



Avocent®

# Cyclades® OnBoard

User Guide



## **FCC Warning Statement**

The Cyclades OnBoard service processor manager has been tested and found to comply with the limits for Class A digital devices, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Installation & Service Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the problem at his or her own expense.

## **Safety and EMC Approvals and Markings**

C-Tick, ICES 003, FCC Part 15 Class A, CE



# **Cyclades<sup>®</sup> OnBoard Service Processor Manager User Guide**

Avocent, the Avocent logo, The Power of Being There and Cyclades are registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners.

© 2006 Avocent Corporation. All rights reserved. 590-662-501A



### **Instructions**

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.



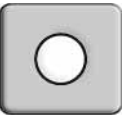
### **Dangerous Voltage**

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.



### **Power On**

This symbol indicates the principal on/off switch is in the on position.



### **Power Off**

This symbol indicates the principal on/off switch is in the off position.



### **Protective Grounding Terminal**

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

# TABLE OF CONTENTS

<b>List of Figures .....</b>	<b>vii</b>
<b>List of Tables .....</b>	<b>ix</b>
<b>Chapter 1: Introduction .....</b>	<b>1</b>
<i>OnBoard Appliance's Advantages for Server Management.....</i>	<i>2</i>
<i>Security Features Used in Access Control .....</i>	<i>3</i>
<i>Cyclades Web Manager.....</i>	<i>3</i>
<i>Types of Users.....</i>	<i>4</i>
<i>User Authorizations, Management Features and Supported Device Types .....</i>	<i>5</i>
<i>SP console management options .....</i>	<i>6</i>
<i>Device console management options.....</i>	<i>7</i>
<i>Event log (SEL) management options.....</i>	<i>8</i>
<i>Native IP options .....</i>	<i>8</i>
<i>Power management options.....</i>	<i>9</i>
<i>Reset commands.....</i>	<i>10</i>
<i>Sensor management options .....</i>	<i>10</i>
<i>Authentication.....</i>	<i>13</i>
<i>Security Profiles' Effects on Users' Actions.....</i>	<i>13</i>
<i>Types of Managed Devices .....</i>	<i>14</i>
<i>Options for Accessing the OnBoard Appliance, Managing User Passwords and Managing IPDU     Power Outlets and Devices.....</i>	<i>15</i>
<i>Command Line Access Through Console Logins .....</i>	<i>16</i>
<i>Accessing the OnBoard Appliance Console .....</i>	<i>16</i>
<i>User Shell (rmenush).....</i>	<i>17</i>
<i>OnBoard Shell (onbdshell) .....</i>	<i>18</i>
<i>Using SSH with the OnBoard Appliance .....</i>	<i>18</i>
<i>The ssh command line format .....</i>	<i>19</i>
<i>Device management commands for use with the ssh command .....</i>	<i>19</i>
<i>Dial-in Access .....</i>	<i>20</i>
<i>Power Management Options on the OnBoard Appliance .....</i>	<i>20</i>
<i>Accessing a Device's Native Features .....</i>	<i>21</i>
<i>Native web .....</i>	<i>21</i>

<i>Native management applications</i> .....	21
<i>Native IP access requirements</i> .....	21
<i>Tasks for creating secure tunnels and obtaining native IP access</i> .....	22
<i>Information Users Need</i> .....	22
<i>Common Tasks for Device Management</i> .....	23
<b>Chapter 2: Accessing the OnBoard Appliance and Connected Devices</b> .....	<b>25</b>
<i>Accessing the OnBoard Appliance's Console</i> .....	25
<i>Accessing Device Management Features From the User Shell Menu</i> .....	26
<i>Accessing the Console of a Device</i> .....	28
<i>Creating an SSH Tunnel</i> .....	29
<i>Creating a VPN Tunnel</i> .....	30
<i>Routing requirements for VPN connections</i> .....	32
<i>Summary of VPN-related requirements for native IP access</i> .....	33
<i>Creating IPSec VPN connections</i> .....	34
<i>Creating PPTP VPN connections</i> .....	36
<i>Accessing native features of an SP when a VPN tunnel exists</i> .....	36
<i>Obtaining and Using One Time Passwords for Dial-ins</i> .....	38
<b>Chapter 3: Web Manager for All Users</b> .....	<b>39</b>
<i>Prerequisites for Using the Web Manager</i> .....	40
<i>Requirements for Java Plug-In Availability</i> .....	40
<i>Logging Into the Web Manager for Regular Users</i> .....	41
<i>Features of Regular Users' Windows</i> .....	42
<i>Web Manager Menu Options for Regular Users</i> .....	43
<i>Using the Devices Screen</i> .....	43
<i>Accessing a Service Processor's Console</i> .....	45
<i>Accessing a Device's Console</i> .....	45
<i>Managing Power Through a Service Processor</i> .....	46
<i>Running Reset on a Service Processor</i> .....	47
<i>Viewing Sensor Data</i> .....	47
<i>Viewing and Clearing Event Logs</i> .....	49
<i>Accessing Native Features on a Service Processor</i> .....	50
<i>Accessing the OnBoard Appliance Console (Web Manager)</i> .....	54
<i>Managing Power Outlets on a Connected IPDU</i> .....	56
<i>Using the Outlets Manager tab to power up and down and check power status</i> .....	57

---

<i>Viewing IPDU information</i> .....	59
<i>Using the Software Upgrade screen to view the IPDU's current software version</i> .....	61
<i>Configuring Your Password</i> .....	61
<b>Appendices</b> .....	<b>63</b>
<i>Appendix A: MindTerm Applet Reference</i> .....	63
<i>Appendix B: Technical Support</i> .....	70
<b>Index</b> .....	<b>71</b>





## LIST OF FIGURES

<i>Figure 1.1: Secure Path to a Connected SP</i> .....	2
<i>Figure 1.2: Example Graph for Readings From a Fan Sensor</i> .....	11
<i>Figure 1.3: Logging In Through the Console Port</i> .....	17
<i>Figure 2.1: Device Access Menu</i> .....	27
<i>Figure 2.2: OnBoard Appliance VPN Example Using IPSec</i> .....	31
<i>Figure 3.1: Web Manager Login Screen</i> .....	41
<i>Figure 3.2: User Options on the Web Manager</i> .....	42
<i>Figure 3.3: Devices Web Manager Screen</i> .....	44
<i>Figure 3.4: Service Processor Console Example</i> .....	45
<i>Figure 3.5: Device Console Example</i> .....	46
<i>Figure 3.6: Power Web Manager Screen</i> .....	46
<i>Figure 3.7: Example of Unformatted Sensor Data</i> .....	48
<i>Figure 3.8: Sensor Plotter Page</i> .....	49
<i>Figure 3.9: Example Event Log Web Manager Screen</i> .....	50
<i>Figure 3.10: Enable / Disabled Links for the Native IP Option</i> .....	51
<i>Figure 3.11: Go to native web interface Link</i> .....	52
<i>Figure 3.12: Example HP iLO Native Web Interface</i> .....	52
<i>Figure 3.13: OnBoard Appliance Console Login Screen</i> .....	55
<i>Figure 3.14: User Menu When Connected to the Console</i> .....	56
<i>Figure 3.15: AUX Port Not Configured Error Message</i> .....	57
<i>Figure 3.16: IPDU Tabs</i> .....	57
<i>Figure 3.17: IPDU Access Failed Message from Outlets Manager</i> .....	58
<i>Figure 3.18: Access-IPDU-Outlets Manager Screen</i> .....	58
<i>Figure 3.19: Outlets Manager Outlets State Close-up</i> .....	59
<i>Figure 3.20: View IPDU Info Screen</i> .....	60
<i>Figure 3.21: IPDU Software Upgrade Screen on the Web Manager</i> .....	61
<i>Figure 3.22: Password Screen</i> .....	62
<i>Figure A.1: Root Log into MindTerm Running an SSH Console Session</i> .....	64
<i>Figure A.2: Terminal Menu</i> .....	65



## LIST OF TABLES

<i>Table 1.1: Access-related Security Features</i> .....	3
<i>Table 1.2: User Type Descriptions and Default Passwords</i> .....	5
<i>Table 1.3: Supported Device Types and Management Options</i> .....	6
<i>Table 1.4: Power Management Options</i> .....	6
<i>Table 1.5: Power Management Options</i> .....	7
<i>Table 1.6: Event Log (SEL) Management Options</i> .....	8
<i>Table 1.7: Event Log (SEL) Management Options</i> .....	8
<i>Table 1.8: Power Management Options</i> .....	9
<i>Table 1.9: Possible Power Management Command Effects</i> .....	9
<i>Table 1.10: Reset Options</i> .....	10
<i>Table 1.11: Sensor Graph Parameters</i> .....	11
<i>Table 1.12: Sensor Management Options</i> .....	13
<i>Table 1.13: Services and Other Functions Controlled by Security Profiles</i> .....	14
<i>Table 1.14: Console Login Types</i> .....	16
<i>Table 1.15: User Shell Default Menu Options</i> .....	17
<i>Table 1.16: Tasks for Creating Tunnels and Obtaining Native IP Access</i> .....	22
<i>Table 1.17: Tasks for Managing Devices</i> .....	23
<i>Table 2.1: Tasks for Enabling and Using Native IP Access Using VPN</i> .....	32
<i>Table 2.2: Tasks for Enabling and Using Native IP Access Using VPN</i> .....	34
<i>Table 3.1: Supported Browser and JRE Versions</i> .....	40
<i>Table 3.2: Device Access Menu Options</i> .....	43
<i>Table 3.3: Management Features Accessed Through the Web Manager</i> .....	44
<i>Table 3.4: Information on the View IPDU Info Screen</i> .....	60
<i>Table 3.5: IPDU Information Under Unit Information</i> .....	60
<i>Table A.1: Console Session Terminal Menu Options</i> .....	65
<i>Table A.2: Hotkeys Available During Console Sessions</i> .....	69



# Introduction

The Cyclades® OnBoard service processor manager controls which users have access to connected devices and creates a secure path between a remote user's workstation and a connected device. Introductory information provided in the sections listed below is needed by all users and administrators for understanding how to use the OnBoard service processor (SP) manager.

- *OnBoard Appliance's Advantages for Server Management* on page 2
- *Security Features Used in Access Control* on page 3
- *Cyclades Web Manager* on page 3
- *Types of Users* on page 4
- *User Authorizations, Management Features and Supported Device Types* on page 5
- *Authentication* on page 13
- *Security Profiles' Effects on Users' Actions* on page 13
- *Types of Managed Devices* on page 14
- *Options for Accessing the OnBoard Appliance, Managing User Passwords and Managing IPDU Power Outlets and Devices* on page 15
- *Command Line Access Through Console Logins* on page 16
- *Accessing the OnBoard Appliance Console* on page 16
- *User Shell (rmenush)* on page 17
- *OnBoard Shell (onbdshell)* on page 18
- *Using SSH with the OnBoard Appliance* on page 18
- *Dial-in Access* on page 20
- *Power Management Options on the OnBoard Appliance* on page 20
- *Accessing a Device's Native Features* on page 21
- *Information Users Need* on page 22
- *Common Tasks for Device Management* on page 23

## OnBoard Appliance's Advantages for Server Management

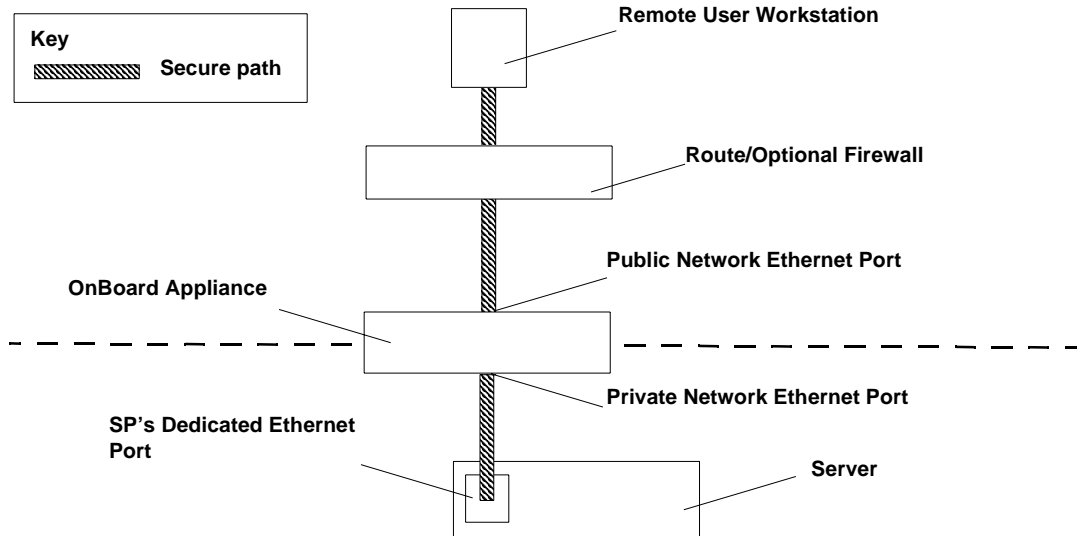
The OnBoard SP manager, or OnBoard appliance, provides access to server-management services that are provided by SPs. SPs are out-of-band management controllers that many vendors include in their servers.

The OnBoard appliance provides a single source for authentication, authorization and management for multiple types of SPs. Through the OnBoard appliance, users can access and manage multiple servers from a single point without having to learn how to use multiple SP-management interfaces.

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

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

Figure 1.1 is a conceptual illustration of a secure path between a remote user and an SP through the OnBoard appliance. (Users can also be on the same LAN as the OnBoard appliance and the connected devices.)



**Figure 1.1: Secure Path to a Connected SP**

In Figure 1.1, the dedicated Ethernet port of a SP is separate from the server's Ethernet ports. The SP's dedicated Ethernet port is connected to one of the OnBoard appliance's private Ethernet ports.

The IP address of the public Ethernet port is the only publicly-defined IP address used for out-of-band management, which reduces the deployment costs for the SPs.

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 Figure 1.1, the remote user accesses the OnBoard appliance through a network connection to the public Ethernet port and then selects an authorized action to perform on a specific SP. (Users may also dial into the OnBoard appliance through an optional external modem or PC modem card.)

After the user selects the desired management action, the OnBoard appliance then creates a secure connection between the user and the SP, acting as a proxy on behalf of the user. While the user is performing any of the authorized SP management actions, the connection between the OnBoard appliance and the SP is kept separate and protected from the connection between the user and the OnBoard appliance. Nothing that happens on the private network is exposed to the public network. Depending on the mode of access (either by browser or by SSH), either HTTPS or SSH is always being used to protect communications that are transported on the public network between the user and the OnBoard appliance.

## Security Features Used in Access Control

The OnBoard appliance allows administrators to enforce an organization's security policies through features that control who can access management features on connected devices. The access-related security features are shown in Table 1.1 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	<i>Types of Users</i> on page 4 <i>User Authorizations, Management Features and Supported Device Types</i> on page 5
The security profile in effect on the OnBoard appliance and the option of turning services on or off	<i>Security Profiles' Effects on Users' Actions</i> on page 13
Separate authentications for accessing the OnBoard appliance and connected devices	<i>Authentication</i> on page 13

## Cyclades Web Manager

Both authorized and administrative users can access the Cyclades 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 Cyclades PM Intelligent Power Distribution Units (IPDUs) and change their own passwords. Only administrative users have access to the OnBoard appliance screens for configuring users or ports.

See Chapter 3 for information about using the Web Manager, required for authorized and administrative users.

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

- Through the Ethernet port
- Through dialing into one of the modem or PC phone card types described in *Authentication* on page 13

## Types of Users

The OnBoard appliance supports two main types of users:

- Users authorized to administer the OnBoard appliance 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. Either root or admin can add regular user accounts and can authorize them to access management features on connected devices. Any regular users added to the admin group become administrative users able to perform OnBoard appliance administration.

The admin user (and any optionally-added administrative users) can do the following:

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

The root user cannot access the Web Manager.



Table 1.2 summarizes the responsibilities of each type of user and provides the default password for each type of user. Only one administrative user can be connected to the appliance at a time.

**Table 1.2: User Type Descriptions and Default Passwords**

User Name	Responsibilities	Default Password
root	Only direct logins to the OnBoard command line are allowed. Can run the cycli utility as described in the Cyclades OnBoard Service Processor Manager Installer and Administrator Guide. Also can run other OnBoard appliance-specific commands and Linux commands on the command line of the Linux shell. Cannot be deleted.	cyclades
admin	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. Cannot be deleted.	cyclades
administrator-assigned	User account optionally configured by an administrator to be able to perform management functions on devices connected to the OnBoard appliance. 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. 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

## User Authorizations, Management Features and Supported Device Types

Users can be authorized for access to management features available on the connected SPs or other types of connected devices. The management features are listed below:

- Service Processor Console-See *SP console management options* on page 6
- Device Console-See *Device console management options* on page 7
- Event Log (SEL)-See *Event log (SEL) management options* on page 8
- Native IP-See *Native IP options* on page 8
- Power-See *Power management options* on page 9 and *Reset commands* on page 10
- Sensors-See *Sensor management options* on page 10 and *Reset commands* on page 10

**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 13.

Table 1.3 shows which management options are available on the supported SP types and on supported devices without SPs.

**Table 1.3: Supported Device Types and Management Options**

Supported Service Processors/Devices	SP Console	Device Console	Power	Event Logs	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

**NOTE:** When a connected device does not have an SP. Device Console and native IP are the only management options available by default. The OnBoard appliance command templates and device management Expect scripts can be customized to make other management features available.

## SP console management options

Table 1.4 shows the SP console management option names and command names used either when you are logged into the Web Manager, when you have selected a device from the onbdshell menu on the OnBoard appliance console or when you are entering the ssh command on a remote workstation. All options give access to the SP console and are only available for managed servers with SPs.

**Table 1.4: Power Management Options**

Method	Option or Command Name
Web Manager	Service Processor Console
onbdshell menu in the OnBoard appliance console	Access the service processor's console
ssh command	spconsole

---

## Device console management options

Table 1.5 shows the device console management option names and command names used when you are logged into the Web Manager, when you have selected a device from the onbdshell menu on the OnBoard appliance console and when you are entering the ssh command on a remote workstation. All options gives access to the console of one of the following:

- A server that allows console access through its SP
- A device without an SP that presents a command line interface through its Ethernet port.

**Table 1.5: Power Management Options**

<b>Method</b>	<b>Option or Command Name</b>
Web Manager	Device Console
onbdshell menu in the OnBoard appliance console	Access the device's console
ssh command	devconsole

## Event log (SEL) management options

Events are messages logged when system management events are detected. The events can be logged by the SP or by the server. Table 1.5 shows the event log management option names and command names used when you are logged into the Web Manager, when you have selected a device from the onbdshell menu on the OnBoard appliance console and when you are entering the ssh command on a remote workstation. These options display the system event log (SEL) menu from the server where the SP resides. The user can view or clear event logs directly on the SP using the ssh command. All options are only available for managed servers with SPs.

**Table 1.6: Event Log (SEL) Management Options**

Method	Option or Command Name	Action
Web Manager	Event Log	Brings up a screen with the event log management options. <ul style="list-style-type: none"> <li>• View event log</li> <li>• Clear event log</li> </ul>
onbdshell menu in the OnBoard appliance console	Manage the event log	Brings up a menu with the event log management options. <ul style="list-style-type: none"> <li>• View event log</li> <li>• Clear event log</li> </ul>
ssh command	sel clearsel	<ul style="list-style-type: none"> <li>• Displays the event log</li> <li>• Clears the event log</li> </ul>

## Native IP options

Native IP options are available when an SP provides access to a native web application or provides a management application that runs on the user's workstation. For more details, see *Accessing a Device's Native Features* on page 21. Table 1.7 shows the native IP options available when you are logged into the Web Manager, when you have selected a device from the onbdshell menu on the OnBoard appliance console and when you are entering the ssh command on a remote workstation. All options are available for managed servers with SPs and for other devices without SPs.

**Table 1.7: Event Log (SEL) Management Options**

Method	Option or Command Name
Web Manager	Native IP
onbdshell menu in the OnBoard appliance console	<ul style="list-style-type: none"> <li>• Enable native IP</li> <li>• Disable native IP</li> </ul>
ssh command	<ul style="list-style-type: none"> <li>• nativeipon</li> <li>• nativeipoff</li> </ul>

## Power management options

Table 1.8 shows the power management option names and command names used when you are logged into the Web Manager, when you have selected a device from the onbdshell menu on the OnBoard appliance console and when you are entering the ssh command on a remote workstation. The power management options are only available for managed servers with SPs.

**Table 1.8: Power Management Options**

Method	Option or Command Name	Action
Web Manager	Power	Brings up a screen with the power management options. <ul style="list-style-type: none"> <li>• Turn power on</li> <li>• Turn power off</li> <li>• Power cycle</li> <li>• Check power status</li> </ul>
onbdshell menu in the OnBoard appliance console	Manage power	Brings up a menu of power management options. <ul style="list-style-type: none"> <li>• Turn power on</li> <li>• Turn power off</li> <li>• Turn power off then on</li> <li>• Get power status</li> </ul>
ssh command	power	Power management options are performed using the following power management commands. <ul style="list-style-type: none"> <li>• poweron</li> <li>• poweroff</li> <li>• powercycle</li> <li>• powerstatus</li> </ul>

The effects of the SP power management commands differ from one vendor's SP to another. Table 1.10 describes the options. If an SP provides more than one of the options shown, the hard power option is performed.

**Table 1.9: Possible Power Management Command Effects**

Power Command	Option
Power off	<ul style="list-style-type: none"> <li>• Hard power off: remove the power</li> <li>• Soft power off: shut down the operating system before removing the power</li> </ul>
Power cycle (turn power off, then on again, to reboot the server)	<ul style="list-style-type: none"> <li>• Hard power cycle: remove the power, wait several seconds and then turn the power on again (to reboot the server)</li> <li>• Soft power cycle: shut down the operating system, wait several seconds and then turn power on again</li> </ul>

See *Power Management Options on the OnBoard Appliance* on page 20 for an overview of all the types of power management that users can perform.

## Reset commands

Table 1.10 shows the reset options available when you are logged into the Web Manager, when you have selected a device from the onbdshell menu on the OnBoard appliance console and when you are entering the ssh command on a remote workstation. The reset management options are only available for managed servers with SPs.

**Table 1.10: Reset Options**

Method	Command or Option
Web Manager	Reset
onbdshell menu in the OnBoard appliance console	reset
ssh command	reset

The effects of the Reset command differ from one vendor's SP to another and sometimes between firmware versions from the same vendor. In addition, some SPs 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)

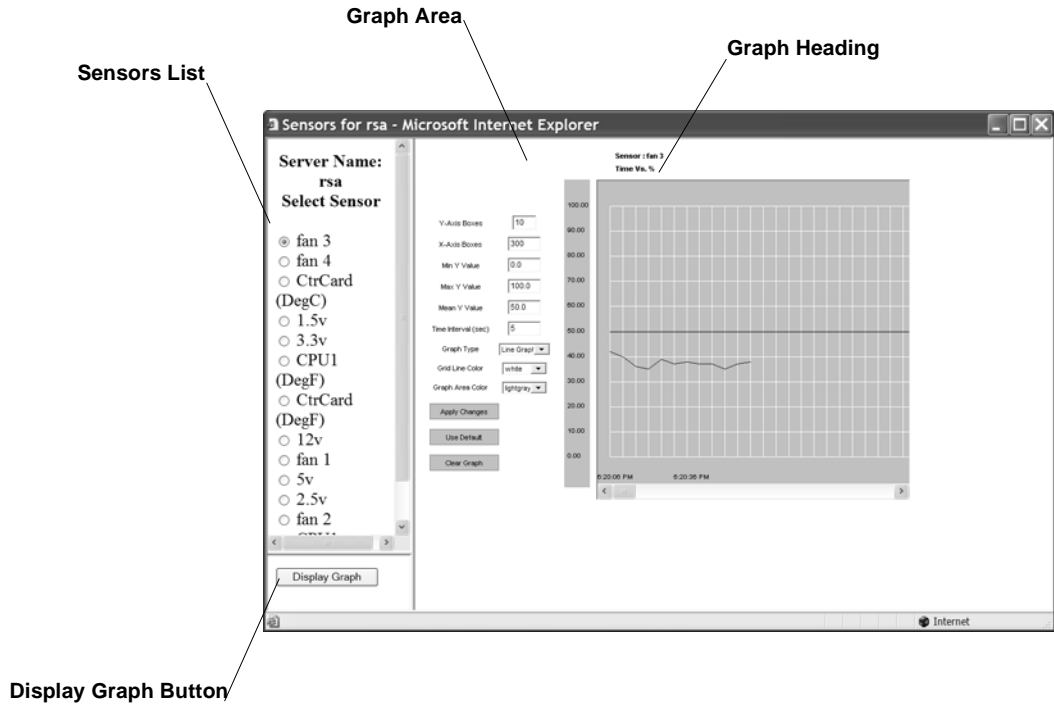
If an SP has more than one type of reset option, the OnBoard appliance Reset command performs the highest level of reset: the cold boot option if available.

If the OnBoard appliance administrator is configuring an SP that provides multiple reset options, the administrator can customize an associated SP management script to cause the Reset command to perform one of the lower levels of reset available on the SP. Customizing SP management scripts is described in the Cyclades OnBoard Service Processor Manager Installer/Administrator Guide.

## Sensor management options

An authorized user or administrative user can view graphical displays of sensor data collected from servers by their SPs. These users can also modify graph display settings through the Web Manager, the user shell menu or by using the ssh command with the sensor commands.

Figure 1.2 shows an example graph.



**Figure 1.2: Example Graph for Readings From a Fan Sensor**

The sensor value in the graph heading varies with the type of data being measured and the type of SP. The example fan sensor reading in Figure 1.2 has a heading Time Vs. % because the sensor is measuring the percentage of total possible fan speed. Examples of other possible values for *sensor\_value* are *Volts*, *Degrees Centigrade* and *Degrees Fahrenheit*.

Table 1.11 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 1.11: Sensor Graph Parameters**

Field/Menu	Use	Default	Allowed Values
<b>y-axis Boxes</b>	Specify a different number of rows.	10	1-55
<b>x-axis Boxes</b>	Specify a different number of columns. Each graph cell represents the interval between readings.	300	1-999
<b>Min Y Value</b>	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

**Table 1.11: Sensor Graph Parameters (Continued)**

Field/Menu	Use	Default	Allowed Values
<b>Max Y Value</b>	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
<b>Mean Y Value</b>	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: <ul style="list-style-type: none"> <li>• Blue – Less than the mean Y value.</li> <li>• Red – Greater than mean Y value.</li> <li>• Black – Equal to the mean Y value.</li> </ul>	Varies with the type of sensor	Varies with the type of sensor
<b>Time Interval</b>	Specify a different frequency in seconds for fetching sensor data. The only valid keys are numeric keys.	5	5-300
<b>Graph Type</b>	Choose another graph type.	Line Graph	Line Graph or Bar Graph
<b>Grid Line Color</b>	Choose another color for the lines.	<ul style="list-style-type: none"> <li>• white</li> </ul>	<ul style="list-style-type: none"> <li>• yellow</li> <li>• green</li> <li>• cyan</li> <li>• gray</li> <li>• darkgray</li> <li>• lightgray</li> <li>• magenta</li> <li>• orange</li> <li>• pink</li> <li>• white</li> </ul>
<b>Graph BG Color</b>	Select the background color.	<ul style="list-style-type: none"> <li>• light gray</li> </ul>	<ul style="list-style-type: none"> <li>• yellow</li> <li>• green</li> <li>• cyan</li> <li>• gray</li> <li>• darkgray</li> <li>• lightgray</li> <li>• magenta</li> <li>• orange</li> <li>• pink</li> <li>• white</li> </ul>

For procedures for monitoring sensors, see *To view a server's sensor data from an SP (Web Manager)*: on page 49.

Table 1.12 shows the sensor management options available when you are logged into the Web Manager, when you have selected a device from the onbdshell menu on the OnBoard appliance console and when you are entering the ssh command on a remote workstation. The sensor options



display unformatted sensor data collected from the server by its SP. The page that appears provides a button that when clicked displays graphs of data from individual sensors.

The sensor management options are only available for managed servers with SPs.

**Table 1.12: Sensor Management Options**

Method	Command or Option
Web Manager	Sensors
onbdshell menu in the OnBoard appliance console	sensors
ssh command	sensors

## Authentication

Anyone accessing the OnBoard appliance 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 appliance) or on an authentication server on the network.

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

- When logging into the OnBoard appliance.  
The authentication method chosen for the OnBoard appliance is used for all access through Telnet, SSH or the Web Manager. By default, logins to the OnBoard appliance use local authentication.
- When accessing an SP or other connected device.

Users may be required to enter different usernames and passwords when accessing the OnBoard appliance than when accessing a connected device.

## Security Profiles' Effects on Users' Actions

The administrator selects a security profile 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.

Each OnBoard appliance has a security profile, which controls which services are turned on and whether authorizations are being checked.

---

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

---

Table 1.13 lists services and other functions controlled by security profiles.

**Table 1.13: Services and Other Functions Controlled by Security Profiles**

Service	Other Functions That May Be Allowed/Disallowed
FTP	N/A
HTTP, HTTPS	Redirect HTTP automatically to HTTPS
ICMP	N/A
IPSec	N/A
PPTP	N/A
RPC	N/A
SNMP v1, v2c, v3	N/A
SSH v1, SSH v2	Allow root login using SSH Assign an alternate port to SSH
Telnet	Allow Telnet to OnBoard appliance

Services can also be turned on and off independently from the security profile. For more details, see the Cyclades OnBoard Service Processor Manager Installer/Administrator Guide.

In addition to turning services on and off, an administrator may select the security profile option to override authorizations, which enables access based on authentication only.

**NOTE:** If you are prevented from using a service you need to use, such as FTP or SNMP, talk with the 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:

- An SP on a server
- A server or other type of device that does not have an SP 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 by means of the OnBoard appliance's native IP access capability

---

**NOTE:** The term device is used in this guide when referring to an SP, server or other connected device, unless otherwise stated.

---

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

Authorized users can access the OnBoard appliance 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 IPDUs
- Managing the user's own password

For details about modem access, see *Authentication* on page 13.

The following means are available for logging into the OnBoard appliance 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 3.
- Using an SSH application or the ssh command on the command line of the user's workstation to connect to the OnBoard appliance's command line, then choosing from a list of menu options. See *Accessing the OnBoard Appliance Console* on page 16, *User Shell (rmenush)* on page 17 and *OnBoard Shell (onbdshell)* on page 18.
- Using ssh on the command line to execute an SP management command directly on the SP. For details, see *Using SSH with the OnBoard Appliance* on page 18. The device management features are described under *Using SSH with the OnBoard Appliance* on page 18.

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

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

## Command Line Access Through Console Logins

Administrators and authorized users can access the command line through the consoles of the OnBoard appliance and of SPs, servers and other connected devices. Users of any type can log into a console using either the Web Manager, menus available through the OnBoard appliance's console, or using the ssh command. The following table provides links to where console access is defined.

**Table 1.14: Console Login Types**

Console Type	Where Documented
OnBoard appliance	<i>Accessing the OnBoard Appliance Console</i> on page 16
Device or SP console	<i>To use the OnBoard appliance console menus to access device management options:</i> on page 28 or <i>To use an ssh command to connect directly to a device's or SP's console:</i> on page 28

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 workstation and the console. MindTerm is an SSH client that includes an integrated xterm/vt100 terminal emulator and runs as a Java applet within a browser window.

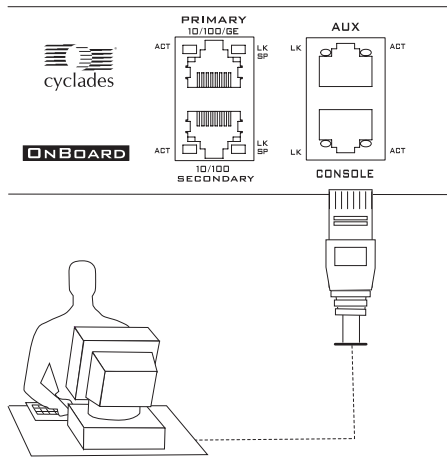
To use MindTerm, the user's browser must have a Java plug-in enabled, as described in *Requirements for Java Plug-In Availability* on page 40.

See *MindTerm Applet Reference* on page 63 for details about use and configuration and about hotkeys that can be used during console sessions through the Web Manager.

## Accessing the OnBoard Appliance Console

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

- By local logins through the console port: Local 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 workstation that is connected to the OnBoard appliance's console port as shown in Figure 1.3. The user or administrator logs in through a terminal or through a terminal emulation program on the connected workstation.



**Figure 1.3: Logging In Through the Console Port**

- By using SSH: Remote administrators and authorized users can access the OnBoard appliance's command line through an SSH connection between the user's workstation and the appliance. See *Using SSH with the OnBoard Appliance* on page 18.
- 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.

The following sections describe the menus available to regular users and administrative users after they log into the OnBoard appliance console.

## User Shell (rmenush)

The default login shell for non-administrative users is `/usr/bin/rmenush`. After logging in as described in *Accessing the OnBoard Appliance's Console* on page 25, regular users see the menu options described in the following table.

**Table 1.15: User Shell Default Menu Options**

Menu Option	Function
Access Devices	Executes <code>onbdshell</code> to display a list of devices the user can access. See <i>OnBoard Shell (onbdshell)</i> on page 18.
Change Password	Allows the user to set a new password.
Logout	Logs the user out of the OnBoard appliance's console.

An OnBoard appliance administrator may modify the menu options and commands shown in Table 1.15 so that you may be presented with a different menu of choices. For an example, see *Obtaining and Using One Time Passwords for Dial-ins* on page 38, where an option for accessing the one time password menu has been added. See *Accessing Device Management Features From the User Shell Menu* on page 26 for more details.

## OnBoard Shell (onbdshell)

When you select *Access Devices* from the login menu shown in Table 1.15, the OnBoard appliance shell, `/usr/bin/onbdshell`, displays a list of devices you are authorized to access, as shown in the following example.

```
Select a device
-rack1_dev2_compaq_proliant_ilo
  rack1_dev1_ibm_e306_rsa
  au_rack1_dev1_ilo
Exit
```

An administrative user can access a list of all devices by entering `/usr/bin/onbdshell` on the command line. A submenu lists the device management actions available to the user. See *Accessing Device Management Features From the User Shell Menu* on page 26 for more details.

## Using SSH with the OnBoard Appliance

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

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

- For accessing the OnBoard appliance console using an SSH client or the `ssh` command, then connecting through the OnBoard appliance to perform device management actions. See *Accessing the OnBoard Appliance's Console* on page 25.
- Using the `ssh` command with special device management commands to perform device management actions without having to log into the OnBoard appliance first. See *Device management commands for use with the ssh command* on page 19. See *Accessing Device Management Features From the User Shell Menu* on page 26 and *Accessing the Console of a Device* on page 28.
- Creating an SSH tunnel to get access to a native web application on a device. See *Accessing a Device's Native Features* on page 21 and *Information Users Need* on page 22.

## The ssh command line format

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

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

where:

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

The username is the account name of the authorized user.

The devicename is the name/alias that was assigned to the device by the OnBoard appliance administrator (used only when accessing a device).

---

**NOTE:** To access the OnBoard appliance console, omit the device name.

---

The onboard\_IP\_or\_DNS\_name is the IP address of the OnBoard appliance or its DNS name.

The command is one of the OnBoard appliance-specific device management commands described in *Device management commands for use with the ssh command* on page 19.

For details, see *Accessing a Device's Native Features* on page 21.

## Device management commands for use with the ssh command

Users can perform device management actions directly on an SP by using the ssh command along with one of the following OnBoard appliance-specific device management commands:

- spconsole
- devconsole
- poweron, poweroff, powercycle, powerstatus
- reset
- sensors
- sel, clearsel
- native\_ip\_on, native\_ip\_off

For details about the management actions performed by the commands, see *Using SSH with the OnBoard Appliance* on page 18.

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

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

Administrative users may want to use the rmenush command when logging into the OnBoard appliance to bring up the user login shell menu:

```
% ssh -t root:@192.168.44.111 rmenush
```

## Dial-in Access

Authorized users can dial into the OnBoard appliance 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 PC slots

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

- The modem or phone card has been configured on the OnBoard appliance 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 appliance and optionally for callback from the OnBoard appliance.
- The user account has been configured for PPP access and the user knows the PPP username and password configured by the OnBoard appliance administrator.

The OnBoard appliance can be accessed from a terminal emulation program on the user's workstation 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 PC modem or phone cards.

## Power Management Options on the OnBoard Appliance

Authorized users and OnBoard appliance administrators can turn power off, turn power on or cycle power to reboot devices.

The OnBoard appliance 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 a Cyclades PM IPDU, when the IPDU is connected to the OnBoard appliance 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 56.

- SP power management

Allows the user to manage power for a server whose SP is connected to the OnBoard appliance when the SP provides power management capabilities. See *Power management options* on page 9 for details about power management of connected servers with SPs.



## Accessing a Device's Native 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. Two types of access, native web and native management applications, are described in this section along with the access requirements for native IP access.

### Native web

Access to native functions on some SPs is through a proprietary web interface on the SP. HP iLO, Dell DRAC and IBM RSA II SPs 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 SPs through 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 SP 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 application is installed on the user's workstation. Some management applications reside on the SP itself.

After an authenticated and authorized user establishes a VPN connection and selects the *Native IP* option, the user can bring up the management application from where it resides on the user's workstation or from the SP's console.

### Native IP access requirements

Native IP access depends on the following being true:

- The SP must provide the desired native management functionality. For example, SPs using IPMI protocols do not provide native web access.
- The user is authorized to access the Native IP option on an SP.
- The user has created a secure tunnel to the OnBoard appliance. An SSH tunnel gives access to native web applications only while 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 1.16: 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	<ul style="list-style-type: none"> <li>• <i>Creating an SSH Tunnel</i> on page 29</li> <li>• <i>To use OpenSSH on a Linux workstation to create an SSH tunnel:</i> on page 29</li> <li>• <i>To use PuTTY on a Windows PC to create an SSH tunnel to a managed device:</i> on page 30</li> <li>• <i>To bring up a native web application after an SSH tunnel exists:</i> on page 30</li> </ul>
Create a VPN tunnel using either IPSec or PPTP and do one of the following: <ul style="list-style-type: none"> <li>• Bring up a browser to access a native web application</li> <li>• Launch a native management application from the device or from a remote workstation</li> </ul>	<ul style="list-style-type: none"> <li>• <i>Creating a VPN Tunnel</i> on page 30</li> <li>• <i>Routing requirements for VPN connections</i> on page 32</li> <li>• <i>Summary of VPN-related requirements for native IP access</i> on page 33</li> <li>• <i>Creating IPSec VPN connections</i> on page 34</li> <li>• <i>To create an IPSec VPN tunnel:</i> on page 35</li> <li>• <i>To enable native IP access through an IPSec VPN tunnel:</i> on page 35</li> <li>• <i>Creating PPTP VPN connections</i> on page 36</li> <li>• <i>To create a PPTP VPN tunnel:</i> on page 36</li> <li>• <i>To enable native IP access through a PPTP VPN tunnel:</i> on page 36</li> <li>• <i>To access a native web application (Web Manager):</i> on page 36</li> <li>• <i>To access a native management application that resides on your workstation:</i> on page 37</li> </ul>

## Information Users Need

Users need to obtain the following information from the OnBoard appliance 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 may perform.
- Information about services that are enabled or disabled on the OnBoard appliance. For example, the administrator may have configured the OnBoard appliance so that HTTP or SSH v1 are disabled.
- A list of any IPDU power outlets the user is 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 appliance.
- For native IP users using IPSec VPN connections, authentication information for either shared secret or RSA key authentication.

## Common Tasks for Device Management

Table 1.17 shows the tasks related to accessing and managing devices and lists the options the user and administrator have for performing those tasks.

**Table 1.17: Tasks for Managing Devices**

Task	Options	Where Described
Connect to a device's or SP's console	Using the Web Manager	<ul style="list-style-type: none"> <li>• <i>Accessing a Device's Console</i> on page 45</li> <li>• <i>Accessing a Service Processor's Console</i> on page 45</li> </ul>
	Using an SSH client or the ssh command to connect to the OnBoard appliance's console before accessing the device's or SP's console through a menu.	<ul style="list-style-type: none"> <li>• <i>To use the OnBoard appliance console menus to access device management options:</i> on page 28</li> <li>• <i>To use the OnBoard appliance console menus to access device management options:</i> on page 28</li> </ul>
	Using the ssh command to connect directly from the user's workstation to the device's console.	<ul style="list-style-type: none"> <li>• <i>To use an ssh command to connect directly to a device's or SP's console:</i> on page 28.</li> </ul>
Manage the following on a server through its SP: <ul style="list-style-type: none"> <li>• Power</li> <li>• SELs</li> <li>• Sensors</li> </ul>	Using the Web Manager	<ul style="list-style-type: none"> <li>• <i>To manage a server's power through its SP (Web Manager):</i> on page 47</li> <li>• <i>Viewing and Clearing Event Logs</i> on page 49</li> <li>• <i>To view a server's sensor data from an SP (Web Manager):</i> on page 49</li> </ul>
	Using an SSH client or the ssh command to connect to the OnBoard appliance's console and then manage power through a menu.	<ul style="list-style-type: none"> <li>• <i>Device management commands for use with the ssh command</i> on page 19</li> <li>• <i>To use the OnBoard appliance console menus to access device management options:</i> on page 28</li> </ul>
	Using the ssh command with power commands	<ul style="list-style-type: none"> <li>• <i>Device management commands for use with the ssh command</i> on page 19</li> </ul>



## Accessing the OnBoard Appliance and Connected Devices

The following topics describe how to access the OnBoard appliance and connected devices:

- *Accessing the OnBoard Appliance's Console* on page 25
- *Accessing Device Management Features From the User Shell Menu* on page 26
- *Accessing the Console of a Device* on page 28
- *Creating an SSH Tunnel* on page 29
- *Creating a VPN Tunnel* on page 30
- *Obtaining and Using One Time Passwords for Dial-ins* on page 38

---

**NOTE:** Chapter 3 describes using the Web Manager to manage devices. This chapter contains procedures that must be performed on the command line.

---

### Accessing the OnBoard Appliance's Console

As described under *User Shell (rmenush)* on page 17 and *OnBoard Shell (onbdshell)* on page 18, authorized users who connect to the OnBoard appliance'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.

This section describes how to access the OnBoard appliance's console using SSH. The following procedure requires the listed prerequisites in order to succeed. The format of the ssh command is described in *The ssh command line format* on page 19.

- The user must know the IP address of the OnBoard appliance.
- The user must have a username and password for the OnBoard appliance.
- The user's workstation is running an SSH client and either has an SSH application such as PuTTY or access to the command line.
- If using the ssh command, the user must know the format described in *The ssh command line format* on page 19.

**To access the OnBoard appliance console:**

1. If you are using a terminal or terminal emulation program installed on a workstation that is physically connected to the console port of the OnBoard appliance, 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. In an SSH application or in an ssh command line, enter the username and the OnBoard appliance IP address or DNS name.

The following example shows entering an ssh command with francisco as the username and 192.168.44.111 as the IP address.

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

3. Log in when prompted.

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

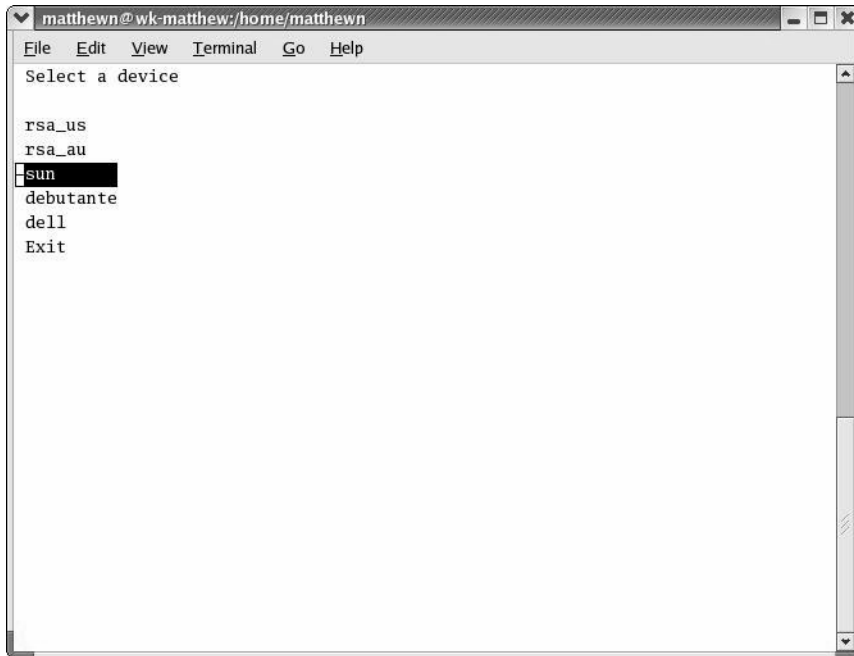
## Accessing Device Management Features From the User Shell Menu

After logging in as described in *Accessing the OnBoard Appliance's Console* on page 25, non-administrative users see a menu like the one shown in the following example.

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

Administrative users can get to the same menu either by entering the rmenush command on the ssh command line or by entering /usr/bin/rmenush on the command line after login. You can move from one item to another on the menu and submenus by using the keyboard arrow keys. A line (-) appears next to the selected item.

As described in *User Shell Default Menu Options* on page 17, if a regular user selects Access Devices, a menu appears with a list of devices that the user is authorized to access, as shown in Figure 2.1.



**Figure 2.1: Device Access Menu**

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 SPs. See *User Authorizations, Management Features and Supported Device Types* on page 5 for details. The following example shows the SP action menu for an rsa-type SP.

```
rsa
  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
```

## Accessing the Console of a Device

Chapter 3 tells how to access an SP or device console through the Web Manager. Any type of authorized user can access the console of a connected SP, server or other type of supported device using one of the two additional methods listed below.

- Connecting to the OnBoard appliance's console and accessing the SP console or the device console
- Invoking the ssh command along with either the `spconsole` or `devconsole` command

See *Device management commands for use with the ssh command* on page 19 for the format of the ssh command line when a device management command is used, if desired.

The prerequisites for using the ssh command line to access a device console are shown in the following list:

- The user has access to the ssh command on the command line of the remote workstation
- The user is authorized to access the console of a device or SP
- The user knows the alias of the device that allows console access
- The user knows the IP address or DNS name of the OnBoard appliance

### To use an ssh command to connect directly to a device's or SP's console:

1. To connect directly to a device's console, enter the **ssh** command with the **devconsole** command.

The following format example shows entering ssh with the `-t` option, the username `francisco`, the device alias `rsa_au`, the appliance 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 an SP's console, use the **ssh** command with the **spconsole** command.

The following example shows entering ssh with the `-t` option, the username `francisco`, the IP address `192.168.44.111` with the `spconsole` command.

```
% 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 SP.

### To use the OnBoard appliance console menus to access device management options:

1. Log into the OnBoard appliance console. If you have connected to the OnBoard appliance console as a regular user, the user shell menu displays.
2. If you are a regular user, use the arrow keys on your keyboard to navigate to the Access Devices option on the menu and press **Enter** or **Return**.



3. If you have connected to the OnBoard appliance console as an administrative or root user, type **/usr/bin/onbdshell** on the command line.
4. Select the name of the device to access.
5. Press **Enter** or **Return**. 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* or *Access the device's console* when the console login prompt appears, log into the console.

**To exit from a console session:**

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

- On the command line of the terminal, type the **exit** command

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

8. Enter the hotkey 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 appliance.

The prerequisites are shown in the following list:

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

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

PuTTY on Windows and OpenSSH on Linux are some of the SSH clients available for creating an SSH tunnel. The feature works with SSH protocol v1 and v2. See <http://www.openssh.com> for additional clients.

Common port numbers are: HTTP 80 and HTTPS 443

Our examples use port 443 for HTTPS for a connected device whose IP address is 10.10.1.181.

The example local TCP port number used is 8080. You can select a random number over 1000.

**To use OpenSSH on a Linux workstation to create an SSH tunnel:**

1. If the workstation is running 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. If the workstation is running SSH v1, enter the following command line.

```
$ ssh -l -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 to a managed device:

1. Open PuTTY.
2. In the Category pane, select *Tunnels* under Connection-SSH.
3. In the main pane, perform the following steps in the Port Forwarding section.
  - a. Type the number of the local TCP port to forward in the Source port field. This example uses 8080. You can select a random number over 1000.
  - b. In the Destination field, type the IP address of the device. Follow it with a colon then the port number of the service you want to access through the SSH tunnel.
  - c. Click *Add*.
4. In the Category pane, select *Session*.
5. Enter the IP address or DNS-managed name of the OnBoard appliance in the Host Name (or IP address) field.
6. Select *SSH* as the protocol.
7. Click *Open*.
8. Enter your username and password when prompted.

### To bring up a native web application after an SSH tunnel exists:

1. Bring up a browser.
2. In the location bar enter **http://localhost:portnumber** where portnumber is the TCP port number you specified for forwarding when you created the tunnel.

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

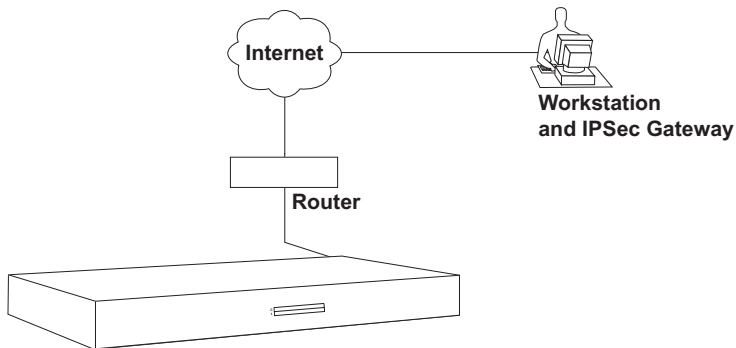
In this step, use the local port number you specified for forwarding. In the examples, we used 8080.

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.

Figure 2.2 shows an illustration of a single user's workstation running IPsec on the right end and the OnBoard appliance on the left end, with a router and the Internet between the OnBoard appliance and the user's workstation.



**Figure 2.2: OnBoard Appliance 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 appliance. The name on the OnBoard appliance end for a VPN connection profile might simply be the name and location of the user.

---

**NOTE:** Most systems, including the OnBoard appliance, 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 prerequisites are shown in the following list:

- The user on the remote workstation and the OnBoard appliance administrator have configured VPN connection profiles from both sides to support the VPN connection. See *Creating a VPN Tunnel* on page 30 for more details.
- The user has created a VPN tunnel between the user's workstation and the OnBoard appliance.
- The user has logged into the OnBoard appliance, either through the Web Manager or through the command line and has been authenticated.

An authorized user can enable native IP access in one of the following two ways:

- If the authorized user is connected to the OnBoard appliance's console, the user can select the Enable native IP option that appears in the onbdshell menu for the selected SP.
- 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 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 2.1: Tasks for Enabling and Using Native IP Access Using VPN**

Task	Where Documented
Set up a VPN connection and route to the OnBoard appliance	<ul style="list-style-type: none"> <li>• <i>Routing requirements for VPN connections</i> on page 32</li> <li>• <i>Summary of VPN-related requirements for native IP access</i> on page 33</li> <li>• <i>Creating IPSec VPN connections</i> on page 34</li> <li>• <i>Creating PPTP VPN connections</i> on page 36</li> </ul>
Create a VPN tunnel	<ul style="list-style-type: none"> <li>• <i>To create an IPSec VPN tunnel:</i> on page 35</li> <li>• <i>To create a PPTP VPN tunnel:</i> on page 36</li> </ul>
Enable native IP access	<ul style="list-style-type: none"> <li>• <i>To enable native IP access through an IPSec VPN tunnel:</i> on page 35</li> <li>• <i>To enable native IP access through a PPTP VPN tunnel:</i> on page 36</li> </ul>
Access a native web application	<i>To access a native web application (Web Manager):</i> on page 36
Access a native management application	<i>To access a native management application that resides on your workstation:</i> on page 37

## Routing requirements for VPN connections

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

### IPSec VPN routing requirements

If a route is necessary for the OnBoard appliance 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 appliance's administrator and the configuration should be shared with the user. Once packets can be exchanged between the OnBoard appliance 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 appliance, 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 appliance, which the user can discover by running the `ifconfig` or `ipconfig` command.

The following 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 OnBoard_PPTP_VPN
...
    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 IP address for the OnBoard appliance 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 appliance and PPTP has assigned to the OnBoard appliance the IP address 192.168.2.1, the user would need to configure a route like the one shown in the following 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 appliance's administrator about 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 appliance is not a viable approach. The route would cause the 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 appliance's administrator the values used in creating the VPN connection profile on the OnBoard appliance 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 appliance'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 appliance, the user must start the VPN connection from the user's workstation.

The OnBoard appliance 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 2.2: Tasks for Enabling and Using Native IP Access Using VPN**

Task	Where Documented
Set up a VPN connection and route to the OnBoard appliance	<ul style="list-style-type: none"> <li>• <i>Routing requirements for VPN connections</i> on page 32</li> <li>• <i>Summary of VPN-related requirements for native IP access</i> on page 33</li> <li>• <i>Creating IPsec VPN connections</i> on page 34</li> <li>• <i>Creating PPTP VPN connections</i> on page 36</li> </ul>
Create a VPN tunnel	<ul style="list-style-type: none"> <li>• <i>To create an IPsec VPN tunnel:</i> on page 35</li> <li>• <i>To create a PPTP VPN tunnel:</i> on page 36</li> </ul>
Enable native IP access	<ul style="list-style-type: none"> <li>• <i>To enable native IP access through an IPsec VPN tunnel:</i> on page 35</li> <li>• <i>To enable native IP access through a PPTP VPN tunnel:</i> on page 36</li> </ul>
Access a native web application	<ul style="list-style-type: none"> <li>• <i>To access a native web application (Web Manager):</i> on page 36</li> </ul>
Access a native management application	<ul style="list-style-type: none"> <li>• <i>To access a native management application that resides on your workstation:</i> on page 37</li> </ul>

## Creating IPsec VPN 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.

The OnBoard appliance administrator needs to give the user a copy of the configuration parameters used to configure the IPsec connection profiles on the OnBoard appliance, usually by providing a copy of the relevant portions of the ipsec.conf file, which the user can insert into 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 to native IP features on a device or devices.

1. Make sure your workstation can exchange packets with the OnBoard appliance.
  - a. Test whether your workstation can access the OnBoard appliance by entering the appliance'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 appliance, configure the route.
2. Create an IPSec VPN connection profile on your workstation, using the values supplied by the OnBoard appliance administrator.

If the OnBoard appliance's administrator sends the relevant portions of the `ipsec.conf` file from the OnBoard appliance'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` command.

4. Enable native IP access as described in the following procedure.

### To enable native IP access through an IPSec VPN tunnel:

---

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

---

1. Create a VPN tunnel. See *To create an IPSec VPN tunnel:* on page 35 or *To create a PPTP VPN tunnel:* on page 36 if needed.
2. To enable native IP access through a browser, perform the following steps.
  - a. Enter the private IP address or virtual IP address assigned to the OnBoard appliance in a browser.
  - b. Log into the OnBoard appliance.
  - c. Select *Devices* 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:@privateIP`.

The following command line example uses user `AllSPs` and a 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.

## Creating 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 appliance administrator:
  - The IP address assigned to the OnBoard appliance'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. After creating a PPTP VPN tunnel, enter the `ifconfig` or `ipconfig` command on your workstation to discover the PPTP address assigned from the OnBoard appliance's IP address pool in the PPTP connection.
2. 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 appliance.
  - 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 appliance.
  - A host route to each device, using the real or virtual IP address assigned to the device.
3. Enter the PPTP address either in a browser or with `ssh` on the command line to access the OnBoard appliance.
4. Access the device and enable native IP access.

See *To access a native web application (Web Manager)*: or *To access a native management application that resides on your workstation*: on page 37.

## Accessing native features of an SP when a VPN tunnel exists

The following procedures describe how to access native features on an SP after either a PPTP, IPSec or SSH tunnel exists.

### To access a native web application (Web Manager):

1. Enter the private or virtual IP address of the OnBoard appliance in a browser. The Web Manager appears.



2. Log into the Web Manager.
3. Select the *Access* menu option.
4. Click the *Go to native web interface* link on the Access Devices screen.

**To access a native web application (from a remote browser):**

On your workstation, enter the IP address of the device in a browser's location field. The native web application appears.

**To access a native web application (using the ssh command):**

On the command line of your workstation, enter the ssh command with the name/alias of the device along with the IP address of the OnBoard appliance. The native web application appears.

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

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

**To access a native management application that resides on your workstation:**

Bring up the management application on your workstation.

**To access a native management application (from an SP):**

If the management application resides on an SP and is an executable that can be invoked on the command line, do one of the following to access the SP's console and launch the management application.

- To use ssh to get to the SP's console to launch the management application, do the following steps.
  - a. Enter **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. Bring up the management application from the SP's command line.
- or-
- To use the Web Manager, do the following steps.
  - a. Log into the Web Manager on the OnBoard appliance.
  - b. Find the entry for the device to access on the Access Devices screen.
  - c. Select the *Service Processor Console* link.
  - d. Log into the SP if prompted.
  - e. Bring up the management application from the SP's command line.

## Obtaining and Using One Time Passwords for Dial-ins

This section is for users authorized to dial into the OnBoard appliance through an external modem, PC modem or phone card when the one time password (OTP) authentication method is configured for logins to that device. With OTP authentication, you supply a different password every time you dial-in, so no one who discovers the password used for one session can use that password later to access your account. An OTP is a group of six English words that are entered all on the same line at the prompt.

When you dial into the OnBoard appliance and enter a username, the system provides a challenge string starting with `otp-md5`, which tells `opiekey` to use the MD5 algorithm, followed by a sequence number and a key and waits for a response. The key includes the first two letters of the hostname and a pseudo random number. In the following example, the sequence number is 499 and the seed is `on93564`.

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

Response:

The user copies the challenge and pastes it into the command line on a non-networked workstation. The `opiekey` program then prompts the user for the user's secret pass phrase.

Each OTP user needs a local user account on the OnBoard appliance, 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. The following procedure is for users who have the `opiekey` program running on a non-networked workstation, who know the secret pass phrase and are able to generate their own passwords.

### To generate an OTP password when prompted at dial-in:

1. Dial into the OnBoard appliance through an external modem, a PC modem or phone card that has been configured to use OTP authentication.
2. Obtain an OTP password by performing the following steps.
  - a. Copy the challenge into a window on a non-networked workstation where the `opiekey` program is installed, as shown in the following example.

```
% otp-md5 499 on93564
```

- b. Enter your secret pass phrase when prompted. The `opiekey` program generates a six word OTP password.
3. Copy the OTP password to the window where the login program is waiting with the Response prompt, as in the following example.

```
Response: MOS MALL GOAT ARM AVID CORK
```

## *Web Manager for All Users*

The following sections describe how all types of users (authorized and administrative) can use the Web Manager to access the OnBoard appliance, manage connected SPs and other devices, manage power outlets on any connected IPDUs and manage their own passwords.

- *Prerequisites for Using the Web Manager* on page 40
- *Requirements for Java Plug-In Availability* on page 40
- *Logging Into the Web Manager for Regular Users* on page 41
- *Features of Regular Users' Windows* on page 42
- *Web Manager Menu Options for Regular Users* on page 43
- *Using the Devices Screen* on page 43
- *Accessing a Service Processor's Console* on page 45
- *Accessing a Device's Console* on page 45
- *Managing Power Through a Service Processor* on page 46
- *Running Reset on a Service Processor* on page 47
- *Viewing Sensor Data* on page 47
- *Viewing and Clearing Event Logs* on page 49
- *Accessing Native Features on a Service Processor* on page 50
- *Accessing the OnBoard Appliance Console (Web Manager)* on page 54
- *Managing Power Outlets on a Connected IPDU* on page 56
- *Configuring Your Password* on page 61

## 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 appliance must be known. Entering the IP address of the OnBoard appliance in the address field of one of the supported browsers listed in Table 3.1 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 appliance 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 appliance, contact your system administrator for help.

- A user account must be defined on the Web Manager. By default, the admin user has an account on the Web Manager. Any 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 workstation that has access to the network where the OnBoard service processor manager is installed and any browser (such as Internet Explorer 5.5 or above, Netscape 6.0 or above, Mozilla or Firefox) with a Java 2 plug-in.

**Table 3.1: 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 appliance and to SPs and other connected devices
- When displaying sensor data

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

Installing the Java 2 Runtime Environment (J2RE) Standard Edition software 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. See the <http://java.sun.com> website for more information.

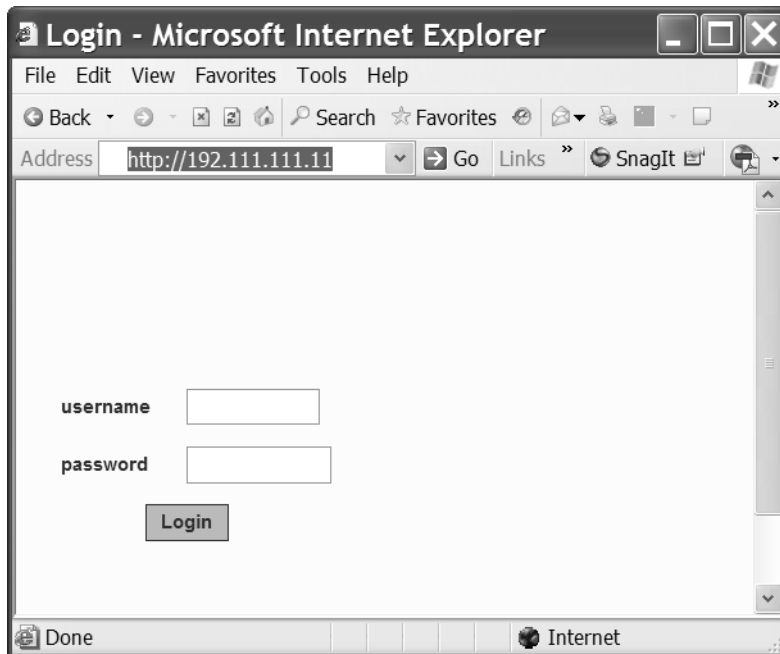
## Logging Into the Web Manager for Regular Users

Both authorized users and OnBoard appliance 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 appliance administrators can perform additional user and device configuration tasks through the Web Manager. See the Cyclades OnBoard Service Processor Manager Installer/Administrator Guide for details.

Figure 3.1 shows the login screen for the Web Manager that appears when the OnBoard appliance IP address is entered in a Microsoft Internet Explorer browser.



**Figure 3.1: Web Manager Login Screen**

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

See *Power Management Options on the OnBoard Appliance* on page 20 for more about how to use the Web Manager and *Prerequisites for Using the Web Manager* on page 40 for the required browsers, preparation and browser plug-ins needed for different types of access.

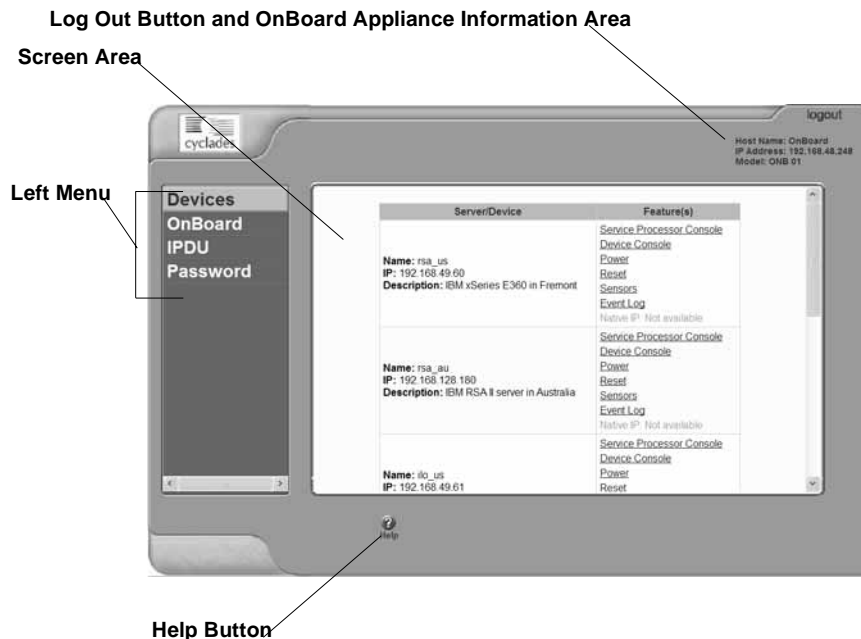
### To log into the Web Manager:

This procedure assumes you have a valid username and password and that your workstation has a network connection or a PPP connection to the OnBoard appliance.

1. Enter the IP address of the OnBoard appliance in a supported browser. See Table 3.1 on page 40 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

Figure 3.2 shows features of the Web Manager that appear when regular users log in.



**Figure 3.2: 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 3.2 to perform the tasks shown in the following table. Links are provided to where the tasks are described.

**Table 3.2: Device Access Menu Options**

Task	Where Described
Connect to a device	<i>Using the Devices Screen on page 43</i>
Connect to the OnBoard appliance	<i>Accessing the OnBoard Appliance Console (Web Manager) on page 54</i>
Manage outlets on an IPDU	<i>Managing Power Outlets on a Connected IPDU on page 56</i>
Change your password	<i>Configuring Your Password on page 61</i>

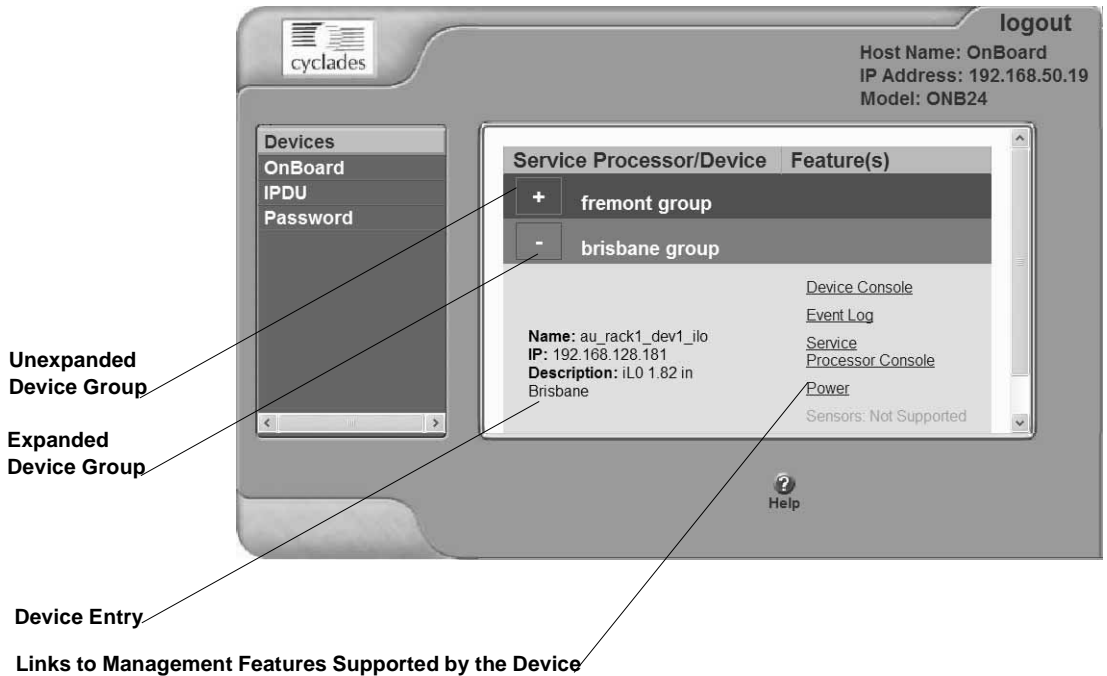
OnBoard appliance administrators see the same list of options shown in Table 3.2 under the administrator's Access tab. The Access tab is one of multiple tabs that are available on the Web Manager whenever an administrator logs in. Administrators can refer to the Cyclades OnBoard Service Processor Manager Installer/Administrator 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



**Figure 3.3: 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 and provides links to more information about accessing these features using the Web Manager.

**Table 3.3: Management Features Accessed Through the Web Manager**

Feature	Where Described
Service Processor Console	<i>Accessing a Service Processor's Console on page 45</i>
Device Console	<i>Accessing a Device's Console on page 45</i>
Power	<i>Viewing and Clearing Event Logs on page 49</i>
Reset	<i>Running Reset on a Service Processor on page 47</i>
Sensors	<i>Viewing Sensor Data on page 47</i>
Event Log	<i>Viewing and Clearing Event Logs on page 49</i>
Native IP	<i>Accessing Native Features on a Service Processor on page 50</i>



## 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 SP. A window running a MindTerm Java applet appears, as shown in Figure 3.4.



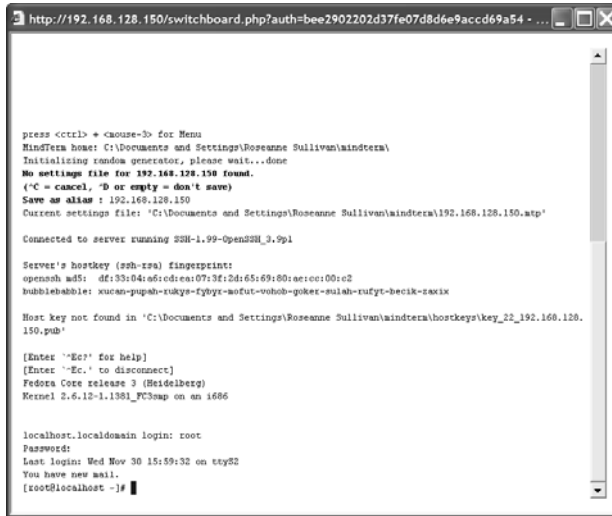
Figure 3.4: Service Processor Console Example

### To connect to an SP's console (Web Manager):

1. Log into the Web Manager.
2. From the list of devices that displays on the Devices screen, click the *Service Processor Console* link associated with the server whose console you wish to access. A MindTerm window displays with an SSH connection to the device.
3. If authentication is enabled for the SP, 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. Figure 3.5 shows an example terminal window with a connection to a device console on a Compaq Proliant server with an iLO type SP.



```

http://192.168.128.150/switchboard.php?auth=bee2902202d37fe07d8d6e9accdd69a54 - ...

press <ctrl> + <mouse> 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.atp'

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:aecce:00:c2
bubblebabble: xucan-pupsh-rukys-fybyr-mofut-vohob-poker-sulsh-rufyt-becik-zaxix

Host key not found in 'C:\Documents and Settings\Roseanne Sullivan\mindterm\hostkey\key_22_192.168.128.150.pub'

[Enter '^E*' for help]
[Enter '^C' to disconnect]
Fedora Core release 3 (Heidelberg)
Kernel 2.6.12-1.1381_FC3mp 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 3.5: Device Console Example

### To connect to a device's console (Web Manager):

1. Log into the Web Manager.
2. From the list of devices that displays on the Devices screen, click the *Device Console* link for the server or device console you wish to access. A MindTerm window displays with an SSH connection to the device.
3. If authentication is enabled for the device, log in 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 SP, as shown in Figure 3.6.

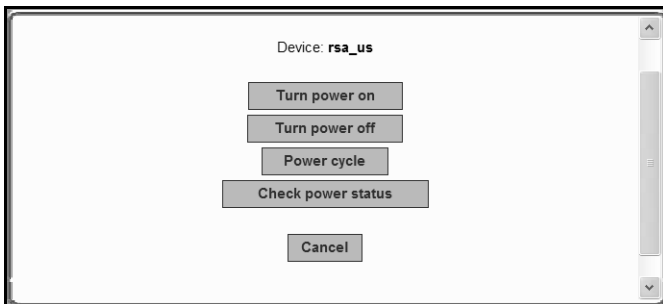


Figure 3.6: Power Web Manager Screen

If an SP supports both a hard power off and a soft power off option, the Turn power off and Power cycle buttons perform the hard power option. See Table 1.10 on page 10 for more information.

Clicking the *Check power status* button brings up a dialog box that shows the server's power status.

**To manage a server's power through its SP (Web Manager):**

1. Log into the Web Manager.
2. From the list of devices that displays on the Devices screen, click the *Power* link that is associated with the server for which you want to manage power.
3. To power up the server, click the *Turn power on* button.
4. To power down the server, click the *Turn power off* button.
5. 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 an SP has more than one type of reset option, the Reset command on the Devices screen performs the highest level of reset, which is the cold boot option (if available). See Table 1.10 on page 10 for more information.

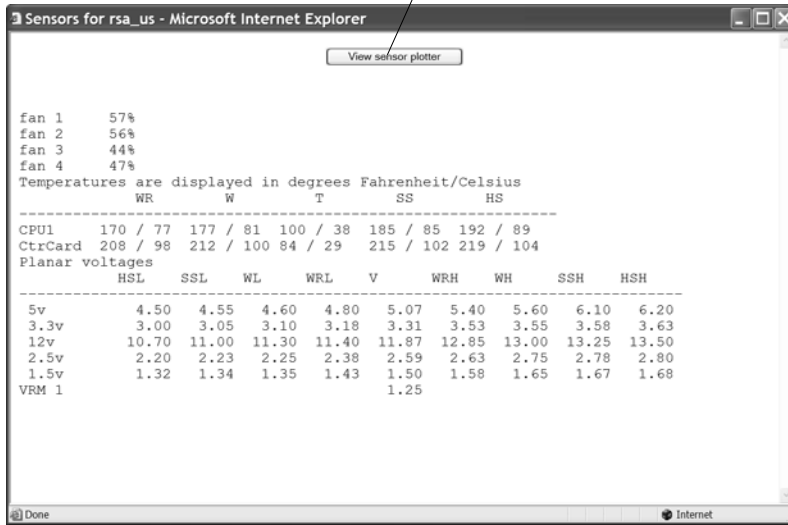
**To reset a server from an SP (Web Manager):**

1. Log into the Web Manager.
2. From the list of devices that displays on the Devices screen, click the *Reset* link that is associated with the server you want to reset.

## Viewing Sensor Data

Clicking the *Sensors* button on the Devices screen displays the SP's sensor plotting page. Figure 3.7 shows the Sensors screen that displays unformatted data.

**View Sensor Plotter Button**



**Figure 3.7: Example of Unformatted Sensor Data**

Clicking the *View sensor plotter* button in Figure 3.7 brings up a screen allowing you to view data from individual sensors on the server.

The sensor plotter page is shown in Figure 3.8 in the default graph format. Click the radio button next to the desired sensor, click *Display Graph* to display 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, which is user-configurable, is five seconds.

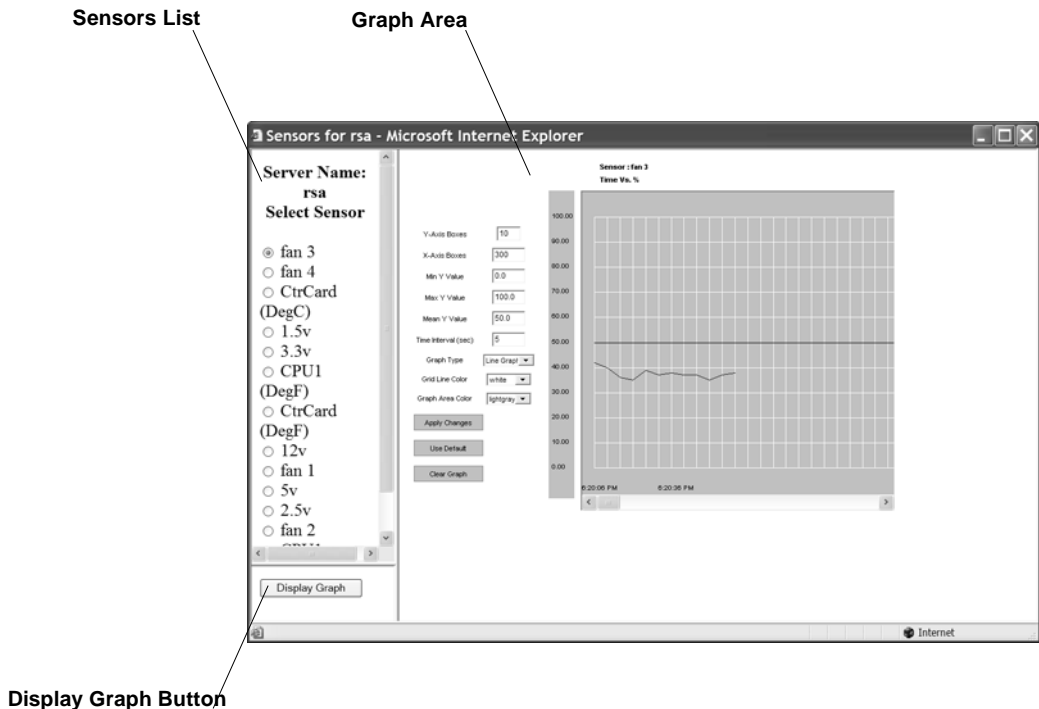


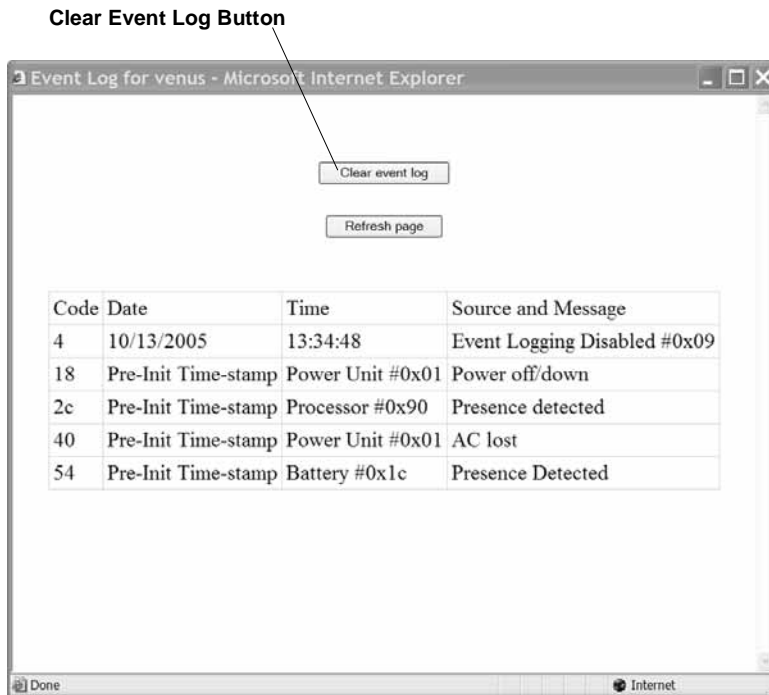
Figure 3.8: Sensor Plotter Page

### To view a server's sensor data from an SP (Web Manager):

1. Log into the Web Manager.
2. From the list of devices that displays on the Devices screen, click the *Sensors* link associated with the server sensors you wish 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 wish 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 SP resides. Event messages are sent by the SP when system management events are detected. The events may be being logged either by the SP or by the server. The Clear event log button appears at the top of the screen, as shown in Figure 3.9.



**Figure 3.9: Example Event Log Web Manager Screen**

Click the *Clear event log* button to clear the log.

## Accessing Native Features on a Service Processor

The Web Manager Access-Device screen displays the Enable Native IP option for an SP only if the following are all true:

- The user is authorized for native IP access to the SP
- The device supports native IP access
- A VPN connection (tunnel) exists between the user and the OnBoard appliance

If a VPN connection is not already up, the Access-Device screen displays a -Native IP: Not available message.

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 an SP or device, including a native web application or a native management application.

For more details, see *Accessing a Device's Native Features* on page 21.

The rules for bringing up the Web Manager to access the Devices screen differ 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 appliance'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 workstation's command line (which command to use depends on the operating system). In the command output, the IP address assigned to the connection appears in the lines following the words PPP adapter, as shown in the following.

```
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 22 for more details.

As shown in Figure 3.10, the words Enable | Disabled appear next to the Native IP option if a VPN connection exists, with the Enable link active.

Service Processor/Device	Feature(s)
<b>Name:</b> hpilo <b>IP:</b> 192.168.49.61 <b>Description:</b>	<a href="#">Service Processor Console</a> <a href="#">Device Console</a> <a href="#">Power</a> <a href="#">Reset</a> <a href="#">Sensors</a> <a href="#">Event Log</a> Native IP: <a href="#">Enable</a>   <b>Disabled</b> <a href="#">Go to native web interface</a>

**Figure 3.10: Enable | Disabled Links for the Native IP Option**

Clicking the Enable link enables native IP and makes the Disable link active. The Go to native web interface link appears, as shown in Figure 3.11.

Service Processor/Device	Feature(s)
<b>Name:</b> hpilo <b>IP:</b> 192.168.49.61 <b>Description:</b>	<a href="#">Service Processor Console</a>
	<a href="#">Device Console</a>
	<a href="#">Power</a>
	<a href="#">Reset</a>
	<a href="#">Sensors</a>
	<a href="#">Event Log</a>
	Native IP: <b>Enabled</b>   <a href="#">Disable</a>
	<a href="#">Go to native web interface</a>

**Figure 3.11: Go to native web interface Link**

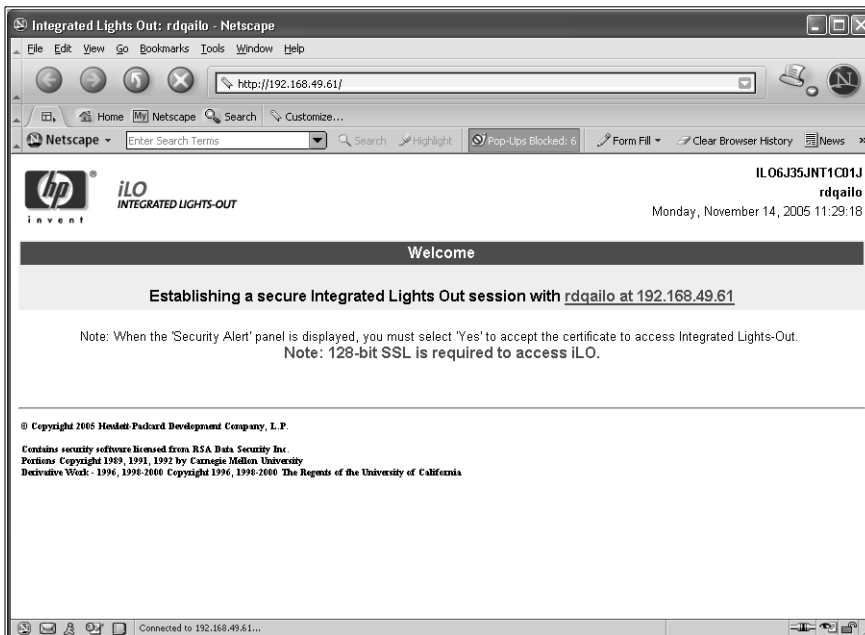
The authorized user can then do one of the following:

Click the link to launch a browser that brings up the native web application on the SP.

-or-

Launch an SP management application from the user's remote workstation.

Figure 3.12 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.



**Figure 3.12: Example HP iLO Native Web Interface**

**CAUTION:**When finished with SP 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.



The following procedures assume the listed prerequisites:

- You are running Windows NT on your remote workstation.
- The OnBoard appliance administrator has done all of the following:
  - Authorized your OnBoard appliance user account for PPTP access
  - Provided you with the PPTP password if it is different from your OnBoard appliance password
  - Enabled the PPTP service
  - Configured the OnBoard appliance for VPN PPTP connections
  - Provided you with an IP address that was assigned while configuring VPN PPTP access on the OnBoard appliance

**To create a PPTP VPN connection profile on Windows:**

1. Login in as an administrator on Windows NT.
2. From the start menu, select *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. Enter an IP address for the *VPN Server Selection* on the next dialog that appears.

---

**NOTE:** The IP address is the one assigned to the public interface of the OnBoard appliance.

---

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 workstation to the OnBoard appliance.

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, enter the IP address that is assigned to the public interface into a browser. This brings up the Web Manager.

-or-

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

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

or-

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

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

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

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

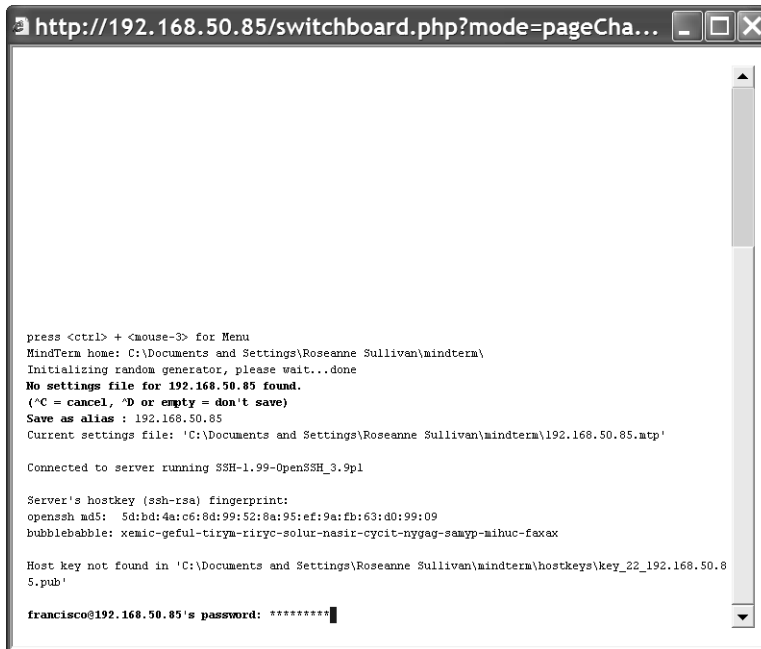
- c. Enter the PPTP IP address in a browser to bring up the Web Manager.
3. Log into the Web Manager and select the *Devices* menu option.
4. From the list of devices that displays on the Devices screen, click *Enable* next to the Native IP link for the device on which you want native IP access.

The Go to native web interface link becomes active.

5. Click the *Go to native web interface* link to launch a browser that brings up the native web application on the SP.
6. From your local workstation, launch a previously-installed SP management application for the server, if desired.
7. Click the *Disable* link.

## Accessing the OnBoard Appliance Console (Web Manager)

Click the *OnBoard* option on the Web Manager menu, then click the *Connect to OnBoard* button to bring up a window running a MindTerm Java applet with an SSH connection to the OnBoard appliance, as shown in Figure 3.13.



```
http://192.168.50.85/switchboard.php?mode=pageCha...

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
bubblebabbie: xemic-geful-tiryu-riryu-solur-nasir-cycit-nygag-samyp-mihuc-faxax

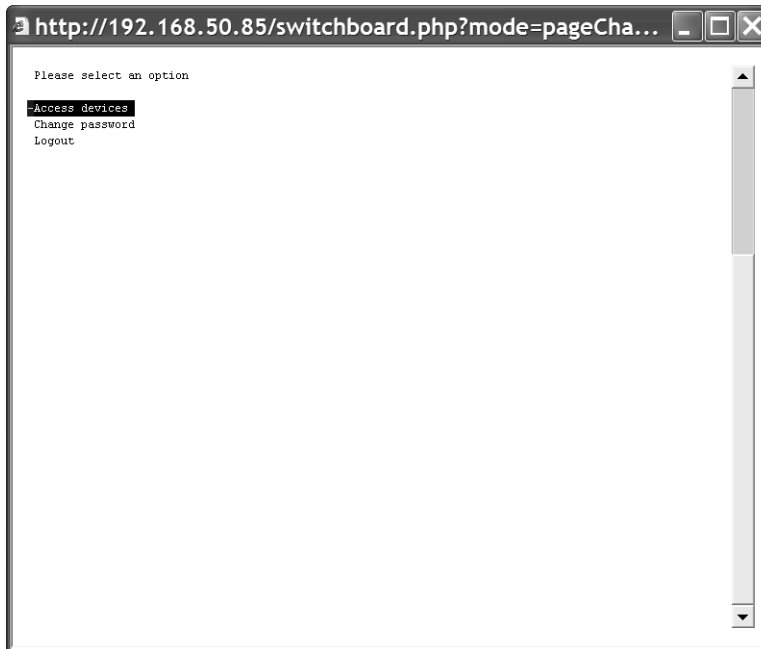
Host key not found in 'C:\Documents and Settings\Roseanne Sullivan\mindterm\hostkeys\key_22_192.168.50.85.pub'

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

**Figure 3.13: OnBoard Appliance Console Login Screen**

Regular users by default are not able to access the shell and they cannot do anything on the console that they could not do from the Web Manager menu options. Users are encouraged to use the Web Manager options instead of going through the Web Manager to use 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.



**Figure 3.14: User Menu When Connected to the Console**

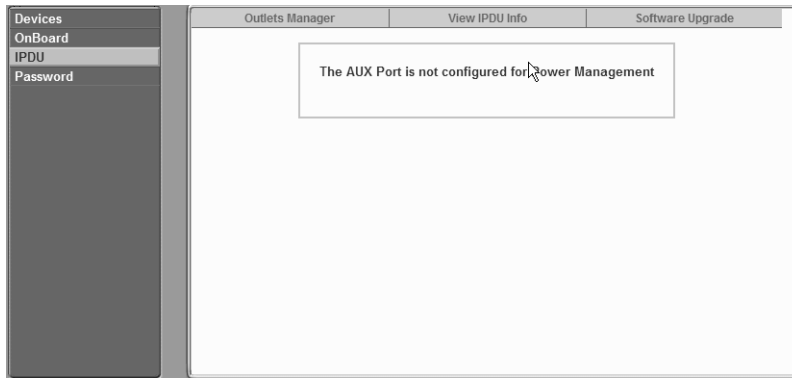
For information about what the administrative user can do on the OnBoard appliance console, see the Cyclades OnBoard Service Processor Manager Installer/Administrator Guide.

**To access the OnBoard appliance's console (Web Manager):**

1. Log into the Web Manager.
2. Click the *OnBoard* option in the left menu. A terminal window displays and establishes a console connection to the OnBoard appliance.
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

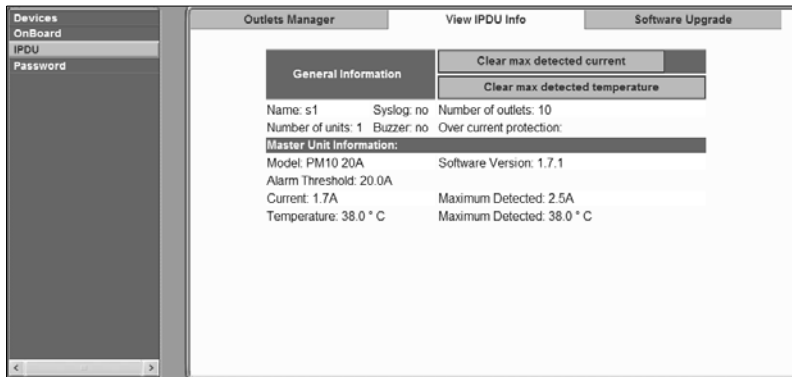
Clicking the *IPDU* option on the Access menu brings up the message shown in Figure 3.15 if the AUX port has not been configured for IPDU power management. Contact the OnBoard appliance administrator for help if you see this message.



**Figure 3.15: AUX Port Not Configured Error Message**

Clicking the *IPDU* option on the Access menu when the AUX port has been configured for IPDU power management brings up the Outlets Manager, the View IPDUs Info and the Software Upgrade tabs, as shown in Figure 3.16. For more information, see *Using the Outlets Manager tab to power up and down and check power status* on page 57 and *Viewing IPDU information* on page 59.

**NOTE:** The regular user can view the Software Upgrade screen but cannot do anything with it.



**Figure 3.16: IPDU Tabs**

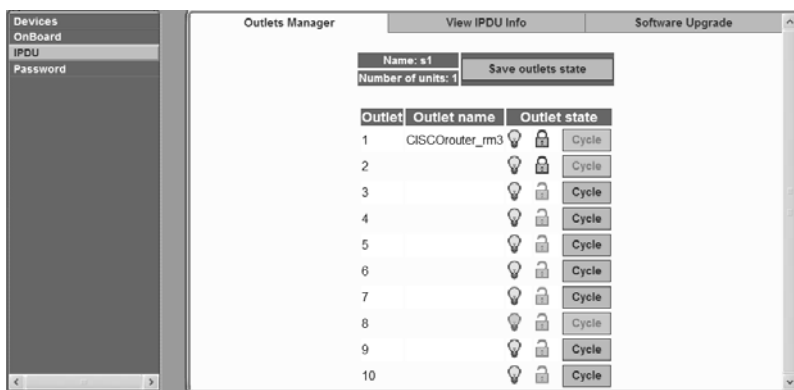
## Using the Outlets Manager tab to power up and down and check power status

If a regular user clicks the *Outlets Manager* tab under the Access-IPDU menu option, the message shown in Figure 3.17 appears if the user is not authorized to manage power on any outlets or if the OnBoard appliance cannot detect an IPDU connected to the AUX port. Contact the OnBoard appliance administrator for help if you receive this message.



**Figure 3.17: IPDU Access Failed Message from Outlets Manager**

If a regular user clicks the *Outlets Manager* tab under the Access-IPDU menu option, the screen displays a list of all the outlets the user is authorized to manage. If an administrative user clicks *Outlets Manager* under the Access-IPDU menu option, all the power outlets on all connected IPDUs are listed, as shown in Figure 3.18.

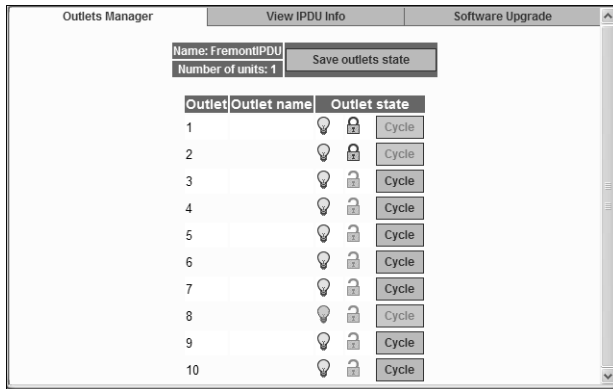


**Figure 3.18: Access-IPDU-Outlets Manager Screen**

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

- Cycle power
- 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 a locked outlet. 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.



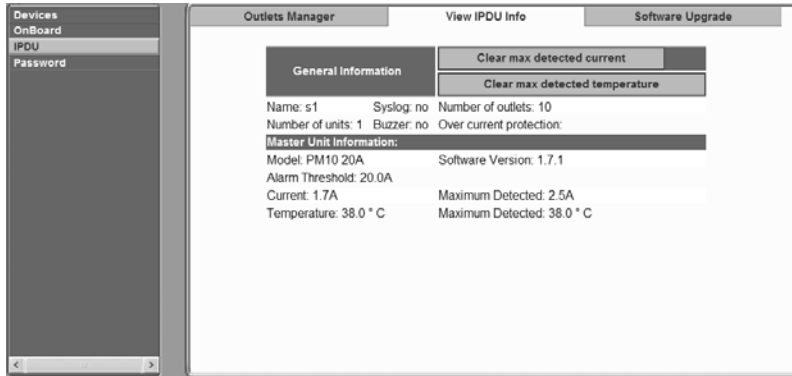
**Figure 3.19: Outlets Manager Outlets State Close-up**

### To manage power outlets on a connected IPDU:

1. Log into the Web Manager.
2. Click the *IPDU* left menu option. 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 cycle power, 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 administrative user selects *Access-IPDU-View IPDU Info*, the View IPDU Info screen appears.



**Figure 3.20: View IPDU Info Screen**

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

**Table 3.4: Information on the View IPDU Info Screen**

Field	Description
Name	Administrator-configured name or the default (s1), which is assigned to the AUX port.
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.
Number of outlets	Total number of outlets on all connected IPDUs.
Buzzer	Whether a buzzer has been configured to sound when a specified alarm threshold is exceeded.
Syslog	Whether syslogging has been configured for messages from this IPDU.
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).

You can view the following information underneath the name of each IPDU (under Unit Information).

**Table 3.5: IPDU Information Under Unit Information**

Field	Description
Model	IPDU model number
Software Version	IPDU firmware version
Alarm Threshold	Number of amperes that triggers an alarm or syslog message if it is reached
Current	Current level on the IPDU



**Table 3.5: IPDU Information Under Unit Information (Continued)**

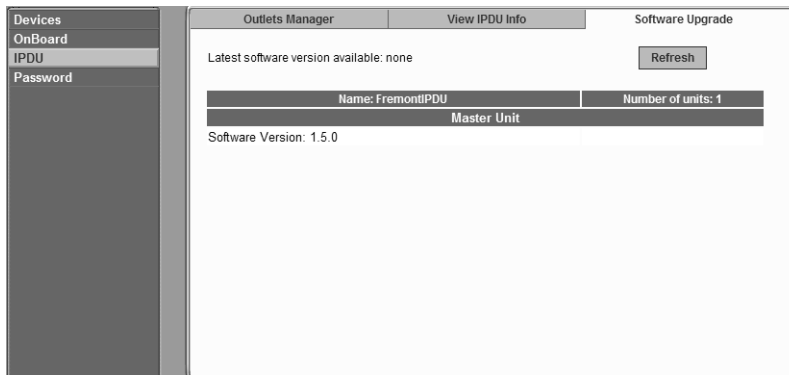
Field	Description
Maximum Detected	Maximum current detected
Temperature	Temperature on the IPDU (only available on selected models that have temperature sensors)
Maximum Detected	Maximum temperature detected

**To view IPDUs information:**

1. Log into the Web Manager.
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

An administrative user can upgrade software on a connected IPDU from this screen. Regular users can use this screen only to view the software version.

**Figure 3.21: 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 Figure 3.22.



**Figure 3.22: Password Screen**

---

**NOTE:** Your password cannot exceed 30 characters.

---

**To change your password:**

1. Log into the Web Manager.
2. Click the *Password* option in the left menu. The Password screen appears.
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 to save the changes in memory.

## Appendix A: MindTerm Applet Reference

MindTerm is an SSH client that includes an integrated xterm/vt100 terminal emulator and that runs as a Java applet within a browser window. 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 workstation and the console.

This appendix describes the topics in the following list.

- *Java plug-in requirements for MindTerm* on page 63
- *Customizing MindTerm* on page 63
- *Example MindTerm window* on page 63
- *MindTerm terminal menu options* on page 64
- *Using hotkeys during console sessions* on page 68

### Java plug-in requirements for 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 40.

### Customizing MindTerm

MindTerm saves session settings in a folder that it creates in the user's home folder on the user's workstation. For example, in a Windows system, the folder is created in C:\Documents and Settings\username\mindterm.

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

- Resize the window.
- 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.

---

- Re-use saved settings like the scroll buffer size

### Example MindTerm window

Figure A.1 shows an example window that appears when the root user is connected to the console of an SP with an alias of rdqailo. The same terminal window appears whether the connection is being made to the console of an OnBoard appliance, an SP, a server or another type of device.



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. Figure A.2 shows the terminal menu that displays if you enter **Ctrl**+mouse right-click and then drag the cursor to pull down the File menu options.

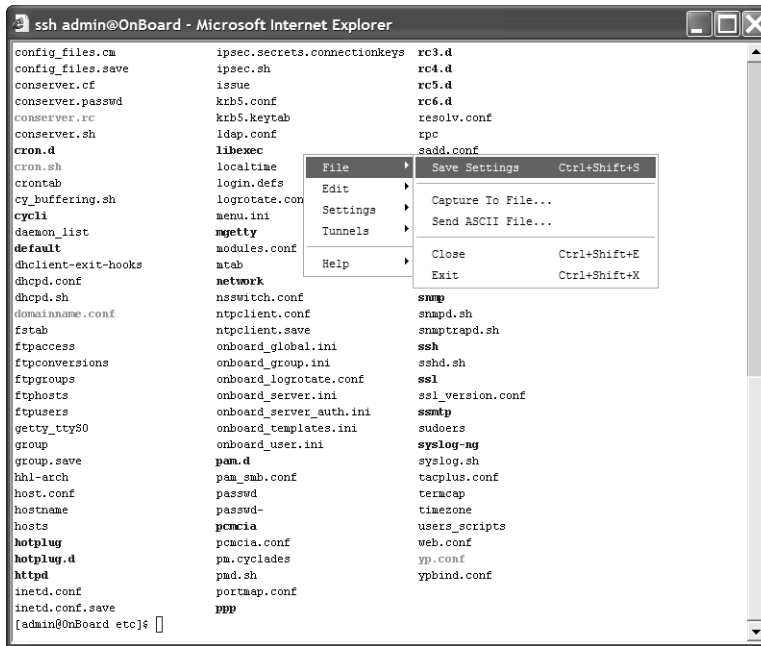


Figure A.2: Terminal Menu

The following table describes the terminal menu options.

Table A.1: Console Session Terminal Menu Options

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.
	Close (Ctrl+Shift+c)	Closes the current window. <b>NOTE:</b> 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.

**Table A.1: Console Session Terminal Menu Options (Continued)**

1st-level Option	2nd-level Option	Description
<b>File (continued)</b>	Exit (Ctrl+Shift+x)	Closes the window without logging out. <b>NOTE:</b> Closing windows without logging out aborts the SSH connection. Enter the <code>exit</code> command in the terminal before using this option.
<b>Edit</b>	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 scrollbar buffer and in the terminal.
	Find (Ctrl+Shift+f)	Displays the Find dialog box, which can be used to search the scrollbar buffer and the currently-displayed text for strings.
	Clear Screen	Clears the screen and positions the cursor at the top left corner.
	Clear Scrollback	Clears the contents of the scrollbar buffer.
	VT Reset	Resets terminal settings to the defaults.
<b>Settings</b>	Connection	Displays a dialog box for setting SSH preferences. General: <ul style="list-style-type: none"> <li>• Server</li> <li>• Username</li> <li>• Authentication</li> </ul> Proxy: <ul style="list-style-type: none"> <li>• Proxy type</li> <li>• Server</li> <li>• Port</li> <li>• Authentication</li> <li>• Username</li> <li>• Password</li> </ul>

**Table A.1: Console Session Terminal Menu Options (Continued)**

1st-level Option	2nd-level Option	Description
<b>Settings (continued)</b>	<b>Connection (continued)</b>	Security <ul style="list-style-type: none"> <li>• Protocol</li> <li>• Host key type</li> <li>• Cipher</li> <li>• Mac</li> <li>• Compression</li> </ul> Features <ul style="list-style-type: none"> <li>• X11 forward</li> <li>• Local display</li> <li>• Send keep-alive</li> <li>• Interval</li> </ul>
	Terminal (Ctrl+Shift+t)	Displays a dialog box for setting terminal characteristics. General: <ul style="list-style-type: none"> <li>• Terminal type</li> <li>• Columns</li> <li>• Rows</li> <li>• Encoding</li> <li>• Font</li> <li>• Size</li> <li>• Scrollback buffer</li> <li>• Scrollback buffer position</li> </ul> Colors <ul style="list-style-type: none"> <li>• Foreground color</li> <li>• Background color</li> <li>• Cursor color</li> </ul> Misc <ul style="list-style-type: none"> <li>• Paste button</li> <li>• Select delimiter (characters for click-selection)</li> </ul>
		VT 1 <ul style="list-style-type: none"> <li>• Enable Passthrough Print</li> <li>• Copy &lt;cr&gt;&lt;nl&gt; line ends</li> <li>• Copy on select</li> <li>• Reverse Video</li> <li>• Auto Wraparound</li> <li>• Reverse Wraparound</li> <li>• Insert mode</li> <li>• Auto Linefeed</li> <li>• Scroll to Bottom On Key Press</li> </ul>

**Table A.1: Console Session Terminal Menu Options (Continued)**

1st-level Option	2nd-level Option	Description
<b>Settings</b> (continued)		VT 2 <ul style="list-style-type: none"> <li>• Scroll to Bottom On Tty Output</li> <li>• Visible Cursor</li> <li>• Local Echo</li> <li>• Visual Bell</li> <li>• Map &lt;CTRL&gt;+&lt;SPC&gt; to ^@</li> <li>• Local PgUp/PgDown</li> <li>• Use ASCII for line draw</li> <li>• Backspace sends: del, bs, erase</li> <li>• Delete sends: del, bs, erase</li> </ul>
	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.
<b>Tunnels</b>	Setup	Displays a dialog box listing any previously configured tunnels. Clicking the Add button displays a dialog box for configuring a tunnel. <p>Type</p> <ul style="list-style-type: none"> <li>• Local</li> <li>• Remote</li> </ul> Bind address <ul style="list-style-type: none"> <li>• localhost</li> <li>• all (0.0.0.0)</li> <li>• ip</li> </ul> Bind port Dest. address Dest. port Plugin <ul style="list-style-type: none"> <li>• None</li> <li>• ftp</li> </ul>
<b>Help</b>	About MindTerm	Displays a dialog box with information about the Mind Term build date, version, platform you are running.

## Using hotkeys during console sessions

MindTerm hotkeys have two components: an escape sequence and a command key. The escape sequence for all the console session hotkeys is **Ctrl+e+c** (shown as **^Ec**). As shown in Figure A.1,



the applet displays hotkey combinations that you can use to get help (**^Ec?**) or disconnect (**^Ec.**). The following table shows all the available hotkeys, which are entered after the escape sequence.

**Table A.2: Hotkeys Available During Console Sessions**

Key	Action	Key	Action
.	Disconnect	a	Attach read/write
<b>b</b>	Send broadcast message	c	Toggle flow control
<b>d</b>	Down a console	e	Change escape sequence
<b>f</b>	Force attach read/write	g	Group info
<b>i</b>	Information dump	l?	Break sequence list
<b>10</b>	Send break per config file	l1-9	Send specific break sequence
<b>o</b>	(Re)open the tty and log file	p	Replay the last sixty (60) lines
<b>r</b>	Replay the last twenty (20) lines	s	Spy read-only
<b>u</b>	Show host status	v	Show version info
<b>w</b>	Who is on this console?	x	Show console baud info
<b>z</b>	Suspend the connection	Enter	Ignore/Abort command
<b>?</b>	Print this message	^R	Replay the last line
<b>\too</b>	Send character by octal code		

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

## Appendix B: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

**To resolve an issue:**

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Check our web site at [www.avocent.com/support](http://www.avocent.com/support) to search the knowledge base or use the online service request.
3. Call the Avocent Technical Support location nearest you.

# INDEX

## A

- AC devices 20
- Add and route IPSec VPN option 32
- admin user
  - described 5
  - capabilities 4
- administrative users
  - accessing the OnBoard appliance 3
  - authorizations defined 4
  - creating 4
  - defined 4
- administrators 16, 41
- AH authentication protocol 34
- authenticated users 5
- authentication
  - overview 13
  - OnBoard appliance as the single source for 2
- authentication methods
  - different for OnBoard appliance than for devices 3
  - requirement for SSH tunnels 29
- authentication servers 13
- authorizations
  - controlled by security profiles 13
  - for access control 3
  - OnBoard appliance as a single source for 2
  - types 5
- authorized users
  - defined 4
  - accessing the OnBoard appliance console 16
  - accessing the Web Manager 3, 41

- responsibilities and default password 5
- autodetect modem and phone card configuration option 20
- AUX ports with IPDUs connected 20

## B

- browsers
  - accessing a native web application 22, 29
    - from a remote browser 37
    - through an SSH tunnel 30
    - through the Web Manager 36
  - accessing the Web Manager through 41
  - accessing Web Manager
    - methods for 4
  - enabling native IP access through 35, 51
  - MindTerm applet running in 16
  - prerequisites for console access and for sensor data display 40
  - supported 40
  - using
    - HTTPS for secure access through 3
    - the IPSec IP address 54
  - using to
    - bring up a native web application 52
    - test packet exchange between user workstation and appliance 35

## C

- callback
  - accessing the Web Manager through 41
  - configuring at the remote caller's end 20
- Caution about disabling native IP access 31

- CDMA PCMCIA card 20
- clearsel device management command 19
- command templates customizing for access to devices without service processors 6
- commands
  - available to different user types 5
  - cycli 4
  - device management 19
  - ifconfig 32, 36, 54
  - ipconfig 32, 36, 54
  - ssh 15
    - device management commands 19
  - sudo 4
  - telnet 13
- connected devices 3, 40
- console
  - access by the admin user 4
  - logins by root 5
  - logout through user menu 17
  - port 16
  - three ways to access 16
- custom security profile with the override authorizations feature set 5
- Cyclades PM IPDUs
  - accessing through Web Manager 3
  - power management options through 20
- cycli utility, who can use 4, 5

## D

- dedicated Ethernet ports 2, 14
- Dell DRAC 21
- DEVCONSOLE 6
- device console 5
- device management
  - actions 15, 18, 19

- commands 15, 18
- devices
  - access control 1, 3
  - accessing 40
  - authorizing access to 4–5
  - list for authorized users 17
  - list in onbdshell menu 18
  - management features 5
  - Web Manager screen 43
- DHCP effects on IP address 40
- dial-ins
  - example 3
  - for accessing the Web Manager 41
  - options 20
- DRAC device type
  - and management features 6
  - and native web application access 21

## E

- encrypted communications 15
- ESP authentication protocol 34
- Ethernet ports of connected devices, illustrated 2
- event log management 5
- expect scripts, options for customizing 6
- external modems 3

## F

- FTP
  - enabling in a security profile 14
  - when it is not available 14

## G

- GSM PCMCIA card 20

## H

- host route 32

HP iLO 21

## HTTP

- availability as an access method 22
- port number to access 29
- security profiles' control of availability 14
- using for Web Manager access 41

## HTTPS

- port number to access 29
- security profiles' control of availability 14
- using for Web Manager access 41
- using to protect communications 3

## I

IBM RSA II 21

ICMP 14

ifconfig command 32, 36, 54

iLO devices

- management features supported 6
- native Web access on 21

information users need 22

Internet access to the OnBoard appliance 15

IP addresses 2

ipconfig command 32, 36, 54

IPDUs

- accessing through Web Manager 3
- power management option 20
- power outlets a user is authorized to manage 22
- Web Manager screen 20

IPMI 1.5 devices

- supported management features 6

IPMI protocols 21

IPSec

- client on user's workstation 35
- service in security profiles 14

VPN

authentication information required 34

making connections 30

routing requirements 32

tunnel, tasks for creating 22

## J

Java plug-in required for MindTerm 16

## L

LAN 2

Linux command line, availability to OnBoard user types 4

local port forwarding for SSH tunnel creation 29

login shell 17

logins

authentication requirements for 13

OnBoard appliance, supported access methods 15

Web Manager prerequisites 40

## M

management

actions 3

features

access control 3

availability on SPs 6

configuring access to 4

user authorizations for 5

OnBoard appliance as a single point for 2

services on SPs 2

managing power 2, 3, 41

MindTerm applet

when a user connects to a console 16

reference 63–69

modems

access option 15

- optional external 20
- remote access through 3
- supported for OnBoard appliance access, overview 20

## N

- native IP
  - access
    - configuring through IPSec VPN tunnel 35
    - prerequisite tasks for creating tunnels 22
    - to devices without service processors 14
  - tasks for enabling 31
  - user authorization type for 5
  - VPN connection requirements for 34
- native management applications
  - defined 21
  - accessing 37
  - options for accessing 8
  - tasks for accessing 22
- native web applications
  - introduction 21
  - accessing through an SSH tunnel 29
  - options for accessing 8
  - tasks for accessing 22
- native\_ip\_off device management command 19
- native\_ip\_on device management command 19
- network
  - local, accessing the OnBoard appliance through 15
  - private 3
  - public 2, 3
- network mask 33
- network route 32
- nexthop 32

## O

- onbdshell
  - list of devices 17–18
  - submenu
    - management commands 18
    - device console management command 7
    - native IP management commands 8
    - power management command 9
    - reset command 10
    - SEL management command 8
    - sensor management command 12
    - SP console management command 6
- OnBoard appliance
  - command line access 15
  - console, access by administrative users 4
  - options for accessing 15
- OTP
  - authentication method for dial-ins 20
  - passwords, obtaining and using 38
- outlets, power 15
- override authorization 5
- P**
- passwords
  - authentication 13
  - changing 3
  - for Web Manager logins 41
  - managing 15
  - user shell Change Password option 17
- PCMCIA cards
  - modem, option for OnBoard appliance access 3
  - supported for dial-ins 20
- phone cards 20
- PM IPDUs, power management options through 20
- port numbers, common, for accessing services on

- devices 29
  - power management
    - IPDU 20
    - OnBoard appliance options for 2
    - options 20
    - service processor 20
    - user authorization type 5
  - powercycle device management command 19
  - poweroff device management command 19
  - poweron device management command 19
  - powerstatus device management command 19
  - PPP
    - access prerequisites 20
    - accessing Web Manager through 41
  - PPTP
    - assigned OnBoard appliance IP address 33
    - interface IP address 54
    - password 33
    - service 14
    - VPN
      - connections 30
      - disabling when done 22
      - routing requirements 32
      - tunnel, tasks for creating 22
  - prerequisites
    - for creating a VPN tunnel 31
    - for creating PPTP VPN tunnels 53
    - for dialing-in using PPP 20
    - for using the Web Manager 40
  - private Ethernet ports 2
  - private network 3
  - private subnets
    - configuring PPTP VPN to communicate with more than one 33
    - routing to 33
  - proxied communications 3
  - public network 2, 3
- ## R
- regular user accounts 4
  - reset device management command 19
  - root user responsibilities 4
  - routing requirements for VPN connections 32
  - RPC 14
  - RSA II devices
    - management features on 6
  - RSA public keys 34
- ## S
- secure connection 3
  - secure path 1
  - security features, introduction 2
  - security policies 3
  - security profiles
    - user introduction 13
    - effect on authorizations 13
    - for access control 3
  - SEL
    - options for viewing 8
    - sel device management command 19
  - sensors 5
    - monitoring overview 10–12
    - sensors device management command 19
  - serial over LAN 14
  - server-management services 2
  - servers 2
  - service processors
    - See SPs*
  - services
    - controlled by security profiles 13

- when unavailable 14
- shared secret 34
- shell 5
- single source 2
- SNMP
  - agents 21
  - in security profiles 14
  - using to access events 14
  - what to do if access unavailable 14
- SoL 14
- sconsole device management command 19
  - accessing a native management application 37
- SPs
  - defined 2
  - accessing the console of 5
  - dedicated Ethernet ports on 2
  - management commands 15
  - power management 20
  - types of user authorizations for 5
- SSH 3
  - example of a disabled service 22
  - in MindTerm 16
  - requirement for managed devices 14
  - service controlled by security profiles 14
  - using to protected communications on public network 3
- SSH clients
  - accessing OnBoard appliance console 17
  - connecting to OnBoard appliance 15
  - for different platforms 29
- ssh command
  - on the OnBoard appliance 15
  - device management commands 19
- SSH tunnel
  - creating 29

- requirement for native IP access to a device 21
- tasks for creating 22
- static route 32
- sudo command 4
- system event log
  - See SEL* 8

## T

- tasks for creating secure tunnels 22
- TCP port number for creating an SSH tunnel 29
- Technical support 70
- Telnet 14
  - telnet command 13
- terminal emulator 20
- tunnels
  - required for native IP access to a device 21
  - tasks for creating 22

## U

- username for authentication 13
- users
  - types and authorizations, defined 4
  - account types 4
  - accounts 40
  - authorized 41
  - default shell 17
  - information they need 22
  - table of types, responsibilities, and default passwords 5
- /usr/bin/onbdshell shell 18
- /usr/bin/rmenush login shell introduction 17

## V

- virtual IP addresses, introduction 3
- virtual media 21
- virtual network, creating a network route to during



- PPTP VPN tunnel creation 36

## VPN connections

- configuring a profile 33
- duration requirements 31
- making using IPsec or PPTP 30

## VPN tunnel

- accessing native SP/device features through 36
- creating with IPsec 35
- requirement for native IP access to a device 21
- tasks for creating 22

## **W**

### Web Manager

- introduction 4

- accessing OnBoard console through 17

- authentication requirements 13

- prerequisites for using 40

- regular users

- features 43

- option for accessing OnBoard appliance,  
connected devices and power 15

- who can access 5, 41

- web server providing native web access to a  
connected SP 21

## Windows

- NT operating system 33

## **X**

- xterm/vt100 terminal emulator 16







**Avocent®**

The Power of Being There®

For Technical Support:

[www.avocent.com/support](http://www.avocent.com/support)

Avocent Corporation  
4991 Corporate Drive  
Huntsville, Alabama 35805-6201 USA  
Tel: +1 256 430 4000  
Fax: +1 256 430 4031

Avocent Asia Pacific  
Singapore Branch Office  
100 Tras Street, #15-01  
Amara Corporate Tower  
Singapore 079027  
Tel: +656 227 3773  
Fax: +656 223 9155

Avocent Canada  
20 Mural Street, Unit 5  
Richmond Hill, Ontario  
L4B 1K3 Canada  
Tel: +1 877 992 9239  
Fax: +1 877 524 2985

Avocent International Ltd.  
Avocent House, Shannon Free Zone  
Shannon, County Clare, Ireland  
Tel: +353 61 715 292  
Fax: +353 61 471 871

Avocent Germany  
Gottlieb-Daimler-Straße 2-4  
D-33803 Steinhagen  
Germany  
Tel: +49 5204 9134 0  
Fax: +49 5204 9134 99

590-662-501A