Into the Web Manager” on page 43, if needed.

2. Click the “IPDU” option in the left menu.

The IPDU screen displays with the “Outlets Manager” screen active.

3. To switch an outlet on or off, click the adjacent light bulb.

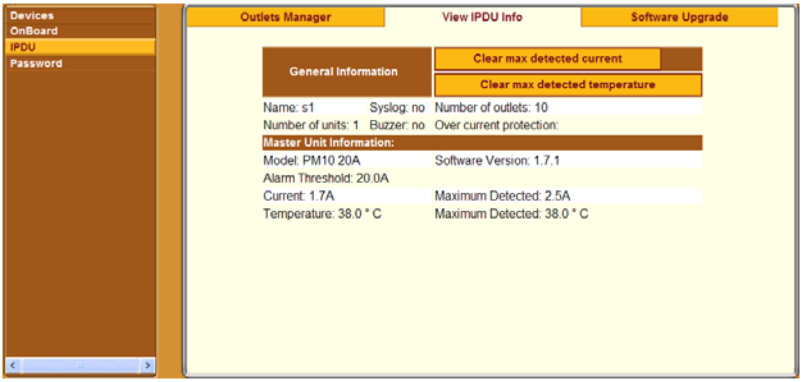
4. To lock or unlock an outlet, click the adjacent padlock.

5. To momentarily power an outlet off and then on again, click the adjacent "Cycle" button.

6. To save the state of the outlet(s), click "Save Outlets State."

Viewing IPDU Information

When a regular user or admin goes to Access –> IPDU –> View IPDU Info, a screen appears like the one shown in the following figure.



Name: s1 Syslog: no Number of outlets: 10

Number of units: 1 Buzzer: no Over current protection:

Model: PM10 20A Software Version: 1.7.1

Alarm Threshold: 20.0A

Current: 1.7A Maximum Detected: 2.5A

Temperature: 38.0 ° C Maximum Detected: 38.0 ° C

Figure 2-20: View IPDU Info Screen

The following table shows the information displayed on the "View IPDU Info" screen for each IPDU.

Table 2-4: Information on the View IPDU Info Screen

	Description	**Example**
Name	Administrator-configured name or the default (s1), which is assigned to the AUX port.	FremontIPDU
Number of units	The number of IPDUs connected to the port. The first IPDU is referred to as the master. Any other IPDUs daisy-chained off the first IPDU are referred to as slaves.	1
Number of outlets	Total number of outlets on all connected IPDUs.	10

Table 2-4: Information on the View IPDU Info Screen

	Description	Example
Buzzer	Whether a buzzer has been configured to sound when a specified alarm threshold is exceeded.	no
Syslog	Whether syslogging has been configured for messages from this IPDU.	no
Over current protection	Whether over current protection is enabled (to prevent outlets from being turned on if the current on the IPDU exceeds the specified threshold).	BUG? This is empty but it should show a value, either yes or no.

You can view the following information about each IPDU (under Unit Information)

	Description	Example
Model	AlterPath PM model number	PM10 20A
Software Version	PM firmware version	1.7.1
Alarm Threshold	Number of amperes that triggers an alarm or syslog message if it is reached	20.0A
Current	Current level on the IPDU	1.7A
Maximum Detected	Maximum current detected	2.5A
Temperature	Temperature on the AlterPath PM (only available on selected models that have temperature sensors)	37.0° C
Maximum Detected	Maximum temperature detected	37.0° C

The following three buttons are also displayed on the screen:

- “Clear max detected current”
- “Clear max detected temperature”

▼ To View IPDUs Information

1. Bring up the Web Manager and log in.

   See “To Log Into the Web Manager” on page 43, if needed.

2. Click the “IPDU” option in the left menu.

   The IPDU screen displays.

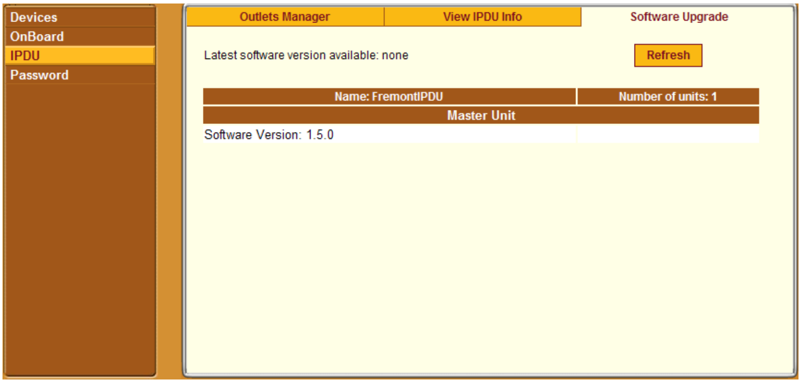
3. Click the “View IPDU Info” tab

4. If desired, clear the “Maximum Detected” value displayed for current by clicking the “Clear max detected current” button.

5. If desired, clear the “Maximum Detected” value displayed for temperature by clicking the “Clear max detected temperature” button.

Using the “Software Upgrade” Screen to View the IPDU’s Current Software Version

The admin user can use this screen to upgrade software on a connected AlterPath PM IPDU. Regular users can use this screen only to view the software version.



Latest software version available: none

Name: FremontIPDU	Number of units: 1
Master Unit	
Software Version: 1.5.0	

Figure 2-21: IPDU “Software Upgrade” Screen on the Web Manager

Configuring Your Password

Clicking the “Password” option on the Web Manager left menu brings up the “Changing password for *username*” screen, as shown in the following screen example.

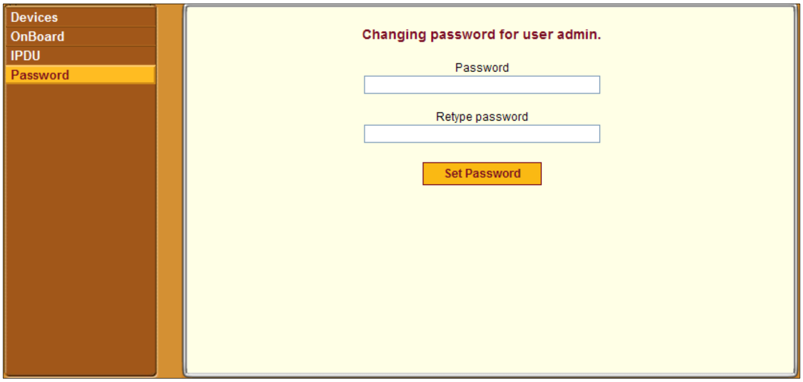


Figure 2-22:“Password” Screen

After the password is entered, clicking “Set Password” saves the changes in memory.

Note: Your password cannot exceed 30 characters. For security, follow commonly available guidelines to create passwords that are not easily guessed.

▼ *To Change Your Password*

1. Bring up the Web Manager and log in.

   See “To Log Into the Web Manager” on page 43, if needed.

2. Click the “Password” option in the left menu.

   The Password screen displays.

3. Enter the new password in the “Password” field.
4. Enter the password again in the “Retype password” field.
5. Click the “Set Password” button.

Chapter 3
Accessing the OnBoard and Connected Devices

This chapter provides information about how authorized users and administrators can access the OnBoard and connected devices in the following ways:

- Use the Web Manager or the `ssh` command to access the OnBoard’s console and use menu options to change passwords and perform device management actions
- Use the `ssh` command with OnBoard-specific device management options to perform device management actions on connected devices
- Access native IP management features on connected devices through the following types of tunnels:
  - VPN
  - SSH

This chapter describes the following topics.

This chapter provides the procedures listed in the following table.

Accessing the OnBoard’s Console

As described under “Accessing the OnBoard’s Console” on page 12, administrators and authorized users can access the OnBoard’s console through either of the following two ways:

- Through a directly-connected terminal or computer that is running a terminal emulation program
- By initiating an `ssh` connection from the user’s workstation

To use the `ssh` command from the user’s workstation, the user enters the username followed by a colon and an at sign (`:@`) followed by the DNS name or the IP address assigned to the OnBoard, either with or without the `rmenush` command, as shown in the following screen example.

```
% ssh username:@onboard_IP_or_DNS_name
% ssh -t username:@onboard_IP_or_DNS_name rmenush
```

Both of the commands shown in the previous screen example give the non-administrative user access to the same menu.

Regular users need to obtain the IP address from the OnBoard administrator.

When root or admin or another administrative user logs in through the console entering the first command line above without the `rmenush` command, the prompt for the unrestricted shell appears. With the `rmenush` command, the administrative user sees the `rmenush` menu.The following screen example shows the shell prompt for the root user.

```
[root@OnBoard root]#
```

The following screen example shows the menu.

```
-Access Devices
 Change Password
 Logout
```

See “Accessing the OnBoard Using SSH” on page 21 for an overview of the format of the `ssh` command and other command options, if desired.

See “User Shell (rmenush)” on page 13 for details about the menu options. See the following procedure for how to access the OnBoard’s console.

To Access the OnBoard’s Console

This procedure requires the following prerequisites in order for anyone to be able to access the command line using SSH.

- The user must know the IP address of the OnBoard
- The user must know a username and password for a user account configured on the OnBoard.

1. To use a terminal or terminal emulation program installed on a computer that is physically connected to the console port of the OnBoard, start the terminal session with the following factory-default console port settings.

Serial Speed: **9600** bps	Parity: **None**	Flow Control: **None**	Data Length: **8** bits	Stop Bits: **1**	ANSI emulation

2. To use an SSH application or the `ssh` command from a remote location, enter the username followed by a colon and an at sign (`:@`) followed by either the DNS name or the IP address assigned to the OnBoard, as shown in the following screen example.

```
% ssh username:@onboard_IP_or_DNS_name
```

   The screen example shows entering the `ssh` command on the command line, using francisco as the username and 192.168.44.111 as the IP address.

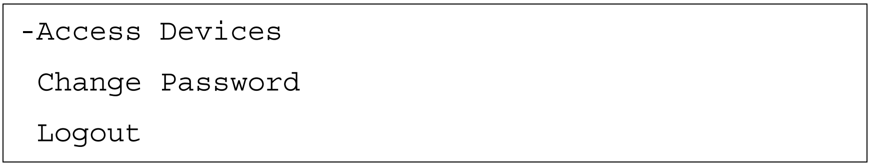
```
% ssh francisco@:192.168.44.111
```

3. Log into the OnBoard when prompted.

   After authentication and login, for administrative users (root, admin, or additional users who are members of the admin group) a shell prompt appears. For authorized non-administrative users, the user shell menu appears.

Accessing Device Management Features From the OnBoard’s Console Menu

After logging in as described in “Accessing the OnBoard’s Console” on page 75, non-administrative users see a menu similar to the menu shown in the following screen example.



```
-Access Devices

 Change Password

 Logout
```

Figure 3-1: User Shell Menu

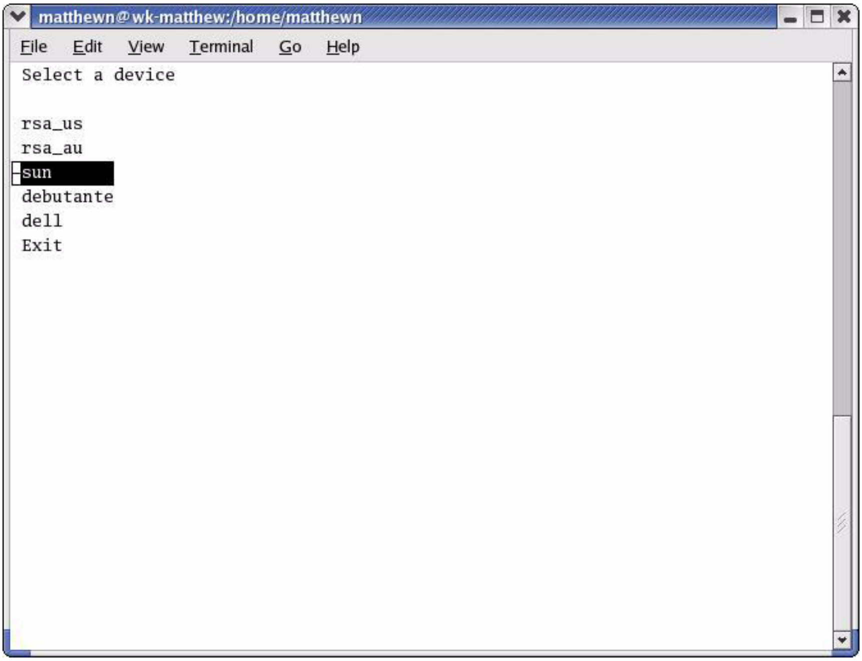
The OnBoard administrator may configure the menu with other options. For an example, see “Obtaining and Using One Time Passwords for Dial-ins” on page 97, where an option for accessing the one time password menu has been added.

Administrative users can see the same menu by entering `/usr/bin/rmenush` on the shell’s command line.

A user move from one item to another on the menu and submenus by using the keyboard’s arrow keys. A line (-) appears next to the selected item.

After an option is selected, pressing the “Enter” or “Return” key brings up a submenu or runs the selected command.

If the “Access Devices” option is selected, a menu appears with a list of devices that the user is authorized to access, as shown in the following screen example.


matthewn@wk-matthew:/home/matthewn
File Edit View Terminal Go Help

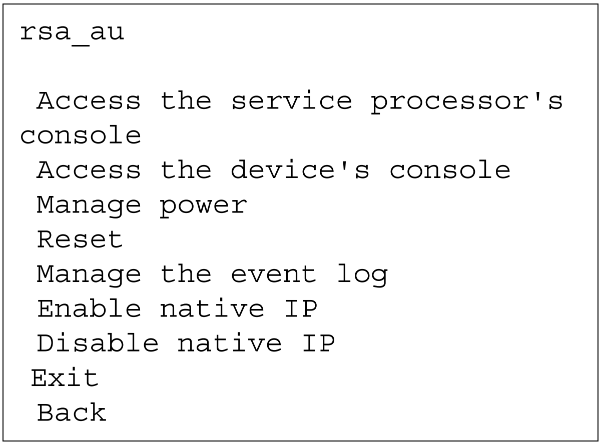
```
Select a device

rsa_us
rsa_au
sun
debutante
dell
Exit
```

Figure 3-2: Device Access Menu

Administrative users can see a similar menu listing all configured devices by entering `/usr/bin/onbdshell` on the shell’s command line.

After a device is selected, pressing the “Enter” or “Return” key brings up the list of actions the user is authorized to perform on the device. Not all listed actions are supported for all service processors.

Figure 3-3 shows the service processor “action” menu for an rsa-type service processor.



```
rsa_au

 Access the service processor's
console
 Access the device's console
 Manage power
 Reset
 Manage the event log
 Enable native IP
 Disable native IP
Exit
 Back
```

Figure 3-3: Service Processor Action Menu

Accessing the Console of a Device Through the OnBoard’s Console or By Using SSH

Any type of authorized user can access the console of a connected service processor, server, or device using one of the two following means:

- Invoking the `ssh` command along with one of the two following OnBoard-specific device management commands:
  - `spconsole`
  - `devconsole`

  See “Device Management Commands for Use With SSH” on page 21 for the format of the `ssh` command line when a device management command is used, if desired.
- Connecting to the OnBoard’s console and selecting one of the following menu options
  - Access the service processor's console
  - Access the device's console

▼ *To Use a SSH Command to Connect Directly to a Device’s or Service Processor’s Console*

This procedure assumes the following are true:

- You have access to the `ssh` command on the command line of your computer
- You know the user name and password of an OnBoard user account that is authorized to access the console of a device or service processor.
- You know the alias of the device that allows console access.
- You know the IP address or DNS name of the OnBoard.

Enter `ssh` with the `-t` option followed by the *`username`*, followed by a colon (`:`), followed by the *`alias`*, followed by the “at” sign (@), followed by the IP address of the OnBoard, followed by the `devconsole` or `spconsole` command.

```
% ssh -t username:device_alias@onboard_IP_or_DNS_name \
[devconsole | spconsole]
```

1. To connect directly to the device’s console, use the `ssh` command with the `devconsole` command.

   The following screen example shows entering `ssh` with the username francisco, the device alias rsa_au, the OnBoard IP address 192.168.44.111 and the `devconsole` command.

```
% ssh -t francisco:rsa_au@192.168.44.111 devconsole
```

2. To connect directly to a service processor’s console, use the `ssh` command with the `spconsole` command.

   The following screen example shows entering `ssh` with the username francisco and the IP address 192.168.44.111 with the `spconsole` command on the command line.

```
% ssh -t francisco:rsa_au@192.168.44.111 spconsole
```

3. When the login prompt appears, log into the console using the username and password configured for the device or service processor.

```
Login: root
Password:
```

▼ To Use OnBoard’s Console Menus to Access the Device Management Options

1. Log into the OnBoard’s console using one of the means described in “To Access the OnBoard’s Console” on page 76.

   If you have connected to the OnBoard’s console as an non-administrative user, the user shell menu displays.

2. If you are a non-administrative user, use the arrow keys on your keyboard to navigate to “Access Devices” option on the menu and press Return.
3. If you have connected to the OnBoard’s console as an administrative or root user, type `onbdshell` on the command line.
4. Select the name of the device you want to access.
5. Press the Enter key.

   A list of actions displays.

6. Select the desired action from the menu that displays:
7. If you have selected either “Access the service processor's console” of “Access the device's console, when the console login prompt appears, log into the console using the username and password configured for the device or service processor.

```
Login: root
Password:
```

▼ *To Exit from a Console Session*

Perform one of the two following steps to exit from the console of the service processor, server, or device before closing the terminal window.

1. On the command line of the terminal, type the `exit` command

```
[root@rdqailo root]# exit
```

2. Enter the hot key combination:

   Ctrl+e+c+.

   The terminal window closes.

Creating an SSH Tunnel

An authorized user can access a native web application after creating an SSH tunnel using local port forwarding. An arbitrarily chosen TCP port number on the user's host is forwarded to the IP address of a device managed by the OnBoard.

Prerequisites are as follows:

- The user's computer is running an appropriate SSH client.
- The authentication type configured for the device is the same as the authentication method configured for the OnBoard.
- The user is authorized for native IP access to the device.

After the user created the SSH tunnel, the user is authenticated, and then the user can launch a browser that runs the native web application on the device.

The following list shows some SSH clients that can be used to create a SSH tunnel. The feature works with SSH protocol v1 and v1. For additional clients, see http://www.openssh.com

- PuTTY on Windows
- OpenSSH on Linux

Common port numbers are:

- HTTP 80
- HTTPS 443

Our examples use port 443 for HTTPS.

▼ To Use OpenSSH on Linux to Create an SSH Tunnel

Perform this procedure on a computer running Linux with OpenSSH installed to create an SSH tunnel to a device managed by the OnBoard. The command lines shown in this procedure forwards local TCP port 8080 on the SSH client to port 443 on the device whose IP address is 10.10.1.181. The final argument can be either the OnBoard's DNS name or its IP address. The OnBoard name used in the example is `onboard.yahoo.com`.

1. To use SSH v2, enter the following command line.

```
$ ssh -l username -f -N -L 8080:10.10.1.181:443 \
onboard_ip_or dns_name
```

2. To use SSH v1, enter the following command line.

```
$ ssh -1 -l username -L 8080:10.10.1.181:443 \
onboard_ip_or dns_name
```

3. Enter your username and password when prompted.

▼ To Use PuTTY on a Windows PC to Create an SSH Tunnel

Perform this procedure on a computer with the PuTTY SSH client installed to create an SSH tunnel to a device managed by the OnBoard. The example forwards local TCP port 8080 on the SSH client to port 443 on the device whose IP address is 10.10.1.181. The final argument can be either the OnBoard's DNS name or its IP address. The OnBoard name used in the example is `onboard.yahoo.com`.

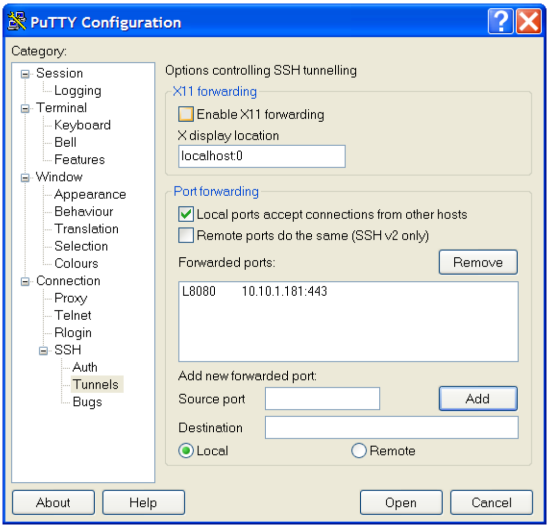
1. Open PuTTY.
2. In the "Category" pane, select "Tunnels" under "Connection > SSH.
3. In the main pane, in the "Port Forwarding" section do the following steps.
   a. Type the number of the TCP port to forward in the "Source port" field.

      This example uses 8080. You can select a random number over 1000.

b. Type the IP of the device followed by a colon followed by the port number of the service you want to access through the SSH tunnel.

c. Click “Add.”

The PuTTY window should look like the example below.



Options controlling SSH tunnelling

X11 forwarding

☐ Enable X11 forwarding

X display location: localhost:0

Port forwarding

☑ Local ports accept connections from other hosts

☐ Remote ports do the same (SSH v2 only)

Forwarded ports:

```
L8080     10.10.1.181:443
```

Add new forwarded port:

Source port

Destination

● Local ○ Remote

4. In the “Category” pane, select “Session.”

5. Enter the IP address or DNS name of the OnBoard in the “Host Name (or IP address)” field.

   This example uses “`onboard.yahoo.com`.”

6. Select SSH as the protocol.

7. Click Open.

8. Enter your username and password when prompted.

To Bring Up a Native Web Application When an SSH Tunnel Exists

Do this procedure to bring up a native web application from a connected device after creating an SSH tunnel from your host to the OnBoard, as shown in the two examples:

- “To Use OpenSSH on Linux to Create an SSH Tunnel” on page 83
- “To Use PuTTY on a Windows PC to Create an SSH Tunnel” on page 83

See “To Access a Native Web Application When a VPN Tunnel Exists” on page 94 when a VPN tunnel exists.

In this procedure, use the local port number you specified for forwarding. In the examples, we used 8080.

1. Bring up a browser.
2. In the location bar enter `http://localhost:`*portnumber*.

   portnumber is the TCP port number you specified for forwarding when you created the tunnel.

```
http://localhost:8080
```

3. The native web application appears in the browser.

Creating a VPN Tunnel

The authorized user creates a VPN tunnel using either IPSec or PPTP. A user authorized for Native IP can access native IP functionality through the Web Manager or through using `ssh` device management commands after creating a tunnel using either IPSec or PPTP.

The following figure shows an illustration of a single user’s workstation running IPSec on the right end and the OnBoard on the left end, with a router and the Internet between the OnBoard and the user’s workstation.

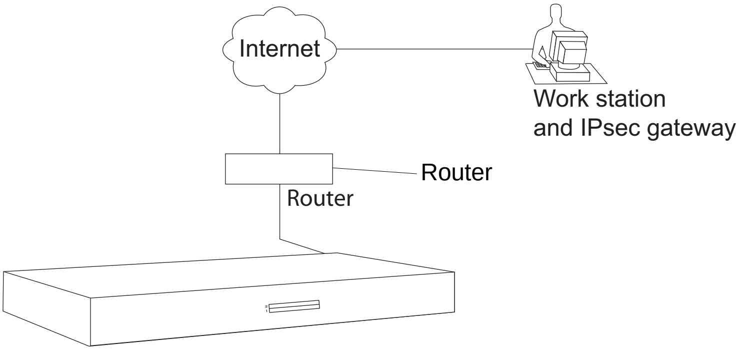


Figure 3-4: OnBoard VPN Example Using IPSec

Typically, the user configures a named VPN connection profile (or shortcut) on the user’s workstation, using either IPSec or PPTP. The name on the user’s end for a preconfigured VPN connection profile might be the name of the OnBoard. The name on the OnBoard end for a VPN connection profile might simply be the name and location of the user.

Note: Some systems, including the OnBoard, refer to configuring a VPN *connection*, but until the connection is actually made, what is informally called a VPN connection is actually a named *connection profile* or *connection shortcut*, which stores the information the computer needs in order to establish the connection.

The following prerequisites must be complete:

- The user on the remote workstation and the OnBoard administrator have configured VPN connection profiles from both sides to support the VPN connection. See “Creating a VPN Tunnel” on page 86 for more details.

- The user has created a VPN tunnel between the user's computer and the OnBoard.
- The user has logged into the OnBoard, either through the Web Manager or through the command line, and has been authenticated.

When all the above are true, an authorized user can enable native IP access in one of the following two ways:

- If the authorized user is connected to the OnBoard's console, the user can select the "Enable native IP" option that appears in the `onbdshell` menu for the selected service processor.
- If the authorized user is logged into the Web Manager, the user can choose "Enable Native IP" for the desired device on the Devices screen.

The VPN connection must remain active for the duration of the native IP session.

Caution! To prevent unauthorized users from accessing the native IP features of the device, when you are finished, always disable any native IP sessions and then close the PPTP VPN connection.

The following table lists the tasks associated with gaining native IP access to a device using VPN and provides links to where the tasks are documented.

Table 3-1: Tasks for Enabling and Using Native IP Access Using VPN

Task	Where Documented
Set up a VPN connection and route to the OnBoard	"Routing Requirements for VPN Connections" on page 88 "Summary of VPN-related Requirements for Native IP Access" on page 90 "VPN Through IPSec Connections" on page 91 "PPTP VPN Connections" on page 93
Create a VPN tunnel	"To Create an IPSec VPN Tunnel" on page 92 "To Create a PPTP VPN Tunnel" on page 93

Table 3-1: Tasks for Enabling and Using Native IP Access Using VPN

Task	Where Documented
Enable Native IP access	"To Enable Native IP Access Through an IPSec VPN Tunnel" on page 92
	"To Enable Native IP Access Through a PPTP VPN Tunnel" on page 94
Access a native web application	"To Access a Native Web Application When a VPN Tunnel Exists" on page 94
Access a native management application	"To Access a Native Management Application" on page 95

Routing Requirements for VPN Connections

These routing requirements assume the user's workstation and the OnBoard can exchange packets.

IPSec VPN Routing Requirements

If a route is necessary for the OnBoard and the user's workstation to exchange packets, a route can be specified by setting one or both of the Right and Left nexthop parameters to the IP address of a host route and selecting "Add and route" as the boot action. This should be configured by the OnBoard administrator, and the configuration should be shared with the user. Once packets can be exchanged between the OnBoard and the user's workstation, IPSec automatically creates the routes needed to get packets flowing through an IPSec VPN tunnel, so neither the user nor the administrator need to create routes to support IPSec VPN tunnels to devices.

PPTP VPN Routing Requirements

If a network or host route is needed to enable communications between the user's workstation and the OnBoard, the user must manually add the route on the user's workstation before creating the PPTP VPN tunnel.

In addition, the user must manually create a static route after the PPTP connection is established to inform the workstation that the device to be contacted is at the other end of the point-to-point link. The route must include the PPTP address assigned to the OnBoard, which the user can discover by running the `ifconfig` or `ipconfig` command.

The following screen example shows the PPTP interface IP address output from the `ipconfig` command on an Windows NT operating system when PPTP has assigned an IP address of `192.168.2.1`.

```
C:\> ipconfig
...
PPP adapter OnBoardPPTPVPN
...
       IP Address.. . . . . . . . . : 192.168.2.1
...
```

If the user needs to communicate with devices on two separate private subnets, the user must create a route to each private subnet or to each device.

For example, to communicate with all devices on a private subnet whose IP address is `192.168.4.0`, when the network mask is `255.255.255.0`, and the PPTP-assigned OnBoard IP address is `192.168.2.1`, the following route would be needed:

```
route add -net 192.168.4.0 mask 255.255.255.0 via 192.168.2.1
```

If additional devices must be accessed on additional private subnets, additional routes must be created to each of the subnets.

To communicate with three devices on a virtual network whose IP address is `172.20.0.0`, whose network mask is 255.255.0.0 via the OnBoard, and PPTP has assigned the OnBoard the IP address `192.168.2.1`, the user would need to configure a route like the one shown in the following screen example:

```
route add -net 172.20.0.0 mask 255.255.0.0 via 192.168.2.1
```

If a virtual network is configured, the user needs to only add a single network route to the virtual network. Check with the OnBoard administrator for which routes you need to configure to connect to the devices for which you are authorized.

Creating a default route on the user’s workstation to the OnBoard would work, but it would result in loss of DNS and other local services (such as Internet and mail service) for the user’s workstation.

Summary of VPN-related Requirements for Native IP Access

The following list summarizes the requirements for configuring a VPN connection:

- Obtain from the OnBoard administrator the values used in creating the VPN connection profile on the OnBoard end and use these values to configure the connection profile on the user's end. Obtain the PPTP password if PPTP is being used. If IPSec is being used, the user may obtain the relevant portion of the OnBoard's `ipsec.conf` file and insert it into the `ipsec.conf` file on the user's workstation.
- Before attempting to access the "Native IP" feature on the OnBoard, the user must start the VPN connection from the user's computer.

The OnBoard listens for the connection attempt from the IP addresses specified in its connection profiles and grants the access.

Note: The VPN connection must remain active for the duration of the native IP session.

The following table lists the tasks associated with gaining native IP access to a device using VPN and provides links to where the tasks are documented.

Table 3-2: Tasks for Enabling and Using Native IP Access Using VPN

Task	**Where Documented**
Set up a VPN connection and route to the OnBoard	"Routing Requirements for VPN Connections" on page 88 "Summary of VPN-related Requirements for Native IP Access" on page 90 "VPN Through IPSec Connections" on page 91 "PPTP VPN Connections" on page 93
Create a VPN tunnel	"To Create an IPSec VPN Tunnel" on page 92 "To Create a PPTP VPN Tunnel" on page 93

Table 3-2: Tasks for Enabling and Using Native IP Access Using VPN (Continued)

Task	Where Documented
Enable Native IP access	“To Enable Native IP Access Through an IPSec VPN Tunnel” on page 92 “To Enable Native IP Access Through a PPTP VPN Tunnel” on page 94
Access a native web application	“To Access a Native Web Application When a VPN Tunnel Exists” on page 94
Access a native management application	“To Access a Native Management Application” on page 95

VPN Through IPSec Connections

For an IPSec VPN connection, the following authentication information is required:

- Username and password
- Connection keys or certificates

The ESP and AH authentication protocols (also called “encapsulation methods”) are supported. RSA Public Keys and Shared Secret are also supported.

If the RSA public key authentication method is chosen, the generated keys are different on each end. When shared secret is used, the secret is shared on both ends.

Note: How to choose an encapsulation method or authentication method and generate the required keys is outside the scope of this document.

The OnBoard administrator needs to give the user a copy of the configuration parameters used to configure the IPsec connection profiles on the OnBoard, usually by providing a copy of the relevant portions of the `ipsec.conf` file, which the user can insert the `ipsec.conf` file on the user’s workstation.

▼ *To Create an IPSec VPN Tunnel*

The authorized user must do the following to enable the IPSec client running on the user's workstation to bring up the VPN tunnel to enable access native IP features on a device or devices.

1. Make sure your workstation can exchange packets with the OnBoard.

   a. Test whether your workstation can access the OnBoard by entering the OnBoard's public IP address in a browser to try to bring up the Web Manager.

   b. If a network or host route is needed to enable communications with the OnBoard, configure the route.

2. Create an IPSec VPN connection profile on your workstation, using the values supplied by the OnBoard administrator.

   If the OnBoard administrator sends the relevant portions of the `ipsec.conf` file from the OnBoard's IPSec configuration, use it to replace the same section in your workstation's `ipsec.conf` file.

3. Bring up the IPSec VPN tunnel.

   Depending on the platform and IPSec client being used, you may use a GUI to create the IPSec VPN connection or execute the `ipsec auto -up` commend.

4. Enable native IP access as described in To Enable Native IP Access Through an IPSec VPN Tunnel."

▼ *To Enable Native IP Access Through an IPSec VPN Tunnel*

Note: The OnBoard administrator must provide the appropriate IP address to use in this procedure, which is not the same as the public IP address assigned to the OnBoard's public interface. (The IP address is either the OnBoard side IP address configured for the private subnet where the device resides or a virtual IP address configured for the OnBoard.)

1. Create a VPN tunnel.

   See "To Create an IPSec VPN Tunnel" on page 92 or "To Create a PPTP VPN Tunnel" on page 93 if needed.

2. To enable native IP access through a browser, do the following steps.
   - **a.** Enter the private IP address or virtual IP address assigned to the OnBoard in a browser.
   - **b.** Log into the OnBoard.
   - **c.** Make sure “Devices” is selected in the Web Manager’s left menu.
   - **d.** Find the entry for the desired device and click “Enable Native IP access.”
3. To enable native IP access using the `ssh` command, perform the following steps.
   - **a.** Enter the `ssh command with the following syntax:` `ssh -t username:@`*`OnBoard_privateIP`*

     The following command line example shows user “AllSPs” with an OnBoard virtual IP address of `172.20.0.1`.

```
ssh -t AllSPs:@172.20.0.1
```

   - **b.** Select “Access Devices” from the menu.
   - **c.** Select the device from the devices menu.
   - **d.** Select “Enable native IP” from the list of management actions.

PPTP VPN Connections

An authorized user can create PPTP VPN connections on Linux, Windows, or Macintosh operating systems.

▼ To Create a PPTP VPN Tunnel

1. Configure a PPTP VPN connection profile with the following information obtained from the OnBoard administrator:
   - The IP address assigned to the OnBoard’s public interface.
   - The PPTP username and password assigned to the user.
2. Create the PPTP VPN connection.

▼ To Enable Native IP Access Through a PPTP VPN Tunnel

1. Create an PPTP VPN tunnel.

   See “To Create a PPTP VPN Tunnel” on page 93.

2. Enter the `ifconfig` or `ipconfig` command on the user’s workstation to discover the PPTP address assigned from the OnBoard’s IP address pool in the PPTP connection.

3. Set up one of the following types of static routes to enable VPN connections:

   - A network route to the private subnet where the device resides via the PPTP-assigned address for the OnBoard.
   - If a virtual network is configured, a network route to the virtual network where the device resides via the PPTP-assigned address for the OnBoard
   - A host route to each device, using the real or virtual IP address assigned to the device.

4. Enter the PPTP address either in a browser or with `ssh` on the command line to access the OnBoard.

5. Access the device and enable native IP access.

   See “To Access a Native Web Application When a VPN Tunnel Exists” on page 94 or

▼ To Access a Native Web Application When a VPN Tunnel Exists

This procedure only works when a VPN tunnel exists. See “To Bring Up a Native Web Application When an SSH Tunnel Exists” on page 85 when an SSH tunnel exists.

Perform one of the following steps, according to which access method you wish to use.

1. To use the Web Manager to launch a native web application, perform the following steps.

  a. Enter the private or virtual IP address assigned to the OnBoard in a browser.

  b. Log into the OnBoard.

  c. Select the Access menu option.

  d. Click the “Go to native web interface” link on the Access Devices screen.

2. To use a browser to launch the native web application from your workstation, enter the IP address of the device in the browser’s location field.

3. To use the ssh command your workstation’s command line, enter the `ssh` command in the following format entering the name/alias of the device along with the IP address of the OnBoard.

   For example, the following `ssh` command line gives the user named “allSPs” access to a device called “sp2” using the OnBoard’s virtual IP address `172.20.0.1`.

   ```
   ssh -t allSPs:sp2@172.20.0.1
   ```

▼ *To Access a Native Management Application*

This procedure only works when a VPN tunnel exists. An SSH tunnel does not provide access to a native management applications.

A management application may be accessed in various ways, depending whether the application is a client on the user’s workstation or resides on the service processor:

1. If the management application resides on the user's workstation, bring up the application from there.

2. If the management application resides on the service processor and is an executable that can be invoked on the command line, do one of the following to access the service processor’s console.

   a. Invoke `ssh` with the `spconsole` command on the command line of your workstation in the following format

   ```
   ssh -t allSPs:sp2@172.20.0.1 spconsole
   ```

   b. To use the Web Manager, do the following steps.

i. Log into the Web Manager on the OnBoard.

ii. Find the entry for the device to access on the Access Devices screen.

iii. Select the “Service Processor Console” link.

iv. Log into the service processor if prompted.

v. Bring up the management application up from the service processor’s command line.

Caution! When finished, always disable the native IP access before terminating the IPSec VPN connection.

Obtaining and Using One Time Passwords for Dial-ins

This section is for users who are authorized to dial into the OnBoard through a external modem or a PCMCIA modem or phone card if the *one time password* (OTP) authentication method is configured for logins to that device. If you are not sure, ask your OnBoard administrator. With OTP authentication, you supply a different password whenever you dial-in, so no one who discovers the password used for one session can use that password later to access your account. A one time password is actually a group of six English words (for example: `GOLD ARK FISH DOVE SON ZION`) that are entered all on the same line at the prompt. You might be given a series of one time passwords; following is an example sequence:

```
495: AMEN FONT STAR SEA WINE RED
496: ART LILY HOLY AID LOVE ALL
497: GOLD ARK FISH DOVE SON ZION
498: SEE PITY JOY HOPE PLAN CITY
```

At the first login, you would enter the password from line 498, on the next login, you would enter line 497, and so forth.

Each user who needs to use OTP needs a local user account on the OnBoard, must be registered with the OTP system, and must be able to obtain the OTP username, OTP secret pass phrase, and OTP passwords needed for logins. See the following list for how the OnBoard administrator may register and give OTP passwords to users:

- Register all users and give OTP usernames and OTP secret pass phrases to each user.

  AND

- Generate the needed OTP passwords on behalf of the each user and give them to each user.

  Some sites choose to print out hard copy lists of OPIE passwords for their users and deliver them by methods such as FAX or FedEx.

  OR

- Make sure users are equipped with an OTP generator that is not on the network to generate their own OTP passwords when challenged at login time.

The OTP generator may be a copy of the `opiekeys` program installed on the user's workstation or may be an OTP token card.

▼ *To Generate an OTP Password When Challenged at Dial-in*

This example procedure works when /etc/`opiekeys` is installed on the user's workstation.

1. Dial into the OnBoard through an external modem or a PCMCIA modem or phone card that has been configured to use OTP authentication.

The OnBoard challenges with a *sequence number* (also called a counter) and a *seed* (or key) associated with the username and asks for a response.The seed includes the first two letters of the hostname and a pseudo random number.

```
login: username
otp-md5 499 on93564
Response:
```

The challenge is `otp-md5 499 on93564`. The sequence number is 499 and the seed is `on93564`.

2. Obtain an OTP password by performing the following steps.

a. Copy the entire challenge into a window on a computer where the `opiekey` program is installed.

The `otp-md5` portion of the challenge is a symbolic link to the `opiekey` program and tells `opiekey` to use the MD5 algorithm. `opiepasswd` and prompts the user for the user's secret pass phrase.

b. Enter your secret pass phrase when prompted.

The `opiekey` program generates a six word OTP password, such as `GOLD ARK FISH DOVE SON ZION`.

3. Copy the OTP password to the window where the login program is waiting with the "Response" prompt.

```
Response: GOLD ARK FISH DOVE SON ZION
```

The sequence number is decremented in the `opiekeys` file.

A
MindTerm Applet Reference

When a user connects to any console using the Web Manager, a window running a MindTerm applet appears with an encrypted SSH connection between the user's computer and the console. MindTerm is an SSH client that includes an integrated xterm/vt100 terminal emulator and that runs as a Java applet within a browser window.

This appendix describes the topics listed in the following table.

Java Plug-In Requirements for Using MindTerm

To use MindTerm, the user’s browser must have a Java plug-in enabled, as described in “Requirements for Java Plug-In Availability” on page 38.

Customizing MindTerm

MindTerm saves session settings in a `mindterm` folder, which it creates in the user’s home folder on the user’s computer. For example, in a Windows system, the `mindterm` folder is created in `C:\Documents and Settings\`*username*`\mindterm`.

Actions you can perform with the terminal window are listed below:

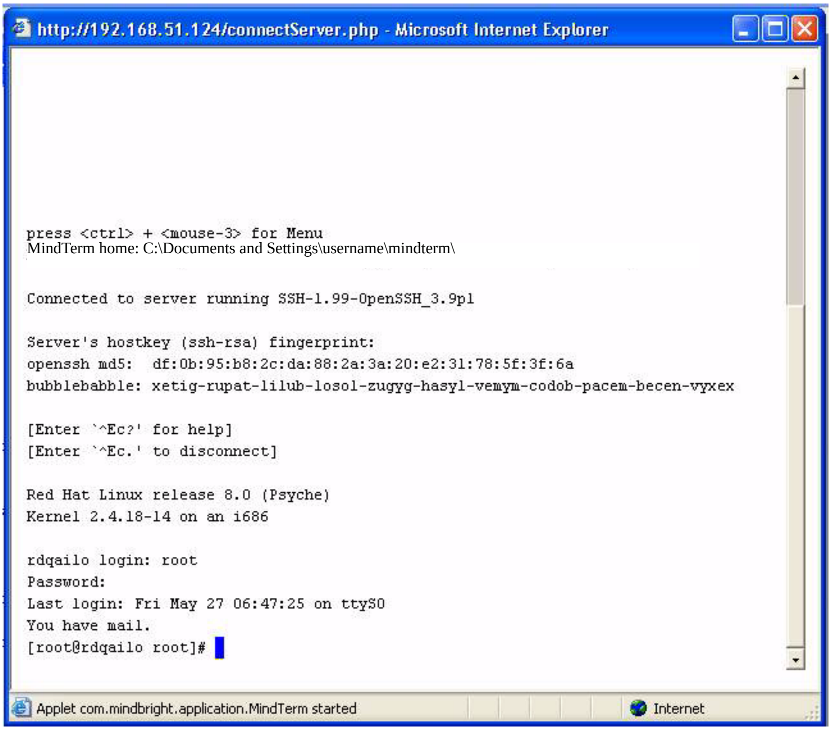
- Resize it.
- Edit text with options that include: “copy,” “paste,” “select all,” “find,” and “clear screen.”
- Change the background and foreground colors.
- Save the contents of the terminal window and buffer to a file.

Note: You can make use of this option if you want to print the window’s contents, by saving the file and then printing it from another application.

- Reuse saved settings like the scroll buffer size.

Example MindTerm Window

The following figure shows an example window that appears when the root user is connected to the console of a service processor whose alias is “rdqailo.” The same terminal window appears whether the connection is being made to the console of an OnBoard, a service processor, a server, or another type of device.

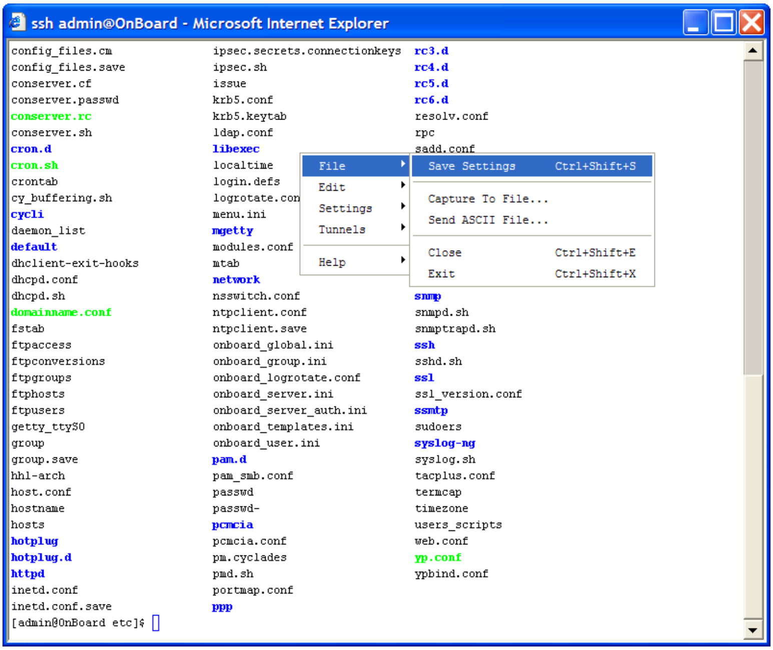

http://192.168.51.124/connectServer.php - Microsoft Internet Explorer
Applet com.mindbright.application.MindTerm started
Internet

```
press <ctrl> + <mouse-3> for Menu
MindTerm home: C:\Documents and Settings\username\mindterm\

Connected to server running SSH-1.99-OpenSSH_3.9p1

Server's hostkey (ssh-rsa) fingerprint:
openssh md5:  df:0b:95:b8:2c:da:88:2a:3a:20:e2:31:78:5f:3f:6a
bubblebabble: xetig-rupat-lilub-losol-zugyg-hasyl-vemym-codob-pacem-becen-vyxex

[Enter `^Ec?' for help]
[Enter `^Ec.' to disconnect]

Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.18-14 on an i686

rdqailo login: root
Password:
Last login: Fri May 27 06:47:25 on ttyS0
You have mail.
[root@rdqailo root]#
```

Figure A-1: Root Log into MindTerm Running an SSH Console Session

MindTerm Terminal Menu Options

As is shown in first line of the screen output shown in Figure A-1, you can bring up the terminal menu by pressing `Ctrl` and the third mouse button at the same time: “Ctrl+[mouse right click]”. The following figure shows the terminal menu that displays if you enter “Ctrl+[mouse right click]” and drag the cursor to pull down the File menu options.



```
config_files.cm               ipsec.secrets.connectionkeys  rc3.d
config_files.save             ipsec.sh                      rc4.d
conserver.cf                  issue                         rc5.d
conserver.passwd              krb5.conf                     rc6.d
conserver.rc                  krb5.keytab                   resolv.conf
conserver.sh                  ldap.conf                     rpc
cron.d                        libexec                       sadd.conf
cron.sh                       localtime
crontab                       login.defs
cy_buffering.sh               logrotate.con
cycli                         menu.ini
daemon_list                   mgetty
default                       modules.conf
dhclient-exit-hooks           mtab
dhcpd.conf                    network
dhcpd.sh                      nsswitch.conf                 snmp
domainname.conf               ntpclient.conf                snmpd.sh
fstab                         ntpclient.save                snmptrapd.sh
ftpaccess                     onboard_global.ini            ssh
ftpconversions                onboard_group.ini             sshd.sh
ftpgroups                     onboard_logrotate.conf        ssl
ftphosts                      onboard_server.ini            ssl_version.conf
ftpusers                      onboard_server_auth.ini       ssmtp
getty_ttyS0                   onboard_templates.ini         sudoers
group                         onboard_user.ini              syslog-ng
group.save                    pam.d                         syslog.sh
hhl-arch                      pam_smb.conf                  tacplus.conf
host.conf                     passwd                        termcap
hostname                      passwd-                       timezone
hosts                         pcmcia                        users_scripts
hotplug                       pcmcia.conf                   web.conf
hotplug.d                     pm.cyclades                   yp.conf
httpd                         pmd.sh                        ypbind.conf
inetd.conf                    portmap.conf
inetd.conf.save               ppp
[admin@OnBoard etc]$
```

Figure A-2: Terminal Menu

The following table describes the terminal menu options.

Table A-1: Console Session Terminal Menu Options (Sheet 1 of 6)

1st-level Option	2nd-level Option	Description
File	Save Settings (Ctrl+Shift+s)	Saves current settings to a user-selected file.
	Capture to File (Ctrl+Shift+c)	Starts capturing terminal output to a file, or if this menu option is selected when output is currently being captured, stops capturing.
	Send ASCII File	Sends the contents of a selected file to the terminal as input, as if the contents were being typed on the keyboard.

Table A-1: Console Session Terminal Menu Options (Sheet 2 of 6)

1st-level Option	2nd-level Option	Description
	Close (Ctrl+Shift+c)	Closes the current window. **Note:** If you close a window without logging out, you abort the SSH connection abnormally. The recommended procedure is to log out in the shell before closing or exiting the MindTerm window.
	Exit (Ctrl+Shift+x)	Closes the window without logging out. **Note:** Closing windows without logging out aborts the SSH connection. Enter the `exit` command in the terminal before using this option.
Edit	Copy (Ctrl+Insert)	Copies selected text to the clipboard. Select text by clicking and holding down the left mouse button and then dragging the mouse over the area to select, releasing the mouse when the desired area is selected.
	Paste (Shift+Insert)	Pastes the clipboard’s contents to the screen as input, as if the contents were being typed on the keyboard.
	Copy & Paste	Copies selected text and pastes it.
	Select All (Ctrl+Shift+a)	Selects all contents in the scrollback buffer and in the terminal.
	Find (Ctrl+Shift+f)	Displays the Find dialog box, which can be used to search the scrollback buffer and the currently-displayed text for strings.
	Clear Screen	Clears the screen and positions the cursor at the top left corner.

Table A-1: Console Session Terminal Menu Options (Sheet 3 of 6)

1st-level Option	2nd-level Option	Description
Edit, Continued	Clear Scrollback	Clears the contents of the scrollback buffer.
	VT Reset	Resets terminal settings to the defaults.
Settings	Connection	Displays a dialog box for setting SSH preferences. General: • Server • Username • Authentication Proxy: • Proxy type • Server • Port • Authentication • Username • Password Security • Protocol • Host key type • Cipher • Mac • Compression Features • X11 forward • Local display • Send keep-alive • Interval

Table A-1: Console Session Terminal Menu Options (Sheet 4 of 6)

1st-level Option	2nd-level Option	Description
Settings, Continued	Terminal (Ctrl+Shift+t)	Displays a dialog box for setting terminal characteristics. General: • Terminal type • Columns • Rows • Encoding • Font • Size • Scrollback buffer • Scrollback buffer position Colors • Foreground color • Background color • Cursor color Misc • Paste button • Select delimiter (characters for click-selection) VT 1 • Enable Passthrough Print • Copy <cr><nl> line ends • Copy on select • Reverse Video • Auto Wraparound • Reverse Wraparound • Insert mode • Auto Linefeed • Scroll to Bottom On Key Press

Table A-1: Console Session Terminal Menu Options (Sheet 5 of 6)

1st-level Option	2nd-level Option	Description
Settings, Continued	Terminal (Ctrl+Shift+t), Continued	VT 2 • Scroll to Bottom On Tty Output • Visible Cursor • Local Echo • Visual Bell • Map <CTRL>+<SPC> to ^@ • Local PgUp/PgDown • Use ASCII for line draw • Backspace sends: del, bs, erase • Delete sends: del, bs, erase
	Auto Save Settings	Enables and disables the automatic saving of settings. When this option is enabled [default], settings are saved automatically whenever you disconnect from a server or exit the terminal. When this option is disabled, you must explicitly save settings to a file in order to preserve them.

Table A-1: Console Session Terminal Menu Options (Sheet 6 of 6)

1st-level Option	2nd-level Option	Description
Tunnels	Setup	Displays a dialog box listing any previously configured tunnels. Clicking the Add button displays a dialog box for configuring a tunnel. Type • Local • Remote Bind address • localhost • all (0.0.0.0) • ip Bind port Dest. address Dest. port Plugin • None • ftp
Help	About MindTerm	Displays a dialog box with information about the Mind Term build date, version, platform you are running...

Using Hot Keys During Console Sessions

Hot keys have two components: an escape sequence, and a command key. The escape sequence for all the console session hot keys is Cntrl+e+c (shown as "^Ec"). As shown in Figure A-1, the applet displays hot key combinations that you can use to get help (^Ec?) or disconnect (^Ec.). The following table shows all the available hot keys, which are entered after the escape sequence.

Table A-2: Hot Keys Available During Console Sessions

Key	Action	Key	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?**	Break sequence list
10	Send break per config file	**l1-9**	Send specific break sequence
o	(Re)open the tty and log file	**p**	Replay the last sixty (60) lines
r	Replay the last twenty (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	**Enter**	Ignore/Abort command
?	Print this message	**^R**	Replay the last line
\too	Send character by octal code		

For example, to send a broadcast message, you would enter "Cntrl+e+c b" and to tell the applet to abort, you would enter "Cntrl+e+c Enter" on a Windows keyboard. To exit the session, press "Ctrl+_".

Glossary

1U

One rack unit (also referred to as 1RU). A standard measurement equal to 1.75” (4.45 cm) of vertical space on a rack or cabinet that is used for mounting computer equipment.

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 the data. 3DES encryption is one of the *security features* provided by Cyclades products to enable customers to enforce their data center security policies. See also *authentication, authorization*, and *encryption*.

ActiveX

A set of technologies developed by Microsoft from its previous OLE (object linking and embedding) and COM (component object model) technologies. Browsers used for accessing KVM output from devices connected to Cyclades AlterPath KVM products must have ActiveX enabled.

advanced lights out manager (See *ALOM*)

AH (*authentication header)*

One of the two main protocols used by IPSec. (*ESP* is the other). AH authenticates data flowing over the connection. AH is not compatible with *NAT*, so it must be employed only when the source and destination networks can be reached without NAT. Does not define the authentication method that must be used.

alias

An easy-to-remember, usually-short, usually-descriptive name used instead of a full name or IP address. For example, on some Cyclades products, port names contain numbers by default (as in Port_1) but the administrator can assign an alias (such as *SunBladeFremont* that describes which server is connected to the ports. Aliases make it easier for users to understand which devices are connected.

ALOM (advanced lights out manager)

A service processor on certain Sun servers that includes an independent system controller and firmware. Provides remote monitoring, logging, alerting, and basic control of the server.

application-specific integrated circuit (See *ASIC*)

ASIC (Application-Specific Integrated Circuit)

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

authentication

The process by which a user’s identity is checked (usually by checking a user-supplied username and password) before the user is allowed to access requested resources. Authentication may be done locally (on the Cyclades device) or on a configured authentication server running one of the widely-used authentication protocols (LDAP, RADIUS, TACACS+, NIS, SMB, and Kerberos) that are supported by Cyclades products. Authentication is one of the *security features* provided on Cyclades products to enable customers to enforce their data center security policies. See also *authorization* and *encryption*.

authentication header (See *AH)*

authorization

Permission to access a controlled resource, which must be granted by administrative action. A user’s authorizations are checked after a user logs into a system and has been authenticated. Each user is restricted to using only the features the user is authorized to access. Checking a user’s authorizations is one of the *security features* provided on Cyclades products to enable customers to enforce their data center security policies. A user who is authorized to access a device or software function is referred to as an *authorized user.* See also *authentication* and *encryption*.

authorized user

One who is given permission to access a controlled resource, which must be granted by administrative action.

backup configuration

On Cyclades products, specifies where to save compressed configuration files for possible later restoration. Some Cyclades products save configuration changes in the affected configuration files while maintaining a backed-up compressed set of configuration files in a separate directory. The backup directory’s contents are available for restoration until the administrator takes a specific action to overwrite the backed-up files.

baseboard

A gender-neutral term for “motherboard.”

baseboard management controller (See *BMC*)

basic input/output system (See *BIOS*)

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 bps. 9600 is the most-common baud rate for devices.

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 in case of a corrupted operating system kernel. How to access the BIOS varies from one manufacturer to the other.

BMC (baseboard management controller)

An internal processor on some servers that is separate from the main system and that operates even if the main processor is not operable. Sits on the server’s baseboard (motherboard), on an internal circuit board, or on the chassis of a blade server. Monitors on-board instrumentation. Provides remote reset or power-cycle capabilities. Enables remote access to BIOS configuration or operating system console information. In some cases provides *KVM* control of the server. Includes a communication protocol that delivers the information and control to administrators.

bonding

See *Ethernet bonding*.

callback

A *security feature* used to authenticate users who are calling into a device. The software authenticates the user, hangs up, and then returns the call to the user before allowing access.

CAT5 (category 5)

A standard for twisted-pair Ethernet cables defined by the Electronic Industries Association and Telecommunications Industry Association (commonly known as EIA/TIA).The support for CAT5 and later cabling (such as CAT5e) in many Cyclades products allows the use of existing cabling in the data center.

CDMA (code division multiple access)

A mobile data service available to users of CDMA mobile phones.

CHAP (challenge handshake authentication protocol)

An authentication protocol used for PPP authentication. See MS-CHAP.

checksum

Software posted at the Cyclades download site is accompanied by a checksum (`*.md5`) file generated using the MD5 algorithm. The checksum of a downloaded file must be the same as the checksum in the file. The checksum is compared automatically when the download is performed through the Web Manager or can be compared manually if the download is performed using `ftp` or `http`. If the checksums do not match, the software file is damaged and should not be used.

CLI (command line interface)

Allows users to use text commands to tell computers to perform actions (in contrast to using a GUI). The user types a text command at an on-screen prompt and presses the Enter or Return key. The computer processes the command, displays output when appropriate, and displays another prompt. Users can save a series of frequently-used commands in a script. Being able to create and run scripts to automate repetitive tasks is one of the reasons many administrators prefer using a CLI.

Cyclades products run the Linux operating system, and most Cyclades products allow access to the command line of the Linux shell. Command line access is achieved through several different means. For one example, a remote administrator can use Telnet or SSH to access an AlterPath OnBoard and then can enter commands on the Linux shell's command line.

Some Cyclades products offer a management utility called the CLI. Administrators type “CLI” or “cli” at the prompt in the Linux shell. Products that provide similar utilities with different names, such as the AlterPath OnBoard `cycli`, provide an alias for users who are familiar with the CLI name. The Cyclades CLI tool provides many commands and nested parameters in a format called the *CLI parameter tree*.

CLI parameter tree

Each version of the Cyclades *CLI* utility has a set of commands and parameters nested in the form of a tree. The CLI for the AlterPath OnBoard and other products use the Cyclades Application Configuration Protocol (CACP) daemon (cacpd). The cacpd uses the `param.conf` file, which defines a different CLI parameter tree for each product.

client-side management software—See *management software*

command line interface (See *CLI*)

community name

A string used as a type of shared password by *SNMP* v1 and v2 to authenticate messages. Hosts that share the same community name usually are physically near each other. The administrator must supply a community name when configuring SNMP on the Cyclades device, and the same community name must be also configured on the SNMP server. For security reasons, the default community name *public* cannot be used.

console

A computer mode that gives access to a computer's command line (see *command line interface*). The console also displays error messages generated by the computer's operating system or *BIOS*. Console access is essential when a device (such as some special-purpose servers, routers, service processors, and other embedded devices) has no window system. Console access is also essential when the window system is not available on a device that has one, either because the system is damaged or it is offline. Access to the console allows remote administrators to control and repair damaged or otherwise-unavailable systems. See also *device console* and *service processor* console.

console servers

Appliances that give consolidated access to the console ports of connected assets, either over the network, through dial-in, or direct serial connection.

Cyclades

A corporation founded in 1989 to provide unique networking solutions. Named after the ground-breaking French packet-switching network created in 1970, which was named after the Greek province of Cyclades. Cyclades in Greece is made up of many islands that when viewed on a map resemble a diagram of nodes in a computer network.

decryption

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

Dell Remote Assistant Cards (See *DRAC*)

Dell Remote Administrator Controller (See *DRAC*)

device console

The console on a server or another type of device that allows access to its console through an Ethernet port that is connected to one of the OnBoard’s private Ethernet ports.

DHCP (dynamic host configuration protocol)

A service that can automatically assign an IP address to a device on a network, which saves administrator’s time and reduces the number of IP addresses needed. Other configuration parameters may also be managed. A DHCP server assigns a dynamic address to a device based on the *MAC address* of the device’s Ethernet card. Many Cyclades devices are shipped with DHCP client software, and with DHCP enabled by default.

dial-in

A method of connecting to a remote computer using communications software, such as *PPP*, along with a modem, and a telephone line, which is supported on many Cyclades products. After the administrator of the Cyclades product has connected a modem from the Cyclades product to a live telephone line and made the phone number available, a remote authorized user can use the phone number to dial into the Cyclades product and access connected devices.

DNS (domain name service or system)

A service that translates domain names (such as `cyclades.com`) to network IP addresses (192.168.00.0) and that translates host names (such as “onboard”) to host IP addresses (192.168.44.11). To enable the use of this service, administrators need to configure one or more DNS servers when configuring AlterPath devices.

DRAC (Dell Remote Access Controller)

All of the following combinations are used for defining this acronym, with multiple definitions appearing even at the Dell website: Dell Remote [Access | Administrator | Administration] [Controller | Card].

Service processors on certain Dell servers may include an independent DRAC system controller. Several incompatible version types exist (DRAC II, DRAC III, DRAC III/XT, DRAC IV) along with several incompatible firmware versions. All controller types have a battery and can have an optional PCMCIA modem installed. Provide remote monitoring, logging, alerting, diagnostics, and basic control of the server. Some types have a *native web interface* and a *native application* “Dell OpenManage Server Administrator,” that runs on the remote administrator’s computer. Dell Open ManageIT Assistant software on the administrators computer can be used to configure and launch access.

The OnBoard provides access to many but not all DRAC management functions on supported DRAC versions. To access all the management functions available through DRAC requires *native IP* access.

encapsulating security payload (See *ESP*)

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. Encryption is one of the security features provided on Cyclades products to enable customers to enforce their data center security policies. See also *authentication* and *authorization*.

ESP (encapsulating security payload)

One of the two main protocols used by IPSec (*AH* is the other). ESP encrypts and authenticates data flowing over the connection. Does not define the authentication method that must be used. DES, 3DES, AES, and Blowfish are commonly used with ESP.

Ethernet bonding

Synonymous with *Ethernet failover.* A way of configuring two Ethernet ports on a single device with the same IP address so that if the primary Ethernet port becomes unavailable, the secondary Ethernet port is used. When bonding is enabled, the active IP address is assigned to bond0 instead of eth0. When the primary Ethernet port returns to active status, the software returns it to operation.

Ethernet failover

See *Ethernet bonding*. See also *failover.*

event log

Referred to as the system event log (SEL) on most service processors, a timestamped record of events such as power on/off, device inserts/removals/ connects/disconnects, sensor threshold events and alerts.

Expect script

A script written using `expect`, a scripting language based on Tcl, the Tool Command Language. Can be written to perform automation and testing operations that are not possible with other scripting languages. Cyclades uses `expect` scripts in some of its AlterPath products, and users can customize some of the default expect scripts. For example administrators of the AlterPath OnBoard can customize the Expect scripts that handle conversations with service processors and other supported devices.

failover

A high-availability feature that relies on two redundant components in a system or a network, with the second component available to automatically take over the work of the primary components if the primary component becomes unavailable for any reason. When the primary component becomes available, it takes over the work again. Automatically and transparently redirects requests from the unavailable component to the backup component. Used to make systems more fault-tolerant. See *Ethernet bonding*.

flash memory

A chip used to store the operating system, configuration files, and applications on some Cyclades products.

GPRS (general packet radio service)

A mobile data service available to users of GSM mobile phones that adds packet data capabilities.

GSM (global system for mobile communications)

Originated by the GSM (Groupe Special Mobile) group in France in 1982. A popular standard for mobile phones.

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 Cyclades Web Manager.

HTTP (hypertext transfer protocol)

Protocol defining the rules for communication between Web servers and browser across the Internet.

HTTPS (secure HTTP over SSL)

Protocol enabling the secure transmission of Web pages by encrypting data using *SSL* encryption. URLs that require an SSL connection start with `https`.

IETF (Internet Engineering Task Force)

Main standards organization for the Internet. Working groups create Internet Drafts that may become RFCs. RFCs that are approved by the Internet Engineering Steering Group (IESG) may become standards. RFCs (Requests for Comments) are the official technical specifications of the Internet protocol suite. For example, the format of *SNMP MIBs* was defined by the IETF, which assigns MIB numbers to organizations.

iLO (Integrated Lights Out)

Hewlett Packard's proprietary service processor (pronounced *EYE-loh*). Even though HP is a major supporter of IPMI, the company also provides iLO because it provides many more functions than IPMI. The iLO processor resides on the *baseboard*. 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. Advanced iLO provides remote KVM and *virtual media* access.

integrated lights out (See *ILO*)

IP address 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 addresses is both expensive and time consuming without consolidation.

IPDU (intelligent power distribution unit)

A device with multiple power inlets into which IIT assets can be plugged for remote power management. Cyclades supports a family of AlterPath PM IPDUs that can be remotely managed when they are connected to AlterPath devices, such as the AlterPath KVM/net or AlterPath OnBoard.

IPMI (Intelligent Platform Management Interface)

An open standards vendor-independent service processor currently adopted by many major server platform vendors. Its main benefit over other service processor types is that it is installed on servers from many vendors, providing one interface and protocol for all servers. Its main disadvantage is that it does not always provide as much functionality as the proprietary service processors. For this reason, IBM’s series e325 and e326 servers use IPMI to manage their BMCs but the top-of-the-line xSeries servers use *RSA II*. IPMI works by interacting with the *BMC*, and since it usually has standby power, it can function even if the operating system is unavailable or if the system is powered down. The OnBoard supports IPMI version 1.5. OnBoard administrators can create custom *Expect* scripts to support IPMI 2.0.

ipmitool

A command line utility that interfaces with any *BMC* that supports either IPMI 1.5 or 2.0 specifications. Reads the sensor data repository (SDR) and prints sensor values, displays the contents of the System Event Log (SEL), prints Field Replaceable Unit (FRU) inventory information, reads and sets LAN configuration parameters, and performs remote chassis power control. Described at SourceForge at: `http://ipmitool.sourceforge.net.` The command options are described on the `ipmitool`(1) man page at SourceForge: `http://ipmitool.sourceforge.net/manpage.html`. `ipmitool` commands can be added to customized scripts on the OnBoard to access unsupported features on a connected service processor.

IPSec (Internet protocol security)

A suite of protocols used for establishing private, secure, connections over IP networks. Only the sending and receiving computers need to be running IPSec. Each computer handles security at its end and assumes that the intermediary nodes between the source and destination computers are not secure. Supported on many AlterPath products. In tunnel mode, IPSec is used to form a *VPN* connection, creating a secure tunnel between either an individual host or a subnet on one end and the AlterPath device on the other end. Has two modes, *transport* and *tunnel* mode. Tunnel mode encrypts the entire packet. Transport mode encrypts application headers, TCP or UDP headers, and packet data, but not the IP header. The method that encrypts the entire packet cannot be used where NAT is required

Kerberos

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

KVM

Remote keyboard, video [monitor], and mouse access to a server through a PS/2 or USB connection on a server that is connected to a KVM switch.

KVM analog switch

A *KVM switch* that requires a local user connection before a user can gain access to any servers that are connected to the switch. Cyclades AlterPath KVM analog switches are one component of the *out-of-band infrastructure*.

KVM over IP switch

A *KVM switch* that supports remote access over a LAN or WAN or telephone line to servers connected to the switch, 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*.

KVM switch

Enables use of only one keyboard, video monitor, and mouse to run multiple servers from a remote location. 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* or greater 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*.

Cyclades AlterPath KVM analog switches are one component of the *out-of-band infrastructure*.

LDAP (lightweight directory access protocol)

A directory service protocol used for authentication. One of many standard authentication protocols supported on Cyclades devices.

MAC address

Also called the Ethernet address. A number that uniquely identifies a computer that has an Ethernet interface. Cyclades equipment displays MAC addresses on a label on the bottom.

management console—See service processor

management network

A network separated from the *production network* that provides remote *out-of-band* access for management of IT assets, including access for returning disconnected IT assets to service without the need for a site visit.

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*. Most of these types of software only manage one server, do not scale, and do not address the need for consolidated access-control, multi-user access, data logging, and event detection, encyrption and other needs. The OnBoard addresses these needs and provides a single interface to access basic features of multiple-vendors' service processors.

MIB

Each *SNMP* device has one or more MIBs (management information bases), which describes the device’s manageable objects and attributes. The MIB name tree for Cyclades starts at 1.3.6.1.4.1.4413.

MIIMON

A value set when configuring Ethernet failure to specify how often the active interface is inspected for link failures. A value of zero (0) disables MII link monitoring. A value of 100 is a good starting point, according to SourceForce bonding documentation.

MS-CHAP (Microsoft challenge handshake authentication protocol)

The Microsoft version of CHAP, which does not require the storage of a clear or reversibly-encrypted password. Can be used with or without AAA (authentication, authorization, and accounting). If AAA is enabled, PPP authentication can be done by TACACS+ and RADIUS.

NAT

Network address translation, an Internet standard that enables the use of one set of IP addresses for internal traffic and another set of IP addresses for traffic over the public network. The AlterPath OnBoard uses NAT to allow access to service processors and managed devices while not revealing their Ethernet addresses. Users can use administratively-assigned virtual IP addresses to access the service processor or device through the OnBoard.

native applications

A management option that gives the user the ability to run *service processor*-specific *native applications* and access the application’s management features from the user's remote computer through the OnBoard. For example, the IBM service processor provides the IBM Director native application.

To obtain this type of access, the authenticated and authorized user selects the “Native IP” option after establishing a VPN connection between the user’s computer and the OnBoard. At that point, the user can bring up the management application from where it resides on the user's computer or on the service processor and use the service processor's server management functions.

n*ative command interface* (See *NCI*)

native IP

A management option that the OnBoard administrator can enable when configuring a *service processor*. Because this option provides full access to all features supported by the service processor, the user must be a trusted user who is specifically authorized to use the option. A *VPN* connection must be made before the user is allow to access the native IP option. When the OnBoard user activates Native IP for a service processor, the OnBoard routes packets between that user’s IP address and the service processor through a secure tunnel. The VPN connection must remain active for the duration of the Native IP session. Authorizing a user for native IP gives the user access to a *native application* or a *native web interface* that may be provided by the service processor and that may provide additional management functions beyond those provided by the OnBoard, including *KVM over IP* access to the server.

native web interface

A service processor feature that allows browser access to the service processor’s information, management, configuration, and actions, by means of a HTTP/HTTPS server running on the service processor. Access to this feature requires the user to be authorized for *native IP*.

NCI (native command interface)

A *service processor* feature that allows direct access to the *console* of the service processor. Access may be provided to features such as power control, hardware auditing, event logs, sensor readings, and service processor configuration, usually by means of a Telnet or *SSH* server running on the service processor.

NEBS (Network Equipment Building System) Certification

Means that equipment has been tested and proven to meet the NEBS requirements for central office equipment that is adhered to in common 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, electromagnetic capability, electrical safety, and manufacturing component characteristics, among other attributes.

network time protocol (See *NTP*)

netmask

The dotted-decimal expression that determines which portion of an IP address represents the network IP address and which is used for host IP addresses, for example, 255.0.0.0.

NIS (Network Information Service)

A directory service protocol used for authentication in UNIX systems. One of many standard authentication protocols supported on Cyclades devices.

NTLM (NT LAN manager)

An authentication protocol used by Microsoft *SMB*.

NTP (network time protocol)

A protocol used to synchronize the time in a client with a high-accuracy network time protocol server.

OID

A unique indentifier for each object in an *SNMP MIB*. The OID naming scheme is in the form of an inverted tree with branches pointing downward. The OID naming scheme is governed by the IETF, which grants authority for parts of the OID name space to individual organizations. Cyclades has the authority to assign OIDs that can be derived by branching downward from the node in the MIB name tree that starts at 1.3.6.1.4.1.4413.

SNMP programs use the OID to identify the objects on each device that can be managed by using SNMP.

onbdshell

The OnBoard shell, `/usr/bin/onbdshell`, which displays a menu of devices an authorized user can access. Accessed by authorized users through selecting the “Access Devices” option from the user shell menu, *`rmenush`*. Selecting a server name from the menu brings up the list of actions the user is authorized to perform on that server's *service processor*. Accessed by administrators by typing `/usr/bin/onbdshell` on the OnBoard's command line; the administrators' version of the menu lists all configured devices.

OOBI (Out-of-band Infrastructure)

An integrated systems approach to remote administration. Consists of components that provide secure, *out of band* access to connect to and manage an organization's *production network*. Components can include console servers, KVM and *KVM over IP* switches, power control appliances, centralized management devices (to control the entire out-of-band infrastructure), and service-processor managers to manage access to multiple vendor's service processors. Allows administrators to remotely connect to disconnected IT assets and to quickly return them to normal operation. Cyclades AlterPath products are designed as building blocks for an OOBI, including AlterPath ACS console servers, AlterPath KVM and KVM over P switches, AlterPath OnSite with consolidated console and KVM ports, AlterPath PM IPDUs, the AlterPath OnBoard service- processor manager, and the AlterPath Manager for centralized control of and access through multiple AlterPath devices to up to 5000 connected devices, and for access to servers that have IPMI controllers.

OTP (one-time passwords)

An authentication system that requires the user to generate and use a new password for every connection. The OTP can only be used once, which ensures that a discovered password is useless. Originally developed at Bellcore (now Telcordia), it started as a freely available program called S/Key that was trademarked. A newer freeware OTP program is OPIE (one time passwords in everything).

out of band

Access to IT assets that is either separate from or independent of the normal *production network*. A term that originated in the telecommunications industry to refer to communications used to control a phone call that are made on a dedicated channel, which is separate from the channel over which the call is made. Allows remote monitoring and control even when a managed IT asset loses connection to the production network. Typically, out-of-band access is through a *console* or management port (typically an RS-232 or Ethernet port), an *intelligent power management device* (IPDU), a *KVM* port, or a *service processor.*

point to point protocol (See *PPP*)

point to point tunneling protocol (See *PPTP*)

PPP (point to point protocol)

A method that creates a connection between a remote computer and a Cyclades device and enables a remote user access using the Web Manager or the command line. Supports the use of the PAP, SPAP, CHAP, MS-CHAP, and EAP authentication methods.

PPTP (point to point tunneling protocol)

A *VPN* method developed by Microsoft along with other technology companies, it is the most widely supported VPN method among Windows clients and the only VPN protocol built into Windows 9x and NT operating systems. Uses the same types of authentication as PPP.

production network

The network on which the primary computing work of an organization is done. Users on a production network expect 24/7/365 availability with access to data and resources as reliable as access to telephone service. Development and testing of new applications are often performed on separate networks to avoid burdening or compromising the production network. Organizations often set up separate *management networks* to provide remote *out-of-band* access to disconnected IT assets.

RADIUS (remote authentication dial in user service)

A widely-supported authentication protocol for centralized user administration. Used by many Internet Service Providers (ISPs) and by devices such as routers and switches that do not have much storage. Combines authentication and authorization in a user profile. Relies on the UDP protocol. One of many standard authentication protocols supported on Cyclades devices.

remote supervisor adapter II (See *RSA II*)

remote system control (See *RSC*)

rmenush

The default login shell for users (`/usr/bin/rmenush`), which allows users only a limited set of menu options, including: access to management actions on devices for which they are authorized; the ability to change the user's password; and the ability to logout. The OnBoard administrator may modify the menu options and commands.

RSA II (remote supervisor adapter II)

Service processor technology on certain IBM servers that includes a service processor PCI card used to manage the BMC that is located on the motherboard. Enables the remote administrator to receive notifications, alerts, to view event logs and the last screen before a failure, to use virtual media (also called "remote media"), to control power and to manage the console through a web browser using a built-in Web server. Provides more options than the IPMI service processor that is available on IBM xseries e325 and e326 servers.

RSC (remote system control)

Service processor technology on certain Sun servers that includes a *service processor* RSC card. 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 the server. The RSC card on some servers include a battery that provides approximately 30 minutes of power to RSC in case of a power failure.

secure rack management (See *SRM*)

security features

Cyclades products provide security features, including *encryption*, *authentication*, and *authorization*, to enable customers to enforce their data center security policies while providing *out-of-band* access to managed systems.

SEL (See *event log*)

serial over LAN (See SoL)

service processor (See SP)

service processor console

The console on a service processor whose dedicated Ethernet port is connected to one of the OnBoard's private Ethernet ports. Sometimes referred to as NCI (for native command interface). [OnBoard only]

service processor manager

An *OOBI* component that provides to users and groups secure, controlled access to basic features required for out-of-band management of servers that have embedded management controllers (also called *BMC*s or *service processors*). Also provides access to the console of servers and other devices without service processors but that have Ethernet ports that allow console access. Provides a single point of access through a single Ethernet address (see *IP address consolidation*) to services that are provided by service processors from several different vendors and to the console of certain servers and other devices. Its administrators are able to use a single interface to manage multiple servers without having to learn multiple management interfaces. The AlterPath OnBoard is the Cyclades service processor manager.

shell

A command interpreter on UNIX-based operating systems (like the Linux operating system that controls most Cyclades products). A shell typically is accessed in a terminal window where the shell presents a prompt. For example: `[admin@OnSite 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. See also *command line interface*. The AlterPath OnBoard has two user shells: *`onbdshell`* and *`rmenush`*.

simple mail transfer protocol (See *SMTP*)

SMB (server message block)

A protocol used for file sharing and other communications between Windows computers. Microsoft uses this protocol along with NTML authentication protocol used to authenticate a client on a server.

SMTP (simple mail transfer protocol)

The most-commonly-used protocol used to send email.

SNMP (simple network management protocol)

A set of network management protocols for TCP/IP and IPX (Internet Packet Exchange) networks, which are part of the TCP/IP protocol suite. Supports management of devices running SNMP agent software by remote administrators using *SNMP manager software*, such as HP OpenView, Novell NMS, IBM NetView, or Sun Net Manager, on remote computers. Devices running SNMP agent software send data from management information bases (*MIBs*) to the SNMP manager software.

On certain Cyclades devices, administrators can enable SNMP to allow a remote administrator to manage the device and can configure the device to send alerts about events of interest. Before enabling SNMP, the administrator needs the following information: The contact person (administrator) of the AlterPath device; the physical location, the *community name* (for SNMP v1, v2c only), IP address or DNS hostname of the *SNMP manager*. The OnBoard supports SNMP v1, v2c, and v3. The SNMP configuration file is located at `/etc/snmp/snmpd.conf`. See also *OID* and *traps*.

SNMP manager

Any computer running SNMP manager software. Also called a network management station or SNMP server.

SNMP manager software

Displays data about managed devices on the console or saves the data in a specified file or database. Some network management programs such as HP OpenView graphically show information about managed devices.

SNMP server (See SNMP manager)

SoL *(*serial over LAN)

Access to the console of a server or other device that supports redirection of serial server data to a dedicated Ethernet port. Permits access to and control of the BIOS and operating system console over the LAN or Internet. Eliminates the need for the device to have a serial port and the need for serial cabling to enable console access. On the OnBoard, once a device’s SoL Ethernet port is connected to one of the OnBoard’s private Ethernet ports, an authorized user can access the server or a device’s console either through the “Device console” or “devconsole” option (available on the *Web Manager*, *`rmenush`*, or *`onbdshell`*`)` or through entering the `devconsole` command with `ssh` on the command line).

SP (service processor)

Ethernet-based management controller on a server, which provides out-of-band management through an interface between the server’s administrator and an internal baseboard management controller (BMC) that enables the management features. Management features can include serial console emulation (using Telnet or IPMI), *KVM over IP*, power control, sensor and log information from the server hardware, and virtual media.

SRM (secure rack management)

An out-of-band infrastructure (OOBI) capability delivered by the AlterPath OnBoard that isolates the management ports (emergency service ports) of servers that have *service processors* from the *production network*. Physically consolidates and logically secures the Ethernet connections between the AlterPath OnBoard and the connected service processors. By providing *IP consolidation*, SRM substantially lowers the cost and complexity of deploying service processors. SRM also lowers the security risks of using service processors by providing centralized authentication and user access control, isolating vulnerable service processor protocols from the production network and communicating with authenticated and *authorized users* over the public network using higher-end secure protocols (such as *SSH*, *SSL*, and *HTTPS*).

SSH

Secure shell, developed by SSH Communications Security, Ltd., is a UNIX-based *shell* and protocol that provides strong authentication and secure communications over unsecured channels. Unlike `telnet`, `ftp`, and the `rcp`/`rsh`/`remsh` programs, SSH encrypts everything it sends over the network. Many Cyclades products support SSH version 1 and SSH version 2. Since SSH1 and SSH2 are entirely different, incompatible protocols, it is important when given a choice between enabling one or the other of the two SSH versions to enable the version that is available on the computer being used to access the Cyclades equipment. The OpenSSH (`www.openssh.org`) package is used on the AlterPath OnBoard. THe OnBoard uses the Open SSH version that is certified by the Cryptographic Module Validation (CMV) program run by the U.S. National Institute of Standards (NIST) and the Canadian government's Communications Security Establishment (CSE). Authorized users on the AlterPath OnBoard can enter an OnBoard-specific set of commands such as poweron, poweroff, powercycle when using `ssh` on the command line to perform *service processor* management actions.

SSL (secure sockets layer)

A protocol for transmitting private documents via the Internet. Also used for the type of connection used for transmitting the information. Uses two keys to encrypt data being transferred: a public key and a private or secret key known only to the message receiver. See also *HTTP/HTTPS*.

system event log (See *event log*)

TACACS+ (Terminal Access Controller Access Control System)

An authentication protocol (pronounced *tak-ak_plus*) that provides separate authentication, authorization, and accounting services. Based on TACACS, but completely incompatible with it. Uses the TCP protocol, which is seen by some administrators as a more-reliable protocol than the UDP protocol used by RADIUS. One of many standard authentication protocols supported on Cyclades devices.

trap

An operation started by an SNMP agent in response to an event of interest on a managed-object in a device, which sends an alert to the *SNMP manager*. The administrator of certain Cyclades device can configure which types of events generate trap messages and trap destinations. Also known as SNMP messages or as “PDUs”—protocol data units.

virtual media

Emulates the use of a floppy or CD drive that is physically connected to the remote administrator’s computer to

VPN (virtual private network)

A mechanism enabling two computers to securely transfer information over an otherwise untrusted network through a secure tunnel. Two common options used for VPN are *IPSec* and *PPTP*.

Web Manager

Cyclades' web management interface. The Web Manager runs in supported browsers and allows remote administrators to configure Cyclades products and to enable remote users to access servers and other devices that are connected to Cyclades products. Authorized users can use the Web Manager to access connected devices.

Index