Oracle® Communications

PMAC User's Guide

Release 6.6

E93272

July 2018

ORACLE

Oracle Communications PMAC User's Guide, Release 6.6

E93272

Copyright © 2008, 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

This documentation is in preproduction status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Contents

1 Introduction

Revision History 1-1
Documentation Admonishments 1-1
Locate Product Documentation on the Oracle Help Center Site 1-1
Customer Training 1-2
My Oracle Support 1-2
Emergency Response 1-2

2 Accessibility

Documentation Accessibility 2-1
Access to Oracle Support 2-1
Accessibility Features 2-1

3 PMAC Overview

PMAC user interface 3-1
Cabinet management 3-2
Enclosure management 3-2
Blade management 3-3
Rack Mount Server Management 3-3
Inventory 3-4
Software installation and upgrade 3-5
Storage device configuration 3-6
Back up PMAC server data 3-6
PMAC Application Configuration 3-6
Administration 3-7
Status and Manage 3-7

4 PMAC User Interface

Components of the PMAC GUI 4-1
Supported browsers 4-5
Browser configuration 4-5
PMAC GUI main menu options 4-5

Accessing the PMAC GUI 4-7
Logging out of the PMAC GUI 4-8
Important note about logging out of the PMAC GUI 4-8
GUI work area 4-8
General Options administration page 4-8
Customizing the splash page welcome message 4-12
Changing the site name on the GUI monitor bar 4-12

5 Inventory Information

System inventory information 5-1
Cabinet inventory 5-1
RMS inventory 5-2
Enclosure inventory 5-8
Bay information 5-13
FRU information 5-22
Software inventory information 5-24
Software Inventory page 5-24
Viewing the software inventory 5-29

6 Background Tasks

Overview 6-1
Add Enclosure background task 6-1
Add Enclosure background task steps 6-2
Add Image background task 6-2
Add Image background task steps 6-3
Backup PMAC background task 6-4
Backup PMAC background task steps 6-4
Configure Storage background task 6-5
Configure Storage background task steps 6-5
Install OS background task 6-6
Install OS background task steps 6-7
Upgrade background task 6-7
Install/Upgrade App background task steps 6-8
Transfer ISO Image background task 6-9
About deleting a background task 6-9
Reconfigure and Initialize background task 6-9
Reconfigure and Initialization background task steps 6-9
Background Task Monitoring page 6-10
Background Task Monitoring elements 6-10
Monitoring background tasks 6-13
About deleting a background task 6-14
Deleting a background task 6-14
Deleting completed background tasks 6-14

Deleting all failed background tasks 6-15

7 Software Installation

Installing the operating system 7-1
Software Install - Select Image page 7-2
Installing/upgrading an application, or upgrading the OS 7-4
Software Upgrade - Select Image page 7-5
Transferring an ISO image 7-7
Image Transfer - Select Image page 7-8
Software image management 7-10
Viewing software images 7-10
Manage Software Images page 7-11
Adding a software image 7-11
Editing a software image's description 7-12
Deleting a software image 7-13

8 Virtual Machine Management

Tekelec Virtual Operating Environment (TVOE) introduction 8-1
Virtual Machine Management page 8-1
Virtual Machine Management elements 8-1
Changing the VM guest power state 8-3
Setting initial power state for a new VM guest 8-3
View VM Host work area 8-3
Viewing VM host information 8-6
View VM Guest work area 8-6
Viewing VM guest information 8-12
Create VM Guest work area 8-12
Creating VM guest information 8-15

9 PMAC Application Processes

About the Sentry process 9-1
What are the PMAC application processes? 9-1
Sentry Process Control page 9-2
Sentry Process Control elements 9-2
Viewing status of PMAC application processes 9-4
Restarting Sentry 9-4
About automatically restarting failed processes 9-4
Automatically restarting failed processes 9-4
About setting Sentry to ignore failed processes 9-5
Setting Sentry to ignore failed processes 9-5

10 Working with Hardware

System configuration data 10-1

System Configuration page ... 10-1
Viewing system configuration data ... 10-2
Cabinets ... 10-2
Configure Cabinets page ... 10-2
Adding a cabinet ... 10-3
Deleting a cabinet ... 10-3
Enclosures ... 10-4
Configure Enclosures page ... 10-4
Adding an enclosure ... 10-8
Editing the enclosure OA IP addresses ... 10-8
Viewing OA IP addresses ... 10-9
Deleting an enclosure ... 10-9
Onboard Administrator ... 10-10
RMS ... 10-10
Configure RMS page ... 10-11
Blades ... 10-15
Storage devices ... 10-16
Configuring the storage devices ... 10-16
Clearing or deleting the storage configuration ... 10-27
Configure Storage page ... 10-36
Configure storage recovery ... 10-36

11 Other Tasks

Logging onto the PMAC server ... 11-1
Uploading files to PMAC via sftp ... 11-1
Backing up PMAC server data ... 11-2
Manage Backup page ... 11-2
Perform Backup page ... 11-3

12 PMAC Initialization and Configuration

PMAC initialization and configuration overview ... 12-1
PMAC initialization overview ... 12-1
PMAC Initialization ... 12-3
PMAC Initialization wizard ... 12-3
Configuration Summary page ... 12-9
Configuration Summary elements ... 12-10
Network Configuration page ... 12-10
Network Configuration elements ... 12-10
Networks page ... 12-11
Add Network page ... 12-12
Network Roles page ... 12-13
Add Network Role page ... 12-13
Network Interfaces page ... 12-14

Add Interface page 12-15
Routes page 12-16
Add Route page 12-17
DHCP IPv4 Ranges page 12-18
DHCP Ranges Add DHCP Range page 12-19
Configuration page 12-20
Feature Configuration page 12-20
Features elements 12-20
Add Role page 12-21

13 Access Control

GUI account basics 13-1
User account basics 13-1
Groups basics 13-2
Session timeout and concurrent login basics 13-2
User accounts 13-3
Users Administration page 13-3
Insert new user page 13-4
Updating user account information 13-6
Deleting a user account 13-7
About enabling or disabling a user account 13-7
Changing a user account's assigned group 13-8
Generating a user report 13-8
User groups 13-9
Groups Administration page 13-9
Group permissions 13-10
Pre-defined users and groups 13-14
Insert new group page 13-14
Updating a group 13-16
Deleting a group 13-16
Viewing a group's members 13-17
Generating a group report 13-17
Passwords 13-17
Setting a password from the Users Administration page 13-18
Setting a password from the System Login page 13-19
Configuring password expiration 13-19
Configuring maximum password history 13-20
Configuring minimum password length 13-20
Configuring minimum password difference 13-21
GUI sessions 13-21
GUI Sessions administration page 13-21
Viewing GUI sessions 13-22
Single sign-on session life 13-22

Deleting GUI sessions 13-22
Certificate Management page 13-23
Certificate Management [Establish SSO Zone] page 13-24
Certificate Management [Create] page 13-25
Certificate Management [Create CSR] elements 13-25
Certificate Management [Import] page 13-26
Certificate Management (Import Certificate) elements 13-26
Certificate Management (Update Certificate) elements 13-27
Certificate Management [Report] page 13-27
Certificate Management [Report] elements 13-27

14 Credentials

SNMP Community String Update page 14-1
SNMP Community String Update elements 14-1

15 Remote Servers

DNS Configuration page 15-1
DNS Configuration elements 15-1
LDAP Authentication 15-3
LDAP Authentication page elements 15-4
LDAP Authentication [Insert] page elements 15-4
LDAP Authentication [Report] page elements 15-6

16 Files Management page

Files Management page 16-1
Files Management elements 16-1

List of Tables

1-1 Admonishments ... 1-1
4-1 GUI Components ... 4-1
4-2 PMAC Main Menu Options ... 4-6
4-3 General Options Administration Elements ... 4-9
5-1 Elements on the Cabinet Inventory Summary Page ... 5-2
5-2 Tabs on RMS Page ... 5-2
5-3 Tab elements on the RMS page ... 5-3
5-4 Button elements on the RMS page ... 5-3
5-5 Elements on the RMS Hardware Tab ... 5-5
5-6 Elements in the Operating System Details Index Card ... 5-5
5-7 Elements in the Application Details Index Card ... 5-6
5-8 Elements on the Networking Details for hostname Index Card ... 5-7
5-9 Elements on the MAC Addresses Index Card ... 5-7
5-10 Elements on the Guests for hostname Index Card ... 5-8
5-11 Elements on the Enclosure Inventory Summary Page ... 5-9
5-12 Elements in the Product Area Table ... 5-11
5-13 Elements in the Board Area Table ... 5-12
5-14 Elements in the Chassis Area Table ... 5-13
5-15 Tabs on Bay Page ... 5-14
5-16 Tab elements on the Bay page ... 5-14
5-17 Button elements on the Bay page ... 5-14
5-18 Elements in the Entity Summary Index Card ... 5-16
5-19 Elements in the Product Area Index Card ... 5-17
5-20 Elements in the Board Area Index Card ... 5-17
5-21 Elements in the Partner Device Index Card ... 5-18
5-22 Elements in the Chassis Area Index Card ... 5-18
5-23 Elements in the Operating System Details Index Card ... 5-19
5-24 Elements in the Application Details Index Card ... 5-19
5-25 Elements in the Networking Details index card ... 5-20
5-26 Elements on the Guests for hostname Index Card ... 5-21
5-27 Elements on the Enclosure FRU Information page ... 5-22
5-28 Elements on the RMS FRU Information page ... 5-23
5-29 Elements on the Software Inventory page ... 5-25
6-1 Add Enclosure Steps ... 6-2
6-2 Add Image Steps ... 6-3
6-3 Backup PMAC Steps ... 6-4
6-4 Configure Storage Steps ... 6-5
6-5 Install OS steps ... 6-7
6-6 Install/Upgrade App steps ... 6-8
6-7 Reconfigure and Initialization Steps ... 6-10
6-8 Elements on the Background Task Monitoring Page ... 6-11
6-9 Elements on the Background Task details view ... 6-13
7-1 Software Install - Select Image Page elements ... 7-3
7-2 Software Install - Select Image Page Table elements ... 7-3
7-3 Software Upgrade - Select Image Page elements ... 7-6
7-4 Software Upgrade - Select Image Table elements ... 7-7
7-5 Image Transfer - Select Image Page elements ... 7-9
7-6 Image Transfer - Select Image Page Table elements ... 7-9
7-7 Elements on the Manage Software Images Page ... 7-11
8-1 View VM Guest work area tabs ... 8-7
8-2 Buttons on the View VM Guest work area ... 8-9

8-3 Buttons on the Create VM Guest page 8-14
9-1 Elements on the Sentry Process Control Page 9-2
9-2 Process table fields 9-3
10-1 Elements on the System Configuration Page 10-1
10-2 Elements on the Configure Cabinets Page 10-2
10-3 Elements on the Configure Enclosures Page 10-5
10-4 Elements on the Configure RMS Page 10-11
10-5 Elements on the Configure Storage Page 10-36
11-1 Elements on the Backup PMAC Configuration Page 11-3
11-2 Elements on the Backup PMAC Configuration Page 11-5
12-1 Configuration Profile Elements 12-2
12-2 Select a Profile elements 12-4
12-3 Elements on the Features Page 12-5
12-4 Elements on the Networks Page 12-6
12-5 Elements on the Network Roles Page 12-7
12-6 Elements on the Network Interfaces Page 12-7
12-7 Elements on the DHCP Ranges Page 12-8
12-8 Elements on the Configuration Summary Page 12-10
12-9 Elements on the Network Configuration Page 12-11
12-10 Elements on the Networks Page 12-11
12-11 Elements on the Add Network Page 12-12
12-12 Elements on the Network Roles Page 12-13
12-13 Elements on the Add Network Role Page 12-14
12-14 Elements on the Network Interfaces Page 12-14
12-15 Elements on the Add Interface Elements Page 12-15
12-16 Elements on the Routes Page 12-16
12-17 Elements on the Add Route Page 12-17
12-18 Elements on the DHCP IPv4 Ranges Page 12-18
12-19 Elements on the Add DHCP Range Page 12-19
12-20 Elements on the Features Page 12-20
12-21 Elements on the Features Add Roles Page 12-21
13-1 Elements on the Users Administration Page 13-3
13-2 Elements on the Insert New User Page 13-4
13-3 Elements on the Groups Administration Page 13-9
13-4 Pre-defined Users and Groups 13-14
13-5 Elements on the insert new group page 13-14
13-6 Elements on the GUI Sessions Administration Page 13-21
13-7 Elements on the Certificate Management Page 13-23
13-8 Single Sign-On Zone Elements 13-24
13-9 Elements on the Certificate Management (Import Certificate) Page 13-26
13-10 Elements on the Update Certificate Page 13-27
13-11 Elements on the Certificate Management [Report] Page 13-27
14-1 Elements on the SNMP Community String Update Page 14-1
15-1 DNS Configuration Page elements 15-1
16-1 Elements on the Files Management Page 16-1

1

Introduction

This online help describes the Platform Management and Configuration (PMAC) application and is updated with each major release of the software.

Revision History

Date	Description
November 2017	Accessibility changes throughout

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of personal injury.)
	Warning: (This icon and text indicate the possibility of equipment damage.)
	Caution: (This icon and text indicate the possibility of service interruption.)

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.

3. Under the Oracle Communications subheading, click **Oracle Communications documentation** link.

   The Communications Documentation page displays. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure and Platforms.

4. Click on your product and then the release number.

   A list of the documentation set for the selected product and release displays.

5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training at http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site at www.oracle.com/education/contacts

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), select **1**
   - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

2

Accessibility

Oracle is committed to delivering products and documentation that meet Oracle's accessibility guidelines and standards. This section presents information regarding Oracle's accessability program, electronic support, and special accessibility features built into the PMAC software. This information is updated with each major release of the software.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Accessibility Features

This release does not contain any application specific accessibility features or custom keystrokes. Accessibility features provided by the browser and operating system of the client workstation are not covered here.

THE PMAC's Web UI supports the following assistive technologies and techniques:

- The web UI has been made to make information visible when the browser's text size is set to 200%.
- Meaningful sequence such that text is presented in proper reading order in HTML.
- Use of color. Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.
-

The PMAC's Web UI does not contain any of the following:

- Audio or Video
- Images of text such as CAPTCHA

3

PMAC Overview

The Platform Management and Configuration (**PMAC**) application provides hardware and platform management capabilities at the site level for the platform. The PMAC application manages and monitors the platform hardware and software. PMAC also installs the operating system and application software onto multiple servers simultaneously from a single interface and manages the software images used in the installation. PMAC also provides upgrade capability for the application software.

PMAC user interface

The PMAC **GUI** (**graphical user interface**) is the user's central point of interaction with the platform. The PMAC GUI is a browser based application that resides on the PMAC server. Authorized users can easily log into the PMAC GUI from any supported browser with network access to the PMAC server's management IP address.

The PMAC GUI facilitates the following tasks:

- Initializing PMAC after deployment. Modifying the configuration after initialization.
- Adding, deleting, and managing the platform's cabinets, enclosures, blades, and rack mount servers.
- Viewing and exporting FRU information.
- Viewing the current software inventory and performing related actions.
- ISO image management including transferring images to a remote server.
- Installing and upgrading the operating system on one or more servers.
- Application install, upgrade, and patch management.
- Virtual Machine management.
- SAN storage configuration.
- Adding, deleting, and managing Users and Groups.
- Certificate management.
- GUI session and backup management.
- SNMP, DNS, and LDAP configuration.
- Viewing PMAC application status and performing related actions.
- File management.

- Task monitoring and management.

If you fail to log in successfully due to invalid credentials, a customizable failed login message is displayed on the login screen. Similarly, if you have numerous consecutive failed login attempts, the account is disabled. The maximum consecutive failed attempts is user defined. Additionally, if you fail to login within a specified number of days, the account is disabled when you next log in using valid credentials. The disabled account message is also customizable. See General Options administration elements for more information on these and other customizable options.

If the account is disabled due to any of the previously defined actions, the account must be re-enabled by the guiadmin user or any user with admin group permissions.

Cabinet management

The PMAC GUI provides the ability to differentiate and manage hardware at the cabinet level. This assists the system administrator in identifying the target hardware and provides an additional layer of confidence that critical operations are being performed on the correct devices.

From the PMAC GUI the user can view the system inventory at the cabinet level. This includes enclosures and rack mount servers. See Cabinet inventory for additional information on viewing the system inventory.

In addition to the initial provisioning of cabinet information the system administrator has the ability to add and delete cabinets at any time. Note that at least one cabinet must be added before any enclosures can be added. Alternately, a cabinet must be empty of enclosures and rack mount servers before it can be deleted. See Cabinets for additional information related to cabinet provisioning and management.

Enclosure management

The PMAC GUI facilitates enclosure management by providing options to view the enclosures provisioned in the hardware inventory and to make additions and changes to that inventory.

Adding an enclosure to the hardware inventory identifies the enclosure to the PMAC application so that PMAC can then begin managing and monitoring the enclosure. Adding the enclosure also associates it to a cabinet. Between 1 and 3 enclosures can be associated to the same cabinet in the PMAC hardware inventory.

The PMAC GUI provides an option to delete an enclosure. Deleting the enclosure removes it from the PMAC hardware inventory. The operation does not shut the enclosure down.

The PMAC GUI provides an option to edit an enclosure configuration. This option is used to inform PMAC of the IP addresses of the enclosure's OAs.

Once enclosures have been provisioned into the PMAC hardware inventory, the PMAC GUI lets you pull up a list of all the provisioned enclosures. You can launch the **Add Enclosure**, **Delete Enclosure,** and **Edit Enclosure** commands from that page.

Enclosure inventory options in the PMAC GUI let you drill-down to view details about a given enclosure and its components.

When an enclosure is added to the inventory, PMAC launches a background task that discovers the hardware present within the enclosure. You can then view from the PMAC GUI the hardware components (server blades, switches, Onboard Administrators, fans, and power supplies) that are discovered in the enclosure.

You can also see from the PMAC GUI if the state of a device changes. An enclosure diagram in the GUI lets you point and click to obtain information or launch a procedure on the selected device.

You can tell from the PMAC GUI menu whether a bay's orientation is front or rear. PMAC appends an **F** on the front bays labels and **R** on the rear bay labels. For example, Bay 7F indicates that the bay is a front bay.

See Enclosures for additional information related to enclosure provisioning and management.

Blade management

The PMAC GUI provides interfaces that enable you to retrieve data about the blades in the PMAC hardware inventory. You can point and click to the bay where a given blade resides. From there, you can view summary or hardware information about the blade. You can obtain detailed information about the blade such as blade type.

A server blade is a general purpose blade that hosts telecommunications software. The PMAC GUI lets you launch operations on a server blade such as installing the TPD operating system on one or more blades simultaneously. You can perform a warm reset on a server blade, which restarts the server blade. Or you can perform a cold reset on a server blade or a switch. The cold reset command restarts the blade.

The Onboard Administrator controls power to the server blades. When a server blade is inserted into a bay, the server blade communicates with the Onboard Administrator to negotiate power and server blade activation.

The Onboard Administrator is configured to activate automatically any server blade coming up, which allows the server blade to get its power allocation.

See Blades for additional information related to blade management.

Rack Mount Server Management

The PMAC GUI facilitates RMS management by providing options to view the RMS provisioned in the hardware inventory and to make additions and changes to that inventory.

The PMAC GUI provides the following:

- An option to add an RMS. Adding an RMS to the hardware inventory allows PMAC to begin managing and monitoring the RMS. Adding the RMS also associates it to a cabinet.
- An option to delete an RMS. Deleting the RMS removes it from the PMAC hardware inventory. The operation does not shut the RMS down.
- An option to edit an RMS configuration. This option is used to inform PMAC of changes to the RMS location or credentials.
- An option to find RMS within the PMACs networks. This option is used to identify and collect information on potential RMS. This list of found RMS can then be added to the PMAC configuration.

On a system with an RMS that has been provisioned into the PMAC hardware inventory, the PMAC GUI lets you access a list of all the provisioned RMSs. You can launch the **Add RMS**, **Delete RMS**, **Edit RMS**, **Find RMS**, and **Found RMS** commands from that page.

The PMAC GUI provides interfaces that enable you to retrieve data about the RMS in the PMAC hardware inventory. You can point and click on the RMS under the cabinet where it resides. From there, you can view hardware, software, network, or virtualization information about the RMS. You can also obtain detailed information about the RMS such as RMS type.

The PMAC GUI lets you launch operations on a RMS such as:

- Installing the TPD or TVOE operating system.
- Perform a cold reset on a RMS. The cold reset command restarts the RMS without a graceful shutdown.
- Toggle the UID LED to physically locate it within the specified cabinet.

See RMS for additional information related to rack mount server provisioning and management.

Inventory

The *discovery* process entails seeking out and identifying the software and hardware components in the PMAC inventory. The user views the discovery data as inventory via the PMAC GUI.

Enclosure Discovery

The PMAC application provides the ability to discover the software and hardware present on the enclosure (such as server blades and power supplies). Discovery is initiated on a per-enclosure basis when PMAC performs an **Add Enclosure** operation. PMAC creates a background task to discover the software and hardware components present in the enclosure when the enclosure is added to the hardware inventory. Once an enclosure is provisioned, discovery occurs again when PMAC gets restarted (after a reboot or after a shutdown).

Once an enclosure is being managed by PMAC, the Onboard Administrator obtains the discovery information and passes it to PMAC. PMAC receives asynchronous events such as server blade insertion and removal from the Onboard Administrator and uses the information to update the hardware inventory data. PMAC periodically retrieves information about the software inventory.

RMS Discovery

The PMAC application provides the ability to discover the software and hardware present on an RMS. Discovery is initiated on a per-RMS basis when PMAC performs an Add/Edit RMS operation. Once an RMS is provisioned, discovery occurs again when PMAC gets restarted (after a reboot or after a shutdown). PMAC also periodically re-discovers RMS hardware information to keep the inventory up-to-date.

The PMAC GUI provides the following types of information for hardware inventory:

- A summary of the system inventory with details about the cabinets, enclosures, and RMSs.
- An enclosure schematic that shows which enclosure bays are occupied, which are empty, and what type of component, such as server blade or power supplies, each bay contains.
- A list of the physical server blade locations in the enclosure.

- Enclosure and enclosure-component (such as power supplies or fan tray) details such as manufacturer, product name, serial number, and part number.
- A list of the physical RMS in the system.
- A cabinet inventory page shows the provisioned enclosures and RMSs for that cabinet. The view within this work area provides the overview of hardware associated with specific cabinet. The rows that are populated in the Provisioned Enclosures index card and Provisioned RMS index card depend on actual hardware of the system associated with the cabinet. It is also possible that an index card will not be displayed at all if it does not contain any entries.
- RMSs not associated with a cabinet are located under Cabinet Unspecified.

The PMAC GUI provides the following types of information for software inventory:

- Operating system name and version
- Application name and version
- Function
- Designation
- Hostname
- Location
- IP Address

See System inventory information for additional information related to system inventory.

Software installation and upgrade

The PMAC GUI manages the installation and upgrade of platform and application software.

During initial setup, the PMAC application is installed on the PMAC server. Oracle personnel perform the initial installation and configuration of PMAC. PMAC is then used to install the TPD operating system and the application software on the server.

From a single PMAC GUI page, an operation can be launched that performs a simultaneous network installation of the operating system onto multiple servers. The application can also be installed on multiple servers at once.

Similarly, the PMAC GUI provides the operator with the ability to launch an upgrade of a server's application. The upgrade can occur on multiple servers simultaneously.

ISO software images are the supported delivery medium for platform installation and for application software installation or upgrade. The TPD software image and all application software images are added and installed onto the PMAC server. Software images can be served to PMAC via USB or via the network or extracted from physical media (CD) in the drive on the PMAC server (if so equipped).

The PMAC GUI provides interfaces to allow users to manage the software images. The PMAC GUI lets users add a new software image, view an inventory of the existing software images, and delete them when they are no longer required.

See Software Installation for additional information related to installing and upgrading software.

Storage device configuration

The PMAC GUI provides an interface to facilitate SAN storage device configuration. The interface allows the storage configuration to be specified in one or more XML files. Sample XML files are provided with PMAC and specify the **Vdisk**s, **Global Spare**s, and **Host Volume**s to be configured on **Controller**s and **Host**s. Before being uploaded to PMAC, the XML file(s) are edited to fill in site-specific information such as IP addresses and volume names. The configuration specified in the XML file(s) is then applied to the hardware via an option on the PMAC GUI.

The interface also provides the capability to remove an existing configuration from a SAN storage device.

Note: This interface is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

See Storage devices for additional information related to storage device configuration.

Back up PMAC server data

The PMAC GUI provides an interface to facilitate the backup of PMAC server data. The backup operation archives configuration data and database tables that contain user-provisioned data.

From a PMAC GUI page, the authorized user can specify to back up to a local disk on the PMAC server or a remote server. The backup is then launched from the GUI as a background task, which can be monitored as it progresses.

Note: The `Restore` procedure is run manually from the command line and is not covered in this help. Please call Customer Access Support (see My Oracle Support) if you need to restore the PMAC server data.

See Backing up PMAC server data for additional information related to backing up PMAC server data.

PMAC Application Configuration

The PMAC configuration feature decouples the PMAC application from the hardware on which it is installed and on the networks that are available. The feature provides the capability to install PMAC as a TVOE guest.

The feature configures the networks that PMAC uses to manage hardware and allows functionality to be enabled or disabled to align with the application being run. PMAC can thus be customized to perform just the functionality required by the application or the platform PMAC is supporting.

The feature is based on a configuration profile, a group of related elements that are packaged in PMAC as a predefined configuration profile. The profile determines the services, networks, and interfaces that are available on the system.

The PMAC GUI provides an initialization wizard that enables personnel to select a profile and modify some of the profile's default networking information. This configuration is performed after the PMAC initial installation and before any PMAC features can be used.

See Configuration Summary page for additional information related to the PMAC application configuration.

Administration

The PMAC GUI provides authorized users with an interface to facilitate administrative tasks:

- Set-up/update individual and group user accounts, including setting passwords and password expiration dates, if desired.
- Administer user sessions.
- Update the splash page welcome message and other site settings for the GUI.
- Administer the PMAC application processes.
- Change/update any type of credentials supported by PMAC.
- Certificate management where you can create and work with certificates.

Status and Manage

The PMAC GUI provides users with an interface to monitor multiple PMAC status and management interfaces.

Note: Currently, only Files is supported.

The interface provides to access and work with files located locally on the PMAC server. The following functions are provided:

- Delete
- View
- Download

See Files Management page for additional information related to files management.

4

PMAC User Interface

This section introduces the PMAC graphical user interface (GUI) and provides procedures for accessing the GUI and making global changes to a site's customizable GUI settings.

Components of the PMAC GUI

The PMAC GUI is a Web-based GUI that enables authorized users to access PMAC application functions.

The table describes the components of the PMAC GUI.

Table 4-1 GUI Components

Component	Location	Function
Banner Area	Top bar across the web page, under web browser menu or bookmarks bar	From left displays the Oracle logo followed by the application name. Following the application name the title bar displays the following: • The current release and version of the application. • A **Pause Updates** checkbox that allows the users to pause any reoccurring updates while on a given page. Note that not all pages support periodic updates. • A **Help** button that, when selected, displays the Oracle help pages in a separate browser tab. • The name of the currently logged-in user displayed as Logged in Account <username>. • A **Log Out** button that, when selected, logs the displayed user out and returns to the Oracle System Login page.

Table 4-1 (Cont.) GUI Components

Component	Location	Function
Main Menu	Left side of web page, under banner area	A tree-structured menu of operations that can be performed with the user interface. The plus sign (+) next to a folder indicates that a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or the text. • To select a menu item that does not have submenu items, click the text or its associated symbol.
Work Area Heading	Across top of work area panel, below banner area	Displays the locator link (window title) of the current page or form. Also displays the date and time in UTC format.

Table 4-1 (Cont.) GUI Components

Component	Location	Function
Work Area Toolbar	Directly below work area heading	Provides access to optional elements of the work area, such as Info and Error messages, a display filter, and a page specific Task Management grid. If one or more of these options is available in the active page or form, the following appear on the toolbar: **Info** Displays the Info window from the toolbar when the system has one or more non-error messages for the user. This typically confirms that a requested action has been performed without error. Clicking **Info** displays the messages in a green floating (movable) window. These messages do not appear the next time the screen is displayed. **Error** Displays the Error window for error messages. Unlike the Info window, the Error window opens automatically when an error message is present. These messages do not appear the next time the screen is displayed **Filter** On some pages that present tabular information, the Toolbar includes a **Filter** button. The Filter window shows page-specific criteria that reduces the amount of information displayed. The capabilities of the filter function vary from page to page according to the type of information presented. The page-specific details appear in the online help with the

Table 4-1 (Cont.) GUI Components

Component	Location	Function
		appropriate page descriptions. The filter is presented in a floating window where you can select or enter criteria to be applied to the contents of the table. If you specify multiple criteria, the data shown includes only those items that satisfy all of them: they are joined by "and". After you have entered criteria for one or more table columns and select **Go**, the table is displayed with the filter in effect. The filter window remains visible for further use. You can close the window by selecting **Filter** in the toolbar or the filter window's **X** button. The work area title includes (Filtered) as a reminder that not all data are being shown. The filter settings are retained when the filter window is closed, as long as you do not navigate to a different GUI page. Upon returning to this page, the filter is cleared and has no effect. **Tasks** Displays most of the information available on the main Task Monitoring screen, but only for tasks related to the current work area. For example, for a Bay-specific work area, only tasks for that Bay are shown; for Manage Software Images, only Add Image tasks are shown. Because of the restricted window size, one or more of the columns that are visible on the main Task Monitoring screen might not be present here.

Table 4-1 (Cont.) GUI Components

Component	Location	Function
		Info, **Error**, **Filter**, or **Tasks** appear on the toolbar.
Work Area	Directly below work area toolbar and to the right of the main menu	A page containing text, input fields, and controls related to the option most recently selected from the main menu. When a user first logs in, a splash page with a user-defined welcome message displays.
Status Area	Bottom bar of web page, under navigation and main work areas	Displays the PMAC site name as defined in **Administration** > **General Options**. Displays the current status of the **Pause Updates** action presented in the title bar. Updates are either enabled or disabled.

Supported browsers

The PMAC GUI requires the use of Microsoft Internet Explorer 9.0, 10.0 or 11.0 with JavaScript and Cookies (earlier releases are not supported).

JavaScript and cookies are required.

Firefox 3.0 or later should work but is not formally supported.

Browser configuration

Some functions in the PMAC GUI require the use of popups. If you have popups blocked (disabled), some functions will not work. To avoid this condition, make sure your browser is set to allow popups.

PMAC GUI main menu options

The figure shows the main menu of the PMAC GUI for a user who has permissions to all main menu options. The menu options that appear on the screen differ according to the permissions assigned to a user's log-in account. If a user does not have permissions, the menu option does not appear.

The main menu of the PMAC GUI provides these options:

Table 4-2 PMAC Main Menu Options

Menu Item	Function
Hardware	Provides options for viewing the system inventory, configuring hardware, and RMS information. The system inventory option enables users to view the installed cabinets and enclosures. The user can also view the bays and see what type of blade (switch, SAN switch, server blade, or Onboard Administrator) each bay contains. The hardware configuration option enables authorized users to add/delete cabinets and enclosures. You can also select the RMS from a cabinet to view hardware, software, network, or virtualization information about the RMS.
Software	Provides options for obtaining software inventory. The user can also manage the software images available in the PMAC repository for installing the TPD operating system and application software. There are also options for installing the TPD operating system and the application software onto multiple servers simultaneously.
VM Management	Provides options for viewing details of a hosts configuration related to guest management. Allows for the creation and management of virtual machines (guests) on hosts controlled by the PMAC.
Storage	Provides an interface to facilitate storage device configuration. This capability is intended for use during initial installation only.
Administration	Provides authorized users with access to these administrative tasks: • Set-up/update individual and group user accounts, including setting passwords and password expiration dates, if desired. • Administer user sessions. • Update the splash page Welcome Message and other general options for the GUI. • Administer the PMAC application processes. • Initialize PMAC during initial setup. • Backup PMAC server data • Display and modify the PMAC network and feature configuration.

Table 4-2 (Cont.) PMAC Main Menu Options

Menu Item	Function
Status and Manage	Allows authorized users PMAC file handling capabilities. Currently only Certificate Signing Requests (CSRs) are presented in the files storage area.
Task Monitoring	Provides an interface for viewing the progress of all background tasks created as a result of a GUI action that requires extended time to complete. Such tasks run in the background so you can perform additional tasks with the GUI. Some examples of background tasks are adding an enclosure, adding a software image, installing the TPD operating system to one or more server blades, and installing or upgrading the application on one or more servers.
Help	Provides an interface for viewing online help.
Legal Notices	Displays the legal notices associated with the PMAC application.
Logout	Logs you out of the PMAC user interface. (Alternatively, you can log out using the **Log Out** link provided in the title bar.)

To access online Help for individual GUI pages, select the **Help** button located in the upper right corner of the Work Area of each GUI page.

Accessing the PMAC GUI

To launch the GUI, you need to have available the PMAC IP address of your network and a valid user account.

1. Launch a Web browser.
2. In the **Address** field, enter the **URI** for your site as follows:
   <customer network PMAC-IP Address>/

   An IPv4 and IPv6 example:

   https://192.168.68.55/

   https://[2606:b400:605:b811:910::43]/
3. Press **Enter.**

   The Security Alert Certificate popup appears.
4. Click **Yes**.

   The Platform Management & Configuration Login page appears.
5. Enter a valid username and password and click **Log In**.

The Platform Management & Configuration splash page appears.

6. When you are ready to log out, perform one of the following actions to close out the user session:

   - Select **Logout** on the main menu.
   - Click the **Logout** link in the upper right corner of the GUI.

A user session on the PMAC GUI starts. Note that the user session remains active until you invoke the **Logout** option or the Single Sign on Session Life is exceeded.

Logging out of the PMAC GUI

Note: It is advisable to log out of PMAC before you exit the Web browser. Covered by the important note below.

1. Perform one of the following actions:

   - Select **Logout** on the main menu of the PMAC GUI.
   - Click the **Logout** link in the banner of the PMAC GUI (upper right corner).

   The Logout page appears. At this point, the user session is closed.

2. Click the **Close** link to close the Web browser.

The user session on the PMAC GUI is closed.

Important note about logging out of the PMAC GUI

If a PMAC GUI user simply exits the Web browser and does not log out of the PMAC GUI, the user session remains active until a session timeout occurs. If the user does not have permission to use additional concurrent login sessions, the user may not be able to log back into the PMAC GUI immediately. For this reason, it is advisable to use the logout functions that the PMAC GUI provides.

If the user encounters the above situation, the user must wait until an active user session times out. The other option available is to request that the administrator delete an active session.

GUI work area

The administrative user has the capability of configuring some of the work area settings on the PMAC GUI on a per-site basis. The site name that displays in the monitor banner, the splash page welcome message, the disabled account message, and the failed login message.

General Options administration page

The General Options page is accessible under **Administration** > **General Options**. The page lets the administrative user make changes that affect the GUI settings on a per-site basis. Additionally, global password options are found here.

General Options administration elements

This table describes the elements of the General Options administration page:

Table 4-3 General Options Administration Elements

Element	Description
Password Expiration (in days)	The number of calendar days that passwords stay active. By default, passwords expire in 90 days. Entering a value of **0** in this field means that passwords never expire. Note that the expiration is retroactive: if the expiration is set to 30 and it has been 45 days since the password was last changed, the password is now expired. A value is required. Format: Numeric Range: 0-90 Default: 90
Maximum Password History	Maximum number of passwords maintained in a history list before reuse of a password is allowed. Entering a value of **0** in this field means that no password history is applied and the same password can be reused. A value is required. Format: Numeric Range: 0-10 Default: 3
Maximum Consecutive Failed	This field indicates the maximum number of failed login attempts that can occur within the **Lockout Window** before the account is disabled. The account must be re-enabled by the guiadmin user or any user with admin group permissions. A value is required. Format: Numeric Range: 1-10 Default: 6

Table 4-3 (Cont.) General Options Administration Elements

Element	Description
Lockout Window (in minutes)	This field indicates the amount of time (in minutes) in which exceeding the **Maximum Consecutive Failed** login attempts will cause an account to be disabled. The account must be re-enabled by the guiadmin user or any user with admin group permissions. Entering a value of **0** indicates the window is unlimited and will disable the **Maximum Consecutive Failed** login attempts setting. A value is required. Format: Numeric Range: 0-unlimited Default: 30
Last Login Expiration (in days)	This field indicates the number of days of inactivity before a user account is disabled. The account will be disabled when the user next logs in using valid credentials. The account must be re-enabled by the guiadmin user or any user with admin group permissions. A value is required. **Note:** This field is enabled and disabled using the **Last Login Expiration Enabled** option. Format: Numeric Range: 1-200 Default: 30
Last Login Expiration Enabled	This field enables or disables the **Last Login Expiration** option. A value is required. Disabled: 0 Enabled: 1 Default: 0
Single Sign On Session Life (in minutes)	This field indicates the maximum session life (in minutes) for a Single-Sign-On session. A value is required. Format: Numeric Range: 1-120 Default: 120

Table 4-3 (Cont.) General Options Administration Elements

Element	Description
Minimum Password Length	This field indicates the minimum number of valid characters that are required for a user password. A value is required. Format: Numeric Range: 8-16 Default: 8
Minimum Password Difference	This field indicates the minimum required character difference between a new and old password. A value is required. Format: Numeric Range: 0-16 Default: 0
Failed Login Message	The message displayed on the GUI login screen when the login fails due to invalid credentials. Format: String (from 0-1024 characters) Default: Login Failed
Disabled Account	The message displayed when an account has been disabled for any reason, and a user attempts to login using valid credentials. Format: String (from 0-1024 characters) Default: Account Disabled
Welcome Message	The system-wide welcome message displayed on the splash page of the PMAC GUI. Format: String (from 0-1024 characters) Default: This is the user-defined welcome message. It can be modified using the General Options page, reached via the Main Menu's 'Administration' submenu.
User Defined Site Name	The site name displayed on the monitor bar of the PMAC GUI. Format: String (from 5-16 characters) Default: [Site Name]
OK Button	Select **OK** to update the General Options with the changes that were entered on the page.
Cancel Button	Select **Cancel** to undo changes made on the General Options page. Current changes will be replaced with previously saved values.

Customizing the splash page welcome message

When you log in to the PMAC GUI, the splash page appears. The splash page displays a system-wide welcome message. Use this procedure to customize the welcome message:

1. Select **Administration** > **General Options**.

   The General Options administration page appears.

2. Enter the desired welcome message text in the **Welcome Message** field.

   To format the welcome message, use HTML formatting tags.

3. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.

The new welcome message is displayed on the next occurrence of the splash page.

Changing the site name on the GUI monitor bar

Use this procedure to change the site name that appears in the monitor bar of every GUI page:

1. Select **Administration** > **General Options**.

   The General Options administration page appears.

2. Enter a site name in the **User Defined Site Name** field.

3. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.

   After clicking **OK** it is necessary to refresh the page for the change to be reflected in the monitor bar.

The new site name now displays in the monitor bar on all GUI pages.

5

Inventory Information

This section provides information about viewing software inventory, hardware inventory and **FRU** information.

System inventory information

The PMAC GUI lets you view hardware inventory data by navigating from the main menu to **Hardware** > **System Inventory**. Expanding the **System Inventory** menu provides access to the inventory information regarding the cabinets, enclosures, rack mount servers and other system components. For a selected enclosure, **System Inventory** shows which bays are occupied, which are empty, and what type of blade or device each bay contains. This includes both front and rear views. In addition, data is provided on any background tasks running on a device.

There is also an option that provides a report of all **FRU**s on the system along with their product version number, part number, and serial number. The report can be exported to file.

Cabinet inventory

The PMAC GUI provides summary information on provisioned cabinets.

Cabinet Inventory Summary page

The Cabinet page is accessible on the GUI main menu under **Hardware** > **System Inventory** > **Cabinet X** where *Cabinet X* indicates the ID of the cabinet. The view in this work area shows an overview of the hardware associated with the selected cabinet.

Note: A special cabinet identifier "unspecified" is used for RMS that have not been assigned to a provisioned cabinet.

Note: The set of rows that is populated in the Provisioned Enclosures and Provisioned RMS index cards depends on the hardware of the system associated with the cabinet. It is also possible that an index card is not displayed if the does not contain any entries.

Cabinet Inventory Summary elements

These elements appear on the Cabinet Inventory Summary page.

Table 5-1 Elements on the Cabinet Inventory Summary Page

Index	Description
Provisioned Enclosures	Displays rows that pertain to one enclosure associated with the specific cabinet. Only the enclosure ID is listed.
Provisioned RMS	Displays two-row sets that pertain to one RMS associated with the specific cabinet. The odd rows list the RMS name and the even rows list the RMS IP address.

RMS inventory

The PMAC GUI provides detailed inventory information on discovered RMSs.

RMS pages

RMS pages are accessible from the main menu under **Hardware** > **System Inventory** > **Cabinet X** > **RMS X**, where **X** specifies the component ID.

The view in this work area provides information accessible from the tab menu for the given rack mount server identified by a unique IP address and name.

The tabs provide hardware, software, network, and virtual machine (VM) information. Only servers with the Tekelec Virtual Operating Environment (TVOE) installed also display VM information.

To view RMS information, click the respective tab. The Hardware tab displays by default.

Table 5-2 Tabs on RMS Page

To view...	...select this tab:
Hardware summary information	RMS Hardware Tab
Software summary information	RMS Software Tab
Network summary information	RMS Network Tab
VM Info summary information	RMS VM Info Tab

For more information about viewing RMS information, see Viewing RMS inventory.

RMS pages make common commands available above and below each tab.

The **Tasks** button on the toolbar displays a floating window containing the Background Task table with the background tasks of actions initiated from this work area.

Other buttons allow you to perform these actions:

- Install the operating system (TPD/TVOE)
- Install, upgrade, or patch an application
- Accept or reject an upgrade or patch

- Perform a reset to shut down and then restart the RMS. Note that the shutdown is not graceful.

RMS page elements

The RMS page contains Table 5-3 and Table 5-4 elements.

Table 5-3 Tab elements on the RMS page

Component	Description
Hardware	Displays hardware information, including an LED state indicator and the ability to refresh table data and toggle the LEDs on or off
Software	Displays information about the operating system and application installed on the RMS
Firmware	Displays firmware information about the server and its components, including interfaces, controllers, and drives.
Network	Displays a content pane with information pertaining to network interfaces and MAC addresses of the RMS
VM Info	Displays information about guest virtual machines

The RMS page contains these button elements:

Table 5-4 Button elements on the RMS page

Component	Description
Tasks	Button in the toolbar that displays a floating window containing the Background task table with the background tasks of actions initiated from this work area.
Update Firmware	Button that lets you update the firmware on a server. Clicking this button opens the Firmware Update - Select Image page.
Install OS	Button that lets you install the operating system (TPD) on the RMS you are on. Clicking this button opens the Software - Select Image page.
Upgrade	Button that lets you install or upgrade the application software on the RMS you are on. Clicking this button opens the Software Upgrade - Select Image page.
Accept Upgrade	Button that lets you accept an upgrade on the RMS.
Reject Upgrade	Button that lets you reject an upgrade on the RMS.

Table 5-4 (Cont.) Button elements on the RMS page

Component	Description
Patch	Button that lets you patch the RMS.
Accept Patch	Button that lets you accept a patch on the RMS.
Reject Patch	Button that lets you reject a patch on the RMS.
Reset	Button that lets you remove any configuration data applied to the RMS.

RMS Hardware Tab

RMS Hardware is accessible under **Hardware** > **System Inventory** > **Cabinet X** > **RMS X** , where **X** specifies the component ID. The **Hardware** tab with the Hardware information table displays by default.

The RMS Hardware tab displays hardware information, including an LED state indicator and the ability to refresh table data and toggle the LED on or off.

To refresh the information in the table, click the **Refresh** symbol in the table header. The animated icon next to the Refresh button in the upper right corner of the table will spin indicating the Refresh is in progress. The state of the RMS LED is indicated below the table. You can change the LED state by clicking the adjacent LED button. If the state of the LED is **UNKNOWN**, this button will be disabled.

RMS Hardware Tab elements

The Hardware tab for an RMS contains the Hardware Information table, an LED state indicator, and a button each to refresh the table data and to toggle the LEDs on or off.

Hardware Information Table

This table provides standard information including:

- Entity Type
- Discovery State
- UUID
- Manufacturer
- Product Name
- Part Number
- Serial Number
- Firmware Type
- Firmware Version
- Status

Buttons and Indicator

The following buttons and indicator are available:

Table 5-5 Elements on the RMS Hardware Tab

Component	Description
LED State Indicator	Shows the current LED light state of the RMS, such as **ON** , **OFF**, or **UNKNOWN.**
LED State-related button	Allows you to change the state of the LED light. The button's label and corresponding action depends on the current LED light state. For example, if the current LED light state is **OFF**, the button label is **Turn On LED**.
Refresh button (depicted by chasing arrows in upper right corner)	Lets you refresh the work area information.

RMS Software Tab

The RMS Software tab is accessible under **Hardware** > **System Inventory** > **Cabinet X** > **RMS X**, where **X** specifies the ID of the component. Select the **Software** tab.

The RMS Software tab displays information about the operating system and application installed on the RMS.

> **Note:** The set of rows that is populated depends on the actual hardware of the system. Not all rows and actions are applicable to all hardware types.

Use the Tasks button on the toolbar to monitor background tasks for actions initiated from this work area.

RMS Software Tab elements

The RMS Software tab provides index cards with data for the following areas:

- Operating System Details
- Application Details

Operating System Details

This index card provides detailed information about the operating system installed on the RMS. The operating system must provide this data; otherwise, the data is left blank.

Table 5-6 Elements in the Operating System Details Index Card

Element	Description
Operating System	Identifies the operating system (TPD) on the RMS.
OS Version	Identifies the TPD version on the RMS.
Hostname	Identifies host name of the RMS.
Platform Software	Identifies the platform software.

Table 5-6 (Cont.) Elements in the Operating System Details Index Card

Element	Description
Platform Version	Identifies the platform version.

Application Details

This index card provides detailed information about the application installed on the RMS. The application must provide this data; otherwise, the data is left blank.

Table 5-7 Elements in the Application Details Index Card

Element	Description
Application	Identifies the application.
Version	Displays the application version or one of the following upgrade states: *Pending Acc/Rej* or *In Upgrade*. **Note:** There might be times during an upgrade when PMAC is not able to query and display the upgrade state.
Function	Identifies the application function.
Designation	Identifies the application designation.

RMS Network Tab

RMS Network is accessible under **Hardware** > **System Inventory** > **Cabinet X** > **RMS X**, where **X** specifies the ID of the component. Select the **Network** tab.

The RMS **Network** tab displays a content pane with information pertaining to network interfaces and MAC addresses of the RMS.

Note: The set of rows that is populated depends on the actual hardware of the system. Not all rows and actions are applicable to all hardware types.

Use the Tasks button on the toolbar to monitor background tasks for actions initiated from this work area.

RMS Network Tab elements

The RMS Network tab elements consist of an index card with data about the following areas:

- Networking Details for hostname
- MAC Addresses

Networking Details for hostname

This index card provides information pertaining to network interfaces of the selected RMS.

Table 5-8 Elements on the Networking Details for hostname Index Card

Element	Description
The Networking Details for *Hostname X* tables provide detailed data for a given host combination. Provisioned IPv4 and IPv6 IP addresses are shown. The following fields appear in the Networking Details tables:	
Interface	The name of the interface.
IP Address	The IP address of the interface.
Admin Status	The administrator-defined status (**up** or **down**) for an interface. The **Admin Status** is differentiated from the **Operating Status** (also **up** or **down**) in that the **Operating Status** is defined by the actual, current state of the interface. For example, when the administrator brings an interface online, the **Admin Status** of the interface would be **up**. If the **Operating Status** then shows that the interface is **down**, the contradictory status indicates that there might be a problem.
Operational Status	The actual status (**up** or **down**) for an interface. The **Operating Status** is differentiated from the **Admin Status** (also **up** or **down**) in that the **Admin Status** is defined by the administrator. For example, when the administrator brings an interface online, the **Admin Status** of the interface would be **up**. If the **Operating Status** then shows that the interface is **down**, the contradictory status indicates that there might be a problem.

MAC Addresses

This index card provides information pertaining to MAC addresses in the current RMS.

Table 5-9 Elements on the MAC Addresses Index Card

Element	Description
Address	The address of the interface.
Description	The MAC address description.

RMS VM Info Tab

RMS VM Info is accessible under **Hardware** > **System Inventory** > **Cabinet X** > **RMS X**, where **X** specifies the component ID. Select the VM Info tab.

The RMS VM Info tab provides detailed information pertaining to guest virtual machines.

Note: This tab is available only for servers running the Tekelec Virtual Operating Environment (TVOE).

Note: The set of rows that is populated depends on the actual hardware of the system. Not all rows and actions are applicable to all hardware types.

Use the Tasks button on the toolbar to monitor background tasks for actions initiated from this work area.

VM Info Tab elements

The RMS VM Info tab elements consist of an index card with data for the following area:

- Guests for hostname

Guests for hostname

Table 5-10 Elements on the Guests for hostname Index Card

Element	Description
Name	Name of the guest virtual machine.
Status	The status of the guest virtual machine.

Viewing RMS inventory

The RMS feature allows PMAC support for Rack Mount Server (RMS) solutions. PMAC facilitates an application's ability to manage and control the platform hardware and software distribution. Although this feature addresses the need to support Rack Mount Servers in general, the use of the Out-of-Band (OOB) management port limits support to specific Rack Mount Servers.

To support Rack Mount Servers, the PMAC needs to have network access to the Out-of-Band (OOB) management port (HP iLO or the Sun Netra iLOM) of the RMS. By gaining access to the RMS OOB, PMAC is able to gather information (hardware discovery) about the RMS in a similar fashion to an enclosure OA. This hardware discovery enables PMAC to support IPM of an RMS.

This access should be across the Management Network. The control network is expanded to include connectivity to the RMS onboard NICs. This control network connectivity allows PMAC to perform software discovery of an RMS. This software discovery enables PMAC to support upgrade of an RMS.

Use the following procedure to view inventory information of a specific RMS.

1. Click **Hardware** > **System Inventory** > **Cabinet X** > **RMS XXX**, where *Cabinet X* indicates the ID of the cabinet and *RMS X* indicates the ID of the RMS.

Enclosure inventory

The PMAC GUI provides summary and detailed inventory information on discovered enclosures. Inventory information is also available for components such as the **PEM** and fan tray.

Enclosure Inventory Summary page

The Enclosure Inventory Summary page is accessible on the GUI main menu under **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** where *Enclosure X* indicates the ID of the enclosure. The page provides an enclosure-specific inventory summary as an interactive schematic.

Enclosure Inventory Summary elements

These elements appear on the Enclosure Inventory Summary page.

Table 5-11 Elements on the Enclosure Inventory Summary Page

Field	Description
Interactive schematic	Depicts the front of the enclosure: the 16 bays and the 6 PEMs. Upon hover over, the schematic identifies and provides additional information about the enclosure component. If you select a bay, further data detailing the configuration of the blade in the bay appears.
Tasks button	Displays a floating window of background tasks pertaining to the Enclosure being viewed.
Rediscover Enclosure (under the schematic)	Provided in case it is necessary to resynchronize the PMAC software with the actual enclosure hardware data.

Rediscovering Enclosure Hardware

Caution: This command is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

The Rediscover Enclosure Hardware page is accessible on the GUI main menu under **Hardware** > **System Inventory** > **Enclosure X** (select **Re-discover Enclosure** button). The **Re-discover Enclosure** operation resynchronizes the PMAC software with the actual enclosure hardware. The operation repopulates the PMAC database with updated enclosure data.

When the command is issued, a dialog box appears to confirm the action.

Click **OK** to display a notification box that indicates success or failure of the re-discover request. Click **Cancel** to close the dialog box and return to the previous work area without any changes.

The **Re-discover Enclosure** option requires that the user have permissions to execute the **Add Enclosure** and **Delete Enclosure** commands.

Viewing inventory of an enclosure

Use the following procedure to view inventory information of a specific enclosure.

1. Select **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X**, where *Enclosure X* indicates the ID of the enclosure.

The Enclosure Inventory Summary page appears.

2. (Optional) To identify a enclosure component in the schematic, place your cursor over the element.
3. (Optional) To obtain additional information about an element, click the component.
4. (Optional) To view additional information for tasks in the Background Tasks table, select the notepad icon in the lefthand column..

   The details appear below the task.

Issuing the Rediscover Enclosure command

Caution: This command is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

Use this procedure to resynchronize the PMAC software with the enclosure hardware and to repopulate the PMAC database with updated enclosure data.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Select **Hardware** > **System Inventory** > **Cabinet** > **Enclosure X** (where *Enclosure X* indicates the Enclosure ID).

   The Enclosure Inventory Summary page appears.
3. Click **Rediscover Enclosure** (under the schematic).

   A Confirmation Dialog Box page appears.
4. Click **OK** to verify that you want to continue.

   A message informs you that the **Add Enclosure** background task has been launched. The message also provides a task ID and a link so that you can monitor the background task.
5. Click the **Task Monitoring** link to monitor the progression of the background task.

   The progress status percentage indicator turns green when it has completed.

The PMAC software is now resynchronized with the enclosure hardware inventory.

Enclosure Details Inventory page

The Enclosure Details Inventory page is accessible under **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info**. The **Enclosure Details Inventory** page provides information on the enclosure's product, board, and chassis area.

Note: The set of rows that is populated on the Enclosure Details Inventory page depends on the hardware on your system. Not all rows are applicable to all hardware types.

The user can also drill-down further (for example, **Hardware** > **System Inventory** > **Enclosure X** > **Enclosure Info** > **PEM**) to obtain information about components such as the PEM and fan tray.

Enclosure Details Inventory elements

These sections describe the elements that appear on each table on the Enclosure Details Inventory page:

- Product area
- Board area
- Chassis Area

Product area

Product Area information is available for the enclosure and for these enclosure components:

- The PEM under **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info** > **PEM**
- The fan tray under **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info** > **Fan Tray**

The Product Area information is automatically discovered by PMAC:

Table 5-12 Elements in the Product Area Table

Element	Description
Manufacturer	The name of the manufacturer of the product as reported from the product's FRU information. The product manufacturer may differ from the board manufacturer if the part is being integrated into a larger product offering.
Product Name	The name of the product as assigned by the product manufacturer.
Product Version	The product version number as assigned by the product manufacturer.
Part Number	The product part number as assigned by the product manufacturer.
Serial Number	The serial number assigned by the product manufacturer. The serial number uniquely identifies this product to the product manufacturer.
Asset Tag	The asset tag assigned to the product by the product manufacturer.
File ID	Optional field for the use of the product manufacturer.

Board area

Board Area information is available for the enclosure and for these enclosure components:

- The PEM under **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info** > **PEM**.
- The fan tray under **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info** > **Fan Tray**.

The Board Area information is automatically discovered by PMAC:

Table 5-13 Elements in the Board Area Table

Element	Description
Manufacturer	The name of the manufacturer of the component as reported from the component's FRU information. Examples of components are a board, a fan tray, and a power supply.
Manufacturer Date/Time	The date and time when the component was manufactured, represented by the number of seconds since 00:00:00, January 1, 1970, Coordinated Universal Time (UTC).
Product Name	The name of the component as assigned by the component manufacturer.
Part Number	The component part number as assigned by the component manufacturer.
Serial Number	The serial number assigned by the component manufacturer. The serial number uniquely identifies this product to the component manufacturer.
File ID	Optional field for the use of the component manufacturer.

Chassis Area

Chassis Area information is available for the enclosure and for these enclosure components:

- The PEM under **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info** > **PEM**.
- The fan tray under **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info** > **Fan Tray**.

The Chassis Area information is automatically discovered by PMAC:

Table 5-14 Elements in the Chassis Area Table

Element	Description
Part Number	The part number assigned to the chassis as reported from the chassis's FRU information.
Serial Number	The serial number assigned to the chassis as reported from the chassis's FRU information.

Viewing inventory of enclosure details

The Enclosure Details Inventory provides a detailed listing of the manufacturer-provided data (product, board, and chassis area data) associated with the selected enclosure. Use the following procedure to view enclosure details:

1. Select **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info** (where *Enclosure X* specifies the ID of the enclosure).

   The Enclosure Details Inventory page appears.

The selected information displays immediately.

Viewing inventory of PEM or fan tray

Use this procedure to display the product, board, and chassis area data for the PEMs and the fan trays.

1. Select **Hardware** > **System Inventory** > **Cabinet X** > **Enclosure X** > **Enclosure Info** > **enclosure_component** (where *Enclosure X* specifies the ID of the enclosure and *enclosure_component* specifies the PEM or fan tray to display).

   The Enclosure Details Inventory page appears.

The selected information appears immediately.

Bay information

PMAC provides blade summary information for a given **bay**. Storage and PCI expansion blades are also supported.

Bay pages

The Enclosure - Bay pages are accessible under **Hardware** > **System Inventory** > **Enclosure X** > **Bay X**, where **X** specifies the component ID.

The Enclosure - Bay pages use tabs to access summary information for the device residing in the bay:

- Pages of bays with server blades provide hardware, software, network, and virtual machine (VM) information. Only servers with the Tekelec Virtual Operating Environment (TVOE) installed also display VM information.
- Pages of bays with Onboard Administrators or switches provide only hardware information.

To view the information, click the respective tab. The Hardware tab displays by default.

Table 5-15 Tabs on Bay Page

To view...	...select this tab:
Hardware summary information	Bay Hardware Tab
Software summary information	Bay Software Tab
Network summary information	Bay Network Tab
VM Info summary information	Bay VM Info Tab

Bay pages make common commands available above and below each tab. The Tasks button on the toolbar displays a floating window containing the Background Task table with the background tasks of actions initiated from this work area.

Other buttons allow you to perform these actions:

- Install the operating system (TPD/TVOE)
- Install, upgrade, or patch an application
- Accept or reject an upgrade or patch
- Perform a reset to shut down and then restart the RMS. Note that the shutdown is not graceful.

Bay page elements

The Bay page contains these tab elements:

Table 5-16 Tab elements on the Bay page

Component	Description
Hardware	Displays hardware information, including an LED state indicator and the ability to refresh table data and toggle the LEDs on or off
Software	Displays information about the operating system and application installed on the RMS
Network	Displays a content pane with details for a given hostname combination
VM Info	Displays information about guest virtual machines

The Bay page contains these button elements:

Table 5-17 Button elements on the Bay page

Component	Description
Tasks	Button in the toolbar that displays a floating window containing the Background task table with the background tasks of actions initiated from this work area.

Table 5-17 (Cont.) Button elements on the Bay page

Component	Description
Install OS	Lets you install the operating system (TPD) on the server blade you are on. Clicking this button opens the Software - Select Image page.
Cold Reset	**Cold Reset** removes power from the blade for a moment.
Warm Reset	**Warm Reset** shuts down and then restarts the server blade.
Upgrade	Lets you install or upgrade the application software on the server blade you are on. Clicking this button opens the Software Upgrade - Select Image page.
Accept Upgrade	Lets you accept an upgrade on the server blade.
Reject Upgrade	Lets you reject an upgrade on the server blade.
Patch	This button allows you to patch the server blade. Clicking this button opens the Software Upgrade - Select Image page.
Accept Patch	This button allows you to accept a pending patch on the server blade.
Reject Patch	This button allows you to reject a pending patch on the server blade.

Bay Hardware Tab

Bay hardware information is accessible under **Hardware** > **System Inventory** > **Enclosure X** > **Bay X** , where **X** specifies the component ID. The Hardware tab displays by default.

The Hardware tab provides hardware information for the hardware component that resides in the bay, such as Onboard Administrators, switches, SAN switches, storage blades, PCI expansion blades, and server blades. The information includes product, board, partner device, and chassis area data.

Note: Partner device data displays only for storage blades, PCI expansion blades, and their partner blades.

Note: The set of rows that is populated depends on the actual hardware of the system. Not all rows and actions are applicable to all hardware types.

Use the Tasks button on the toolbar to monitor background tasks for actions initiated from this work area.

Bay Hardware Tab elements

The Bay Hardware tab elements provide index cards with data for the following areas:

- Entity Summary
- Product Area
- Board Area
- Partner Device
- Chassis Area

Entity Summary

Entity Summary includes standard information, if applicable, including Entity Type, Enclosure, Bay and Hot-swap State.

Table 5-18 Elements in the Entity Summary Index Card

Element	Description
Entity Type	The Onboard Administrator, server blade, switch, SAN switch, or storage blade that resides in the bay.
Enclosure	The enclosure ID.
Bay	The bay location: 0AR or 1 - 16F or R. Note that PMAC appends a character to the bay location to indicate the orientation (F for front and R for rear). An example is 1F, which represents bay 1 on the front of the enclosure.
Hot-swap State	One of the following hardware states as defined in the HPI specification for an entity in the system: • Not Present • Insertion Pending • Extraction Pending • Active (Blade is not safe to remove from the enclosure). • Inactive (Blade is safe to remove from the enclosure).

Product Area

Product Area information is automatically discovered by PMAC.

Table 5-19 Elements in the Product Area Index Card

Element	Description
Manufacturer	The name of the manufacturer of the product as reported from the product's FRU information. The product manufacturer may differ from the board manufacturer if the part is being integrated into a larger product offering.
Product Name	The name of the product as assigned by the product manufacturer.
Part Number	The product part number as assigned by the product manufacturer.
Product Version	The product version number as assigned by the product manufacturer.
Serial Number	The serial number assigned by the product manufacturer. The serial number uniquely identifies this product to the product manufacturer.
Asset Tag	The asset tag assigned to the product by the product manufacturer.
File ID	Optional field for the use of the product manufacturer.

Board Area

Board Area information is automatically discovered by PMAC.

Table 5-20 Elements in the Board Area Index Card

Element	Description
Mfg Date/Time	The date and time when the component was manufactured, represented by the number of seconds since 00:00:00, January 1, 1970, Coordinated Universal Time (UTC).
Manufacturer	The name of the manufacturer of the component as reported from the component's FRU information. Examples of components are a board, a fan tray, and a power supply.
Product Name	The name of the component as assigned by the component manufacturer.
Part Number	The component part number as assigned by the component manufacturer.

Table 5-20 (Cont.) Elements in the Board Area Index Card

Element	Description
Serial Number	The serial number assigned by the component manufacturer. The serial number uniquely identifies this product to the component manufacturer.
File ID	Optional field for the use of the component manufacturer.

Partner Device

Partner Device information is automatically discovered by PMAC.

Note: This index card is only displayed for storage blades, PCI expansion blades, and their partner blades.

Table 5-21 Elements in the Partner Device Index Card

Element	Description
Name	The name of the partner device.
Bay	The bay identifier of the partner device. This identifier is also a hyperlink that can be used to display the hardware page of the partner device.

Chassis Area

Chassis Area information is automatically discovered by PMAC.

Table 5-22 Elements in the Chassis Area Index Card

Element	Description
Part Number	The part number assigned to the chassis as reported from the chassis's FRU information.
Serial Number	The serial number assigned to the chassis as reported from the chassis's FRU information.

Bay Software Tab

Bay software information is accessible under **Hardware** > **System Inventory** > **Enclosure** > **Bay X**, where **X** specifies the component ID. Select the Software tab.

Note: This tab is available only for server blades.

The Software tab provides software information for the server blade in the bay. The information includes operating system and application details.

Note: The set of rows that is populated depends on the actual hardware of the system. Not all rows and actions are applicable to all hardware types.

Use the Tasks button on the toolbar to monitor background tasks for actions initiated from this work area.

Bay Software Tab elements

The bay Software tab elements consist of index cards with data for the following areas:

- Operating System Details
- Application Details

Note: The set of rows that is populated depends on the actual hardware of the system. Not all rows and actions are applicable to all hardware types.

Operating System Details

This index card provides detailed information about the operating system installed on the server blade. The operating system must provide this data; otherwise, the data is left blank.

Table 5-23 Elements in the Operating System Details Index Card

Element	Description
Operating System	Identifies the operating system (TPD) on the server blade.
OS Version	Identifies the TPD version on the server blade.
Hostname	Identifies host name of the server blade.
Platform Software	Identifies the platform software.
Platform Version	Identifies the platform version.
Upgrade State	Identifies if the system has an unaccepted upgrade state pending. May display "Not In Upgrade", "In Upgrade", or "Pending Acc/Rej".

Application Details

This index card provides detailed information about the application installed on the server blade. The application must provide this data; otherwise, the data is left blank.

Table 5-24 Elements in the Application Details Index Card

Element	Description
Application	Identifies the application.

Table 5-24 (Cont.) Elements in the Application Details Index Card

Element	Description
Version	Displays the application version or one of the following upgrade states: Pending Acc/Rej or In Upgrade. **Note:** There might be times during an upgrade when PMAC is not able to query and display the upgrade state.
Function	Identifies the application function.
Designation	Identifies the application designation.

Bay Network Tab

Bay network information is accessible under **Hardware** > **System Inventory** > **Enclosure X** > **Bay X**, where **X** specifies the component ID. Select the Network tab.

Note: This tab is available only for server blades.

The Network tab provides network information for the server blade in the bay. The information includes details for a given hostname combination.

Note: The set of rows that is populated depends on the actual hardware of the system. Not all rows and actions are applicable to all hardware types.

Use the Tasks button on the toolbar to monitor background tasks for actions initiated from this work area.

Bay Network Tab elements

The Bay Network tab consists of an index card with data about the following area:

- Networking Details for hostname

Networking Details for hostname

This index card provides information pertaining to network interfaces of the server blade in the current bay.

Table 5-25 Elements in the Networking Details index card

Element	Description
The Networking Details for Hostname X tables provide detailed data for a given host combination. Provisioned IPv4 and IPv6 IP addresses are shown. The following fields appear in the Networking Details tables:	
IP Address	The IP address of the interface.

Table 5-25 (Cont.) Elements in the Networking Details index card

Element	Description
Admin Status	The administrator-defined status (**up** or **down**) for an interface. The **Admin Status** is differentiated from the **Operating Status** (also **up** or **down**) in that the **Operating Status** is defined by the actual, current state of the interface. For example, when the administrator brings an interface online, the **Admin Status** of the interface would be **up**. If the **Operating Status** then shows that the interface is **down**, the contradictory status indicates that there might be a problem.
Operational Status	The actual status (**up** or **down**) for an interface. The **Operating Status** is differentiated from the **Admin Status** (also **up** or **down**) in that the **Admin Status** is defined by the administrator. For example, when the administrator brings an interface online, the **Admin Status** of the interface would be **up**. If the **Operating Status** then shows that the interface is **down**, the contradictory status indicates that there might be a problem.

Bay VM Info Tab

Bay virtual machine information is accessible under **Hardware** > **System Inventory** > **Enclosure X** > **Bay X**, where **X** specifies the component ID. Select the VM Infotab.

> **Note:** This tab is available only for servers running the Tekelec Virtual Operating Environment (TVOE).

The VM Info tab provides detailed information pertaining to guest virtual machines.

Bay VM Info Tab elements

The bay VM Info tab elements provides an index cards with data for the following area:

- Guests for hostname Index Card

Guests for hostname Index Card

Table 5-26 Elements on the Guests for hostname Index Card

Element	Description
Name	Name of the guest virtual machine.
Status	The status of the guest virtual machine.

FRU information

The PMAC GUI lets you pull up a FRU information report for all hardware discovered on the system. This section describes the report and provides procedures for exporting the report data to a file.

FRU Information page

The FRU Information page is accessible under the **Hardware** > **System Inventory** > **FRU Info** menu option.

The report provides information such as the product version number, part number, and serial number for all field replaceable units. The report can also be exported to a .csv file.

FRU Information elements

The FRU Information page contains these tabs:

- Enclosure FRU Information tab
- RMS FRU Information tab

Table 5-27 Elements on the Enclosure FRU Information page

Element	Description
Enclosure ID	Indicates the enclosure where the FRU item is located.
Bay #	Indicates the bay where the FRU item is located.
Product Name	The name of the product as assigned by the product manufacturer.
Product Version	The product version number as assigned by the product manufacturer.
Part Number	The product part number as assigned by the product manufacturer.
Serial Number	The serial number assigned by the product manufacturer. The serial number uniquely identifies this product to the product manufacturer.
Export Enclosure FRU	Exports the FRU data as a text file to disk.

Table 5-28 Elements on the RMS FRU Information page

Element	Description
RMS Name	The name of the provisioned RMS.
RMS IP	The IP address of the provisioned RMS.
Product Name	The name of the product as assigned by the product manufacturer.
Part Number	The product part number as assigned by the product manufacturer.
Serial Number	The serial number assigned by the product manufacturer. The serial number uniquely identifies this product to the product manufacturer.
Firmware Version	The current version of firmware associated with the remote management port.
Export RMS FRU	Exports the FRU data as a text file to disk.

Viewing FRU information

Use this procedure to view a report providing FRU information for your system:

1. Select **Hardware** > **System Inventory** > **FRU info**.

   For field definitions of the displayed data, see FRU Information elements.

2. Select the desired tab to view either the enclosure FRU info or the RMS FRU info.

3. (Optional) Click any of the column headers in the table to sort the table by that column. Click again on the same column header to reverse the direction of the sort (ascending or descending).

The FRU Information page appears for the selected tab.

To export the FRU information, perform Exporting FRU information.

Exporting FRU information

This procedure assumes that you have the data to export displayed on your screen. If you do not, access the FRU Information page.

Use this procedure to export FRU data from the FRU Information page to disk. The exported file is in CSV (comma-separated value) format.

This procedure was written for Microsoft Internet Explorer 9.0, 10.0, or 11.0 (earlier releases are not supported). The procedure may vary slightly for other browsers or later browser versions.

1. Click **Export**.

   The File Download dialog appears.

2. Make a note of the filename.

3. Click **Save**.

You will be prompted to specify the location for the file.

4. Specify the location and then click **Save**.

   The file is saved to disk at the specified location. The Download Complete dialog appears. Alternatively, a download in-progress dialog might appear. This depends on your browser setup.

5. (Optional) Click **Close** to close file, or if you'd like to view the contents of the file, click **Open**.

   This applies only if you elect to open the file instead of saving it.

The file is now available in CSV format at the specified location.

Software inventory information

The PMAC GUI provides a software inventory report on the discovered software in the inventory of servers under the control of PMAC. This section describes the report and provides a procedure for accessing it.

Software inventory lists the applications on the platform for discovered TPD servers and provides data on the application's version, function, IP address, and identity information. The software inventory option also provides data on the operating system. The user can also view the software inventory for PMAC, for servers without applications, and for servers without an operating system.

To retrieve application data, the application must be configured to make the software inventory data available to PMAC.

While the discovery process is in-progress (for example, after the PMAC server has been rebooted or restarted), the information in the report will be incomplete. The following variations may occur:

- If the software discovery is complete but the hardware discovery is not, a server would show up in the software inventory report with blank identity information. Once the hardware in the bay of the enclosure is discovered, the identity information data is populated.
- If the hardware discovery is complete but the software discovery is not, the only data provided for a server is the identity information. During software discovery an IPv6 address for the server may appear for a moment. When the software discovery completes, the IPv4 address replaces the IPv6 address and any additional discovered software data is provided.

Software Inventory page

The Software Inventory page is accessible under the **Software** > **Software Inventory** menu option. The table on the Software Inventory page is the software inventory report, which shows the discovered software in the inventory of servers under the control of PM&C. In addition, you can access more information about a given enclosure, bay, or RMS. You can also install an OS, upgrade an application, patch a server, accept/reject an upgrade or patch on one or more target servers. In addition, you can transfer an ISO Image.

Note: Click on the Enclosure ID link in the Ident column to be redirected to the Enclosure XXX - Inventory Summary page.

Click on the Bay ID in the Ident column to be redirected to the Enclosure XXX - Bay XXX page.

Click on an RMS name link to be directed to the RMS XXXXX with IP XXX page. Click on a guest name link to be directed to the View VM Guest work area for the guest.

One or more rows in the Software Inventory table can be selected for use as targets for one of the action buttons at the bottom of the page. Clicking a single row will select only that row. Clicking one row, then holding down Shift while clicking another row will select those two rows and all rows between them; Holding down Ctrl and clicking a row will add or remove that row from the selection.

Software Inventory elements

The Software Inventory page contains the following elements:

Table 5-29 Elements on the Software Inventory page

Element	Description
Ident	The identity information of the server. The field will always be blank for any unprovisioned server. An **Enclosure** link takes you to the Enclosure Inventory Summary page. A **Bay** link takes you to the Bay Summary tab. An RMS link takes you to the RMS Hardware tab. A guest link takes you to the View VM Guest work area for the guest.
IP Address	The IP address of the server where the application resides. If available, IPv4 addresses are displayed. In some cases during the installation, PMAC is unable to obtain the IPv4 addresses via SNMP. In such cases, PMAC displays the IPv6 address (for example, fe80::226:55ff:fe7d:9b10).
Hostname	The configured hostname of the server.
Plat Name	The name of the operating system.
Plat Version	The version of the operating system. This field also indicates the TPD architecture as follows: • **TPD (i686)** indicates a 32-bit TPD. • **TPD (x86_64)** indicates a 64-bit TPD.

Table 5-29 (Cont.) Elements on the Software Inventory page

Element	Description
The remaining fields on the page are defined by the application. If the application is not set up to display data in these fields, these fields will appear blank.	
App Name	The name of the application.
App Version	The version of the application or one of the following upgrade states: **Pending Upgrade Acc/Rej**, **Pending Upgrade and Patch Acc/Rej**, or **In Upgrade**. **Note:** There might be times during an upgrade when PMAC is not able to query and display the upgrade state.
Desig	The designation used to identify the server.
Function	The function of the application.

Table 5-29 (Cont.) Elements on the Software Inventory page

Element	Description
Buttons	The following links are provided: **Install OS** This button is enabled if one or more rows of the grid are selected. Clicking the button opens the Software Install - Select Image page. Use this page to install an operating system (OS). **Upgrade** This button is enabled when one or more rows containing a server with an installed OS are selected. Clicking the button opens the Software Upgrade - Select Image page. Use this page to upgrade an OS or to install or upgrade an application. **Accept Upgrade** This button is enabled if one or more rows containing servers in the **Pending Upgrade Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** upgrade state are selected. Click **Accept Upgrade** to accept upgrades on the selected servers. **Reject Upgrade** This button is enabled if one or more rows containing servers in the **Pending Upgrade Accept/Rej** or **Pending Upgrade and Patch Acc/Rej** upgrade state are selected. Click **Reject Upgrade** to reject upgrades on the selected servers. **Patch** This button is enabled when one or more rows containing a server with an installed OS are selected. Clicking the button opens the Software Upgrade - Select Image page. Use this page to patch software on the selected servers. **Accept Patches** This button is enabled if one or more rows containing servers in the **Pending Patch Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state are selected. Click Accept Patches to accept patches on the selected servers.

Table 5-29 (Cont.) Elements on the Software Inventory page

Element	Description
	Reject Patches This button is enabled if one or more rows containing servers in the **Pending Patch Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** state are selected. Click Reject Patches to reject patches on the selected servers. **Transfer ISO Image** This button transfers the selected single ISO image to one or more selected remote servers on the PM&C control network. The button will become enabled only if all of the selected items have been discovered by PM&C (PM&C itself not included) as having a TPD OS installed. **Map Device Aliases** Selecting **Map Device Aliases** regenerates ISO for the selected guests. After you click the button, a Dialog box confirms the action. For any guest that is running PM&C application, an additional dialog box is displayed to let you to skip such guest. If a regenerate ISO action fails for a given guest, it is added to the Error window below the Software Inventory heading. If the action is successful, it is displayed in the Info window. Note that **Map Device Aliases** is enabled only if all selected entries are virtual guests. **Refresh** This button is enabled if one or more rows containing discovered servers are selected. Click **Refresh** to rediscover the details of the selected servers. **Note:** These buttons act on the server or servers that are selected in the grid. If multiple servers are selected, the operation is applied to all of the servers.

Table 5-29 (Cont.) Elements on the Software Inventory page

Element	Description
Pause Updates	Allows the user to temporarily suspend ("pause") the automatic page refresh that occurs automatically when the page is entered. If the checkbox is "checked", a manual page Refresh will "uncheck" the checkbox.

Display filter

The Software Inventory page includes a Display Filter, which allows filtering the inventory display according to the contents of one or more columns of the table.

You can filter the display based on the content of one or more columns by selecting an operator and entering text to compare against. Selecting an operator of "Ignored" for a column allows for any value in that column.

Note: The Ident column of the table actually consists of a combination of Enclosure, Bay, and Guest or RMS and Guest (whatever is known about a managed server), but the filter presents those components separately.

Viewing the software inventory

Use this procedure to view the software inventory for your system:

1. Click **Software** > **Software Inventory**.
2. Select an item from the Ident column to view additional information about the selected item.

6

Background Tasks

This section describes the **background task**s that run on PMAC and how to monitor them.

Overview

PMAC executes some operations as background tasks so that the user can continue to use the PMAC GUI while the background task is in progress. This section describes the background tasks that PMAC executes: **Add Enclosure**, **Add Image**, **Backup PMAC**, **Configure Storage**, **Install OS**, and Install/Upgrade App.

Each of the background tasks has a specific set of states that it transitions through as it progresses to completion. The PMAC GUI provides the capability of monitoring the progress of each background task.

When an error condition is encountered, the background task stops progressing and remains in a failed state. Upon successful completion, the background task indicates success and remains in the completed state. If a background task exceeds a defined timeout, then the task is marked as failed and the task is no longer tracked.

By default, records in the table are sorted in the order that the background tasks were initiated. Clicking a column heading sorts the table by that field. The Background Task table's contents auto-refreshes every 15 seconds, unless the pause updates checkbox is checked.

You can view the background tasks on the Background Task Monitoring page. The page is accessible from the main menu under **Task Monitoring**. This section provides instructions on using the **Task Monitoring** functions.

Note: A smaller version of the table is also available on the **Tasks** toolbar button on pages from which background tasks are launched. On those pages, tasks pertaining only to the given page are displayed. For example, the Configure Enclosures page provides the table to monitor exclusively the Add Enclosure background task.

Add Enclosure background task

Caution: This command is not intended for general customer use and should be used only as directed by My Oracle Support.

The **Add Enclosure** command lets the PMAC application begin executing a background task to add an enclosure to the PMAC hardware inventory. This configuration also establishes connectivity between PMAC and the Onboard

Administrators. PMAC fails the background task if communication cannot be established with an Onboard Administrator.

The **Edit Enclosure** command, which is used to change or add an OA IP address, also causes the PMAC application to execute the **Add Enclosure** background task. The Rediscover Enclosure command also causes the PMAC application to execute the Add Enclosure background task.

If an authorized user deletes an in-progress **Add Enclosure** background task, the background task is cancelled. The deletion of the **Add Enclosure** background task takes approximately 4 minutes to complete. An error is issued if an attempt to start a new **Add Enclosure** background task is made during that time.

On the Background Task Monitoring page on the PMAC GUI, the user can monitor the progress of the **Add Enclosure** background task. The **Status** field shows the current step being executed.

Add Enclosure background task steps

The table shows the steps associated with the **Add Enclosure** background task. Note that as a step completes, the page must be refreshed for the next step to display.

Table 6-1 Add Enclosure Steps

Step	Status Field	Description
1	Starting Add Enclosure.	The user has initiated the **Add Enclosure** command via the PMAC GUI and the PMAC application begins the **Add Enclosure** background task.
2	Configuring Enclosure.	Starting the OpenHPI daemon to monitor the enclosure.
3	OpenHpi Daemon Started.	OpenHPI Daemon has been spawned.
4	Enclosure added - starting monitoring.	The **smacMon** process has established communication with the enclosure and monitoring has begun. The **Add Enclosure** background task is complete.
5	Success.	

Add Image background task

The **Add Image** command allows PMAC to move a software image from any of these locations to the PMAC image repository:

- `/var/TKLC/upgrade/`
- `/var/TKLC/smac/image/isoimages/home/smacftpusr/`
- From Oracle-provided media in the PMAC host's CD/DVD drive.

The time it takes to move an image depends on the size of the image.

When the **Add Image** command is executed, the **Add Image** background task is launched.

On the Background Task Monitoring page of the PMAC GUI, you can monitor progress as the **Add Image** background task executes. The **Status** field shows the current step being executed.

Once issued, the **Add Image** command cannot be stopped. An authorized user can delete the background task from the GUI. The deletion stops the tracking of its status but not its execution.

Add Image background task steps

The table shows the steps of the Add Image background task.

Table 6-2 Add Image Steps

Step	Status Field	Description
1	Verifying image source.	PMAC verifies that the software image exists. Also verifies that the software image is not already in the image repository.
2	Mount source image.	PMAC temporarily mounts the software image to examine the files.
3	Validate source image.	PMAC validates the software image as follows. If the source software is a TPD image, PMAC looks for a TPD-based validation mechanism. If the mechanism is present, PMAC uses it to validate the contents of the image. If no validation mechanism exists, the image is assumed to be valid.
4	Extract boot files.	PMAC copies the boot configuration files from the image if the image is bootable.
5	Unmount source image.	PMAC unmounts the temporary mount.
6	Copy image.	PMAC copies the image to permanent storage and the PMAC database is updated with information about the image.
7	Mount image.	PMAC mounts the imported image on the file system.

Table 6-2 (Cont.) Add Image Steps

Step	Status Field	Description
8	Share image.	PMAC sets up the image for use by other server blades. The mounted software image is exported to make it available on the server blade.
9	Removing image from temporary path.	PMAC performs clean up prior to completing the operation.
	Success.	

Backup PMAC background task

The **Backup PM&C** command lets the PMAC application begin executing a background task to back up the PMAC server data to the specified location.

If an authorized user deletes an in-progress **Backup PM&C** background task, the deletion stops the tracking of its status, but not its execution.

Only one **Backup PM&C** background task can run at a time. An error is issued if an attempt is made to start a new **Backup PM&C** background task before the first background task completes.

On the Background Task Monitoring page on the PMAC GUI, you can monitor the progress of the **Backup PM&C** background task. The **Status** field shows the current step being executed.

Backup PMAC background task steps

The table shows the steps associated with the **Backup PMAC** background task.

Table 6-3 Backup PMAC Steps

Status Field	Description
Backing up PMAC.	The user has initiated the **Backup PM&C** command via the PMAC GUI and the PMAC application launches the **Backup PM&C** background task.
One of these status messages displays: • PMAC backup successful • Failed to backup PMAC server: <*reason*>	There are two possible status messages for this step: • The backup was successful. • The backup failed. Instead of <*reason*>, the output provides the reason that the backup failed if it is known.

Configure Storage background task

Caution: This command is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

The **Configure Storage** command is issued using the PMAC GUI under **Storage** > **Configure SAN Storage**. The command accesses one or more XML files containing the configuration settings for the storage devices. The files specify the Vdisks, Global Spares, and Host Volumes to be configured on the Controllers and Hosts. The files also can be used to remove an existing configuration. The command executes as a background task.

Once issued, the **Configure Storage** command cannot be stopped. An authorized user can delete the background task.The deletion stops the tracking of its status but does not stop the actual installation.

On the Background Task Monitoring page on the PMAC GUI, the user can monitor the progress as the **Configure Storage** background task executes. The **Status** field shows the current step being executed.

Configure Storage background task steps

The table shows the main steps of the **Configure Storage** background task.

Table 6-4 Configure Storage Steps

Step	Status Field	Description
1	Starting Storage Configuration.	The XML file has been loaded and the storage configuration is starting.
2	Storage Configuration File Parsed.	The XML file has been parsed.
	The following steps vary according to the actions requested in the XML file. Some steps may not appear at all; some steps may appear multiple times. For this reason, the step numbers have been omitted in this table.	
	Configuring Vdisk <*vdiskname*> on Controller <*controller ip*>.	This step appears once for each Vdisk. This step appears only if a Vdisk is being configured. Instead of <*vdiskname*> and <*controller ip*>, the Vdisk Name and Controller IP address from the XML file appear in the respective fields.

Table 6-4 (Cont.) Configure Storage Steps

Step	Status Field	Description
	Configuring Global Spares <*disk list*> on Controller <*controller ip*>.	This step appears only once. The one step is used for any Global Spare(s) being requested. This step appears only if a Global Spare is being configured. Instead of <*disk list*> and <*controller ip*>, the disk list of the Global Spare(s) and the Controller IP address from the XML file appear in the respective fields.
	Configuring <*size*> MB Host Volume for Host <*host ip*>.	This step appears once for each host volume. This step appears only if a host volume is being configured. Instead of <*size*> and <*host ip*>, the size (in megabytes) of the Host Volume and the Host IP address from the XML file appear in the respective fields.
	These steps appear for all **Configure Storage** background tasks that complete successfully.	
	Storage Configuration Completed.	The storage configuration has completed.
	Storage Configuration successful.	The storage configuration and cleanup have completed successfully.
	In the event of a failure, there is detailed reporting on what failed and the step where the failure occurred.	

Install OS background task

Caution: This command is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

The PMAC GUI provides a command to load the TPD operating system on server blades, guests, and RMSs. Both commands execute as background tasks:

Click **Install OS** to initiate the installation. The Select Image page appears. Select the Image Name from the list, then click **Install OS**. PMAC creates an **Install OS** background task for each target server blade.

After it is issued, the **Install OS** command cannot be stopped. An authorized user can delete the background task. The deletion stops the tracking of its status but may not stop the actual installation.

PMAC fails the background task if a successful installation is not detected within 45 minutes.

On the Background Task Monitoring page on the PMAC GUI, the user can monitor the progress as the **Install OS** background task executes. The **Status** field shows the current step being executed.

Install OS background task steps

The table shows the main steps of the **Install OS** background task.

Table 6-5 Install OS steps

Step	Status Field	Description
1	Network PXE Boot.	The process has been launched.
2	MAC Address Discovery	Determining the MAC address and creating the **PXE** configuration file.
3	Waiting for target server to boot	PMAC has told the target server to reboot and is now waiting for it to start requesting files for installation.
4	Installing packages from ISO	The target server has begun requesting files from PMAC.
5	Final reboot.	The final boot occurs after the installation of the operating system. All configuration files associated with the installation are cleaned up. If PMAC waits more than 45 minutes for the Post Install Inform notification from TPD, PMAC fails the background task.
6	Success.	

Upgrade background task

Issue the **Upgrade** command via the PMAC GUI (see Installing/upgrading an application, or upgrading the OS). The command executes as a background task to install or upgrade a TPD operating system-compatible application on any server blade.

The PMAC GUI provides the Upgrade and Patch buttons on several pages, including hardware inventory, software inventory, and VM management pages.

Click **Upgrade** or **Patch** to initiate the process. The Select Image page appears. PMAC creates an **Upgrade** background task for each target server blade.

After it is issued, the upgrade task cannot be stopped. The background task can be deleted, which stops the tracking of the software upgrade status, but may not stop the actual upgrade from being performed.

PMAC fails the background task if a successful application install/upgrade is not detected within 60 minutes or a patch within 15 minutes.

On the Background Task Monitoring page on the PMAC GUI, the user can monitor the progress as the upgrade or patch background task executes.

Install/Upgrade App background task steps

The **Status** field for the background task provides this information.

Table 6-6 Install/Upgrade App steps

Step	Status Field	Description
1	Installing upgrade	The software upgrade request has been written to the PMAC database and PMAC has initiated the software upgrade on the target server blade.
2	ID assigned	PMAC interfaces with the installed TPD operating system of the target server blade to start the upgrade. TPD assigns a unique ID to the task.
3	In progress	The PMAC-initiated upgrade task is in progress. To determine the status of the upgrade running on the target server blade, PMAC polls TPD on the target server blade. When the upgrade is processing normally, TPD responds to the poll with a status message that reports 'In Progress'. If an error is detected in the upgrade, TPD responds to the poll with a task status of 'Complete', and PMAC performs a `get` of the task result with a 'Failed' status. After a timeout (60 minutes) occurs, the upgrade task enters a probationary timeout. This is indicated by a warning icon on the task row and text is displayed in the status column on the task monitoring page. The text asks for a manual verification of the upgrade and gives the IPv4 address of the upgrading server.For an application install or upgrade, after a timeout (60 minutes) occurs, the upgrade task enters a probationary timeout. This is indicated by a warning icon on the task row and text is displayed in the status column on the task monitoring page. The text asks for a manual verification of the upgrade and gives the IPv4 address of the upgrading server. If the upgrade completes in the probationary timeout state, it is complete, but the text note continues to be displayed. The probationary timeout restarts the timeout clock (60 minutes). After the timeout expires again, the upgrade is cleared and PMAC then fails the background task.
4	Complete	The PMAC-initiated upgrade has completed, and a status of success or failure is displayed in the PMAC GUI.

Transfer ISO Image background task

Caution: This command is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

The PMAC GUI provides the **Transfer ISO Image** command to transfer a single ISO image to one or more selected target servers. The transfer process executes as a background task for each selected server.

The **Transfer ISO Image** command is available under **Software** > **Software Inventory**, The command appears as a button on the Software Inventory page.

Clicking the **Transfer ISO Image** button opens the Image Transfer - Select Image page with a list of images available in the repository. The process starts by selecting an image and clicking the **Start Image Transfer** button. At this point, the process cannot be stopped.

PMAC creates a Transfer ISO Image background task for each target server. The user can monitor the progress by clicking the Tasks drop-down box in the Image Transfer - Select Image window. The **Status** field shows the current step being executed. An authorized user can delete the background task which stops only the tracking of the status, but it does not stop the actual process.

About deleting a background task

A background task remains displayed on the GUI until the user deletes the background task. If a user deletes a background task while it is in progress, ask from the GUI display and one of the following behaviors also occurs:

- The deletion stops the following background tasks: **Add Frame**, **Add Shelf**, and **Edit Shelf.**
- The following background tasks continue to run but are no longer tracked by the PM&C application:**Configure Fabric Switches**, **Install OS**, **Install/Upgrade App**, **Add Image,** and**FRU Shelf**.

Reconfigure and Initialize background task

Caution: This command is not intended for general customer use and should be used only as directed by My Oracle Support

PMAC Network Configuration launches a background task to perform the platform configuration. After this instruction is issued, it cannot be stopped. A success or failure will be reported within one minute of launch time. The network reconfiguration will cause the page to pause

Reconfigure and Initialization background task steps

The **Status** field for the background task provides this information. Note that as a step completes, the display must be refreshed for the next step to display on the screen.

Table 6-7 Reconfigure and Initialization Steps

Step	Status Field	Description
1	Process started	The process is launched.
2	ID assigned	A status screen is displayed. It will show either **PMAC Reconfigured** or **PMAC Reconfiguration Failure**. To determine the reason for a failure, review the log file.

Background Task Monitoring page

The Background Task Monitoring page is accessible from the main menu. The page is also accessible as a pane on the GUI pages from which a background task is launched; for example, the Add Enclosure page provides a pane to monitor the **Add Enclosure** background task.

The Background Task Monitoring page displays an historical list of background tasks. For each background task, the process or procedure performed is shown along with the hardware/physical component affected. The current status of the background task is also shown.

For an in-progress background task, the page enables you to monitor each step of the background task as it executes. The page also provides additional details for selected tasks.

By default, records in the table are sorted in the order that the background tasks were initiated. Clicking a column heading sorts the table by that field.

Each task is color-coded to indicate status:

Green
Indicates success.

Red
Indicates failure.

Blue
Indicates in progress.

Controls are also available for deleting selected background tasks, all completed background tasks, or all failed background tasks.

Background Task Monitoring elements

This section includes the following topics:

- Background Task Monitoring page
- Background task monitoring show details view

Background Task Monitoring page

Background tasks might consist of multiple steps, which are shown in the Status column. The display is updated periodically to show the task progress.

The Background Task Monitoring page contains these elements:

Table 6-8 Elements on the Background Task Monitoring Page

Field	Description
Task step details (Notepad icon)	Displays a floating window showing the steps constituting the selected task. Each step in this window includes a description and its completion time in seconds since the task started. **Note:** This is the leftmost column in the Task Monitoring grid. This column does not have a column heading.
ID	Identifies a unique ID for each task.
Task	Identifies the process or procedure such as installing an operating system or adding an enclosure.
Target	Identifies the server affected by the task. The format of this field varies depending on the information known about the affected target. For example: • Enc:1215 Bay:2F refers to the server blade located in enclosure number 1215, bay 2F (Front). • Enc:1215 Bay:2F Guest:test refers to the VM guest named "test" running on that blade. • Host IP: …99ff:fec1:58a0 Guest: main refers to the VM guest named "main" running on a server with the given IP address.
Status	Describes the progress made, thus far, toward completing the background task.
State	Describes the current state of the background task (COMPLETE, IN_PROGRESS, IN_PROGRESS_WITH_ISSUE, CANCELLED).
Start Time	Denotes the task's start time.
Running Time	Denotes the amount of time (hh:mm:ss) that has passed since the previous status update for the background task. For example, an **Running Time** entry of 2:9:4 would indicate that 2 hours, 9 minutes, and 4 seconds has elapsed since the previous status update.
Progress of a background task	Conveys the progress a background task.

Table 6-8 (Cont.) Elements on the Background Task Monitoring Page

Field	Description
Delete Completed	Deletes completed background tasks from the task history. **Note:** The deleted tasks will not appear in any other Background task table.
Delete Failed	Deletes all failed background tasks from the task history **Note:** The deleted tasks will not appear in any other Background task table.
Delete Selected	Deletes all selected background tasks from the task history. **Note:** The deleted tasks will not appear in any other Background task table.

Color codes indicate the status of the background task:

Red
Indicates failure.

Green
Indicates success.

Blue
Indicates in progress.

Additional background task information

You can view additional background task information in the Status column. Select a task and Hover over the text in the Status field to display:

Field	Description
Task ID	The task's ID value as shown in the main Task Monitoring grid.
State	Stage of completion; for example, COMPLETE, IN_PROGRESS, or CANCELLED.

Field	Description
In step *n* of *m*	The latest step to have started execution. If the task's state is FAILED, this indicates the step that was in progress when the failure occurred.
Elapsed	The time that has elapsed since the task was started.

Background task monitoring show details view

You can select the view details icon in the left-most column of the page to view additional details about the selected task.

This shows the following elements:

Table 6-9 Elements on the Background Task details view

Field	Description
step	A field that indicates where one step is stored in the database.
description	Description of the step being performed.
state	Describes the state of the step (COMPLETE, IN_PROGRESS, IN_PROGRESS_WITH_ISSUE, CANCELLED).
time	The amount of time the step took to execute.

Monitoring background tasks

After you issue a command such as **Add Enclosure** that launches a background task, PMAC provides a Tasks button where you can view background task information. The provided button is the most convenient way to monitor a background task. Alternatively, use the following procedure to monitor background tasks.

1. Select **Task Monitoring from the main menu.**.

   The Background Task Monitoring page appears.

   For field definitions, see Background Task Monitoring elements.

2. (Optional) Click a column heading to sort the table by a given field. Sorting on the leftmost (Notepad) column or the by Progress column is not supported.

3. (Optional) Click the Notepad icon in the leftmost column to display a floating window that contains details about the individual steps of the selected background task.

4. (Optional) To view additional details about a background task, and hover over the text in the Status field.

   The details appear immediately below the background task.

About deleting a background task

A background task will continue to display in the GUI until an authorized user deletes it. If it is deleted while in progress, one of the following behaviors occurs depending on the background task being deleted:

- The deletion stops the **Add Enclosure** background task.
- These background tasks continue to run but are no longer tracked by the PMAC application: **Install OS**, **Install/ Upgrade App**, **Backup PMAC**, **Configure Storage**, and **Add Image**.

Deleting a background task

Use the following procedure to delete a background task from the Background Task Monitoring page.

> **Note:** If the background task is **Add Enclosure**, the deletion stops the background task from running. All other background tasks will continue to run but will no longer be tracked by PMAC.

To execute this procedure, you must have **Background Task Admin** permission.

1. If the Background Task Monitoring page is not already displayed on your screen, select **Task Monitoring**.
2. You can delete all completed tasks, or all failed tasks, or selected tasks.

   The designated background task or tasks disappear immediately from the list. A popup window may appear briefly and then disappear. The window is not indicative of a problem.

The selected background task disappears immediately from the list.

Deleting completed background tasks

Use this procedure to delete all completed background tasks from the Background Task Monitoring page.

To execute this procedure, you must have Background Task Admin permission.

1. If the Background Task Monitoring page is not already displayed on your screen, select **Task Monitoring**.
2. Click **Delete All Completed**
3. A confirmation popup appears. Select OK to proceed with the deletion.

.

All completed background tasks disappear immediately from the list.

Deleting all failed background tasks

Use this procedure to delete all failed background task from the Background Task Monitoring page.

To execute this procedure, you must have administrative permission.

1. If the Background Task Monitoring page is not already displayed on your screen, select **Task Monitoring**.
2. Click **Delete All Failed.**

All failed background tasks disappear immediately from the list.

7

Software Installation

The PMAC GUI allows software installations and upgrades (**operating system** (**OS**), applications) using ISO images stored in the PMAC ISO image repository. These tasks can be applied to one or more HP ProLiant server(s) simultaneously: Up to 16 servers for newly installed systems (pre-OS installation), or up to 8 servers for operational systems (post-OS installation). The HP ProLiant server can be a blade in an enclosure, a **rackmount server** (**RMS**), or a guest virtual machine running on a blade or RMS.

> **Note:** The server on which PMAC is running to perform these tasks cannot be upgraded using this feature. The management server requires a manual upgrade by on-site personnel.

The installation or upgrade process performs in the background and can be monitored for each affected server.

Installing the operating system

Pre-requisites:

> **Caution:** This procedure is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

> **Caution:** Before applying an ISO image to multiple servers, ensure that the network allows for the bandwidth required by the multiple simultaneous processes. A slow-down of the image data transfer can cause PMAC to fail the background task automatically if it cannot detect a successful installation within 45 minutes for each server.

- OS image has been loaded into the software repository.
- Permissions:
  - User group admin or ops: Install OS, monitor operation, delete background task
  - guest: Monitor operation

This procedure describes how to install the TPD operating system (OS) on one or more server(s) using an ISO image.

The ISO image of the TPD operating system is bootable. During the installation process, the PM&C server performs a one-time boot from the network to load the ISO image. Then, the PM&C server installs the operating system onto the target server(s) as an individual background task per server.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Locate the target server(s):
   - To install the OS on a single server, click **Hardware** > **System Inventory** > **Cabinet** to locate the rack mount server (RMS), or the Enclosure and Bay of the server blade. If the target is a Guest server, go to **VM Management** to locate the name of the target guest.
   - To install the OS on multiple servers, go to **Software Inventory** and select the servers from the Software Inventory list.
3. Click **Install OS**.

   The Software Install - Select Image page appears.

   The Targets pane shows the server(s) to receive the installation. Verify the component label(s) to make sure that they match the desired targets. The Image table shows the available images.
4. Select the ISO image to be installed.
5. Supply software install arguments (if any) in the provided text box.
6. Click **Start Software Install**.
7. Click **OK** to confirm that you want to start the installation.

   A background task launches for each installation. A tracking number for the background task displays when the background task starts processing.
8. Select the **Task Monitoring** menu item to view the progress of the background task(s).

The operating system has been installed successfully when the Status field in the Background Task Monitoring window returns `Done` for the respective image.

Software Install - Select Image page

The Install OS Distribution page is accessible under Hardware Inventory , where *Enclosure X* is the Enclosure ID of the selected Enclosure and *Bay X* is a server blade bay. The **Install OS** command appears as a link on the Bay page.

You have accessed this page through the **Install OS** button of either the Hardware Inventory , Software Inventory, or VM Management page.

The Software Install - Select Image page lets you start the installation process by selecting an ISO image, providing software install arguments (if any), and clicking the **Start Software Install** button.

Caution: This procedure command is not intended for general customer use and should be used only as directed by Customer Access Support. See My Oracle Support.

The Software Install - Select Image page has these elements:

- A Targets pane that lists the server(s) to have the OS installed. The Status column of the Targets pane shows the Task IDs of the installations started on this page. You can follow their progress on the Task Monitoring page.
- A Software Install - Select Image table that allows you to select one image from the software repository.
- A button that starts the software install. This button is disabled until an image is selected.
- An optional Supply Software Install Arguments text box that provides arguments for the installation to be performed.

For details of the various elements, refer to Table 7-1 and Table 7-2.

Table 7-1 Software Install - Select Image Page elements

Element	Description
Targets pane	A target pane that informs the user which hardware will be receiving the installation. The information includes Entity identification and status information. The Status column of the Targets pane shows the Task IDs of installations started on this page. Their progress can be followed on the Task Monitoring page.
Select Image table	A table from which the appropriate image from the software repository can be selected. See Table 7-2.
Supply Software Install Arguments (Optional) text box	A text box that supplies arguments for the action to be performed. Each argument must be of the form **key=value** and supported by the TPD version that also supports the software being acted on. Multiple arguments must be separated by spaces or entered on new lines. If no arguments need to be supplied, leave the arguments text box empty. **Note:** PMAC does not validate the supplied arguments.
Start Software Install button	A button that begins installation.

Table 7-2 Software Install - Select Image Page Table elements

Element	Description
Image Name	Name of the available OS ISO image.You can select only one image at a time.

Table 7-2 (Cont.) Software Install - Select Image Page Table elements

Element	Description
Type	Bootable OS installations can be performed only with bootable images.
Architecture	Each image's application is optimized for either 32 (i386) or 64 (x86_64) bit architecture.
Description	This field is optionally filled in by the user when the image is uploaded to the PMAC repository.

Installing/upgrading an application, or upgrading the OS

Pre-requisites:

Caution: This procedure is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

Caution: Before applying an ISO image to multiple servers, ensure that the network allows for the bandwidth required by the multiple simultaneous processes. A slow-down of the image data transfer can cause PMAC to fail the background task automatically if it cannot detect a successful installation within 45 minutes for each server.

- The TPD OS must be installed.
- The image used for the upgrade must be of a newer version.
- The image has been loaded into the software repository.
- Permissions:
  - User group admin or ops: Install an application, upgrade to a newer version of the OS or application, monitor operation.
  - guest: Monitor operation

This procedure describes how to install an application, or how to upgrade an application or operating (OS) system to a newer version, on one or more HP ProLiant server(s) using an ISO image.

Application ISO images are of type Upgrade, the ISO image of the TPD operating system is bootable. A patch ISO is a type of upgrade. Patch ISOs are of type Patch and are not bootable. During the upgrade process of an OS ISO image, the PMAC server initiates a remote upgrade onto the target server(s) as an individual background task per server.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.

2. Locate the target server(s):

   - To install or upgrade an application on a single server, or to upgrade the OS, go to **Hardware** > **System Inventory** > **Cabinet** to locate the rackmount server (RMS), or the Enclosure and Bay of the server blade. If the target is a Guest server, go to **VM Management** to locate the name of the target guest.
   - To install an application, or upgrade an application or OS on multiple servers, go to **Software Inventory** and select the servers from the Software Inventory list.

3. Click **Upgrade** (or **Patch** if patching a server).

   The Software Upgrade - Select Image page page appears.

   The Targets pane shows the server(s) to receive the upgrade or patch. Verify the server label(s) to make sure that they match the desired target servers. The Image table shows the available bootable and upgrade ISO images.

4. Select the ISO image to be used.
5. Supply software upgrade arguments (if any) in the provided text box.
6. Click **Start Software Upgrade**.
7. Click **OK** to confirm that you want to start the upgrade or patch.

   A background task launches for each upgrade. A tracking number for the background task displays when the background task starts processing.

8. Select the **Task Monitoring** menu item to view the progress of the background task.

The application or operating system has been upgraded successfully when the Status field in the Background Task Monitoring window returns `Done` for the respective image.

Software Upgrade - Select Image page

You have accessed this page through the **Upgrade** or **Patch button** of either the Hardware Inventory, Software Inventory, or VM Management page.

The Software Upgrade - Select Image page lets you start the process to install an application, or to upgrade an application or the operating system (OS) to a newer version, or to patch the OS or application, by selecting an ISO image, providing upgrade arguments (if any), and clicking the **Start Software Upgrade** button.

> **Caution:** This procedure is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

The Software Upgrade - Select Image page has these elements:

- A Targets pane that lists the server(s) to be upgraded.

  The Status column of the Targets pane shows the Task IDs of upgrades started on this page. You can follow their progress on the Task Monitoring page.

- A Software Upgrade or Patch - Select Image table that allows you to select one image from the software repository.
- An optional Supply Software Upgrade Arguments text box to provide arguments for the upgrade to be performed.
- An optional Supply Patch Arguments group of checkboxes to provide arguments for the patch to be performed.
- The **Start Software Upgrade** button that starts the upgrade. This button is disabled until an image is selected.

For details of the various elements, refer to Table 7-3 and Table 7-4.

Table 7-3 Software Upgrade - Select Image Page elements

Element	Description
Targets	A target pane that informs the user which servers will be receiving the upgrade. The information includes Entity identification and status information. The Status column of the Targets pane shows the Task IDs of upgrades started on this page. Their progress can be followed on the Task Monitoring page.
Software Upgrade Select Image table	See Table 7-4.
Supply Software Upgrade Arguments	A text box that supplies arguments for the action to be performed. Each argument must be of the form **key=value** and supported by the TPD version that also supports the software being acted on. Multiple arguments must be separated by spaces or entered on new lines. If no arguments need to be supplied, leave the arguments text box empty. **Note:** PMAC does not validate the supplied arguments.
Supply Patch Arguments	A group of checkboxes controlling the behavior of the patching process. • **Reboot** will reboot the server after the patch has been applied when checked. • **No runlevel change required** will not shutdown applications on the server during the patch when checked. • **Modify runlevel timeout** allows for specifying a number of minutes to wait for application shutdown before the patch times out. **Note:** **Reboot** and **No runlevel change required** cannot both be checked. Additionally, **Reboot** and **Modify runlevel timeout** cannot both be checked.

Table 7-3 (Cont.) Software Upgrade - Select Image Page elements

Element	Description
Start Software Upgrade button	A button that begins the installation or upgrade.

Table 7-4 Software Upgrade - Select Image Table elements

Element	Description
Image Name	Name of the available image. **Note:** you can select only one image at a time.
Type	Bootable, Upgrade, Patch OS upgrades use bootable images. Application images are of type Upgrade. OS or Application patch images are of type Patch.
Architecture	Each image's application is optimized for either 32 (i386) or 64 (x86_64) bit architecture.
Description	Optional field that is filled in by the user when the image is uploaded to the PMAC image repository.

Transferring an ISO image

Caution: This procedure command is not intended for general customer use and should be used only as directed by Customer Access Support. See My Oracle Support.

Use this procedure to select a single ISO image from the list of available images in the repository and transfer that ISO image to a visible server.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Select **Software** > **Software Inventory**.

   The Software Inventory page appears.
3. Select the servers that the image is to be transferred to.
4. Click the **Transfer ISO Image** button at the bottom of the page.

   The Image Transfer - Select Image page appears.
5. In the **Select Image** table, select the ISO image that you want to transfer.
6. In the **Image Transfer Entity Arguments** table, enter all of the following field values, so that the transfer will complete:

   - **Path** - The path on the remote server to which the file is to be copied. The path must be in the format /xxx/yyy/zzz (with or without a / at the end).

- **User** - The Username of the user required to log into the remote server.
- **Password** - Password of the user required to log into the remote server. For security, the password is displayed on the screen as "·····" when it is entered.

  Click in the field to open the **Define a Password** dialog box, enter the password in the **Password:** field in the dialog box, and click **Done**.

7. Click **Start Image Transfer**.

   A dialog box appears requesting confirmation of the transfer of the selected file.

   - Click **OK** to confirm and continue with the transfer.

     When **OK** is clicked and all field values are not entered or are not valid, an error message appears:

   - Click **Cancel** to discontinue the transfer and return to the Image Transfer - Select Image page

   A background task launches for each ISO image transfer. A tracking number for the background task displays when the background task starts processing.

Image Transfer - Select Image page

You have accessed this page through the **Transfer ISO Image** button of the **Software** > **Software Inventory** page.

The Image Transfer - Select Image page lets you start the image transfer process by selecting an ISO image, providing image transfer entity arguments, and clicking the **Start Image Transfer** button.

> **Caution:** This procedure command is not intended for general customer use and should be used only as directed by Customer Access Support. See My Oracle Support.

The Image Transfer - Select Image page has the following elements:

- A Targets pane that lists the server(s) to which the image can be transferred.

  The Status column of the Targets pane shows the Task IDs of the Transfers started on this page. You can follow their progress on the Task Monitoring page.

- A Select Image table that allows you to select one image from the software repository.
- An Image Transfer Entity Arguments table that provides arguments for the transfer to be performed.
- A button that starts the image transfer. This button is disabled until an image is selected.

For details of the various elements, refer to Table 7-5 and Table 7-6.

Table 7-5 Image Transfer - Select Image Page elements

Element	Description
Targets pane	A target pane that informs the user which hardware will be receiving the image transfer. The information includes Entity identification and status information. The Status column of the Targets pane shows the Task IDs of transfers started on this page. Their progress can be followed on the Task Monitoring page.
Select Image table	A table from which the appropriate image from the software repository can be selected. See Table 7-6.
Image Transfer Entity Arguments table	A table that supplies arguments for the action to be performed. The path, user, and password for each target entity can be supplied by entering them into the fields in the table. • Path - Click in the box, and enter the pat the designate the directory on the target entity to which the ISO image will be transferred. • User - Click in the box, and enter a username that PM&C will use to transfer the image. • Password - Click in the field to open a dialog box. Enter the password that PM&C will use to transfer the image. Click **Done**.
Start Image Transfer button	A button that begins the image transfer.

Table 7-6 Image Transfer - Select Image Page Table elements

Element	Description
Image Name	Name of the available ISO image. You can select only one image at a time.
Type	Bootable Upgrade ISO transfers can be performed only with bootable upgrades.
Architecture	Each image's application is optimized for either 32 (i386) or 64 (x86_64) bit architecture.
Description	This field is optionally filled in by the user when the image is uploaded to the PMAC repository.

Software image management

PMAC maintains a repository of software images that are used for installing the application software, and the operating system onto server blades. This section describes the GUI pages that provide management functions for the software images.

PMAC requires a software image to install an operating system or application or on a server blade. You make the image available to PMAC by issuing the **Add Image** command on the PMAC GUI. There are several methods of supplying the image to PMAC:

- Place the image in `/var/TKLC/upgrade`. This directory is used to move an image via the network using `scp` to a directory on PMAC. This directory is typically big enough to move one image at a time.
- Transfer an image via the network using sftp to the PMAC using the pmacftpuser account. This directory is used to move an image via the network using `sftp` to a directory on PMAC.
- Provide the image on a CD or DVD inserted into the DVD drive of the server on which PMAC is running.

Each software image in the repository is mounted on the file system and made available on the network (exported) for network-based installations. A PMAC database tracks all images in the repository.

When a software image is added to the repository, it is copied so that the original source file is no longer required on the system.

Before a software image is added to the image repository, PMAC validates that the image exists on the file system and that the image does not already exist in the PMAC image repository. Additionally, PMAC checks for a TPD-based validation mechanism, and if present, uses it to validate the contents of the image.

The **Add Image** command can take more than 30 seconds to complete depending on the size of the image. For this reason, the command runs as a background task. The PMAC GUI shows the progress of the **Add Image** background task.

The PMAC GUI enables you to delete software images from the repository. When an image is deleted, it is first unmounted from the file system, and then the file is deleted. All references to the image are removed from the PMAC database.

By default, the PMAC **admin** and **ops** user groups can add images to the repository, delete images from the repository, and view the images in the repository. The **guests** user group can only view the images in the repository.

Only **ISO** image files are supported in the repository.

PMAC allocates 60 GBs of file system storage for storing images in a repository. The image repository is capable of storing a maximum of 255 software images (constrained by a maximum number of loop mounts).

Viewing software images

Use this procedure to display a list of all software images in the repository and their type (upgrade or bootable):

1. Select **Software** > **Manage Software Images**.

The Manage Software Images page appears with a list of all available images and their type.

Manage Software Images page

The Manage Software Images page is accessible under **Software** > **Manage Software Images**. The page provides a list of the available software images and their type (upgrade or bootable). The page also provides options for adding and deleting images from the repository and for editing an image's description. The **Tasks** button in the toolbar displays a floating window showing "Image Related" background tasks.

Manage Software Images elements

The Manage Software Images page contains these elements:

Table 7-7 Elements on the Manage Software Images Page

Element	Description
Images	Lists the images providing the following information: • Image name • Type (**Upgrade** or **Bootable**)(Upgrade, Bootable, or Patch). Images marked as **Bootable** are available as OS images to install. If they are not marked bootable, they are available for applications to use over the network. Patch images are for upgrade only. • Architecture (**i386**, **x86_64**, or **noarch**). A value of **i386** indicates a 32-bit software image. A value of **x86_64** indicates a 64-bit software image. A value of **noarch** indicates that the image architecture cannot be detected. • Description. The description of the software image. An information message is displayed if there are no provisioned images available.
Add Image	Provides data entry fields for entering parameters prior to executing the **Add Image** command.
Edit Image	Provides data entry fields for editing an image's description or for adding a description. The image description may not exceed 255 characters.
Delete Image	Deletes the selected image from the list.
Pause Updates	Allows the user to temporarily suspend ("pause") the automatic page refresh that occurs automatically when the page is entered. If the checkbox is "checked", a manual page Refresh will "uncheck" the checkbox.
Background Task Monitoring pane	Provides status information on the **Add Image and Delete Image** background tasks as they execute.

Adding a software image

For a procedure to upload a file using `sftp`, see Uploading files to PMAC via sftp.

Use this procedure to add a software image to the PMAC repository.

1. Use one of the following choices to make a software image available to PMAC:

   - Oracle-provided CD/DVD media in the PMAC host's CD/DVD drive (see Note below).
   - Oracle-provided USB media attached to a USB port on the PMAC host. (see Note below).

   Note: CD and USB images mounted on PMAC's VM host must first be made accessible to the PMAC VM guest. To do this, see the Media tab information in View VM Guest work area.

   - External mounts. Prefix the directory with `extfile://`.
   - Upload the image using sftp to the PMAC server.

2. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
3. Click **SoftwareManage Software Images** and then click **Add Software Image**.
4. Select the software image in the list, add a description, and then click **Add New Image**. Click **OK** to remove the image from /var/TKLC/upgrade directory as it is added to the repository. Click **Cancel** to retain the image.

   A tracking number for the **Add Image** background task is displayed as the background task starts processing. Progress can be viewed directly from the Background Task Monitoring pane of the Manage Software Images or from the main Task Monitoring page.

Editing a software image's description

Use this procedure to edit the description associated with a software image or to add a description to an existing software image.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Select **Software** > **Manage Software Images**.

   Select the software image whose description you want to change in displayed list.
3. Click **Edit Image**.

   Click **OK** to continue.
4. Click **Edit Image**.

   The filename and the current description for the file (if any) appear.
5. Edit the description as desired (maximum length is 255) and then click **Edit Image**.

   By default, the field is prefilled with current description in the system.

   A verification message appears.

The changes are saved to the database and show up on the Manage Software Images page.

Deleting a software image

Use this procedure to delete a software image from the PMAC image repository. You can delete one software image at a time.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Select **Software** > **Manage Software Images**.
3. Select an image to delete, and click **Delete Image**.
4. On the confirmation screen, perform one of the following actions:
   - Click **OK** to confirm the delete action.

     A message appears indicating the success or failure of the delete action. If the delete is successful, the image will no longer appear in the list on the Manage Software Images page.
   - Click **Cancel** to close the dialog box. The image is not deleted and still appears on the Manage Software Images page.

8

Virtual Machine Management

This section covers the virtual machine management tasks that are performed from the PMAC GUI. This allows the user to manage all hosts and virtual guests that are controlled by the PMAC.

Tekelec Virtual Operating Environment (TVOE) introduction

TVOE is an Oracle software product that provides an environment for running Kernel-based Virtual Machines (KVM).

PMAC includes virtualization support within the Oracle platform software. The KVM virtualization technology that is implemented here is highly integrated with the TPD operating system. The following software components within platform implement virtualization:

TVOE
A platform product that is a combination of operating system and application software that together provide an operating environment for running virtual machines. TVOE is comprised of the TPD operating system, KVM modules and associated management tools, as well as selected RPMs from TPD to assist with management.

TPD
Contains enhancements that allow it to run inside a Guest VM.

PMAC
Contains enhancements that support installation and upgrade of a TVOE Host, creation and management of Guest VMs, and installation and upgrade of Oracle applications running in Guest VMs.

PMAC supports applications running on native hardware as well as applications running in Guest VMs. The PMAC application is deployed as a guest VM on the management server.

Virtual Machine Management page

The Virtual Machine Management page is accessible under **Main Menu** > **VM Management**.

The **Virtual Machine** (**VM**) Management page enables you to modify the VM Hosts and VM Guests managed by the PMAC.

Virtual Machine Management elements

The Virtual Machine Management page contains these elements:

- VM Entities list
- VM Management work area

VM Entities list

The VM Entities list shows the managed entities. It is continually visible and can be collapsed or expanded by selecting the left arrow in the upper-right corner of the VM entities list. The list is automatically updated when the GUI perceives any action warranting an update (for example, a VM Guest was just created or deleted from the GUI). Additionally, the list is refreshed automatically approximately every minute. A Refresh button allows the user to manually refresh the list to determine whether it has been changed, perhaps by some other login.

Selecting the **Pause updates** checkbox in the title bar allows the users to pause any reoccurring updates while on a given page including the VM Entities list. While the **Pause updates** checkbox is selected the page will not be automatically refreshed and the list will not be updated. Selecting the Refresh button will still refresh the VM Entities list.

There is also a "Pause Updates" checkbox available at the bottom of the VM Entities list. This checkbox, when checked, pauses the continuous refresh of the VM Entities list that occurs when a user enters this page. When the page is refreshed, the "Pause Updates" checkbox will reset to unchecked. When this checkbox is checked, selecting the Refresh button will still refresh the VM Entities list.

When an entity is selected in this list, its current data will be retrieved and displayed in the VM Management work area. This work area displays additional details on the selected entity (VM Host or VM Guest).

VM Management work area

Use the VM entities list to interact with VM host or guest entities (for example, create, view, or edit). The appearance and content of the VM Management work area depends on the selected entity and what action is being taken.

Select a VM host or guest entity to populate the VM Management work area with informational index cards that are associated with the following tabs:

- VM Info
- Software
- Network
- Media

> **Note:** Details about the contents of these tabs are given in the work area topics.

The bottom of the work area shows action buttons that can be selected at any time. The set of buttons will change and some can be disabled according to the current entity type and the action being performed on it.

You can select action buttons on the VM Management page at any time. The buttons that are displayed depend on the selected entity type.

Note: When any action is taken that requires a request to be sent to the PMAC server, the work area is inactive (grayed out), which indicates that a request is in progress and no controls can be accessed in the work area. You can still select another entity to view from the VM Entities list instead of waiting for the current response.

Related Topics

- View VM Host work area
- View VM Guest work area
- Create VM Guest work area

Changing the VM guest power state

The Current Power State is displayed while viewing the selected guest. You can change the power state by doing the following:

1. From the View VM Guest page, make a selection from the power state pulldown menu, and then click **Change**

Setting initial power state for a new VM guest

You can set the initial power state from the Create VM Guest page.

1. From the Create VM Guest page, make a selection from the power state pulldown menu. This power state will be set upon creation of the new guest.

View VM Host work area

The View VM Host work area is accessible under **Main Menu** > **VM Management**. Then, select a host entity from the VM Entities list to display the View VM Host work area (the VM Info tab is the default selection).

Note: The general layout of the View VM Guest work area does not change, regardless of the action that is currently in progress.

The top of the host screen shows the identification information for this host. Host can be described by Enclosure/Bay or RMS name. The following VM host identification information is displayed on this work area:

- Host name
- Enclosure (if known and applicable)
- Bay (if known and applicable)
- RMS name (if known and applicable)

Use the **Tasks** button on the toolbar to monitor tasks for actions initiated from the selected work area that are being executed in the background.

Elements

The following tabs are displayed in this work area:

Tab	Description	Contents
VM Info	This tab contains data specifically pertaining to the configuration of the VM Host.	**Guests index card** Lists guests and their power status. **Bridges index card** Lists available bridges that the guest can choose from. **Storage Pools index card** Lists available storage pools. **Memory index card** Lists the following: • Amount of memory utilized by the host and all guests • Amount of memory installed and available on the host (only available on newer TVOE host systems) **Note:** For Platform 6.0 and earlier hosts, only the guest memory is displayed. • If editing a guest on a Platform 6.5 or later host, the edit will fail if the memory is exceeded. • When adding a guest on a Platform 6.5 or later host, the create will fail if the memory is exceeded.

Tab	Description	Contents
Software	This tab enables you to view information specific to the software that is running on the host. This includes the data found on the Enclosure/Bay or RMS screen's Software tab.	**Operating System Details index card** Provides detailed information about the operating system installed on a host. The operating system must provide this data; otherwise, the data is left blank. **Application Details index card** Provides detailed information about the application installed on a host. The application must provide this data; otherwise, the data is left blank.
Network	This tab enables you to view the Network Interfaces list of the host. This includes the data found on the Enclosure/Bay or RMS screen's Network tab.	**Network Interfaces index card** Provides detailed information on the network interfaces.
Media	This tab shows media on the host that is available to attach to guests. No action may be performed.	**Label** The ISO 9660 label on the media. **Image Path** The device path to the ISO image (for example, filepath to an ISO image on a device or on a local filesystem). The list of media is retrieved from tpdProvd.

Buttons

The following button is available from the View VM Host work area:

- **Create Guest**

The only action that can be performed on a VM Host is to create a VM guest. Click **Create Guest** to open the Create VM Guest page with the Host field pre-populated to the name/IP address of the host that was being viewed.

To complete this action, fill out the required fields, and click **Create Guest**.

See Create VM Guest work area for more information about import profile.

Viewing VM host information

1. Select **VM Management**. Then select a host from the VM Entities list.

   The View VM Host work area appears.

2. Select a tab to view additional details.

View VM Guest work area

The View VM Guest work area is accessible via **Main Menu** > **VM Management**. Then, select a guest from the VM Entities list.

> **Note:** The general layout of the View VM Guest work area does not change, regardless of the action that is currently in progress.

The following identification information is displayed at the top of this area:

- Name
- Host information
- Current Power State

> **Note:** The Current Power State is displayed while viewing the selected guest. To change the power state, make a selection from the menu, then select **Change** .

Elements

The following tabs (based on the data type) are also displayed in the work area:

Table 8-1 View VM Guest work area tabs

Tab	Description	Contents
VM Info	This tab displays information about the configuration of the VM Guest. See Rules for VM Guest creation for the applicable work area rules.	The following information is displayed: • Number of CPUs • Memory (MBs) • VM UUID • Virtual Watchdog state (present only if the Guest is on a version of TVOE that supports this feature) **Virtual Disk index card** Lists Primary, Size, Pool, Name, and TPD Device information. **Virtual NICs index card** Lists Host Bridge, Guest Device, and MAC address information (only visible when viewing a guest).

Table 8-1 (Cont.) View VM Guest work area tabs

Tab	Description	Contents
Software	This tab contains information specific to the software (if any) that is running on the guest.	**Operating System Details index card** Provides detailed information about the network interfaces on a guest . The operating system must provide this data; otherwise, the data is left blank. **Application Details index card** Provides detailed information about the application installed on a guest The application must provide this data; otherwise, the data is left blank The Version field will display the application version or one of the following upgrade states: Pending Acc/Rej or In Upgrade. **Note:** There might be times during an upgrade when PMAC is not able to query and display the upgrade state.
Network	This tab contains the Network Interfaces list of the guest.	**Network Interfaces index card** Provides detailed information on the network running on the server blade in the selected bay.

Table 8-1 (Cont.) View VM Guest work area tabs

Tab	Description	Contents
Media	This tab contains information specific to ISO media attached and available to the guest. The information is not dynamically updated.	**Attached Media static table** Lists images currently attached to the guest. Field information is similar to the Host Media tab. The **Detach** button detaches the image from the guest. The mapping-iso media cannot be detached. **Available Media static table** Lists ISO images on the host. Field information is similar to the Host Media tab. **Attach** attaches media to the guest. Use Attach and detach actions on a running guest only. If the guest is restarted, user attached media is removed when the guest is restarted. A limit of 4 media images may can be attached to a guest. The host media can be mounted multiple times to the same or different guests. Device enumeration on the guest is not controlled; media is attached to the next free device, and detach removes the last device matching the image name.

Buttons

The following buttons are available (if applicable) on the View VM Guest work area:

Table 8-2 Buttons on the View VM Guest work area

Component	Description
Edit	**Edit** is visible when viewing a guest. It is selectable only when the guest's power state is **ShutDown** or when viewing the active PMAC VM guest. This exception is required to edit the PMAC VM configuration without shutting down the running PMAC. A restart is required before the changes take effect. Selecting **Edit** puts the user in edit mode for the selected guest.

Table 8-2 (Cont.) Buttons on the View VM Guest work area

Component	Description
Delete	**Delete** is visible when viewing a guest. Selecting **Delete** attempts to delete the guest being displayed.
Install OS	**Install OS** is visible when viewing a guest. Selecting it takes the user to the Software Install - Select Image screen where the selected guest is displayed as the target.
Clone Guest	**Clone Guest** is visible when viewing a guest. Selecting **Clone Guest** displays the Create VM Guest screen where the data from the previously viewed guest populates the data fields. **Note:** Cloning a guest will create specified virtual disks, but will not copy the actual content of the disks.
Upgrade	**Upgrade** is visible when viewing a guest. It is selectable when the guest has an OS installed. Selecting **Upgrade** takes the user to the Software Upgrade - Select Image screen where the selected guest is displayed as the target.
Accept Upgrade	**Accept Upgrade** is visible when viewing a guest. It is selectable when the guest is in the **Pending Upgrade Accept/Rej** or **Pending Upgrade and Patch Acc/Rej** upgrade state. Selecting **Accept Upgrade** initiates an accept upgrade on the guest.
Reject Upgrade	**Reject Upgrade** is visible when viewing a guest. It is selectable when the guest is in the **Pending Upgrade Accept/Rej** or **Pending Upgrade and Patch Acc/Rej** upgrade state. Selecting **Reject Upgrade** initiates a reject upgrade on the guest.
Patch	**Patch** is visible when viewing a guest. It is selectable when the guest has an OS installed. Selecting **Patch** takes the user to the Software Upgrade - Select Image screen where the selected guest is displayed as the target.

Table 8-2 (Cont.) Buttons on the View VM Guest work area

Component	Description
Accept Patch	**Accept Patch** is visible when viewing a guest. It is selectable when the guest is in the **Pending Patch Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** upgrade state. Selecting **Accept Patch** initiates an accept patch on the guest.
Reject Patch	**Reject Patch** is visible when viewing a guest. It is selectable when the guest is in the **Pending Patch Acc/Rej** or **Pending Upgrade and Patch Acc/Rej** upgrade state. Selecting **Reject Patch** initiates a reject patch on the guest.
Refresh Device Map	**Refresh Device Map** is visible when viewing a guest. Selecting **Refresh Device Map** regenerates ISO for the guest that is kept on its TVOE host. A dialog box confirms the action. If the action fails, an error window below the Virtual Machine Management heading. If the task succeeds, an information window is displayed.

Current Power State indication

The Current Power State indication shows the current power state of the VM Guest, such as **Running** or **Shut Down**.

Change button

Use the **Change** button to change the VM Guest's power state to **On**, **Shutdown**, or **Destroy**.

Note: You do not need to be in Edit mode to change the power state.

Rules for VM Guest creation

Several create mode and edit rules apply to the View VM Guest work area. For example, rules apply to the work area before the Create button can be clicked when in Create mode. To minimize the amount of data that needs to be entered in most situations, initial default values are provided.

The following create mode rules apply to this work area:

- All fields in the VM Info tab are editable except the MAC addresses of NICs. Those are filled in by PMAC.
- There must be at least one virtual disk.
- There must be one and only one primary disk.
- You can add zero or more NICs. A control NIC will automatically be created.

The following edit mode rules apply to this work area:

- Both Number of CPUs and Memory are editable.
- The **Enable Virtual Watchdog** checkbox is editable. This will not be available if the guest host's TVOE version does not support watchdogs.
- Virtual disks can only be deleted and added. You cannot edit an existing virtual disk.
- You must delete a guest in order to delete the primary disk.
- You cannot delete or change the primary virtual disk.
- NICs can only be deleted and added. You cannot edit an existing NIC.

The Task list is a common GUI element that is found on the toolbar of many different screens. In this instance of View VM Guest, the list is filtered to show only the tasks for the entities currently selected on the screen.

Viewing VM guest information

1. Select **VM Management** Then select a guest from the VM Entities list.

   The ViewVM Guest page appears.

2. Select a tab to view additional details.

Create VM Guest work area

The Create VM Guest work area is accessible in the following ways:

- From the View VM Guest work area, select **Clone Guest**.
- From the View VM Host work area, select **Create Guest**.

The following identification information is on this page:

- **Name** (editable field where you enter the name of the new guest)

  Note: This field is required and should be unique.

- **Host** (selectable field where you designate the host for the guest)
- Initial power state (selectable field where you choose whether or not the guest should be running)

  Note: Choices include On, Shutdown, and Destroy. Destroy is disabled because it is not applicable for guest creation.

Elements

The VM Info tab contains:

Number of vCPUs
Specify the number of virtual CPUs. Valid values are 1 through 32, inclusive.

Memory (MBs)
Specify the amount of memory in MBs. Valid values are 1 through 262144, inclusive.

Note: A warning alerts you not to oversubscribe host memory to guests, and on newer TVOE hosts, the create guest task will fail with an error if memory is oversubscribed.

VM UUID
Initially, the **VM UUID** field is blank, but it can be modified using the **Edit UUID** button. You can chose to leave the VM UUID field blank in order to let the system generate the UUID during the actual guest creation. Clicking the **Edit UUID** button displays the Edit UUID window.

VM UUID
Initially, the **VM UUID** field is blank, it will be generated upon completion of guest creation.

Edit UUID
Change the value in the **UUID** text field by typing a value or choose a UUID from a profile. The UUID must adhere to RCF 4122: 128 randomly-generated bits, for example AA97B177-9383-4934-8543-OF91A7A02836. The digit after the second dash is always 4 and the digit or letter after the third dash is always either 8, 9, A, or B. Clicking the **Use this UUID** button closes the Edit UUID window and populates the **VM UUID** field with the new value.
The **Profile** content is automatically generated and is dependent on the content of the /usr/TKLC/smac/etc/uuidprofiles directory. Clicking on a profile within the Profile menu displays the UUID entries from the profile just beneath it. Select one of the UUID entries to populate the value in **UUID**.

Enable Virtual Watchdog
Select to enable or disable the Virtual Watchdog (present only if the Guest is on a version of TVOE that supports this feature) during the guest creation.

Virtual Disks index card
Use this selectable, editable grid to add or delete virtual disk information. To delete a row pertaining to a disk, select the row and click **Delete** in the upper right corner of the grid. To add a new row, click **Add** in the upper right corner of the grid, and then proceed to edit related fields:

Primary
Use to designate the primary disk. Only one and only disk must be primary.

Size
Specify the disk size in MBs. Valid values are 1 through 1047527424, inclusive.

Host Pool
Choose the host pool from this dropdown list.

Host Vol Name
Enter the name of the host volume.

Guest Dev Name
Enter the guest development name.

Add
Click to add Virtual Disks.

Delete
Click to delete Virtual Disks.

Virtual NICs index card
Use this selectable, editable grid to add or delete virtual NIC information. To delete a row pertaining to a NIC, select the row and click **Delete** in the upper right corner of the grid. To add a new row, click **Add** in the upper right corner of the grid, and then proceed to edit related fields:

Host Bridge
Enter the host bridge.

Guest Dev Name
Enter the Guest Dev Name.

Add
Click to add Virtual NICs.

Delete
Click to delete Virtual NICs.

Buttons

The following buttons are available on the Create VM Guest work area:

Table 8-3 Buttons on the Create VM Guest page

Button	Description
Create	**Create** is enabled only when all of the information that is required to create a guest is provided. Clicking **Create** attempts to initiate a new background task that you can monitor on the Task Monitoring page. A message is displayed to confirm success or indicate failure of the action. **Note:** You can watch the progress of the background task in the Tasks table.
Import Profile	Select to pre-populate most of the information needed to create a guest from one of the guest profiles delivered as part of a software image. Clicking **Import Profile** displays the Import Profile page that contains the **ISO/Profile** dropdown menu. Clicking on a profile within the **ISO/Profile** dropdown menu displays the content of the profile beneath it. Clicking on **Select Profile** fills out the Create VM Guest using the selected profile content. When you are finished, close the Import Profile window by clicking the **X** in the upper right corner of the window.

Info list on toolbar

This is an instance of the common status list GUI element that is found on the toolbar of different screens. In this instance, the list is filtered to only show the information for the entities currently selected on the screen.

Task list on toolbar

This is an instance of the common task list GUI element that is found on the toolbar of many different screens. In this instance, the list is filtered to only show the tasks for the entities currently selected on the screen.

Related Topics

- Creating VM guest information
- View VM Host work area
- View VM Guest work area

Creating VM guest information

1. Select **VM Management**. Then, select a guest from the VM Entities list.

   The View VM Guest page appears.

2. Select a tab to view additional details.

9

PMAC Application Processes

This section introduces the Sentry process and the PMAC application processes that Sentry monitors. This section also describes how to view the status of the application processes and how to change the mode of the Sentry process.

About the Sentry process

The Sentry daemon process (`sentryd`) monitors the PMAC application processes and attempts to restart them automatically if a failure occurs.

By default, Sentry is configured to run in **Active** mode. In **Active** mode, if `sentryd` determines that any or all of the processes are not present in that table, it restarts the process(es) within 5 seconds. In **Passive** mode, `sentryd` does not restart any processes that stop running on the host.

Additionally, Sentry automatically sends a request to the PMAC server to look at the status of each process. PMAC queries Sentry to determine process status and displays the status information in the PMAC GUI on the Sentry Process Control page (accessible on the main menu under **Administration** > **PMAC Application**).

What are the PMAC application processes?

The PMAC application processes are as follows:

- **smacMon**

  Monitors each provisioned enclosure in the system and executes and monitors the background tasks (for example, **Install OS**) that are initiated by users via the PMAC GUI.

- **smacTalk**

  Responds to all requests from the PMAC GUI. Its primary responsibilities are to validate incoming provisioning requests, update provisioning databases, collect data for user queries, and initiate background tasks.

- **hpiPortAudit**

  For each enclosure provisioned in PMAC, an **openhpi** daemon is created to monitor and communicate with the Onboard Administrators on that enclosure. The **hpiPortAudit** process monitors the health of each of the **openhpi** daemons and ensures that one is running for each enclosure provisioned in the PMAC database.

- **snmpEventHandler**

  Processes the SNMP traps received from server blades after a successful **Install OS** operation.

- **eclipseHelp**

  Launches the PMAC online help and restarts the help automatically when the PMAC server restarts.

Sentry Process Control page

The Sentry Process Control page is accessible under **Administration** > **PMAC Application**. The page provides a view of status information for each PMAC application process.

Authorized users can change the mode of the Sentry process so that application processes are restarted or not restarted automatically.

Caution: You should change the mode of the Sentry process only if directed by Customer Access Support (see My Oracle Support).

Sentry Process Control elements

The Sentry Process Control page contains the following elements:

Table 9-1 Elements on the Sentry Process Control Page

Element	Description
Command status field	Shows that the Sentry process is currently sending a status command to the host. This field is followed by the title of the output.
sentryd started	Provides the date and time that the Sentry process was last started.
Current Activity Mode	Shows the current mode of the Sentry process. For mode definitions, see the **Pulldown Menu** element in this table.
Process column table	Displays the names of the process that Sentry is monitoring. Displays information about the processes that Sentry is monitoring. See Table 9-2 for a description of each field.
PID	Displays the process ID of the process.
Status	Displays the status (running or not running) of the process.
StartTS	(Start timestamp) Displays the timestamp of when the process was started. The format is Day-MMM-DD-hh-mm-ss-YYYY, for example, Tue Nov 24 13:39:44 2009
NumR	(Number of Restarts) The number of times a process has been restarted.
Date/Timestamp and Comment	Displays the date and timestamp for the executed command and status information relating to the command.

Table 9-1 (Cont.) Elements on the Sentry Process Control Page

Element	Description
Sentry command pulldown list	Enables an authorized user to select one of the following commands to effect a mode change of the Sentry process: • **Display Status-**Sentry reads the database of a host to obtain information about the processes that Sentry monitors and displays the status information on this GUI page. The Display Status mode does not affect Active Mode or Passive Mode. In other words, you can still view status information on processes regardless of whether Sentry is in Active Mode or Passive Mode as long as Display Status is selected. • **Active Mode-**Sentry tries to restart failed processes on the host. • **Passive Mode-**Sentry does not try to restart any processes that stop running on the host. • **Restart Sentry-**Sentry is restarted.
Go button	Executes the selected Sentry command.
Pause Updates	Allows the user to temporarily suspend ("pause") the automatic page refresh that occurs automatically when the page is entered. If the check box is "checked", a manual page Refresh will "uncheck" the check box.
Page Refresh Interval	Provides information about how often the Sentry Process Control page (automatically) refreshes.

Table 9-2 Process table fields

Element	Description
PID	Displays the process ID of the process.
Process	Displays the name of the process.
Status	Displays the status (running or not running) of the process.
StartTS	(Start timestamp) Displays the timestamp of when the process was started. The format is Day-MMM-DD-hh-mm-ss-YYYY, for example, Tue Nov 24 13:39:44 2009
NumR	(Number of Restarts) The number of times a process has been restarted.

Viewing status of PMAC application processes

Use this procedure to view the status of PMAC application processes:

1. Select **Administration** > **PMAC Application**.

   The page shows the status of the application processes.

Sentry automatically displays the status of the application processes (is in the **Display Status** mode) when a user accesses the Sentry Process Control page.

Restarting Sentry

Note: This command is not intended for general customer user. You should change the mode of the Sentry process only if directed by My Oracle Support.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Click **Administration** > **PMAC Application**.
3. Select **Restart Sentry** from the list and click **Go** to execute the command.

If Sentry was in active mode when restarted, Sentry restarts in active mode. If Sentry was in passive mode when restarted, any PMAC processes that are down will not get restarted until Sentry is put back into active mode.

About automatically restarting failed processes

Caution: You should change the mode of the Sentry process only if directed by My Oracle Support.

In active mode, Sentry automatically attempts to restart failed processes within 5 seconds of detecting their failure. This mode is the default mode.

Sentry Admin privileges are required to change Sentry modes.

Automatically restarting failed processes

Caution: This command is not intended for general customer user. You should change the mode of the Sentry process only if directed by My Oracle Support.

Use this procedure to put Sentry in active mode so that Sentry will automatically restart failed processes:

1. Log into the PMAC GUI as the guiadmin or pmacop user.
2. Click **Administration** > **PMAC Application**.
3. Select **Active Mode** from the list and click **Go**.

The Sentry Process Control page shows that the command is being sent.

4. Select **Display Status** from the list and click **Go**.

   The Sentry Process Control page shows **Active** in the **Current activity mode** field. Sentry continues to monitor the processes. **Display Status** mode does not affect the active mode status.

The change to active mode takes effect immediately.

About setting Sentry to ignore failed processes

Caution: You should change the mode of the Sentry process only if directed by My Oracle Support.

In passive mode, Sentry ignores failed processes.

Sentry Admin privileges are required to change Sentry modes.

Setting Sentry to ignore failed processes

Caution: This command is not intended for general customer user. You should change the mode of the Sentry process only if directed by My Oracle Support.

Use this procedure to put Sentry in passive mode:

1. Log into the PMAC GUI as the guiadmin or pmacop user.
2. Select **Administration** > **PMAC Application**.
3. Select **Passive Mode** from the list and click **Go**.

   The Sentry Process Control page shows that the command is being sent.

4. Select **Display Status** from the list and click **Go**.

   The Sentry Process Control page shows **Passive** in the **Current activity mode** field. Sentry continues to monitor the processes. **Display Status** mode does not affect the passive mode status.

The change to passive mode takes effect immediately.

10

Working with Hardware

This section describes the configuration tasks for the platform hardware.

System configuration data

The PMAC GUI provides an interface for viewing the system configuration data. The following tasks are supported:

- Viewing the data provisioned during system setup on the cabinets and enclosures.
- Viewing the data provisioned during system setup on rack mount servers.

System Configuration page

The System Configuration page is accessible on the PMAC main menu under **Hardware** > **System Configuration**. The page displays all provisioned Cabinets and their IDs, as well as all provisioned Enclosures, their IDs, and their OA IP addresses and all provisioned RMS, their IP addresses and names. The data is view-only.

System Configuration elements

The System Configuration page displays these elements:

Table 10-1 Elements on the System Configuration Page

Element	Description
Provisioned Cabinets Table	
Cabinet ID	Cabinet identification.
Provisioned Console Servers Table (not supported in this release)	
Provisioned Enclosures Table	
Enclosure ID	Enclosure identification.
Bay 1 OA IP	Onboard Administrator IP network address. This address is always associated with the OA in bay 1.
Bay 2 OA IP	IP network address for the redundant OA if provisioned.
Provisioned RMS Table	
In Cabinet	Cabinet Location of the RMS.
Name	The name of the provisioned RMS.
IP	IP network address for the RMS.

Viewing system configuration data

Use this procedure to view data provisioned during initial setup:

1. Click **Hardware** > **System Configuration**.

The page is populated with provisioned data.

Cabinets

PMAC lets an authorized user perform these operations:

- Add cabinets into the hardware inventory.
- Delete a cabinet from the hardware inventory.
- View a list of the provisioned cabinets in the hardware inventory.

Configure Cabinets page

The Configure Cabinets page is used during initial configuration. The option is accessible under **Hardware** > **System Configuration** > **Configure Cabinets**. The page provides a list of the provisioned cabinets in the system. The page also provides options for adding and deleting cabinets from the system.

Caution: These commands are not intended for general customer use and should be used only as directed by My Oracle Support.

Configure Cabinets elements

The Configure Cabinets page contains these elements:

Table 10-2 Elements on the Configure Cabinets Page

Element	Description
Provisioned Cabinet	Provides a table that lists each discovered cabinet ID.
Add Cabinet	Adding a cabinet is required before an enclosure can be added. This option launches the **Add Cabinet** page. The page lets you enter the **Cabinet ID** prior to executing the **Add Cabinet** command. This command takes the following parameter: • **Cabinet ID**-The cabinet identification number. The number must be unique for the site. Format: Numeric Range: 1- 654

Table 10-2 (Cont.) Elements on the Configure Cabinets Page

Element	Description
Delete Cabinet	If a cabinet is deleted, PMAC no longer manages or monitors the cabinet. Select a **Cabinet ID** in the Provisioned Cabinets table and select **Delete Cabinet**. Confirm or cancel the deletion in the displayed in the dialog box. **Note:** A cabinet cannot be deleted if there are enclosures or rack mount servers in the PMAC hardware inventory that are associated with the cabinet.
Pause Updates	Allows the user to temporarily suspend ("pause") the automatic page refresh that occurs automatically when the page is entered. If the checkbox is "checked", a manual page refresh will "uncheck" the checkbox.

Adding a cabinet

Caution: This command is not intended for general customer use and should be used only as directed by Customer Access Support (see My Oracle Support).

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Select **Hardware** > **System Configuration** > **Configure Cabinets**.
3. Click **Add Cabinet**.
4. Enter a value between 1 and 654 in the **Cabinet ID** field.
5. Click **Add Cabinet**.

   A message informs you when the operation has completed.

The cabinet has been added to the PMAC hardware inventory.

Deleting a cabinet

Caution: This command is not intended for general customer use and should be used only as directed by My Oracle Support.

Deleting a cabinet removes the cabinet from the PMAC hardware inventory. PMAC will no longer manage or monitor the cabinet.

As part of this procedure to delete a cabinet, you will need to provide the Cabinet ID. For a list of provisioned cabinets, select **Hardware** > **System Configuration** from the main menu. Also make a note of the Enclosure ID of any enclosures on the cabinet. You will need to delete those as well.

Use the following procedure to delete a cabinet from the system inventory.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Delete any enclosures in the cabinet.

   A request to delete a cabinet will be rejected if enclosures are present.
3. Select **Hardware** > **System Configuration** > **Configure Cabinets**.
4. Select a cabinet from the **Provisioned Cabinets** table.
5. Click **Delete Cabinet**.
6. Confirm or cancel the action.

   <Cabinet ID> has been successfully deleted from the system.

   where <*Cabinet ID*> is the ID of the cabinet being deleted.

The cabinet is deleted from the inventory.

Enclosures

The PMAC GUI lets an authorized user perform these operations:

- Add an enclosure with two **OA**s (**Onboard Administrator**) to the hardware inventory.
- Delete an enclosure from the hardware inventory.
- Edit the OA IP addresses of an existing enclosure configuration or add a second OA to the enclosure.
- View a list of the provisioned enclosures in the hardware inventory.

Configure Enclosures page

The Configure Enclosures page is accessible under **Hardware** > **System Configuration** > **Configure Enclosures**. The page provides a list of the provisioned enclosures in the hardware inventory. The page also provides commands for adding, editing, and deleting enclosures from the hardware inventory. The background task that is launched as part of the **Add Enclosure** operation can be viewed directly from the Configure Enclosures page.

Configure Enclosures elements

The Configure Enclosures page contains these elements:

Table 10-3 Elements on the Configure Enclosures Page

Element	Description
Provisioned Enclosure ID	Displays the enclosure identification for enclosures that exist in the hardware inventory.

Table 10-3 (Cont.) Elements on the Configure Enclosures Page

Element	Description
Add Enclosure	Adding an enclosure to the hardware inventory identifies the enclosure to the PMAC application so that PMAC can begin managing and monitoring the enclosure. The **Add Enclosure** option launches the Add Enclosure page. The page lets you enter parameters prior to executing the **Add Enclosure** command. The **Add Enclosure** command takes the following parameters: • **Cabinet ID**-The cabinet identification number to associate with the enclosure. Between 1 and 4 enclosures can be associated with the same cabinet. The pulldown list shows only **Cabinet ID**s that are already in the hardware inventory. Format: Pulldown list This value is required. • **Location ID**-The **Location ID** of the enclosure within the cabinet. The application(s) running on the platform determine whether enclosures are numbered from top to bottom or vice versa. The **Location ID** must be unique within the cabinet. PMAC uses the **Cabinet ID** along with the **Location ID** to create a unique **Enclosure ID** (the concatenation of the **Cabinet ID**, 0, and the **Location ID**). For example, if you select **Cabinet ID=506** and enter **Location ID=1**, the **Enclosure ID** would be **50601**. PMAC validates that the combination of the **Cabinet ID** and **Location ID** are unique for PMAC. Format: Numeric Range: 1-4 This value is required. • **Bay 1 OA IP**-The IP address of the OA (Onboard Administrator). The OA IP address must be unique across all other enclosures within the PMAC hardware inventory. PMAC supports two OAs per enclosure: one active and one standby. Format: IP address (4 octets, each between 0 and 255)

Table 10-3 (Cont.) Elements on the Configure Enclosures Page

Element	Description
	Format: An IPv4 address in dotted quad format (4 octets, each between 0 and 255) or IPv6 address in colon hex format. • **Bay 2 OA IP**-The IP address of the OA. The OA IP address must be unique across all other enclosures within the PMAC hardware inventory. PMAC supports two OAs per enclosure: one active and one standby. Format: IP address (4 octets, each between 0 and 255) Format: An IPv4 address in dotted quad format (4 octets, each between 0 and 255) or IPv6 address in colon hex format.
Edit Enclosure	Launches the Edit Enclosure page. The page lets you add, edit, or delete an OA IP address for the selected enclosure prior to executing the **Edit Enclosure** command. The **Edit Enclosure** command takes the following parameters: • **Bay 1 OA IP**-Displays the OA IP address if one is currently provisioned. The user can add or remove an IP address, edit the existing IP address, or leave the field blank. The OA IP address must be unique across all other enclosures within the PMAC hardware inventory. PMAC supports two OAs per enclosure: one active OA and a standby OA. Format: An IPv4 address in dotted quad format (4 octets, each beteen 0 and 2550 or IPv6 address in colon hex format. • **Bay 2 OA IP**-Displays the OA IP address if one is currently provisioned. The user can add or remove an IP address, edit the existing IP address, or leave the field blank. The OA IP address must be unique across all other enclosures within the PMAC hardware inventory. PMAC supports two OAs per enclosure: one active OA and a standby OAs. Format: An IPv4 address in dotted quad format (4 octets, each between 0 and 255) or IPv6 address in colon hex format.
Delete Enclosure	Deletes the selected enclosure.

Table 10-3 (Cont.) Elements on the Configure Enclosures Page

Element	Description
Pause Updates	Allows the user to temporarily suspend ("pause") the automatic page refresh that occurs automatically when the page is entered. If the checkbox is "checked", a manual page refresh will "uncheck" the checkbox.
Background Tasks table	The Tasks button on the toolbar displays a floating window containing the Background task table that shows tasks pertaining only to the selected enclosure's configuration.

Adding an enclosure

Caution: This command is not intended for general customer use and should be used only as directed by My Oracle Support.

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Click **Hardware** > **System Configuration** > **Configure Enclosures**.
3. Click **Add Enclosure**.
4. Populate the fields with data.

   For field definitions, see Configure Enclosures elements.
5. Click **Add Enclosure**.

   A message informs you that a background task has been launched. The message also provides a task ID and a link so that you can monitor the background task.
6. Select the **Task Monitoring** link to monitor the background task.

   Click **Refresh** to update the data on the page.
7. Monitor the task until it has completed.

   The progress status percentage indicator turns green when it has completed.

The enclosure has been added to the PMAC hardware inventory.

Editing the enclosure OA IP addresses

- Use this procedure to Change the active or standby OA's IP address.

Caution: This command is not intended for general customer use and should be used only as directed by My Oracle Support.

1. Log into the PMAC GUI as the guiadmin or pmacop user.
2. Click **Hardware** > **System Configuration** > **Configure Enclosures**
3. Click **Edit Enclosure**.
4. Select an enclosure from the **Enclosure ID** list.
5. Click **Edit Selected Enclosure**.

   The Edit Enclosure page shows the selected enclosure and the IP addresses of the associated OA(s).
6. Perform one of the following actions:
   - Edit one or both of the IP addresses to inform PMAC of a change to the active or standby OA's IP address.
   - Add an IP address to add a standby OA to the enclosure configuration.
   - Delete an IP address to remove the connection between PMAC and an OA. Note that you cannot remove both OA IP addresses; at least one OA IP address is required.
7. Click **Submit**

   This action launches the **Add Enclosure** background task. A message informs you that the background task has been launched. The message also provides a task ID and a link so that you can monitor the background task.
8. Select the **Task Monitoring** link to monitor the background task.

   Click **Refresh** to update the data on the page.
9. Monitor the task until it has completed.

   The progress status percentage indicator turns green when it has completed.

The enclosure is reloaded into the hardware inventory with the OA IP address changes. PMAC launches a rediscovery operation of the system configuration.

Viewing OA IP addresses

Use this procedure to view the provisioned OA(s) and their IP addresses in the system inventory:

1. Click **Hardware** > **System Configuration**.

   The currently provisioned OA(s) and associated IP addresses are shown for each enclosure.

Deleting an enclosure

Caution: This command is not intended for general customer use and should be used only as directed by My Oracle Support.

Deleting an enclosure removes the enclosure from the PMAC hardware inventory. When you delete an enclosure, the blades are still running and the network is still up and configured, but PMAC no longer monitors and manages the enclosure.

Use this procedure to delete an enclosure from the hardware inventory:

1. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Select **Hardware** > **System Configuration** > **Configure Enclosures**.
3. Select an enclosure from the **Provisioned Enclosures** table.
4. Click **Delete Enclosure**.
5. Confirm or cancel the action.

   <Enclosure ID> has been successfully deleted from the system.

   where <*Enclosure ID*> is the ID of the Enclosure being deleted.

The enclosure is deleted from the inventory.

Onboard Administrator

To be added to the PMAC hardware inventory, OA hardware must be physically installed and in service. Then OAs are added to the enclosure configuration. PMAC is provisioned with the OA IP address of the active OA and the standby OA. If a failure occurs, the standby OA automatically takes over the role of active OA and PMAC automatically uses the new OA.

Caution: Both OA IP addresses must be installed, the OA IP address must be configured in PMAC using the **Add Enclosure** or the **Edit Enclosure** command. If this configuration is not performed, PMAC does not have a connection to the newly active OA after an OA failover, and consequently, has no knowledge of the system hardware.

The PMAC GUI lets an authorized user perform the following operations:

- Add an Onboard Administrator to the hardware inventory as part of the enclosure configuration (see Adding an enclosure).
- Add a standby OA to an existing enclosure configuration.
- Inform PMAC of a change in the active or standby OA's IP address.
- Remove an OA from an enclosure configuration.
- View a list of the provisioned OAs in the hardware inventory.

Any changes to the configuration cause the enclosure to be rediscovered by PMAC.

RMS

The PM&C GUI lets an authorized user perform operations on Rack Mount Servers (RMS).

Configure RMS page

The Configure RMS page is accessible under **Hardware** > **System Configuration** > **Configure RMS**. This work area allows an authorized user to:

- Add a rack mount server (RMS) to the hardware inventory
- Delete a rack mount server from the hardware inventory
- Edit the name, cabinet ID, user and password credentials of an existing rack mount server
- Initiate a background task to find rack mount servers in the network
- View the found rack mount servers and perform related tasks
- View a list of the provisioned rack mount servers in the hardware inventory

Configure RMS elements

The Configure RMS page contains these elements:

Table 10-4 Elements on the Configure RMS Page

Element	Description
Provisioned RMS Table	Contains the iLO IP addresses and names of RMS currently existing in the system. **Note:** You can delete or edit only one RMS at one time.
Add RMS	This displays the **Add RMS** page within the work area.
Edit RMS	Displays the Edit RMS page within the work area **Note:** **Edit** is disabled unless a RMS is selected.
Delete RMS	Deletes the selected RMS and a confirmation box is displayed. **Note:** **Delete** is disabled unless a RMS is selected.
Find RMS	Displays the **Find unprovisioned RMS** page within the work area.

Table 10-4 (Cont.) Elements on the Configure RMS Page

Element	Description
Found RMS	Displays the **Found RMS** page within the work area.
Pause Updates	Allows the user to temporarily suspend ("pause") the automatic page refresh that occurs automatically when the page is entered. If the checkbox is "checked", a manual page refresh will "uncheck" the checkbox.
Background Monitoring Pane	The **Tasks** button on the toolbar displays a floating window containing the Background task table that shows tasks pertaining only to the selected RMS's configuration.

Add RMS page

The Add RMS page is accessible under **Hardware** > **System Configuration** > **Configure RMS**.

Add RMS elements

The Add RMS page contains these elements:

Element	Description
IP Name	Enter the iLO IPv4 address in dotted quad format or IPv6 address in colon hex format of an RMS that you want to add to the hardware inventory. This field is required.
Field Name	Use this field to help you remember specific function, location, and so on. The name can contain spaces and must be unique. If the Name field is not supplied, it is assigned automatically.
Cabinet	Use this pulldown menu to specify a cabinet from a list of provisioned cabinet IDs in the system, as well as option “-----“ to indicate that the RMS is not to be associated with a specific cabinet.
User Field	Enter the username that PM&C should use to discover the RMS. If the username is specified, the password field must also be populated. If no credentials are given, the default credentials are used.

Element	Description
Password Field	Enter the password that PM&C should use to discover the RMS. If the password is specified, the username field must also be populated. If no credentials are given, the default credentials are used.
Add RMS	Select **Add RMS** to add the defined RMS. If any of the input fields contain an invalid value, an error message is displayed. If all of the input fields contain valid values, a success message is displayed and the new RMS entry appears in the table containing provisioned RMSs.

Edit RMS page

The Edit RMS page is accessible under **Hardware** > **System Configuration** > **Configure RMS**.

Edit RMS elements

The Edit RMS page contains these elements:

Element	Description
Name	Edit this field to help you remember specific function, location and so on. The name can contain spaces and must be unique. If you leave the field blank, a name is automatically added to the edited RMS entry.
Cabinet	Use this pulldown menu to specify a cabinet ID from a list of provisioned cabinet IDs in the system, as well as option "-----" to indicate that the RMS is not to be associated with a specific cabinet.
User	Enter the username that PM&C should use to discover the RMS. If the username is specified, the password field must also be populated. If no credentials are given, the default credentials are used.
Password	Enter the password that PM&C should use to discover the RMS. If the password is specified, the username field must also be populated. If no credentials are given, the default credentials are used.

Element	Description
Edit RMS	Select **Edit RMS** to edit the defined RMS. If any of the input fields contain an invalid value, an error message is displayed. If all of the input fields contain valid values, a success message is displayed and the new RMS entry appears in the table containing provisioned RMSs.

Find RMS page

The Find RMS page is accessible under **Hardware** > **System Configuration** > **Configure RMS [Find RMS]**.

Use the Tasks button on the toolbar to monitor tasks for actions initiated from this work area that are being executed in the background.

The Find RMS page contains these elements:

Element	Description
Find all unprovisioned RMS	Select this option to conduct a search of software discovered RMS entities running an Oracle-provided OS.
Find unprovisioned RMS within IP range	Select this option to conduct a network search within an IPv4 or IPv6 address range for unprovisioned RMS. Only the **Starting IP Address** is required. If the network mask **Netmask/Prefix** field is left blank, the network mask 255.255.255.0 will be applied as the default for IPv4 addresses during the search. The **Ending IP Address** field can be configured to limit searches that exceed reasonable time expectations.
Submit	Select to initiate the background task for the RMS search. If the background task was successfully initiated, a notification box is displayed; in case of network wide search, you see a new RMS TPD Search; or in case of an IP range search, you see RMS IP Search.

Found RMS page

The Found RMS page is accessible under **Hardware** > **System Configuration** > **Configure RMS [Found RMS]**.

Use the Tasks button on the toolbar to monitor tasks for actions initiated from this work area that are being executed in the background.

The Found RMS page contains these elements:

Element	Description
Found RMS editable field table	Contains the results of previous find RMS actions. Each row represents one RMS along with its iLO IPv4 or IPv6 address, product type, and the time the RMS was found. In addition, optional editable fields are Name, Cabinet ID, User, and Password.
Name field	Edit this field to help you remember specific function, location and so on. The name can contain spaces and must be unique. If you leave the field blank, a name is automatically added to the edited RMS entry.
Cabinet ID	Use this pulldown list to specify a cabinet ID from a list of provisioned cabinet IDs in the system, as well as option "-----" to indicate that the RMS is not to be associated with a specific cabinet.
User ID	Enter the username that PMAC should use to discover the RMS. If the username is specified, the password field must also be populated. If no credentials are given, the default credentials are used.
Password	Enter the password that PMAC should use to discover the RMS. If the password is specified, the username field must also be populated. If no credentials are given, the default credentials are used.
Add the selected RMS	Selecting one or more RMS entries enables the **Add the selected RMS**, which allows you to add the selected RMS entries to the system inventory. If the operation is successful, a dialog box is displayed, and the new RMS entries appear in the table containing provisioned RMS should you choose to navigate to the Configure RMS work area.
Delete the selected RMS	Selecting one or more RMS entries enables **Delete the selected RMS**, which allows you to delete the selected RMS entries. If the operation is successful, a dialog box is displayed, and the previously selected RMS entries no longer appear in the Found RMS table.
Delete all RMS	Select to flush the Found RMS table. If the operation is successful, a dialog box is displayed, and the message "There are no found RMS available for provisioning" appears in the Found RMS table.

Blades

The PMAC GUI lets the authorized user perform these operations:

- Install an operating system on a server blade.

- Install or upgrade an application on a server blade.
- Issue the **Warm Reset** command for server blades. This command gracefully shuts down and then restarts the server blade.
- Issue the **Cold Reset** command for server blades and switches. This command shuts down and then restarts the server blade or switch.

Storage devices

PMAC provides an interface to facilitate storage device configuration. It is the application that runs on this platform that determines the requirements of the configuration. This section provides general guidelines on how to use the interface. It is expected that these guidelines will require customization to meet the needs of the applications being used.

The interface consists of a GUI page, sample XML files used to specify the configuration or to remove an existing configuration, and a background task. The sample XML files are provided with PMAC and are edited with site-specific information. The configuration specified in the XML file(s) is applied to the hardware via an option on the PMAC GUI. Processing occurs in the background, and the user is provided the capability to monitor the background task's progress.

Note: This interface is not intended for general customer use and should be used only as directed by My Oracle Support.

Caution: The order in which Vdisks, Host Volumes, Global Spares are created or deleted is important. The procedures in this section do not state or imply the order to use. The operator with site-specific knowledge has the responsibility to configure the Vdisks, Host Volumes, and Global Spares in the proper order.

Configuring the storage devices

This section provides information on configuring the storage devices. There are two phases to the process:

1. Preparing the XML file(s) used in the configuration with site-specific data.
2. Processing the XML file with the Configure Storage background task that PMAC provides.

Note: This interface is not intended for general customer use and should be used only as directed by My Oracle Support.

Preparing XML file for Vdisk or Global Spare configuration

This procedure prepares the XML file to configure a Vdisk or Global Spare. A Global Spare is a spare disk not assigned to any particular Vdisk.

Note: This interface is not intended for general customer use and should be used only as directed by My Oracle Support.

Caution: The order in which Vdisks, Host Volumes, Global Spares are created or deleted is important. The procedures in this section do not state or imply the order to use. The operator with site-specific knowledge has the responsibility to configure the Vdisks, Host Volumes, and Global Spares in the proper order.

1. Log into the PMAC server as `admusr`.
2. Copy the file `example_SharedStorageConfig_Vdisks_GlobalSpares.xml` to a location where you can edit it from the following directory location on the PMAC server: `/usr/share/doc/TKLCsmac-config-<release_number>/examples/`.
3. For the `<Controller>` element, enter an IP v4 address or a hostname that resolves to an IP Address. This element specifies the controller to which this configuration will be applied. You can have multiple `<Controller>` elements in one file. This element is required.

   Note: Specify only one Controller per Controller Enclosure. Each Controller Enclosure has two Controllers, but they are a redundant pair. Applying the same configuration to both would attempt to configure the Controller Enclosure twice.

4. Locate `<Name>` under the <Vdisk> element and enter the name for the Vdisk.

   The name will be used to reference this Vdisk when configuring the Host Volumes. You can repeat the `<Vdisk>` element multiple times to add multiple Vdisks.

5. (Optional) For `<Owner>`, enter one of the following values to specify the controller to own the virtual disk:

   - `A`

     Specifies that Controller A within the Controller Enclosure will be used for this Vdisk.

   - `B`

     Specifies that Controller B within the Controller Enclosure will be used for this Vdisk.

   - `auto`

     Specifies that PMAC is to automatically assign this Vdisk to a Controller. This is the default.

   Vdisks may be assigned to different Controllers to achieve static load balancing between the Controllers. If one Controller in a redundant pair fails, ownership of its Vdisks will be taken over by the surviving controller.

6. For the `<RaidLevel>` element, enter a value to specify the RAID level. Valid values are as follows: nraid, 0,1,3,5,6,10 and 50.
7. Under `<Disks>`, enter one or more `<Disk>` elements in the form of *Enclosure_Bay*. Shown here are the examples from the relevant section of the XML file:

Note: Disk setup is the same for the P2000 Controller as for the MSA2324.

```
<!--
            Disks are specified in form "Enclosure.Bay" as in the
    following examples:

            MSA2012:

              Enclosure 0 (controller enclosure): Disks 0.0..0.X
              Enclosure 1 (drive enclosure):      Disks 1.0..1.X
              Enclosure 2 (drive enclosure):      Disks 2.0..2.X

    MSA2324, P2000 and newer:

              Enclosure 0 (controller enclosure): Disks 1.1..1.X
              Enclosure 1 (drive enclosure):      Disks 2.1..2.X
              Enclosure 2 (drive enclosure):      Disks 3.1..3.X
           -->
          <Disks>
            <Disk>0.0</Disk>
            <Disk>0.1</Disk>
            <Disk>0.2</Disk>
            <Disk>0.3</Disk>
          </Disks>
```

RAID 10 requires a minimum of two RAID-1 sub-Vdisks each having two drives. RAID 50 requires a minimum of two RAID-5 sub-Vdisks each having three drives.

8. (Optional) Under `<SpareDisks>`, enter one or more `<Disk>` elements. The notation is the same as in Preparing XML file for Vdisk or Global Spare configuration.

   This element specifies up to four Vdisk spares to assign to a RAID 1, 3, 5, 6, 10, or 50 virtual disk.

9. (Optional) Under `<GlobalSpares>`, enter one or more `<Disk>` elements. The notation is the same as Preparing XML file for Vdisk or Global Spare configuration.

10. At this point, if you would like to combine several XML files under the `<SharedStorageConfig>` element, you may do so.

    To view an example of a combined XML file, see Sample combined configure storage file.

11. If necessary, upload the XML file(s) back to the PMAC server by using `sftp`. See Uploading files to PMAC via sftp if you need help uploading the file.

12. On the PMAC server, copy the XML file to `/usr/TKLC/smac/etc/storage/`.

    For instance,

    ```
    sudo /bin/cp /var/TKLC/smac/image/isoimages/home/smacftpusr/<filename> /usr/
    TKLC/smac/etc/storage/
    ```

13. To process the XML file, continue with the procedure Processing the XML files.

The XML file is now prepared and ready for processing.

Preparing XML file for Host Volume configuration

The Configure Host Volume capability configures the Host Volume on the specified server blade and creates the corresponding configuration on the Controller.

Note: This interface is not intended for general customer use and should be used only as directed by My Oracle Support.

Caution: The order in which Vdisks, Host Volumes, Global Spares are created or deleted is important. The procedures in this section do not state or imply the order to use. The operator with site-specific knowledge has the responsibility to configure the Vdisks, Host Volumes, and Global Spares in the proper order.

1. Log into the PMAC server as `admusr`.
2. Copy the file `example_SharedStorageConfig_HostVolume.xml` to a location where you can edit it from the following directory location on the PMAC server: `/usr/share/doc/TKLCsmac-config-<release_number>/examples/`.
3. Locate the `<HostVolume>` element.

   The relevant section from the XML file is shown:

```
<HostVolume>

      <!--
        A Host may be specified by its IP address or a name that
        resolves to its IP address.
      -->
      <Host>10.2.3.1</Host>

      <VolumeMB>1300000</VolumeMB>

      <!--
        A volume can be created with the following file system types:
ext2, ext3 (default), and raw.
      -->
      <Filesystem>ext3</Filesystem>

      <MountPoint>/mnt/dbVolume</MountPoint>

      <Controller>10.2.3.4</Controller>

      <VdiskName>Vdisk2</VdiskName>

      <MountOptions>exec,ro</MountOptions>
      <!--
        The VolumeName is optional but it's recommended that you provide
        a meaningful name.  If none is provided, one will be generated
        automatically by PM&C.
      -->
      <VolumeName>FirstVolume</VolumeName>

      <LUN>20</LUN>
```

```
</HostVolume>
```

4. For the <Host> element, enter an IP v4 address or a hostname that resolves to an IP Address. This element specifies the target server blade. You can have multiple <HostVolume> elements in one file.
5. For the <VolumeMB> element, enter the size in megabytes for the Volume.
6. For <Filesystem>, enter one of the following file system types: ext2, ext3, and raw.

   If no value is specified, the default ext3 is used.
7. For <MountPoint>, enter the location on the host to mount the Volume.
8. Under <Controller>, enter the Controller IP v4 address or hostname to associate with this Host Volume.
9. Under <VdiskName>, enter the Vdisk name to associate with this Host Volume.
10. For <MountOptions>, enter one or more of the following options:

    - async

      All I/O to the file system should be done asynchronously.
    - atime

      Update inode access time for each access. This is the default.
    - auto

      Can be mounted with the -a option.
    - defaults

      Use default options: rw, suid, dev, exec, auto, nouser, and async.
    - dev

      Interpret character or block special devices on the file system.
    - exec

      Permit execution of binaries.
    - _netdev

      The filesystem resides on a device that requires network access (used to prevent the system from attempting to mount these filesystems until the network has been enabled on the system).
    - noatime

      Do not update inode access times on this file system (for example, for faster access on the news spool to speed up news servers).
    - noauto .

      Can only be mounted explicitly (i.e., the -a option will not cause the file system to be mounted).
    - nodev

Do not interpret character or block special devices on the file system.

- `noexec`

  Do not allow execution of any binaries on the mounted file system. This option might be useful for a server that has file systems containing binaries for architectures other than its own.

- `nosuid`

  Do not allow set-user-identifier or set-group-identifier bits to take effect.

- `nouser`

  Forbid an ordinary (for example, non-root) user to mount the file system. This is the default.

- `remount`

  Attempt to remount an already-mounted file system. This is commonly used to change the mount flags for a file system, especially to make a read-only file system writeable. It does not change the device or mount point.

- `ro`

  Mount the file system read-only.

- `rw`

  Mount the file system read-write.

- `suid`

  Allow set-user-identifier or set-group-identifier bits to take effect

- `sync`

  All I/O to the file system should be done synchronously.

- `dirsync`

  All directory updates within the file system should be done synchronously. This affects the following system calls: create, link, unlink, symlink, mkdir, rmdir, mknod and rename.

- `user`

  Allow an ordinary user to mount the file system. The name of the mounting user is written to `mtab` so that he can unmount the file system again. This option implies the options `noexec`, `nosuid`, and `nodev` (unless overridden by subsequent options, as in the option line `user,exec,dev,suid`).

- `users`

  Allow every user to mount and unmount the file system. This option implies the options `noexec`, `nosuid`, and `nodev` (unless overridden by subsequent options, as in the option line `users`, `exec`, `dev`, `suid`).

Some of the mount options are useful only when they appear in the `/etc/fstab` file. The mount options apply to any file system that is being mounted (but not every file system actually honors them, for example, the `sync` option has an effect only for ext2, ext3 and ufs):

11. For `<VolumeName>`, enter a name.

If you do not specify a name, PMAC will generate one.

12. At this point, if you would like to combine several XML files under the `<SharedStorageConfig>` element, you may do so.

    To view an example of a combined XML file, see Sample combined configure storage file.

13. If necessary, upload the XML file(s) back to the PMAC server by using `sftp`. See Uploading files to PMAC via sftp if you need help uploading the file.

14. On the PMAC server, copy the XML file to `/usr/TKLC/smac/etc/storage/`.

    For instance,

    ```
    sudo /bin/cp /var/TKLC/smac/image/isoimages/home/smacftpusr/<filename> /usr/
    TKLC/smac/etc/storage/
    ```

15. To process the XML file, continue with the procedure Processing the XML files.

The XML file is now prepared and ready for processing.

Processing the XML files

Caution: The storage configuration capability is intended for use only by trained installation personnel.

Note: If a prior attempt to configure the storage device failed, you must perform some cleanup before any further attempts are made to execute this procedure. For recovery information, see Configure storage recovery.

One or more storage devices can be configured after the following setup tasks have been completed:

- The MSA (Modular Storage Array) for networking and remote access is set up.
- The SAN switch and the switches are set up.
- PMAC is installed and initialized on the PMAC server.

Note: This procedure assumes that the XML file(s) containing the storage configuration data has been created and placed in the appropriate location on the PMAC server: `/usr/TKLC/smac/etc/storage/`. See Preparing XML file for Host Volume configuration or Preparing XML file for Vdisk or Global Spare configuration if you need guidelines for preparing the XML file(s).

1. Log onto the PMAC GUI as the **guiadmin** or **pmacop** user.
2. Click **Storage** > **Configure SAN Storage**.
3. In the **Configure Storage** list, select the XML file and then click **Configure Storage**.

Note: You cannot select multiple XML files. If you have the storage configuration on more than one XML file, you will need to execute this procedure once per file.

The **Configure Storage** background task is launched. An ID for the background task and a link to **Task Monitoring** is provided.

4. Click **Task Monitoring** to monitor progress as the background task executes.
5. Use the **Refresh** link to monitor the background task until you have verified that the background task completes successfully. If the background task completes successfully, the last step in the Background Task Monitoring display reads Storage configuration successful. If the display indicates failure, see Configure storage recovery.

The storage device is configured.

Sample configure storage files

The storage configuration is specified in one or more XML files that define the Vdisks, Global Spares, and Host Volumes to be configured on Controllers and Hosts.

The file(s) is created by editing the sample XML files that are provided with PMAC. The sample XML files have comments and instruction in-line to facilitate the editing process.

The sample storage configuration files are follows:

- `example_SharedStorageConfig_HostVolume.xml`
- `example_SharedStorageConfig_Vdisks_GlobalSpares.xml`

Sample VdiskConfig configure storage file

A sample `<VdiskConfig>` file follows:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<SharedStorageConfig>

  <!--
    A CheckHealthStatus is optional. If one is not provided, PM&C will
    assume the value to be ON. If CheckHealthStatus is ON, PM&C includes
    storage health status checks in its error checking, and may not
    proceed with the configuration if problems are found.
  -->
  <CheckHealthStatus>OFF</CheckHealthStatus>

  <VdiskConfig>

    <Controllers>

      <!--
        Provide the IP addresses (or names that resolve to IP addresses)
        of one or more Controllers here.  The configuration in this file
        will be applied to each controller listed.

        At least one <Controller> must be provided, prior to the VDisks section.

        Specify only one Controller per Controller Enclosure.  Each
        Controller Enclosure has two Controllers, but they are a
```

```
    redundant pair.  Applying the same configuration to both would
    attempt to configure the Controller Enclosure twice.
  -->
  <Controller>10.240.6.150</Controller>

  <Vdisks>

    <Vdisk>

      <!--
        This is the name by which the Vdisk will be specified when
        configuring HostVolumes.
      -->
      <Name>Vdisk1</Name>

      <!--
        The Owner is the Controller (A or B) within the Controller
        Enclosure that will be used for this Vdisk.  Vdisks may be
        assigned to different Controllers to achieve static load
        balancing between the Controllers.  If one Controller in a
        redundant pair fails, ownership of its Vdisks will be taken
        over by the surviving controller.
      -->
      <Owner>A</Owner>

      <RaidLevel>5</RaidLevel>

      <!--
        Disks are specified in form "Enclosure.Bay" as in the
following examples:

        MSA2012:

          Enclosure 0 (controller enclosure): Disks 0.0..0.X
          Enclosure 1 (drive enclosure):      Disks 1.0..1.X
          Enclosure 2 (drive enclosure):      Disks 2.0..2.X

MSA2324, P2000 and newer:

          Enclosure 0 (controller enclosure): Disks 1.1..1.X
          Enclosure 1 (drive enclosure):      Disks 2.1..2.X
          Enclosure 2 (drive enclosure):      Disks 3.1..3.X
       -->
      <Disks>
        <Disk>0.0</Disk>
        <Disk>0.1</Disk>
        <Disk>0.2</Disk>
        <Disk>0.3</Disk>
      </Disks>

      <SpareDisks>
        <Disk>0.4</Disk>
      </SpareDisks>

    </Vdisk>

    <Vdisk>

      <Name>Vdisk2</Name>

      <Owner>B</Owner>
```

```
          <RAIDlevel>5</RAIDlevel>

          <Disks>
            <Disk>0.5</Disk>
            <Disk>0.6</Disk>
            <Disk>0.7</Disk>
            <Disk>0.8</Disk>
          </Disks>

          <SpareDisks>
            <Disk>0.9</Disk>
          </SpareDisks>

        </Vdisk>

      </Vdisks>

      <!--
        Global Spares are spare disks not assigned to any particular
        Vdisk.
      -->
      <GlobalSpares>
        <Disk>0.10</Disk>
        <Disk>0.11</Disk>
      </GlobalSpares>

    </Controllers>

  </VdiskConfig>

</SharedStorageConfig>
```

Sample HostVolumeConfig configure storage file

A sample <HostVolumeConfig> file follows:

```
  <?xml version="1.0" encoding="ISO-8859-1" ?>
- <SharedStorageConfig>
- <!--
    A CheckHealthStatus is optional. If one is not provided, PM&C will
    assume the value to be ON. If CheckHealthStatus is ON, PM&C includes
    storage health status checks in its error checking, and may not
    proceed with the configuration if problems are found.

  -->
  <CheckHealthStatus>OFF</CheckHealthStatus>
- <HostVolumeConfig>
- <!--
      One or more HostVolumes may appear here.  Each creates a
      Volume on a Vdisk and makes it accessible to a Host.

  -->
- <HostVolume>
- <!--
       A Host may be specified by its IP address or a name that
       resolves to its IP address.

  -->
  <Host>10.2.3.1</Host>
  <VolumeMB>1300000</VolumeMB>
- <!--
```

```
        A volume can be created with the following file system types:
ext2, ext3 (default), and raw.


  -->
  <Filesystem>ext3</Filesystem>
  <MountPoint>/mnt/dbVolume</MountPoint>
- <!--

        Specifying MountOptions is optional.  Please refer to online help
        for a list of options.

  -->
  <MountOptions>ro</MountOptions>
  <Controller>10.2.3.4</Controller>
  <VdiskName>Vdisk2</VdiskName>
- <!--
        The VolumeName is optional but it's recommended that you provide
        a meaningful name.  If none is provided, one will be generated
        automatically by PM&C.

  -->
  <VolumeName>FirstVolume</VolumeName>
- <!--
        Ensure that Volume is assigned an unique LUN value

  -->
  <LUN>20</LUN>
  </HostVolume>
  </HostVolumeConfig>
  </SharedStorageConfig>
```

Sample combined configure storage file

A combined XML file can be created by combining elements under a single instance of the <SharedStorageConfig> element. This example shows the combined XML file for a Host Volume and Vdisk configuration:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
      <SharedStorageConfig>
              <VdiskConfig>
                          <Controllers>
                          <Controller>10.240.17.54</Controller>
                          <Vdisks>
                             <Vdisk>
                              <Name>myVdisk</Name>
                              <Owner>A</Owner>
                              <RAIDlevel>1</RAIDlevel>
                               <Disks>
                                       <Disk>1</Disk>
                                       <Disk>2</Disk>
                                       <Disk>3</Disk>
                                </Disks>
                                <SpareDisks>
                                       <Disk>4</Disk>
                                 </SpareDisks>
                          </Vdisk>
                         <GlobalSpares>
                              <Disk>5</Disk>
                        </GlobalSpares>
                  </Controllers>
              </VdiskConfig>
```

```
        <HostVolumeConfig>
              <HostVolume>
                      <Host>192.168.43.2</Host>
                      <VolumeMB>120</VolumeMB>
                      <Filesystem>ext3</Filesystem>
                      <MountPoint>/mt/dbVolume</MountPoint>
                      <Controller>10.240.17.54</Controller>
                      <VdiskName>myVdisk</VdiskName>
                      <MountOptions>exec,ro</MountOptions>
                      <VolumeName>myVolume</VolumeName>
                      <LUN>20</LUN>
               </HostVolume>
        </HostVolumeConfig>
  </SharedStorageConfig>
```

Clearing or deleting the storage configuration

The XML configuration files provide elements for removing or clearing a storage configuration. The following capabilities are provided:

Clear the Controller configuration
Clears the Controller configuration but does not affect the Host Volume configuration on the server blades. This option executes a forced cleaning of all identified Controllers, Vdisks, Global Spares, and Volumes.

Clear the Host Volume configuration
Clears the Host Volume configuration but does not affect the Controller.

Delete Host Volume
Deletes all Host configuration on a specified server blade and deletes the corresponding configuration on the Controller.
To see examples of the XML files provisioned with these elements, see Sample clear or delete storage files .

Deleting a Host Volume

The Delete Host Volume capability deletes the Host Volume configuration on the specified server blade and deletes the corresponding configuration on the Controller.

> **Caution:** The order in which Vdisks, Host Volumes, Global Spares are created or deleted is important. The procedures in this section do not state or imply the order to use. The operator with site-specific knowledge has the responsibility to configure the Vdisks, Host Volumes, and Global Spares in the proper order.

1. Log into the PMAC server as `admusr`.
2. Copy the file `example_SharedStorageConfig_Delete_HostVolume.xml` to a location where you can edit it from the following directory location on the PMAC server: `/usr/share/doc/TKLCsmac-config-<release_number>/examples/`.
3. Locate the `<HostVolume ConfigAction="Delete">` tag.

   The relevant section from the XML file is shown:

```
<HostVolume ConfigAction="Delete">
    <!--
        A Host may be specified by its IP address or a name that
        resolves to its IP address.
    -->
    <Host>10.2.3.1</Host>
    <Controller>10.2.3.4</Controller>
    <VolumeName>FirstVolume</VolumeName>
</HostVolume>
```

4. Fill in the necessary site-specific information such as the IP addresses and Volume Names. You can have multiple `<HostVolume>` elements in one file.
5. If necessary, upload the XML file back to the PMAC server by using `sftp`. See Uploading files to PMAC via sftp if you need help uploading the file.
6. On the PMAC server, copy the XML file to `/usr/TKLC/smac/etc/storage/`.

   For instance,

   ```
   sudo /bin/cp /var/TKLC/smac/image/isoimages/home/smacftpusr/<filename> /usr/
   TKLC/smac/etc/storage/
   ```

7. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
8. Click **Storage** > **Configure SAN Storage**.
9. In the **Configure Storage** list, select the XML file and then click **Configure Storage**.

   The **Configure Storage** background task is launched. An ID for the background task is provided.

10. Click **Task Monitoring** to monitor progress as the background task executes.
11. Use the **Refresh** link to monitor the background task until you have verified that the background task completes successfully. If the background task completes successfully, the last step in the Background Task Monitoring display reads Host Volume successfully deleted. If the display indicates failure, make a note of the point at which the failure occurred and see Configure storage recovery.

The Host Volume configuration has now been deleted on the specified server blade. The corresponding configuration on the Controller has also been deleted.

Clearing a Host Volume

The Clear Host Volume capability clears the Host Volume configuration on the specified server blade but does not affect the corresponding configuration on the Controller.

Note: This interface is not intended for general customer use and should be used only as directed by My Oracle Support.

Caution: Prior to starting this procedure, clear the corresponding configuration data for the Host Volume from the Controller. After PMAC processes the XML file, you will be directed to reboot the target server blade(s). If the reboot occurs while the Host Volume data is on the Controller, the system goes into an "unknown state."

1. Log into the PMAC server as `admusr`.
2. Copy the file `example_SharedStorageConfig_Delete_HostVolume.xml` to a location where you can edit it from the following directory location on the PMAC server: `/usr/share/doc/TKLCsmac-config-<release_number>/examples/`.
3. Locate the `<HostVolume ConfigAction="Clear">` tag.

   The relevant section from the XML file is shown:

   ```
   <HostVolume ConfigAction="Clear">

       <!--
         A Host may be specified by its IP address or a name that
         resolves to its IP address.
       -->
       <Host>10.2.3.2</Host>

    </HostVolume>
   ```

4. Fill in the necessary site-specific information such as the IP addresses or hostnames. You can have multiple `<HostVolume>` elements in one file.

   The only child element for the host volume should be `<Host>`. Any other child elements would cause the configuration to fail with an XML_PARSE_ERROR.
5. If necessary, upload the XML file back to the PMAC server by using `sftp`. See Uploading files to PMAC via sftp if you need help uploading the file.
6. On the PMAC server, copy the XML file to `/usr/TKLC/smac/etc/storage/`.

   For instance,

   ```
   sudo /bin/cp /var/TKLC/smac/image/isoimages/home/smacftpusr/<filename> /usr/TKLC/smac/etc/storage/
   ```

7. Log into the PMAC GUI as the **guiadmin** or **pmacop** user.
8. Click **Storage** > **Configure SAN Storage**.
9. In the **Configure Storage** list, select the XML file and then click **Configure Storage**.

   The **Configure Storage** background task starts. An ID for the background task is provided.
10. Click **Task Monitoring** to monitor progress as the background task executes.
11. Use the **Refresh** link to monitor the background task until you have verified that the background task completes successfully. If the background task completes successfully, the last step in the Background Task Monitoring display reads Host Volume successfully cleared. If the display indicates failure, make a note of the point at which failure occurred and see Configure storage recovery.
12. Reboot each of the target server blades.

All Host Volume configuration has been cleared from the specified server blade.

Clearing a Controller

The Clear Controller capability clears all Vdisks, Global Spares, and Volumes for the specified Controller(s). This action does not affect any Host Volume configuration on the server blades.

1. Log into the PMAC server as `admusr`.
2. Copy the file `example_SharedStorageConfig_Delete_Clear_Controller.xml` to a location where you can edit it from the following directory location on the PMAC server: `/usr/share/doc/TKLCsmac-config-<release_number>/examples/`.
3. Locate the `<Controller ConfigAction="Clear">` element and specify an IP v4 address or a hostname that resolves to the IP address for the Controller.

   You can specify more than one Controller, and the clear configuration will be applied to each. Specify only one Controller per Controller Enclosure. Each Controller Enclosure has two Controllers, but they are a redundant pair. Applying the same configuration to both would attempt to configure the Controller Enclosure twice.

   The relevant section from the XML file is shown:

   ```
   <Controller configAction="Clear">10.240.6.150</Controller>
   ```

4. If necessary, upload the XML file(s) back to the PMAC server by using `sftp`. See Uploading files to PMAC via sftp if you need help uploading the file.
5. On the PMAC server, copy the XML file to `/usr/TKLC/smac/etc/storage/`.

   For instance,

   ```
   sudo /bin/cp /var/TKLC/smac/image/isoimages/home/smacftpusr/<filename> /usr/TKLC/smac/etc/storage/
   ```

6. Log onto the PMAC GUI as the **guiadmin** or **pmacop** user.
7. Click **Storage** > **Configure SAN Storage**.
8. In the **Configure Storage** list, select the XML file and then click **Configure Storage**.

   The **Configure Storage** background task is launched. An ID for the background task is provided.

9. Click **Task Monitoring** to monitor progress as the background task executes.
10. Use the **Refresh** link to monitor the background task until you have verified that the background task completes successfully. If the background task completes successfully, the last step in the Background Task Monitoring display indicates success. If the display indicates failure, make a note of the point at which the failure occurred and see Configure storage recovery.

The Controller configuration has now been cleared.

Deleting a Vdisk or Global Disk

The Delete Vdisk capability forces a clearing of the identified Vdisk or Global Spare.

Caution: The order in which Vdisks, Host Volumes, Global Spares are created or deleted is important. The procedures in this section do not state or imply the order to use. The operator with site-specific knowledge has the responsibility to configure the Vdisks, Host Volumes, and Global Spares in the proper order.

1. Log into the PMAC server as `admusr`.
2. Copy the file `example_SharedStorageConfig_Delete_Vdisks_GlobalSpares.xml` to a location where you can edit it from the following directory location on the PMAC server: `/usr/share/doc/TKLCsmac-config-<release_number>/examples/`.
3. If the Vdisk to delete is associated with a Host Volume, you must turn off `<CheckHealthStatus>` as follows:

   ```
   <CheckHealthStatus>OFF</CheckHealthStatus>
   ```

   By default, PMAC includes storage health status checks in its error checking and will not proceed with the configuration if problems are found. In this case, you would not be allowed to delete a Vdisk that has an associated Host Volume.
4. Locate the `<Controller>` element and specify an IP address or hostname for the Controller. The configuration information for the Vdisk will be deleted from the specified Controller.

   The relevant section from the XML file is shown:

   ```
     <VdiskConfig>
       <Controllers>
         <!--
           Provide the IP addresses (or names that resolve to IP addresses)
           of one or more Controllers here.  The configuration in this file
           will be applied to each controller listed.

           At least one <Controller> must be provided, prior to the VDisks
   section.

           Specify only one Controller per Controller Enclosure.  Each
           Controller Enclosure has two Controllers, but they are a
           redundant pair.  Applying the same configuration to both would
           attempt to configure the Controller Enclosure twice.
         -->
         <Controller>10.240.6.150</Controller>
   ```
5. Locate the `<Vdisk ConfigAction="Delete">`element and under `<Name>` specify the Vdisk to delete. Perform this step for each Vdisk to delete.

   The relevant section from the XML file is shown:

   ```
   <Vdisk ConfigAction="Delete">
             <!--
             It is necessary to specify which Vdisk to delete.
             -->
             <Name>Vdisk1</Name>
           </Vdisk>
           <Vdisk ConfigAction="Delete">
   ```

```
    <Name>Vdisk2</Name>
  </Vdisk>
```

6. If necessary, upload the XML file(s) back to the PMAC server by using `sftp`. See Uploading files to PMAC via sftp if you need help uploading the file.
7. On the PMAC server, copy the XML file to `/usr/TKLC/smac/etc/storage/`.

   For instance,

   ```
   sudo /bin/cp /var/TKLC/smac/image/isoimages/home/smacftpusr/<filename> /usr/
   TKLC/smac/etc/storage/
   ```

8. Log onto the PMAC GUI as the **guiadmin** or **pmacop** user.
9. Click **Storage** > **Configure SAN Storage**.
10. In the **Configure Storage** list, select the XML file and then click **Configure Storage**.

    The **Configure Storage** background task is launched. An ID for the background task is provided.

11. Click **Task Monitoring** to monitor progress as the background task executes.
12. Use the **Refresh** link to monitor the background task until you have verified that the background task completes successfully. If the background task completes successfully, the last step in the Background Task Monitoring display reads Vdisk configuration successfully deleted.. If the display indicates failure, make a note of the point at which the failure occurred and see Configure storage recovery.
13. After the operation executes, reboot the Host blade.

The Vdisk configuration has now been deleted on the specified server blade. The corresponding configuration on the Controller has also been deleted.

Sample clear or delete storage files

The following sample XML files are provided for clearing or deleting a storage configuration:

- `example_SharedStorageConfig_Clear_Controller.xml`
- `example_SharedStorageConfig_Delete_HostVolume.xml`
- `example_SharedStorageConfig_Delete_Vdisks_GlobalSpares.xml`

Sample clear Controller XML file

A sample of the file to clear the Controller follows:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<SharedStorageConfig>

  <!--
    A CheckHealthStatus is optional. If one is not provided, PM&C will
    assume the value to be ON. If CheckHealthStatus is ON, PM&C includes
    storage health status checks in its error checking, and may not
    proceed with the configuration if problems are found.
  -->
  <CheckHealthStatus>OFF</CheckHealthStatus>

  <VdiskConfig>
```

```
    <!--
      The configAction tag is optional; if a tag is not provided, the
      default action is add.  The clear tag will clear all Vdisks,
      global spares and volumes for the specified SAN controller.  This
      will not affect any host volume configuration on host server blades.
    -->
  <Controllers ConfigAction="Clear">

    <!--
      Provide the IP addresses (or names that resolve to IP addresses)
      of one or more Controllers here.  The configuration in this file
      will be applied to each controller listed.

      Specify only one Controller per Controller Enclosure.  Each
      Controller Enclosure has two Controllers, but they are a
      redundant pair.  Applying the same configuration to both would
      attempt to configure the Controller Enclosure twice.

    -->
    <Controller>10.240.6.150</Controller>

  </Controllers>

</VdiskConfig>

</SharedStorageConfig>
```

Sample delete Host Volume XML file

A sample of the file to delete a Host Volume follows:

```
?xml version="1.0" encoding="ISO-8859-1" ?>
<SharedStorageConfig>

  <!--
    A CheckHealthStatus is optional. If one is not provided, PM&C will
    assume the value to be ON. If CheckHealthStatus is ON, PM&C includes
    storage health status checks in its error checking, and may not
    proceed with the configuration if problems are found.
  -->
  <CheckHealthStatus>OFF</CheckHealthStatus>

  <HostVolumeConfig>

    <!--
      The default ConfigAction for the HostVolumeConfig element is add; its
      usuage is shown in detail in example_SharedStorageConfig_HostVolume.xml.
      The delete tag will delete all host configuration on a specified server
      blade, and it will delete the corresponding configuration on the SAN
      controller
    -->
    <HostVolume ConfigAction="Delete">

      <!--
        A Host may be specified by its IP address or a name that
        resolves to its IP address.
      -->
      <Host>10.2.3.1</Host>

      <Controller>10.2.3.4</Controller>

      <VolumeName>FirstVolume</VolumeName>
```

```
    </HostVolume>

    <!--
      The default ConfigAction for the HostVolumeConfig element is add; its
      usuage is shown in detail in example_SharedStorageConfig_HostVolume.xml.
      The clear tag will delete all host configuration on a specified server
      blade, but it will not affect the corresponding configuration on the SAN
      controller.
    -->
    <HostVolume ConfigAction="Clear">

      <!--
        A Host may be specified by its IP address or a name that
        resolves to its IP address.
      -->
      <Host>10.2.3.2</Host>

  </HostVolumeConfig>

</SharedStorageConfig>
```

Sample delete Vdisk XML file

A sample of the file to delete a Vdisk follows:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<SharedStorageConfig>

  <!--
    A CheckHealthStatus is optional. If one is not provided, PM&C will
    assume the value to be ON. If CheckHealthStatus is ON, PM&C includes
    storage health status checks in its error checking, and may not
    proceed with the configuration if problems are found.
  -->
  <CheckHealthStatus>OFF</CheckHealthStatus>

  <VdiskConfig>

    <Controllers>

      <!--
        Provide the IP addresses (or names that resolve to IP addresses)
        of one or more Controllers here. The configuration in this file
        will be applied to each controller listed.

        At least one <Controller> must be provided, prior to the VDisks section.

        Specify only one Controller per Controller Enclosure. Each
        Controller Enclosure has two Controllers, but they are a
        redundant pair. Applying the same configuration to both would
        attempt to configure the Controller Enclosure twice.
      -->
      <Controller>10.240.6.150</Controller>

      <Vdisks>

         <!--
           The Vdisk element has an optional ConfigAction attribute. The
           attribute can be set to Add or Delete. If no attribute is specified,
           the default action is add. Refer to
example_SharedStorageConfig_Vdisks_GlobalSpares.xml
```

```
            for additional information regarding Vdisk addition.  Note that
            a Vdisk delete will fail if the volume associated with that Vdisk
            has not been deleted.
          -->
          <Vdisk ConfigAction="Delete">

            <!--
            It is necessary to specify which Vdisk to delete.
            -->
            <Name>Vdisk1</Name>

          </Vdisk>

          <Vdisk ConfigAction="Delete">

            <Name>Vdisk2</Name>

          </Vdisk>

        </Vdisks>

        <!--
          Global Spares also have an optional ConfigAction attribute. The
          attribute can be set to Add or Delete. If no attribute is specified,
          the default action is add. Refer to
example_SharedStorageConfig_Vdisks_GlobalSpares.xml
          for additional information regarding GlobalSpare addition.
        -->
        <GlobalSpares ConfigAction="Delete">
          <Disk>0.10</Disk>
          <Disk>0.11</Disk>
        </GlobalSpares>

      </Controllers>

    </VdiskConfig>

</SharedStorageConfig>
```

Sample combined delete XML file

A single XML file can be created by combining elements under a single instance of the <SharedStorageConfig> element. This example shows a combined XML file that deletes a Host Volume and a Vdisk configuration:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
      <SharedStorageConfig>
             <HostVolumeConfig>
                   <HostVolume ConfigAction="Delete">
                          <Host>192.168.43.2</Host>
                          <Controller>10.240.17.54</Controller>
                          <VolumeName>myVolume</VolumeName>
                    </HostVolume>
             </HostVolumeConfig>
         <VdiskConfig>
            <Controllers>
               <Controller>10.240.17.54</Controller>
            <Vdisks>
                <Vdisk ConfigAction="Delete">
                    <Name>myVdisk</Name>
                </Vdisk>
            </Vdisks>
```

```
            </Controllers>
        </VdiskConfig>
    </SharedStorageConfig>
```

Configure Storage page

The Configure Storage page is accessible under **Storage** > **Configure SAN Storage** on the main menu. The page lets the **pmacop** or **guiadmin** user add a storage configuration file for use by one or more hosts.

This capability is intended for use during initial installation and to modify an existing storage configuration.

Caution: This command is not intended for general customer use and should be used only as directed by My Oracle Support.

Configure Storage elements

The Configure Storage page contains these elements.

Table 10-5 Elements on the Configure Storage Page

Element	Description
Storage Configuration	A pulldown list of the directory contents of `/usr/TKLC/smac/etc/storage`. The list enables you to select the XML file containing the configuration settings for the storage device(s).
Configure Storage button	Initiates the configuration process by launching the **Configure Storage** background task.

Configure storage recovery

The basic strategy for a failure scenario is as follows:

1. View the **Configure Storage** background task to determine what failed and where the failure occurred.

   If an attempt to configure the storage fails, the **Configure Storage** background task stops processing and lets you know that a failure has occurred. The background task also provides information on what failed and where the failure occurred. The steps of the **Configure Storage** background task show the point of failure, which would be the starting point for recovery efforts.

2. Address the problem that caused the failure.

3. Edit the appropriate XML file to remove any configuration that was done up to the point of failure.

   This cleanup must be performed because **Configure Storage** cannot back out of the operation when a failure occurs. The state is left as it was at the point of failure. PMAC provides XML files to facilitate removing any previous configurations of the Vdisks, Global Spares, and Host Volumes and to clear the Hosts and Controllers.

   See Clearing or deleting the storage configuration for information on removing configuration data.

4. Reattempt the storage configuration.

11

Other Tasks

This section provides useful procedures in relation to PMAC.

Logging onto the PMAC server

You can log onto the PMAC server from any terminal that has an **ssh** (Secure Shell) utility client installed.

> **Note:** If your terminal does not already have **ssh** installed, PuTTY is an open source **ssh** utility for Linux that you can download from the web. (Oracle does not make any representations or warranties about this product.)

You must have a user ID and password before you can log on.

1. From a command-line prompt, enter the following command to start a secure shell session with the PMAC server:

   ```
   ssh -x <username>@<PMAC_server_IP_address>
   ```

   Instead of <*username*>, enter the user name for your user account. Instead of <*PMAC_server_IP_address*>, enter the IP address for the PMAC server.

2. When prompted, enter the password associated with the user name.

The secure shell session with the PMAC server is initiated.

Uploading files to PMAC via sftp

There at two methods to upload files to PMAC:

- Using `sftp` from any server that connects to PMAC's IP address.
- Installing the file on PMAC as a software image.

This procedure covers the `sftp` method. For a procedure to install the file as a software image, see Adding a software image.

1. Enter the following command from the machine with the file you want to upload:

   ```
   sftp pmacftpusr@<ip_address>
   ```

   where `<ip_address>` is the IP address of the PMAC server.

   The message Connecting to <ip_address> is returned and a password prompt appears.

2. Enter the appropriate password.

The `sftp>` prompt is returned.

3. At the `sftp>` prompt, enter the following command:

   ```
   put <filename>
   ```

   where <filename> is the file to upload.

   The following message is returned:

   Uploading <filename> to /home/smacftpusr/<filename>

4. Enter the following command to exit the `sftp` session and return to the command prompt:

   ```
   quit
   ```

5. Enter the following commands on the PMAC server to verify that the file is uploaded:

   ```
   cd /var/TKLC/smac/image/isoimages/home/smacftpusr/
   ls
   ```

The file is now uploaded onto the PMAC server. If you intend to install the file into the PMAC software image repository, the file is already in a location where PMAC will find it. The home directory of the `pmacftpusr` is part of the standard search path that PMAC uses.

Backing up PMAC server data

The PMAC GUI provides a backup option that backs up the PMAC server data to optical media, local storage on the PMAC server, or to a remote server (for example, a redundant management server where the PMAC application is installed).

In addition to initiating an automatic backup, a user can configure the backup frequency rate.

When the remote backup feature is enabled and a remote server IP address is provisioned, application ISO images located in the PMAC image repository are replicated on the remote server. This can occur only when Remote Server is the selected media type.

Backup files and provisioned ISO images are replicated when an automatic backup occurs. Data stored in /usr/TKLC/smac/etc/ are part of the backup file. This is the same behavior that occurs when a backup is manually initiated from the **Perform Backup** page. Also, a remote server IP address can be provisioned from the **Manage Backup** page.

Manage Backup page

The Manage Backup page is accessible under **Administration** > **PMAC Backup** > **Manage Backup**. This page lets the user modify backup settings such as the automatic backup frequency and the remote server IP address.

Manage Backup elements

The Manage Backup page contains these elements:

Table 11-1 Elements on the Backup PMAC Configuration Page

Element	Description
Backup Frequency	Provides lists to set the frequency at which the automatic backup will occur. The Backup Frequency list contains supported backup frequencies. The currently configured frequency is displayed initially. Use the downward arrow to view and select a backup frequency. If you select Daily, a new list that contains the Backup Time appears to the right of the Backup Frequency pulldown list. Use this menu to select the time of day (in 24-hour format) to perform the backup. Backups will be performed daily at the selected time. If you select Weekly, two new lists appear to the right of the Backup Frequency list. Use the Backup Day menu to select the day of the week on which to perform the backup. Use the Backup Time menu to select the time of the day to perform the backup. A backup will be performed at the selected time on the selected day of the week. If you select the Hourly option, a backup will be performed each hour.
Remote IP Address	This field contains the provisioned remote server IP address. You can modify the value; however, the IP address that you specify should belong to a redundant management server running the PMAC application. This text field is disabled (grayed-out) when the remote backup feature is disabled. To de-provision a remote server IP address, you must delete the IP address in the text field and select Update Settings.
Update Settings	A button that initiates the launch of a background task that updates the backup settings.

The **Tasks** button on the toolbar displays a floating window showing PMAC Backup tasks.

Perform Backup page

The Perform Backup page is accessible under **Administration** > **PMAC Backup.**

The backup procedure archives the following data:

- Database tables that contain user-provisioned data or changed data. Database tables are not backed up if they are static and would be recreated during disaster recovery when PMAC is reinstalled.

- Specific configuration files in the `/etc` directory
- All files in the `/usr/TKLC/smac/etc` directory that were not delivered as part of the installation.

The following media types are supported:

- Disk
- Remote Server (this option is available only if the remote backup feature is enabled and a remote server IP address is provisioned)

A backup to disk puts the backed up files on the PMAC server in the following location: `/var/TKLC/smac/backup/`.

The **Perform Backup** option lets you select configuration options prior to executing the operation. The backup operation is launched as background task so that you can monitor its progress.

Note: The backup replicates provisioned ISO images on the remote server when the Remote Server is selected.

1. Log into the PMAC GUI as **guiadmin** or **pmacop**.
2. On the main menu, select **Administration** > **PMAC** > **Perform Backup**.
3. Select a value from the **Media** list to indicate where to archive the data.
4. (Optional) Enter comments into the **Comment** field.
5. Click **Backup**.

   A message similar to the following message is displayed. Note that the specified Media value is shown.

   PMAC backup to PMAC Disk will proceed in the background.

   The **Backup PMAC** background task is launched. A tracking ID number for the background task is also displayed.
6. Click **Task Monitoring** to view the progress of the background task.

The PMAC server data is written to the specified optical media or to the `/var/TKLC/smac/backup/` directory on the PMAC server. If the Remote Server option is selected, this data is written to `/var/TKLC/smac/backup/` on the remote server.

Use the Task button to can view and monitor tasks for actions initiated from this work area that are being executed in the background.

Backup PMAC Configuration page

The Backup PMAC Configuration page is accessible under **Administration** > **PMAC Backup.** The page lets you configure and initiate a backup of the PMAC server data.

Only users in the **admin** and **ops** groups have access to this page.

Perform Backup elements

The Backup PMAC Configuration page contains these elements:

Table 11-2 Elements on the Backup PMAC Configuration Page

Element	Description
Media	A list to indicate where to store the backed-up data.
Comment	A text field for user comments. The comments are written to a file that is included in the backup archive.
Backup	A button to launch the backup operation.
Tasks Button	Button to control a background task monitoring plane.

The **Tasks** button on the toolbar displays a floating window showing PMAC Backup tasks.

12

PMAC Initialization and Configuration

This section describes the PMAC configuration process.

PMAC initialization and configuration overview

Caution: These features are not intended for general customer use and should be used only as directed by My Oracle Support.

Initialization performs PMAC platform configuration based upon a user-guided GUI wizard or a CLI procedure. Profiles simplify the path through the wizard and help define features, roles, and network topologies. Network reconfiguration is a streamlined version of the initialization wizard (no profile or feature selection is needed). Feature configuration (unlike initialization or reconfiguration) is not done through the use of a wizard. It uses a single view that you use to modify features. Only the platform services are reconfigured (a PMAC restart is not performed).

PMAC configuration refers to platform configuration to support the PMAC application. The platform's services and interfaces are configured by the application, not directly through TPD or OS interfaces. The host firewall is also configured based on the required application features.

The PMAC GUI allows you to display the current provisioned PMAC and notifies you if a reconfiguration is in progress. This configuration supports the PMAC application. The platform's services and interfaces are configured by the application, they should not be configured though TPD or OS interfaces directly. The host firewall is also configured based upon the required application features.

Note: Initialization and reconfiguration is an infrequent activity, and the platform should not remain in this state for very long. There is no external indication that a configuration task is in progress, but if you try to start a new task during this time, a warning message is displayed. It is safer to cancel the activity and reconfigure.

PMAC initialization overview

Caution: These features are not intended for general customer use and should be used only as directed by My Oracle Support.

When logging in following a fresh install of the PMAC application or following a configuration reset, you are redirected to the PMAC Initialization wizard. You cannot access the wizard unless you are in an `uninitialized` state. If you are in this state,

Administration > **PMAC Configuration** takes you to the first step of the wizard, which is documented in this section. If you are in any other state, the Configuration Summary page is displayed.

PMAC initialization uses the configuration profile as the starting point for configuring the PMAC server. As shown in the table below, the configuration profile is a group of related elements that are predefined and packaged in PMAC. The configuration profile determines the PMAC services that are available and the networks that need to be configured. The **PMAC Initialization** wizard enables the user to select a profile and modify some of the profile's default networking information.

In summary, the profile configuration profile defines:

- Features to be enabled
- Mapping of features to network roles

The features page now determines the PMAC services that are available.

A configuration profile is comprised of these elements:

Table 12-1 Configuration Profile Elements

Element	Description
Features	The services that PMAC provides such as hardware discovery or switch configuration. The set of features is static and is defined within the PMAC application.
Network role	A grouping of features assigned to one or more networks. This element simplifies mapping a set of features to a network.
Network	The IP network that PMAC will use to communicate with managed or monitored equipment. The network is identified by a network ID within the PMAC initialization feature.
Network interface	A PMAC interface (physical or logical) on which a network is defined. A network may have one or more network interfaces.
Network service	A network service, such as DHCP, required by a feature to implement its functionality.

The relationship among the elements of the configuration profile are not one to one. A network can have one or more network interfaces. A network role associates a set of features to one or more networks. A feature may require one or more network services.

In summary, the configuration profile defines:

- The features to be enabled
- The mapping of features to network roles
- The networks available
- The mapping of networks to network roles
- The set of network interfaces that must be configured.

- Optionally, the routes that must be configured.
- Optionally, the platform setup or tear-down configuration tasks.

After the PMAC Initialization has successfully completed, the features that were enabled by the profile are available to the user and the PMAC server network is configured.

PMAC Initialization

This section describes the PMAC initialization process. The initialization is intended for use only during initial setup and only by trained installation personnel.

PMAC Initialization wizard

Caution: The initialization feature is not intended for general customer use and should be used only as directed by My Oracle Support.

The **PMAC Initialization** wizard is accessible on the PMAC menu under **Administration** > **PMAC Initialization**. If the initialization state is Uninitialized when a user logs into the PMAC GUI, the first page of the **PMAC Initialization** wizard launches automatically. An administrative (**admin** group) user needs to perform the initialization before users can use PMAC.

Note that the **PMAC Initialization** wizard is available only to **guiadmin** and **pmacop** users.

The wizard guides you through the following process:

1. Select a network configuration profile.
2. Modify the default network data associated with the selected profile.
3. Enabling and disabling features.
4. View the relationship between the networks and their assigned network roles.
5. Modify the IP address and description of the network interface.
6. If the selected profile enabled a feature requiring DHCP, set up the IP address range for DHCP.
7. If the selected profile specified a route, modify the IP information for the route.
8. View a summary of all data configured with the wizard prior to applying the configuration.

Note: The back button will not move backwards through previous pages. In order to change anything on a previous page, you must perform a cancel, or finish the initialization and reconfigure.

At any point during the initialization, you can execute a **cancel** command. **Cancel** discards all changes to the configuration and sets the initialization state to Uninitialized.

Once initialization successfully completes, the wizard is not accessible again from the GUI. If you need to reconfigure PMAC, call My Oracle Support.

Information you will need

The **PMAC Initialization** wizard allows you to change the default network values obtained from the configuration profile. If you would like to use values other than the defaults, you will need to have the following information available to complete the PMAC initialization.

- The appropriate configuration profile for the system you are installing.
- The Network IP address and Network Mask for the IP network that PMAC uses to communicate with the equipment that PMAC monitors or manages.
- The IP address assigned to each network interface.
- If route configuration is applicable to your configuration profile, you will need to know the destination IP address, Network Mask, and the Gateway IP address for the route.
- If DHCP configuration is applicable to your configuration profile, you will need to know the start and end range of the IP address allocation for DHCP.

If you need additional explanation of the above values, familiarize yourself with the help pages on the **PMAC Initialization** wizard in this section.

Profiles page

The Profiles page is the first page of the **PMAC Initialization** wizard and is available only if the PMAC initialization state is Uninitialized. This page displays a selectable table that contains the profiles currently existing on the platform. The page enables you to select one, and only one, **profile**.

Profiles elements

These elements appear on the Select a Profile page.

Table 12-2 Select a Profile elements

Element	Description
File Name	Lets you select one profile from the list of profiles.
Name	Provides a description for each **Profile Name**.
Comment	Gives a description of the selected profile.
Version	Shows any version information applicable to a profile. If the version is not applicable, a value of **0.0.0** is shown.

Table 12-2 (Cont.) Select a Profile elements

Element	Description
Initialize	Select a row in the Profiles table, and then select **Next**. This displays the next step of the wizard in the work area as described in the PM&C Initialization - Features page. **Note:** This button is disabled until an entry is selected.

Features page

The Features page is accessible under **PMAC Initialization** > **Profiles [Next]**. This page displays an editable table that summarizes the features that have been defined as user-configurable. User-configurable implies the feature can be enabled or disabled, and the network role associated with the feature can be changed.

Features elements

The Features page contains these elements:

Table 12-3 Elements on the Features Page

Element	Description
Feature	List of the features.
Description	An optional comment can be entered to help identify the feature.
Role	The Role name for the feature can be specified from the pulldown menu. The menu contains known network roles. Select a name from the pulldown the list to associate the feature to all network interfaces with this role.
Enabled	Enables the feature when checked, or disables when unchecked. Enabling means to configure any services and firewall rules that are applicable to the feature.
Cancel	Select to cancel this PMAC Initialization task. A Dialog box confirms the action. Select **OK** within the dialog box to display a new work area, documented in the Configuration Summary - Chancel page. Select **Cancel** within the dialog box to close the dialog box, and the current work area remains unchanged.
Add Role button	To define a new role to be used by features, select a feature and click on the **Add Role** button. Enter the **Role Name** in the dialog box, an click **Add**.
Next button	Select to proceed to the next step of the initialization wizard. This saves the changes made in the **Features** table and displays the work area in the PM&C Initialization - Network page.

Networks page

The Networks page of the **PMAC Initialization** wizard appears when you click **Next** from the Features page. The Networks page displays an editable table that contains network definitions as derived from profile or provisioned on the platform when the initialization wizard was launched.

Networks elements

The Networks page contains these elements:

Table 12-4 Elements on the Networks Page

Element	Description
Network IPAddress	Lets you modify the network IP address. The value entered must be a valid IP address. Format=P address: 4 octets, each octet between 0 and 255 a valid IPv4 netmask in dotted quad format or an IPv6 network prefix in decimal format
Network Mask/Prefix	Lets you modify the network mask. The value entered must be a valid IP address. PMAC validates that the binary representation of the network mask is a series of 1s followed by a series of 0s. PMAC also validates that the IP address is a valid network IP address for the given network mask. Format=IP address: 4 octets, each octet between 0 and 255 a valid IPv4 netmask in dotted quad format or an IPv6 network prefix in decimal format.
Add	Select to define an additional network. A new view is displayed as shown in the Networks page.
Delete	Select to delete the selected network. A dialog box confirms the action.
Cancel	Select to cancel this Initialization task. A dialogue box confirms the action. Select **OK** to display the new work area as shown in the Configuration Summary - Cancel page. **Select Cancel** to close the dialog box, and the current work area remains unchanged.
Next	Select to navigate to the next step of the initialization wizard. this saves the changes made in the Network table and displays the work area in the Network Roles page.

Network Roles page

The Network Roles page of the **PMAC Initialization** wizard appears when you click **Next** from the Networks page. The Network Role page displays and editable table that lists network roles from information derived from profile.

Network Roles elements

The Network Roles page contains these elements:

Table 12-5 Elements on the Network Roles Page

Element	Description
Network IPAddress	The network IP address.
Network Mask/Prefix	The network mask or prefix IP address.
Role	A set of features that are grouped together and mapped to one or more networks. Examples of network roles are the *customer network* or *control network*. The menu contains role names provisioned in the system, as well as option NULL to indicate that the network is not associated with any network role.
Add	Select to define an additional network. A new view is displayed as shown in the Networks page.
Delete	Select to delete the selected network. A dialog box confirms the action.
Cancel	Select to cancel this Initialization task. A dialogue box confirms the action. Select **OK** to display the new work area as shown in the Configuration Summary - Cancel page. **Select Cancel** to close the dialog box, and the current work area remains unchanged.
Next	Navigates to the next step in the initialization wizard. This saves the changes and displays a new work area as shown in the Network Interfaces page.

Network Interfaces page

The Network Interfaces page of the **PMAC Initialization** wizard appears when you click **Next** from the Network Roles page. The Network Interfaces page shows an editable table that contains network interface-related information as derived from the profile and provisioned on the platform when the initialization wizard was launched.

Network Interfaces elements

The Network Interfaces page contains the following elements:

Table 12-6 Elements on the Network Interfaces Page

Element	Description
Device	The device on which the network interface is being defined. This field is view only.
IP Address	A valid IPv4 address in dotted decimal quad format or IPv6 prefix as a decimal integer to be configured on the identified device.
Description	An optional comment to help you identify the interface.
Add	Select to add a network interface not shown in the table. This displays the work area in the Network Interfaces - Add Interfaces page.

Table 12-6 (Cont.) Elements on the Network Interfaces Page

Element	Description
Delete	Select to delete a network interface in the table. A dialog box confirms the action. **Note:** Selecting **OK** displays a notification box, and the deleted network is removed from the table. Selecting **Cancel** within the dialog box closes the dialog box and returns to the work area. **Note:** **Delete** is disabled if no entry is selected.
Cancel	Select to cancel this Initialization task. A dialogue box confirms the action. Select **OK** to display the new work area as shown in the Configuration Summary - Cancel page. **Select Cancel** to close the dialog box, and the current work area remains unchanged.
Next	Select to navigate to the next step of the initialization wizard. this saves the changes made in the Network table and displays the work area in the Network Roles page.

Routes page

The Routes page is accessible under **Administration** > **PMAC Configuration** > **Network Interfaces [Next]**.

This page displays an editable table that summarizes the currently defined IP routes.

Network route elements are explain on the Routes elements page.

DHCP Ranges page

The DHCP Ranges page of the **PMAC Initialization** wizard appears for some profiles when you click **Next** from the Routes page. This page displays an editable table that contains DHCP pools as derived from the profile.

DHCP Ranges elements

The DHCP Ranges page contains these elements:

Table 12-7 Elements on the DHCP Ranges Page

Element	Description
Start DHCP	A valid IPv4 address in dotted quad format for the first address in the DHCP pool.
End DHCP	A valid IPv4 address in dotted quad format for the last address in the DHCP pool.
Add	Select to define a DHCP pool not shown in the table. This displays the work area in the DHCP Ranges - Add DHCP Range page.

Table 12-7 (Cont.) Elements on the DHCP Ranges Page

Element	Description
Delete	To delete a DHCP pool, select a DHCP Range entry in the table, then select **Delete**. A dialogue box confirms the action. Clicking **OK** within the dialog box, displays a notification box beneath the title PM&C Configuration if successful, and the deleted range is removed from the table. Clicking **Cancel** within the dialog box, closes the dialog box and returns to the work area. **Note:** **Delete** is disabled when no entry is selected.
Cancel	Select to cancel this PMAC Initialization task. A dialog box confirms the action. Select **OK** to display the work area in the Configuration Summary - Cancel page. Select **Cancel** to close the dialog box, and the current work area remains unchanged.
Next	Select **Next** to proceed to the next step of the initialization wizard. This saves the changes made in the **DHCP Ranges** table and display the work area in the DHCP Ranges page.

Configuration Summary page

The Configuration Summary page is the final page of the **PMAC Initialization** wizard. This page displays a table that contains the configuration data that will be applied if you select **Finish.**

Configuration Summary page

This page lets you display the current configuration provisioned by PMAC (this is not necessarily the current state of the platform, nor all the network resources). This is for display purposes only.

The following summaries are displayed on this page:

- Network Description
- Network and Roles Description
- Network Interface Description
- Route Configuration
- DHCP Configuration

Note: Use the down arrows in each work area to collapse or expand the list.

When a configuration or initialization task is in progress, this work area displays a warning. The use can cancel or complete an unfinished configuration task.

If you cancel the wizard from any view, a new view is displayed with a notification box appearing at the top of the work area. This alerts you of the success or failure of the task.

After completing the Configuration wizard, the work area displays a notification box and a task manager box identifying the background task that should be tracked to verify a successful reconfiguration.

The static table on the page shows the data entered into the wizard for review and acceptance.

Note: Concurrent or session based configuration is not supported.

Configuration Summary elements

The Configuration Summary page contains these elements:

Table 12-8 Elements on the Configuration Summary Page

Element	Description
Display areas	Displasys the current configuration provisioned by PMAC .
Cancel (available during specific activities)	To cancel this PMAC configuration task, select **Cancel**. A dialog box confirms the action. Select **OK** within the dialog box to display a new work area shown in the Configuration Summary - Cancel page. Select **Cancel** within the dialog box to close the dialog box; the current work area remains unchanged. **Note:** The active task might not be your own. Canceling the task might interrupt another user's work.
Finish (available during specific activities)	The PMAC Configuration task with the data shown in the summary can be finished by selecting **Finish**. This launches a background task, and then displays the summary work area as shown in the PM&C Configuration - Configuration page.

Network Configuration page

The Network Configuration page is accessible under **Administration** > **PMAC Configuration** > **Network Configuration**. The PMAC Network Configuration wizard configures the platform according to PMAC application requirements. You can use it after the PMAC application is initially installed and initialized to reconfigure the application for network changes. There is no need to reinitialize the application or deleted managed resources. After this is started, exit this wizard with **Cancel** or **Finish** only.

Reconfiguration is incremental. This allows you to make changes to the existing configuration.

If the application is complete, a work area allowing you to begin a new configuration task is displayed. Otherwise, the Configuration Summary work area is displayed.

Network Configuration elements

The Network Configuration page contains these elements:

Table 12-9 Elements on the Network Configuration Page

Element	Description
Display area	If the application state is complete, a work area that allows you to begin a new configuration task that is displayed; otherwise, another the Configuration Summary - task in progress work area is displayed.
Reconfigure	To begin a new reconfiguration task, select **ReConfigure**. If you do not want to begin the task, navigate to another menu.

The **Tasks** button on the toolbar displays a floating window showing PMAC Background tasks.

Networks page

This page displays an editable table that summarizes the currently defined networks under the Networks heading.

Networks elements

The Networks page contains the following elements:

Table 12-10 Elements on the Networks Page

Element	Description
Network IP field Address	A valid IPv4 address in dotted quad format or IPv6 address in colon hex format.
Network Mask/Prefix	A valid IPv4 netmask in dotted quad format or an IPv6 network prefix in decimal format.
Add	Select to define an additional network. This displays a new view within the work area in **PMAC Configuration** > **Networks** > **Add Network** page.
Delete	Select to delete a network entry in the table. A dialog box confirms the action. **Note:** Selecting **OK** displays the notification box beneath the title PMAC Configuration, and the deleted network is removed from the table. Routes and interfaces for the deleted network are deleted as well. Selecting **Cancel** within the dialog box closes the dialog box and returns to the work area. **Delete** is disabled when no entry is selected.

Table 12-10 (Cont.) Elements on the Networks Page

Element	Description
Cancel	Select to cancel a PMAC configuration task. A dialog box confirms the action. **Note:** Selecting **OK** displays a new work area in the Configuration Summary - Cancel page. Selecting **Cancel** within the dialog box closes the dialog box and work area remains unchanged.
Next	Select to save the changes made in the Networks table and display a new task step work area in the PMAC Configuration - Network Roles page.

Add Network page

The Add Network page is accessible under **Administration** > **PMAC Configuration** > **Networks** > **Add Network**.

This page displays editable fields for adding networks.

Add Network elements

The Add Network page contains these elements:

Table 12-11 Elements on the Add Network Page

Element	Description
Network Address	A valid IPv4 address in dotted quad format or IPv6 address in colon hex format.
Network Mask/Prefix	A valid IPv4 netmask in dotted quad format or an IPv6 network prefix in decimal format.
Add Network	Select to validate fields, and upon success, returns to the Networks work area showing the newly added network with a notification box confirming the event. If the fields do not validate, an error box is displayed, and the work area remains in Add Network. Some validations errors are show after returning to the Network work area.
Cancel	Select to return to **PMAC Configuration** > **Networks** without changes.

Network Roles page

This page displays an editable table that summarizes the currently defined network role associations.

Network Roles elements

The Network Roles page contains these elements:

Table 12-12 Elements on the Network Roles Page

Element	Description
Network IP Address	The IP address of the network.
Network Mask/ Prefix	The IPv4 network mask or IPv6 prefix.
Role	The role name can be specified from the pulldown menu. The menu contains role names provisioned in the system, as well as option NULL to indicate that the network is not associated with any network role. To associate the network to a new role name, select a name from the pulldown list. To define a new role name, use Feature Configuration.
Add	Select to associate a defined network not shown in the table to a network role. This displays the work area in the Add Network Role page.
Delete	Select a network entry in the table, then select **Delete** to remove the network role association. A dialog box confirms the action. Clicking **OK** within the dialog box displays a notification box beneath the title **PM&C Configuration** if successful, and the deleted network is removed from the table. Selecting **Cancel** within the dialog box closes the dialog box and returns to the work area. **Delete** is disabled if no entry is selected.
Cancel	Select to cancel this PM&C Configuration task. A dialog box confirms the action. Selecting **OK** within the dialog box, displays a new work area as shown in the Configuration Summary - Cancel page. Select Cancel within the dialog box closes the dialog box and the current work area remains unchanged.
Next	Select to proceed to the next step of the configuration wizard. This saves the changes made in the **Network Roles** table and displays the new task step work area shown in the Network Configuration page.

Add Network Role page

The Add Network Role page is accessible under **Administration** > **PMAC Configuration** > **Networks Roles** > **Add Network Role**.

This page displays an editable table that lets you add network role associations.

Add Network Role elements

The Add Network Role page contains these elements:

Table 12-13 Elements on the Add Network Role Page

Element	Description
Network Address	The IP address of the network.
Role Name	The role name can be specified from the list. The menu contains role names provisioned in the system, as well as option NULL to indicate that the network is not associated with any network role. To associate the network to a new role name, select a name from the list. To define a new role name, use the work area in the Feature Configuration page.
Add Network Role	Select to return to the Networks Roles work area showing the newly added network role with a notification box confirming the event.
Cancel	Select to return to work area in the Network Roles page without changes.

Network Interfaces page

This page displays an editable Static table that summarizes the currently defined IPv4 or IPv6 network interfaces.

Network Interfaces elements

The Network Interfaces page contains these elements:

Table 12-14 Elements on the Network Interfaces Page

Element	Description
Device	The name of the selected device.
IP Address	A valid IPv4 address in dotted quad format or IPv6 prefix as a decimal integer for the selected device.
Description	Enter a comment to help identify the interface.
Add	Select to add a network interface not shown in the table. This displays the work area in the Network Interfaces - Add Interfaces page.

Table 12-14 (Cont.) Elements on the Network Interfaces Page

Element	Description
Delete	Select to delete a network interface in the table. A dialog box confirms the action. **Note:** Selecting **OK** displays a notification box, and the deleted network is removed from the table. Selecting **Cancel** within the dialog box closes the dialog box and returns to the work area. **Note:** **Delete** is disabled if no entry is selected.
Cancel	Select to cancel a PMAC configuration task. A dialog box confirms the action. Selecting OK displays a new work area shown in the Configuration Summary - Cancel page.
Next	Select to proceed to the next step of the configuration wizard. This saves the changes and displays the work area in the PM&C Configuration - Routes page.

Add Interface page

The Add Interface page is accessible under **Administration** > **PMAC Configuration** > **Network Interfaces – Add Interface**.

This page displays an editable table that allows you to add a network interface.

Add Interface elements

The Add Interface page contains these elements:

Table 12-15 Elements on the Add Interface Elements Page

Element	Description
Device	A new device can be specified from the list. The menu contains known interfaces on the platform. To associate the interface with an existing device, select a name from the list. To define a device not in the menu, enter a new name in the list. The named device must be a valid interface for the configuration task to complete successfully. PMAC running in a guest VM should not need to define devices that are not in the menu. On native hardware, alias or 802.1Q interfaces can be configured.
IP Address	A valid IPv4 address in dotted quad format or IPv6 prefix as a decimal integer for the selected device.

Table 12-15 (Cont.) Elements on the Add Interface Elements Page

Element	Description
Description	An optional comment can be entered to help identify the interface.
Add Interface	Select to add validate fields, and upon success will return to the Network Interfaces work area showing the newly added interface with a notification box confirming the event. If the fields do not validate, an error box is displayed, and the work area remains in Add Interface.
Cancel	Select to return to the work area in the Network Interfaces page without changes.

Routes page

This page displays an editable table that summarizes the currently defined IP routes.

Routes elements

The Routes page contains these elements:

Table 12-16 Elements on the Routes Page

Element	Description
Device	The name of the device.
Destination IP Address	A valid IPv4 address in dotted quad format or IPv6 address in colon hex format identifying the destination route. It is used to defined a host route, network route or default route over the specified device.
Network Mask/Prefix	A valid IPv4 netmask address in dotted quad format or IPv6 network prefix in decimal.
Gateway IP	A valid IPv4 address in dotted quad format or IPv6 address in colon hex format identifying the next hop for the route. It must be a local address on the network attached to the specified device.
Add button	Select to define a new route not shown in the table. This displays the work area in the Routes - Add Route page.

Table 12-16 (Cont.) Elements on the Routes Page

Element	Description
Delete button	To delete a route, select a route entry in the table, and click **Delete**. Click **OK** on the confirmation screen. A notification box displays beneath the PM&C Configuration title, if successful, and the deleted route is removed from the table. Click **Cancel** to close the dialog box and return to the work area. **Note:** **Delete** is disabled when no entry is selected.
Cancel button	Select to cancel this configuration task. A dialog box is displayed to confirm this action. Click **OK** to display a new work area in the Configuration Summary - Cancel page. Click **Cancel** to close the dialog box and the current work area remains unchanged.
Next button	Select to proceed to the next step of the configuration wizard. This saves the changes made in the Network Interfaces table and displays the work area in the DHCP Ranges page.

Add Route page

The Add Route page is accessible under **Administration** > **PMAC Configuration** > **Routes - Add Route**.

This page displays editable fields to add a route.

Add Route elements

The Add Route page contains these elements:

Table 12-17 Elements on the Add Route Page

Element	Description
Device	A egress device can be specified from the list. The menu contains known interfaces on the platform. Select a name from the drop down the list to apply the new destination route to use this device.

Table 12-17 (Cont.) Elements on the Add Route Page

Element	Description
Destination Address	A valid IPv4 address in dotted quad format or IPv6 address in colon hex format identifying the destination route. It is used to defined a host route, network route, or default route over the specified device.
Destination Mask	A valid IPv4 netmask address in dotted quad format or IPv6 address in decimal.
Gateway	A valid IPv4 address in dotted quad format or IPv6 address in colon hex format identifying the next hop for the route. It must be a local address on the network attached to the specified device.
Add Route	Select to validate fields, and upon success returns to the Routes work area showing the newly added route with a notification box confirming the event. If the fields do not validate, an error box is displayed, and the work area remains in Add Route.
Cancel	Select **Cancel** to return to the work area in the PM&C Configuration - Routes page without changes.

DHCP IPv4 Ranges page

The DHCP IPv4 Ranges page displays an editable table that summarizes the currently defined IPv4 DHCP pools as ranges of IPv4 addresses. Only one pool per network is allowed.

DHCP IPv4 Ranges elements

The DHCP Ranges DHCP IPv4 Ranges page contains these elements:

Table 12-18 Elements on the DHCP IPv4 Ranges Page

Element	Description
Start DHCP	A valid IPv4 address in dotted quad format for the first address in the DHCP pool. The pool is a sequential pool of addresses with this starting address less than the end address.
End DHCP	A valid IPv4 address in dotted quad format for the last address in the DHCP pool. The pool is a sequential pool of addresses with this starting address less than the end address.
Add	Select to define a DHCP pool not shown in the table. This displays the work area in the DHCP Ranges - Add DHCP Range page.

Table 12-18 (Cont.) Elements on the DHCP IPv4 Ranges Page

Element	Description
Delete	To delete a DHCP pool, select a DHCP Range entry in the table, then select **Delete**. A dialogue box confirms the action. Clicking **OK** within the dialog box, displays a notification box beneath the title PM&C Configuration if successful, and the deleted range is removed from the table. Clicking **Cancel** within the dialog box, closes the dialog box and returns to the work area. **Note:** **Delete** is disabled when no entry is selected.
Cancel	Select **Cancel** to cancel this PMAC Configuration task. A dialogue box confirms the action. Select **OK** within the dialog box to display the work area in the Configuration Summary - Cancel page. Select **Cancel** within the dialog box to close the dialog box and the current work area remains unchanged.
Next	To proceed to the next step of the configuration wizard, select **Next**. This saves the changes made to **DHCP Ranges** and displays the Configuration Summary work area.

DHCP Ranges Add DHCP Range page

The DHCP Ranges Add DHCP Range page is accessible under **Administration** > **PMAC Configuration** > **DHCP Ranges - Add DHCP Range**.

This page displays an editable table that lets you add a DHCP range.

Add DHCP Range elements

The Add DHCP Range page contains these elements:

Table 12-19 Elements on the Add DHCP Range Page

Element	Description
Starting address in range	A valid IPv4 address in dotted quad format for the first address in the DHCP pool.
Ending address in range	A valid IPv4 address in dotted quad format identifying the last address in the DHCP pool.
Add DHCP Range	Select to return to the DHCP Ranges work area showing the newly added DHCP pool with a notification box confirming the event. Select **Next** to return to the Configuration Summary work area.
Cancel	Select **Cancel** to return to the work area in the DHCP Ranges page without changes.

Configuration page

After completing the Configuration wizard, the work area displays a notification box and a task manager box identifying the background task that should be tracked to verify a successful reconfiguration.

The static table on the page shows the data entered into the wizard for review and acceptance.

Feature Configuration page

This page displays an editable table that summarizes the features that have been defined as user-configurable. User-configurable implies the feature can be enabled or disabled, and the network role associated with the feature can be changed.

Features are declared as user editable by profiles during PMAC initialization. The current profiles expose the following features:

- PMAC.NETBACKUP is an optional feature that should be enabled if NetBackup is used.
- PMAC.REMOTE.BACKUP is an optional feature for backup to a redundant PMAC server.
- DEVICE.NETWORK.NETBOOT allows netConfig to initialize Cisco 3020 switches that use TFTP.
- DEVICE.NTP allows non-managed devices such as switches to use PMAC as an NTP server.
- PMAC.MANAGED allows remote systems to manage the PMAC server via SNMP.
- PMAC.IPV6.NOAUTOCONFIG is an optional feature that when enabled, disables IPv6 auto-configuration on any interfaces assigned to the feature role.

Features elements

The Features page contains these elements:

Table 12-20 Elements on the Features Page

Element	Description
Feature	List of the features.
Description	An optional comment can be entered to help identify the feature.
Role	The Role name for the feature can be specified from the pulldown menu. The menu contains known network roles. Select a name from the pulldown the list to associate the feature to all network interfaces with this role.
Enabled	Enables the feature when checked, or disables when unchecked. Enabling means to configure any services and firewall rules that are applicable to the feature.

Table 12-20 (Cont.) Elements on the Features Page

Element	Description
Add Role	Roles are uses to associate a network to a feature. The name is immaterial; it is the association that determines the behavior. To define a new role to be used by features and networks, select **Add Role** to display the work area in the Features - Add Role page.
Apply	Select to save the Feature Configuration and reconfigure the platform. Unlike Network Configuration or Initialization, this is not a background task. The work area displays a notification box to indicate a successful reconfiguration. An Error box indicates a problem with the Feature Configuration. Select to save the Feature Configuration and reconfigure the platform. The PM&C Feature Reconfiguration work area displays a notification box to indicate the start of the reconfiguration. The Tasks manager box identifies the Reconfigure PM&C Features background task and its status, where `PM&C Feature set reconfigured` indicates a successful completion. An *Error box* will indicate a problem with the start of the reconfiguration.

Add Role page

The Add Role page is accessible under **Administration** > **PMAC Configuration** > **Feature Configuration [Add Role]**. This page allows you to assign a name to a selected role.

Features Add Role elements

The Features Add Role page contains these elements:

Table 12-21 Elements on the Features Add Roles Page

Element	Description
Display area	Table of information about the selected role.
Role Name	Enter the desired name of the role.
Add	To define a new role to be used in Feature Configuration on the **Role** list, enter a new unique name for the role and select **Add**. To cancel the add request, click on **X** action icon.

13

Access Control

This section describes the Access Control features which include user account management, groups administration, and certificate management.

GUI account basics

This section discusses the basics on user accounts, groups, and session functions for the PMAC GUI. You should become familiar with this information prior to setting up the user and group accounts on the PMAC.

These tasks and responsibilities are reserved for users belonging to the **admin** group or a group with similar permissions. Users who belong to this group or have group permissions to user account functions are referred to as administrative users in this documentation.

The menu items for user account functions are all located under the **Administration** menu and reside in the following:

- **General Options**
- **GUI Sessions**
- **Access Control > Users**
- **Access Control > Groups**

Users with lesser permissions may not see some or all of the users and groups menu items in the GUI.

User account basics

Each user who is allowed access to the PMAC GUI is assigned a unique **Username**. This **Username** and the associated password must be provided during log-in. After a user defined number of consecutive failed login attempts within a user defined window, a user account is disabled. See General Options administration elements for details on setting the **Maximum Consecutive Failed** and **Lock out window** variables.

Each user is also assigned to a group (multiple users who need access to the same set of functions). Permissions to a set of functions are assigned to the group. The permissions determine the functions and restrictions for the users belonging to the group.

A user must have **Users** or **Groups** administrative permissions to view or make changes to user accounts or groups. The authorized user can set up or change user accounts and groups, enable or disable user accounts, set password expiration intervals, configure session timeouts, and change user passwords.

By default the PMAC comes with three user accounts already provisioned; the first is the guiadmin account. This account is also known as the PMAC GUI superuser and

belongs to the admin group. It has access to all views and menu items. This account is always enabled, and the maximum concurrent logins is unrestricted and cannot be changed. The second default account is pmacop and belongs to the ops group. As the name implies it has permissions suitable for most operations personnel. Members of the admin group can make changes to this user account. The third default account is guest and belongs to the guests group. It has permissions suitable for guests with limited administrative permissions. Members of the admin group can make changes to this user account.

Groups basics

PMAC uses the concept of groups to assign user permissions. A group is a collection of permissions to which one or more users can be assigned. All users of that group will have access to the same set of functions. Permissions are assigned to the group for each application function. All users assigned to the same group have the same permissions for the same functions. In other words, you cannot customize permissions for a user within a group.

Functions correspond to a specific web page or group of web pages and the actions that a group can perform on the page(s). If a group has permission to perform a function, the function is visible to all users assigned to that group. A group of related functions fall under a permissions section. For example, **Users** and **Groups** fall under the **Administrative Permissions** section. Permissions can be granted on a function basis or globally on a section basis.

By default the PMAC comes with three groups already provisioned; the first is the admin group. This group is the most powerful in the context of permissions. Any user belonging to this group has access to all views and menu items. The second default group is ops. As the name implies it provides any user belonging to this group access suitable for most operations personnel. The third default group is guests. Any user belonging to this group has permissions suitable for guests with limited administrative permissions.

You can add, delete, and update groups except for the predefined admin group.

Session timeout and concurrent login basics

A session timeout, or **Session Inactivity Limit**, is the period of inactivity permitted, in minutes, before a PMAC user session is terminated. Concurrent logins, or **Maximum Concurrent Logins**, is the number of instances of current active PMAC GUI user sessions the same user account can have. Both options are configurable on a per-user-account basis with the exception of the guiadmin user.

By default a newly added user is given unlimited concurrent logins. The administrative user has the ability to change the number of concurrent logins allowed for a specific user. The valid range is 0-50 with a default of 0 which is the setting for unlimited concurrent logins.

If a user attempts to log in and the maximum number of active sessions are active, the login attempt fails, and the user is notified of the reason. As soon as an active session logs out or expires, the user can start a new session.

If a PMAC GUI user simply exits the web browser (instead of logging out of PMAC), the user session remains active until a session timeout occurs. If the number of active sessions exceeds the number of allowed user sessions, the user will not be able to log in until one of following events occurs:

- One of the user sessions times out.

- The administrator deletes one of the user sessions.
- One of the user sessions is terminated because a user logs out.

If a session timeout occurs, the user is presented with the login page so that the user can log into the GUI again.

Only the administrative user has the ability to change any of the session timeout settings.

User accounts

This section provides procedures for user account administration including inserting (adding), editing, viewing, deleting, reporting, enabling or disabling, and changing a user's assigned group. Additionally, a user's password can be changed here.

Related Topics:

User account basics

Users Administration page

The Users administration page is accessible under **Administration** > **Access Control** > **Users**. The page lets the administrative user view user account data and launch operations to insert, edit, and delete users. Report and Change Password operations are also accessible from this page.

Note: Each user is a member of at least one group. User permissions are associated with groups, not individual users.

Users administration elements

The Users administration page contains these elements:

Table 13-1 Elements on the Users Administration Page

Element	Description
Username	The currently selected Username. The Username allows access to the GUI and must be unique.
Account Status	The current account status which is either enabled or disabled. If a user account is disabled, the user is unable to log in until an administrative user manually enables the account.
Remote Auth(entication)	The current account status of remote authentication which is either enabled or disabled.
Local Auth(entication)	The current account status of local authentication which is either enabled or disabled.
Consecutive Failed Login Attempts	The number of consecutive failed login attempts.
Concurrent Logins Allowed	The number of concurrent logins allowed.

Table 13-1 (Cont.) Elements on the Users Administration Page

Element	Description
Inactive Limit	The limit set on account inactivity after login.
Comment	An optional field for user-defined text about this account (64 character maximum).
Groups	The groups to which the selected Username is assigned. A user's groups determine the permissions assigned to the user. The permissions determine the functions and restrictions for the users belonging to the group.
Insert button	Allows an administrative user to add a new user to the database, enabling the user to log in to the GUI and access all or part of its functions.
Edit button	Allows an administrative user to edit the attributes of the selected user.
Delete button	Allows an administrative user to delete one or more selected users from the database after confirming that the delete operation is intended. After the user is deleted, the next time the user attempts to log in, access to the GUI will be denied. If the user is logged in when the delete operation is performed, this action does not disrupt the current session.
Report button	Allows an administrative user to generate an account usage report on one or more users. This type of report provides information about a user's account usage including last login date, the number of days since the user last logged in, and the user's account status.
Change Password button	Sets or changes a password that is associated with a particular Username.

Insert new user page

The Users [Insert] administration page is accessible under **Administration** > **Access Control** > **Users**. Select **Insert** to launch the page.

Insert new user elements

The Users [Insert] administration page displays the following elements:

Table 13-2 Elements on the Insert New User Page

Element	Description	Data Input Notes
Username	Username associated with the account. Must be unique. Once set, the username cannot be changed. A value is required.	Format: String Range: 5-16 lowercase alphanumeric characters (a to z, 0 to 9)

Table 13-2 (Cont.) Elements on the Insert New User Page

Element	Description	Data Input Notes
Group	The group(s) to which this user account belongs. Groups define the permissions assigned to the user. The permissions determine the functions and restrictions for the users belonging to the group. A selection of one or more groups is required.	Range: provisioned groups
Authentication Options	Authentication options used with the account. When using local authentication, the account is disabled until a password is established. If using remote authentication, an authentication server must be configured.	Format: Checkbox Range: Allow Remote Auth or Allow Local Auth Default: Local Auth enabled, Remote Auth disabled
Access Allowed	Allows the administrative user to enable or disable this user account.	Format: Checkbox Default: Account Enabled
Maximum Concurrent Logins	Maximum concurrent logins for this user account.	Range: 0-50 Default: 0 0 = unrestricted
Session Inactivity Limit	The time, in minutes, after which a user session expires from inactivity.	Range: 0-3600 Default: 120 0 = session never expires
Comment	A field for user-defined text about this account. A value is required.	Format: String Range: 1-100 characters

Insert new user account

Use this procedure to insert (add) a new user account to the database, enabling the user to log in to the PMAC GUI and access all or part of its functions.

> **Note:** As part of this procedure, the administrative user assigns each user account to a group (the group assignment determines the functions that a user can access). If you need to create a new group for this user, do so before you begin this procedure.

1. Select **Insert** from the Users administration page.

   The Users [Insert] administration page appears.

2. Enter a **Username** for the new account.

Once set, the username cannot be changed.

3. Select a **Group** or groups to assign to this account.
4. Select one or both **Authentication Options** for this user account:
   - **Allow Remote Auth(entication)**

     Note: Choose this option to authenticate user credentials through an LDAP server. See LDAP Authentication for more information on LDAP server configuration.

   - **Allow Local Auth(entication)**

     Note: Choose this option to authenticate user credentials locally. By default, a newly created user account using this option only is disabled until the **Change Password** action is used to create a password.

5. Select whether the account is enabled using the **Access Allowed** checkbox.

   Newly created accounts using the local authentication option are initially disabled, regardless of this setting, until the change password action is used to create a password.
6. Enter the **Maximum Concurrent Logins** allowed.
7. Enter the **Session Inactivity Limit** in minutes.
8. Enter informative text about this account in the **Comment** field.

   This field is mandatory.
9. Perform one of the following actions:
   - Click **OK**.

     The new user is added to the database. The Users administration page reappears with the new user displayed.

   - Click **Apply**.

     A confirmation message appears at the top of the Users [Insert] page to inform you that the new user has been successfully added to the database. To close the Users [Insert] page, click **Cancel**. The Users administration page reappears with the new user displayed.
10. If **Allow Local Auth(entication)** was selected for this user account, now is a good time to create a temporary or permanent password. See Setting a password from the Users Administration page for information on this procedure.

The new user account is added to the database.

Updating user account information

Use this procedure to update (edit) user account information on a user account basis:

1. Select **Administration > Access Control > Users**.

The Users administration page appears.

2. Select a user from the listing.
3. Select **Edit**.

   The Users [Edit] administration page appears.

4. Modify one or more of the user account information fields.
5. Click **Apply** to update the database or **Ok** to update the database and return to the Users administration page.

   The user account information is updated in the database. The changes take effect immediately.

Deleting a user account

Use this procedure to delete a user account from the database. The next time the user attempts to log in, access to the PMAC GUI will be denied. If the user is currently logged in to the system, this operation will not disrupt the user's current session. To stop a current user session, see Deleting GUI sessions, or to disable a user's account, see Enabling or disabling a user account.

1. Select **Administration** > **Access Control** > **Users**.

   The Users administration page appears.

2. Select the appropriate user from the **Username** list.
3. Click **Delete User**.

   A confirmation box appears.

4. Click **OK** to delete the user.

   The Users administration page reappears.

The user account has been deleted from the database, and the user no longer appears in the **Username** list.

About enabling or disabling a user account

The PMAC GUI automatically disables a user account after a user defined number of consecutive failed log-in attempts. See General Options administration elements for details on setting the **Maximum Consecutive Failed** variable. An administrative user can also manually disable a user account to prevent a user from logging on to the system. If a user account is disabled, the user is unable to log in until the account is reenabled.

Enabling or disabling a user account

Use this procedure to enable or disable a user account.

1. Select **Administration** > **Access Control** > **Users**.

The Users administration page appears.

2. Select the desired **Username** from the list.
3. Click **Edit**.
4. Locate the Access Allowed attribute. Click the **Account Enabled** checkbox to enable/disable the account. A check mark indicates that the account is enabled.
5. Click **Apply** to update the database or **OK** to update the database and return to the Users administrative page.

The account is enabled/disabled as selected.

Changing a user account's assigned group

Use this procedure to change a user's assigned groups. The group assignment determines the functions that a user has access to. See User groups for more information.

1. Select **Administration** > **Access Control** > **Users**.

   The Users administration page appears.
2. Select the appropriate user from the **Username** list.
3. Select **Edit**.

   The Users [Edit] administration page appears.
4. Select the desired group or groups from the **Group** list. Scroll down to see all options.
5. Click **Apply** to update the database or **OK** to update the database and return to the Users administrative page.

The user's assigned group is updated in the database and will take effect the next time the user attempts to log in to the PMAC GUI. If the user is currently logged in to the system, this operation will not affect the user's current session.

Generating a user report

A user account usage report can be generated from the users page. This type of report provides information about a user's account usage including last login date, the number of days since the user last logged in, and the user's account status.

Use this procedure to generate a user account usage report.

1. Select **Administration** > **Access Control** > **Users**.

   The Users administration page appears.
2. Select one or more users.

   Note: If no users are selected, then all users appear in the users report.
3. Click **Report**.

   The Users Report is generated. This report can be printed or saved to a file.

4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

User groups

This section describes the GUI pages used in administering groups. Procedures are provided for inserting, deleting, and editing groups as well as reporting on groups.

Groups Administration page

The Groups administration page is accessible under **Administration** > **Access Control** > **Groups**. Administrative users can launch operations to add, delete, or modify a user group as well as generate reports. See Groups basics for more information.

The Groups [Insert] administration page presents a check box matrix of functions vs actions. Functions correspond to a menu option or submenu function and are closely grouped according to the main menu's structure. Actions determine at what level you are allowed to access a function. Five actions are available; View, Insert, Edit, Delete, and Manage. If a check box is checked, the group has access to this option on the menu. If a check box is not checked, the group does not have access to this option, and the option is not visible on the GUI menu. Selecting one or more check boxes defines a set of permissions for members of that group.

A group of related functions fall under a permissions section. For example, **Users** and **Groups** fall under the **Administrative Permissions** section. Permissions can be granted on a function basis (individually), or globally on a section basis. Alternatively, permissions can be granted on a global action basis. For example, selecting the **Global Action Permissions** checkbox immediately under the **View** action allows any user belonging to this group to view all GUI pages and options.

By default the PMAC comes with three groups already provisioned; The first is the **admin** group. Any user belonging to this group has access to all GUI pages and functions. The second default group is **ops**. As the name implies it provides any user belonging to this group access suitable for most operations personnel. The third default group is **guests**. Any user belonging to this group has permissions suitable for guests with limited administrative permissions.

Note: The pre-defined admin group that comes with the system cannot be modified. The other two pre-defined groups, ops and guests, can be modified to meet specific needs. A user can be assigned to multiple groups.

Groups administration elements

The Groups administration page contains these elements:

Table 13-3 Elements on the Groups Administration Page

Element	Description
Group Name	The name of the group.
Description	A brief description of the group.
Users	A list of all users belonging to this group. Note that a user can belong to multiple groups.

Table 13-3 (Cont.) Elements on the Groups Administration Page

Element	Description
Insert button	Allows an administrative user to add a new group to the database.
Edit button	Allows an administrative user to edit the attributes of the selected group.
Delete button	Allows an administrative user to delete one or more selected groups from the database after confirming that the delete operation is intended. After a group is deleted, any users belonging only to that group will be denied GUI access the next time they attempt to log in. If the user is logged in when the delete operation is performed, this action does not disrupt the current session.
Report button	Allows an administrative user to generate an account usage report on one or more groups. Clicking **Report** without selecting a group generates a report with all groups included.

Group permissions

This section covers the permission options presented on the **Groups [Insert]** administration page. See Groups Administration page for information on **Global Action Permissions**.

Note: The five columns of checkboxes grant permission to View, Insert, Edit, Delete, or Manage the specified Resource. The View permission is applicable to every Resource; Insert, Edit, and Delete apply to provisioned Resources such as software images, server hardware, and VM guests. The Manage permission covers other actions applicable to the particular Resource.

Hardware permissions

These items appear in the **Hardware Permissions** section.

Resource	Description
System Inventory	Grants permission to view system inventory data.
System Configuration	Grants permission to view system configuration data.
FRU Information	Grants permission to view and export FRU information for enclosures and rack mount servers.
Cabinets	Grants permission to view, insert, and delete cabinets.
Enclosures	Grants permission to view, insert, edit, and delete enclosures.

Resource	Description
RMSs	Grants permission to view, insert, edit, delete, and manage rack mount servers. Permissions granted by the manage checkbox include resetting an RMS; getting and setting RMS LED state.
RMSs-Find	Grants permission to view and manage rack mount servers. Permissions granted by the manage checkbox include all find RMS actions.
RMSs-Found	Grants permission to view and manage rack mount servers. Permissions granted by the manage checkbox include all found RMS actions.
Compute Blades	Grants permission to view and manage blades servers. Permissions granted by the manage checkbox include cold and warm reset actions.
Switches	Grants permission to view and manage enclosure switches. Permissions granted by the manage checkbox include cold and warm reset actions.

Software permissions

These items appear in the **Software Permissions** section.

Resource	Provides Access To...
Software Inventory	Grants permission to view software inventory data.
Software Images	Grants permission to view, insert, edit, delete, and manage software images. Permissions granted by the manage checkbox include ISO image transfer.
OS Installation	Grants permission to view and manage OS installs. Permissions granted by the manage checkbox include all OS installation actions.
OS Installation (Bulk)	Grants permission to view and manage bulk OS installs. Permissions granted by the manage checkbox include all bulk OS installation actions.
App Upgrade	Grants permission to view and manage application upgrades. Permissions granted by the manage checkbox include all app upgrade actions.

Resource	Provides Access To...
App Upgrade (Bulk)	Grants permission to view and manage bulk application upgrades. Permissions granted by the manage checkbox include all bulk app upgrade actions.

Virtualization permissions

These items appear in the **Virtualization Permissions** section.

Note: Both **Virtualization** permissions are prerequisites for **VM Guests** permissions.

Resource	Provides Access To...
Virtualization	Grants permission to view hosts and guests. The edit permission is a prerequisite for all VM Guest permissions.
VM Guests	Grants permission to view, insert, edit, and delete virtual guests.

Storage permissions

These items appear in the **Storage Permissions** section.

Resource	Provides Access To...
SAN Storage	Grants permission to view and manage SAN storage. Permissions granted by the manage checkbox include all SAN storage actions.

Administration permissions

These items appear in the **Administration Permissions** section.

Resource	Provides Access To...
Users	Grants permission to view, insert, edit, delete, and manage users including password change and reporting. Permissions granted by the manage checkbox are equivalent to the view permission.
Groups	Grants permission to view, insert, edit, and delete groups including reporting.
GUI Sessions	Grants permission to view and manage GUI sessions. Permissions granted by the manage checkbox include all GUI session actions.

Resource	Provides Access To...
PMAC Sentry	Grants permission to view and manage the sentry process control page. Permissions granted by the manage checkbox include sentry active, passive, and restart commands.
PMAC Features	Grants permission to view and manage PMAC configuration data. Permissions granted by the manage checkbox include all PM&C feature and network configuration.
Certificate Management	Grants permission to view, insert, edit, delete, and manage security certificates. Permissions granted by the manage checkbox are equivalent to the view permission.
Backup	Grants permission to view, insert, edit, delete, and manage PMAC backups. Permissions granted by the manage checkbox include all PMAC backup actions.
SNMP Credentials	Grants permission to view and manage SNMP credentials. Permissions granted by the manage checkbox include all SNMP credentials actions.
Domain/DNS Configuration	Grants permission to view and manage DNS data. Permissions granted by the manage checkbox include all domain/DNS configuration actions.
Remote LDAP Authentication	Grants permission to view, insert, edit, and delete LDAP including account creation and management.
General Options	Grants permission to view and edit the general options page which includes password and session management settings as well as site specific settings.

Status & Manage permissions

These items appear in the **Status & Manage Permissions** section.

Resource	Provides Access To...
Files	Grants permission to view and manage system generated files such as CSR certificates. Permissions granted by the manage checkbox include all files actions.

Task Monitoring permissions

These items appear in the **Task Monitoring Permissions** section.

Resource	Provides Access To...
Background Task Monitor	Grants permission to view and delete tasks from the Task Monitoring view.

Pre-defined users and groups

These user accounts and groups are delivered with the system.

Table 13-4 Pre-defined Users and Groups

User	Group	Description
guiadmin	admin	Full access (read/write privileges) to all functions including user/group administration functions. This group cannot be deleted or modified.
guest	guests	Provides read-only access to view inventory information, software images, process and background task status, PMAC GUI preferences, and configuration data.
pmacop	ops	Provides operators with full access (read/write privileges) to all functions except the following: • User/group administration functions. • GUI site setting.

Insert new group page

The Groups [Insert] administration page is accessible under **Administration** > **Access Control** > **Groups**. Select **Insert** to launch the page.

This page lets the administrative user insert (add) a new user group and assign permissions to the group.

Insert new group elements

The Groups [Insert] administration page displays the following elements:

Table 13-5 Elements on the insert new group page

Element	Description
Group Name	The name of the group. A group is a name for multiple users who need to access the same set of functions. Permissions are assigned to the group for each function in the PMAC application. All users assigned to the same group have the same permissions for the same functions. Format=String (alphanumeric (A-Z, a-z, 0-9) between 5 and 16 characters long). This field is required.
Description	A field for user-defined text about this group. Format=String (alphanumeric (A-Z, a-z, 0-9) between 0 and 64 characters long). This field is optional.

Table 13-5 (Cont.) Elements on the insert new group page

Element	Description
Permissions	Provides a check box matrix of functions vs actions (View, Insert, Edit, Delete and Manage). Permissions can be granted on a function basis (individually), or globally on a section basis. Alternatively, permissions can be granted on a global action basis.
Buttons	• **OK** - Saves changes and returns to the Groups administration page. • **Apply** - Saves changes and remains on the Groups [Insert] page. • **Cancel** - Returns to the Groups [Insert] page without saving any changes.

Insert new group

Use this procedure to insert (add) a new group:

1. Select **Administration** > **Access Control** > **Groups**.

   The Groups administration page appears.

2. Click **Insert**.

   The Groups [Insert] administration page appears.

3. Enter a unique name in the **Group Name** field. Optionally, enter text to describe the group in **Description** field.

4. To allow View, Insert, Edit, Delete or Manage actions on all pages accessed from the GUI, selectively check mark each action in the **Global Action Permissions** row.

5. Check mark the remaining menu permissions to which you want this group to have access.

   Note: To quickly select all permissions in a given section, place a check beside the desired section under the desired action. For example, if the group needs only view access for the **Software Permisions** section, place a single check next to **Software Permissions** and under the **View** action.

6. Perform one of the following actions:

   - Click **Apply**.

     A confirmation message appears at the top of the page to inform you that the new group has been added to the database. To close the page, click Cancel.

   - Click **OK**.

     The Groups administration page re-appears with the new group displayed.

   - Click **Cancel**.

     The changes are discarded and the Groups administration page re-appears.

The new group is added to the database.

Updating a group

Use this procedure to update (edit) group information including the description and permissions.

> **Note:** You cannot modify a predefined group provided during installation. See Pre-defined users and groups for more information on this topic.

1. Select **Administration** > **Access Control** > **Groups**.

   The Groups administration page appears.

2. Select a group from the listing.

3. Select **Edit**.

   The Groups [Edit] administration page appears.

4. Modify the description or group permissions as needed. For information on permission options, see Group permissions.

5. Select **Ok** or **Apply**.

   Selecting **Ok** returns you to the Groups administration page. Selecting **Apply** leaves you in the Groups [Edit] page but applies the changes.

The modifications are written to the database. The main GUI menu of the affected user(s) is not changed until the user logs out and back in to the system, or the user refreshes the menu (using the web browser's Refresh function). The change in accessibility to menu options for affected user(s) takes effect immediately.

Deleting a group

> **Note:** The system does not allow any user to delete a predefined group provided during installation. See Pre-defined users and groups for more information on this topic.

Use this procedure to delete a group:

1. Select **Adminstration** > **Access Groups** > **Groups**

   The Groups administration page appears.

2. Select the desired group from the Groups administration page and take note of any users presented in the **Users** pane.

> **Note:** The **Users** pane lists all users associated with the group. If there are users associated with the group, you must delete the users or assign them to another group prior to deleting the group. See Changing a user account's assigned group.

3. Once all users have been cleared from the **Users** pane click **Delete**.

   A Confirmation box appears.

4. Click **OK** to delete the group.

   A status box displays the results of the action.

The group is removed from the database.

Viewing a group's members

Use this procedure to view a list of users assigned to a group.

1. Select **Administration** > **Access Control** > **Groups**.

   The Groups administration page appears.

2. Scroll down as needed to bring the desired group into the viewing area.

   The Users pane displays all users belonging to that group.

A list of group members is displayed.

Generating a group report

A group report can be generated from the Groups administration page. This type of report provides information about a groups global action and administrative permissions.

1. Select **Administration** > **Access Control** > **Groups**.

   The Groups administrative page appears.

2. Select one or more groups.

   Note: If no groups are selected then all groups appear in the group report.

3. Click **Report**.

   The group report is generated. This report can be printed or saved to a file.

4. Click **Print** to print the report or **Save** to save the report to a file.

Passwords

Password configuration and management is accomplished from two locations within the PMAC GUI. General password options related to access control are presented in the General Options administration page. Account specific password management is handled from the Users administration page.

General options, such as password expiration, password history rules, password length, and minimum password difference are covered in the PMAC User Interface chapter. See General Options administration elements to view these options.

The application provides two ways to set passwords: through the Users administration page, see Setting a password from the Users Administration page, and at login, see Setting a password from the System Login page.

Note: Only an administrative user can manage passwords from the Users administration page. Password changes for non-administrative users are handled from the System Login page.

During the creation of a new user account, the administrative user has the option to force a password change the first time the new user logs into the account. This is normal practice for single user accounts but may not be practical for group accounts.

The criteria for a valid password:

- must contain from 8 to 16 characters (this is default behavior, minimum password length is a global option and may be changed).
- must contain at least three of the four types of characters: numerics, lower case letters, upper case letters, or special characters (! @ # $ % ^ & * ? ~).
- cannot be the same as the Username or contain the Username in any part of the password (for example, **Username=jsmith** and **password=$@jsmithJS** would be invalid).
- cannot be the inverse of the Username (for example, **Username=jsmith** and **password=$@htimsj** would be invalid).
- cannot contain three or more consecutively repeated characters, or three or more ascending or descending alpha-numeric characters in a row, for example, **1234, aaaa, dcba**.
- cannot reuse any of the last three passwords (this is default behavior, maximum password history is a general option and may be changed.

Setting a password from the Users Administration page

Use this procedure to change an existing user's password and/or make the password temporary.

Note: Only an administrative user may use this procedure. For information about how a non-administrative user can change a password, see Setting a password from the System Login page.

1. Select **Administration > Access Control > Users**.

   The Users administration page appears.

2. Select the appropriate user from the listing.

3. Click **Change Password**.

   The User [Set Password] administration page appears. The selected user account name appears in bold at the top of the change password dialogue box.

4. Enter a password in the **New Password** field. Retype the same password in the **Retype New Password** field.

The system verifies that the values entered in both fields match. For information on valid passwords, see Passwords.

5. Select the checkbox next to **Force password change on next login** if desired.

   Administrators typical select this for single user accounts.

6. Click **Continue**.

   The Users administration page re-appears. A confirmation message is displayed at the top of the page indicating the result of the action.

The password has been updated in the database. The change will take effect the next time the user attempts to log in to the user interface.

Setting a password from the System Login page

Use this procedure to change a existing, non-administrative user's password on login.

> **Note:** This procedure is for non-administrative users. For information about how an administrative user can set a password, see Setting a password from the Users Administration page.

1. Select **Change password** checkbox on the System Login page.
2. Enter the user name and password.
3. Click **Login**.

   The Password Change Requested page appears.

4. Enter a password in the **New Password** and **Retype New Password** fields. For information on valid passwords, see Passwords.

   The system verifies that the values entered are valid and that both fields match.

5. Click **Continue**.

   The password has been updated in the database and will take effect the next time the user attempts to log in to the user interface.

You have now completed this procedure.

Configuring password expiration

Password expiration controls the number of calendar days for passwords to stay active. Note that the expiration is retroactive: if the expiration is newly set to 30 days and it has been 45 days since the password was last changed, the password is now expired.

Note: Another form of password expiration is used during the creation of a new user account. The administrative user creating the new account has the option to force a password change the first time the new user logs into the account. In effect, the password expires upon first use. See Setting a password from the Users Administration page for more information on this type of password expiration.

Use the following procedure to set the password expiration global option.

1. Select **Administration > General Options**.

   The General Options page appears.

2. Locate **Password Expiration** in the **Variable** column.

3. Enter the desired number of days in the **Value** column.

   Enter **0** to disable password expiration.

4. Click **OK** to submit the changes or **Cancel** to return the changed options to their previous values.

The password expiration variable is changed to the new value.

Configuring maximum password history

Maximum password history defines the number of passwords maintained in history before reuse of a password is allowed.

Use the following procedure to set the maximum password history global option.

1. Select **Administration > General Options**.

   The General Options page appears.

2. Locate **Maximum Password History** in the **Variable** column.

3. Enter the desired number in the **Value** column. A value is required.

   Enter **0** to disable password history.

4. Click **OK** to commit the changes or **Cancel** to return all changed options to their previous values.

The password history variable is changed to the new value.

Configuring minimum password length

Minimum password length defines the minimum number of valid characters a password is allowed to be.

Use the following procedure to set the minimum password length global option.

1. Select **Administration > General Options**.

   The General Options page appears.

2. Locate **Minimum Password Length** in the **Variable** column.

3. Enter the desired value in the **Value** column.
4. Click **OK** to commit the changes or **Cancel** to return all changed options to their previous values.

The minimum password length variable is changed to the new value.

Configuring minimum password difference

Minimum password difference defines the minimum required character difference between a new and old password.

Use the following procedure to set the minimum password difference global option.

1. Select **Administration > General Options**.

   The General Options page appears.
2. Locate **Minimum Password Difference** in the **Variable** column.
3. Enter the desired number in the **Value** column. A value is required.

   Enter **0** to disable password difference.
4. Click **OK** to commit the changes or **Cancel** to return all changed options to their previous values.

The minimum password difference variable is changed to the new value.

GUI sessions

The GUI Sessions administration page enables the administrative user to view a list of active user sessions and to delete those sessions as needed. In addition to session management, this section will also cover global session options related to access control. These options are presented in the General Options administration page. See General Options administration elements for more information.

GUI Sessions administration page

The GUI Sessions administration page is accessible under **Administration** > **GUI Sessions**. This page presents a list of active sessions and allows the administrative user select one or more sessions and delete them.

GUI Sessions Administration elements

This table describes elements of the GUI Sessions page.

Table 13-6 Elements on the GUI Sessions Administration Page

Element	Description
ID	Shows a system-assigned ID for the session.
Expiration	Shows the date and time (in UTC) the session will expire.

Table 13-6 (Cont.) Elements on the GUI Sessions Administration Page

Element	Description
User	Displays the **Username** of the account that belongs to the session.
IP address	Displays the IP address of the machine from which the user connected to the system.

Viewing GUI sessions

Use this procedure to view a list of GUI session.

1. Select **Administration** > **GUI Sessions**.

   The GUI Sessions administration page appears. The page lists all the active sessions on the system. The list is ordered by expiration from first to expire to last to expire.

Single sign-on session life

Use this procedure to set the single sign-on session life.

1. Select **Administration** > **General Options**.

   The General Options administration page appears.

2. Locate **Single Sign on Session Life** in the variable column.

3. Enter the desired number of minutes in the Value column.

   Default is 120 minutes. A value is required.

4. Click **OK** to submit the changes or **Cancel** to return the changed options to their previous values.

   The single sign-on session life variable is changed to the new value.

Deleting GUI sessions

Use this procedure to delete a GUI session.

Note: You cannot delete your own session.

1. Select **Administration** > **GUI Sessions**.

   The GUI Sessions administration page appears.

2. Click to select the appropriate session from the table.

   To distinguish the appropriate session, locate either the User or the IP address found in the corresponding pane.

Note: You can select multiple rows to delete at one time. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.

3. Click the **Delete Session** button.

   The session is deleted, and the user is no longer logged in to the system. The next time the user attempts to perform an action, the user is redirected to the System Login page.

Certificate Management page

Access the Certificate Manage page by clicking **Administration** > **Access Control** > **Certificate Management**.

The Certificate Management page allows the configuration of certificates for:

- HTTPS/SSL to allow secure login without encountering messages about untrusted sites.
- LDAP (TLS) to allow the LDAP server's public key to encrypt credentials sent to the LDAP server.
- Single Sign-On (SSO) to allow users to navigate among several applications without having to re-enter login credentials.

The Certificate Management page also lists the website certificates installed on the current system. The certificate in use is displayed in green text.

Before setting up Certificate Management on your system:

1. Assign a system domain name for the DNS Configuration. See DNS Configuration page.
2. Configure the LDAP authentication servers used if configuring Single Sign-On. See LDAP Authentication.

Certificate Management elements

The Certificate Management page contains these elements:

Table 13-7 Elements on the Certificate Management Page

Element	Description
A (possibly empty) list of website certificates currently installed on the PMAC system.	This information includes: • Certificate Name • Certificate Type • Certificate Subject • Certificate Issuer • Valid Dates

Table 13-7 (Cont.) Elements on the Certificate Management Page

Element	Description
Establish SSO Zone / **Reestablish SSO Zone** button	**Establish SSO Zone** and **Reestablish SSO Zone** are the same button. Once a Zone has been established and an SSO certificate created, the Certificate Management page will include the SSO certificate and the **Establish SSO Zone** button will be renamed to **Reestablish SSO Zone**. **Establish SSO Zone** opens the Establish SSO Zone page. The **Reestablish SSO Zone** button reestablishes (recreates) a selected certificate. Click **OK** when a message indicates that reestablishing the local zone will invalidate configured SSO key-exchanges for this machine.
Create CSR button	Opens the Certificate Management [Create CSR] page.
Import/**Update** button	**Import** and **Update** are the same button. Its function toggles from import to update if an existing certificate is selected in the list. The **Import** button opens the Import Certificate page. The **Update** button opens the Update Certificate page.
Delete button	**Delete** is enabled if an existing certificate is selected on the Certificate Management page. Select **Delete** to delete the selected certificate. PMAC will revert to using its default (self-signed) website certificate.
Report button	Opens the Certificate Management [Report] page.

Certificate Management [Establish SSO Zone] page

This page is available under **Administration** > **Access Control** > **Certificate Management** > **Certificate Management [Establish SSO Zone]**.

The Certificate Management [Establish SSO Zone] page allows the configuration of the single sign-on authentication zones.

Table 13-8 Single Sign-On Zone Elements

Element	Description
Zone Name	Name of the SSO-compatible remote zone Range: A to Z, a to z, 0-9 and periods - maximum 15 characters
OK button	Submits the Establish SSO Zone form and returns the user to the main Certificate Management page.
Apply button	Same as **OK** button but does not return to the main Certificates Management page after creating the certificate.
Cancel button	Cancels the creation of the certificate and returns to the main Certificates Management page

Certificate Management [Create] page

The Certificate Management [Create] page is accessible under **Administration** > **Access Control** > **Certificate Management**.

This page provides entry fields for the information in a Certificate Signing Request (CSR) pertaining to the server and the organization the certificate will identify.

Certificate Management [Create CSR] elements

The Certificate Management [Create CSR] page contains these elements:

Element	Description
Country	The two-letter ISO code for the country where your organization is located (for example, US).
State or Province	The full name of the state or province where the entity being described resides.
Locality	The locality name (for example, city) where the entity being described resides.
Common Name	This list contains up to two entries having different host name components: • PMAC host name • A wildcard (*) The hostname-specific value results in a website certificate for use by this PMAC server only. Use the wildcard option to create a certificate applicable to all servers in the same domain as PMAC. Both of these options are based on the value of the **Domain Name** field on the **Administration** > **GUI Site Settings** page. When in doubt, choose the host-specific option. This list includes only those entities that do not already have an associated certificate. An empty list indicates that both a host-specific certificate and a wildcard certificate already exist. To replace either certificate, you must first delete the existing one.
Organization	The name of the organization to which the entity belongs.
Organizational Unit	The organizational unit name to which the entity belongs.
Email Address	The email address of the entity being described.

Element	Description
Generate CSR button	Select to generate the new Certificate Signing Request (CSR) containing the entered information. The CSR is written to a new file accessible using **Status and Manage** > **Files**. This button also creates and installs an associated self-signed certificate and private key and puts them into use by PMAC. This certificate change requires you to re-establish the session with PMAC and accept the new self-signed certificate. To avoid these prompts, retrieve the CSR from PMAC and submit it to your Certificate Authority (CA). The CA returns a CA-signed certificate. Return to the Certificate Management page, select the self-signed certificate, and use the **Update** button to replace it with the CA-signed certificate.
Back button	Select to return to the Certificate Management page without generating a new Certificate Signing Request. No change is made to any existing certificates or keys.

Certificate Management [Import] page

The Certificate Management [Import] page is accessible under **Administration** > **Access Control** > **Certificate Management.**.

This page provides entry fields for a certificate, an associated private key, and a passphrase for decrypting the private key. If the private key is encrypted, a passphrase must also be supplied in the Passphrase field for decrypting it. PMAC uses this key once to decrypt the key. PAMC re-encrypts the key using its own passphrase. Your private key is not retained. If the private key is not encrypted, the Passphrase field should be left blank.

Note: You can use copy and paste for all three fields.

Certificate Management (Import Certificate) elements

The Certificate Management [Import Certificate] page contains these elements:

Table 13-9 Elements on the Certificate Management (Import Certificate) Page

Element	Description
X.509 Certificate	Entry field for a PEM encoded X.509 certificate.
Private Key	Entry field for a PEM encoded Private Key.

Table 13-9 (Cont.) Elements on the Certificate Management (Import Certificate) Page

Element	Description
Passphrase	Entry field for the passphrase with which the Private Key has been encrypted. Leave this blank if the key is not encrypted.

Certificate Management (Update Certificate) elements

The Update Certificate page contains these elements:

Table 13-10 Elements on the Update Certificate Page

Element	Description
X.509 Certificate field	Display field for a PEM encoded X.509 certificate.

Certificate Management [Report] page

The Certificate Management [Report] page is accessible under **Administration** > **Access Control** > **Certificate Management**.

This page displays the content of any certificates present on the PMAC system other than PMAC's default certificate.

Certificate Management [Report] elements

The Certificate Management [Report] page contains these elements:

Table 13-11 Elements on the Certificate Management [Report] Page

Element	Description
Print	Invokes the browser's printing capability to print the report. Specific printer behavior is browser-dependent.
Save	Invokes the browser's file saving capability to save the report in a local file on the PC. The exact behavior is browser-dependent.
Back	Returns to the Certificate Management page.

14

Credentials

This section describes the PMAC capacity to the change/update any type of credentials supported by PMAC.

Note: Currently, only **SNMP** is supported.

SNMP Community String Update page

The SNMP Community String Update page is accessible under **Administration** > **Credentials** > **SNMP**.

Use this page to update the SNMP **Read Only** and **Read/Write** Community Strings on all supporting servers that host the TVOE application and the PMAC guest supporting TPD. The TVOE applications and PMAC guest that support the update functionality should be at TPD release of 6.5.0_82.4.0 or later. Servers that do not meet this requirement are bypassed when the update occurs, and are not treated as failures.

SNMP Community String Update elements

The SNMP Community String Update page contains these elements:

Table 14-1 Elements on the SNMP Community String Update Page

Element	Description
Tasks	A pulldown list that displays selectable tasks and their related information. This information includes: • ID number • Task name • Target • Status • State • Running Time • Start time (includes date) • Progress Select a Task notepad icon to view Detail Step information for the selected task.
Read Only or Read/ Write	Provides the ability to select either the **Read Only** or **Read/Write** SNMP Community String to be updated to each supporting TVOE server and PMAC guest on the PMAC control network.

Table 14-1 (Cont.) Elements on the SNMP Community String Update Page

Element	Description
Use Site Specific <**Read Only** or **Read/Write**> Community String: <community_string>	Indicates that you want to update all known TVOE servers and PMAC guest on the PMAC control network that support the update functionality with the existing SNMP **Read Only** or **Read/Write** Community String maintained in the PMAC database. Selecting this checkbox clears and disables the **Community String** textbox and enables the **Update Servers** button. **Note:** This checkbox is provided as a means to update servers that have been added (or IPM'd) after the SNMP Community String has already been updated on this PMAC. Default - Unchecked
Community String	Allows you to enter a user-specific Community String to be updated on each supporting TVOE server and PMAC guest on the PMAC control network. Format: • Must be 1-31 characters in length. • If the string includes the whole words public, private, or password in any upper/lower case combination, a warning is issued and you can choose to allow this string. • Characters must be a-z, A-Z, or 0-9.
Update Servers	Initiates the background task to set the **Read Only** or **Read/Write** SNMP Community String on all TVOE servers and PMAC guest on the PMACs control network that support the update functionality. This button is not enabled until one or more characters are entered into the **Community String** textbox or the **Use Site Specific** checkbox has been checked.

15

Remote Servers

This section describes LDAP authentication and the PMAC ability to enable/disable the PMAC DNS Configuration.

DNS Configuration page

The DNS Configuration page is accessible under **Administration** > **Remote Servers** > **DNS Configuration**.

Use this page to configure and enable/disable the PMAC DNS Configuration.

DNS Configuration elements

The DNS Configuration page contains the following elements:

Table 15-1 DNS Configuration Page elements

Element	Description
Domain Name	A text box where you can enter a valid Domain Name. The Domain Name is used with the PMAC hostname to produce the Common Name field in website Certificate Signing Requests created with the **Administration** > **Access Control** > **Certificate Management [Create CSR]** button. Format: • Can be 1 to 255 characters in length. All alpha-numeric characters including period (.) and underscore (_) are allowed. **Note:** This field can be set as blank.
Name Server 1 Address	A text box where you can enter a valid IPV4 or IPV6 address that indicates the IP of the first Name Server in the DNS Configuration. **Note:** This field can be set as blank.

Table 15-1 (Cont.) DNS Configuration Page elements

Element	Description
Name Server 2Address	A text box where you can enter a valid IPV4 or IPV6 address that indicates the IP of the second Name Server in the DNS Configuration. **Note:** This field can be set as blank.
Name Server 3Address	A text box where you can enter a valid IPV4 or IPV6 address that indicates the IP of the third Name Server in the DNS Configuration. **Note:** This field can be set as blank.

Table 15-1 (Cont.) DNS Configuration Page elements

Element	Description
Update DNS Configuration	Updates the DNS Configuration settings according to the following rules: • If all fields are blank, the DNS Configuration file /etc/resolv.conf is set to the TPD default. This includes basic comments only instructing the user on how to configure this file. DNS Configuration is disabled for the PMAC. • If a valid Domain Name is entered and the Name Servers are all blank, the Domain Name is saved in the PMAC database for use by other PMAC configuration applications. The /etc/resolv.conf file is set to the TPD default. DNS Configuration is disabled for the PMAC. • If there is one or more valid Name Server addresses entered (in any order) and the Domain Name is blank, validation fails. The Domain Name must always be included if any Name Servers are included. • If a valid Domain Name is included and one or more valid Name Servers are included, this information is written to the /etc/resolv.conf file and DNS Configuration is enabled. **Note:** When clicking the **Update DNS Configuration** button, a message appears that this action may interrupt any existing GUI sessions because the PM&C Web Server has to be restarted. Click **OK** to continue. Then click the **DNS Configuration** menu selection again to refresh the page with your updates. If you click **Cancel,** the configuration will not be updated.

LDAP Authentication

TheLDAP Authentication page is accessible under **Administration** > **Remote Servers** > **LDAP Authentication** .

The LDAP server is a remote server used to authenticate user credentials within a domain. LDAP authentication is an additional method to authenticate users when using single sign-on (SSO) access.

Single sign-on (SSO) can be configured to work either with or without an LDAP authentication server shared between SSO zones. SSO is configured per user, excluding the default user.

There is no limit on the maximum number of LDAP servers that can be configured, but for PMAC, only the first four servers are searched for authentication.

If the system is not using a DNS server or IP address for the LDAP server, the LDAP server must be added to the `/etc/hosts` file.

Use this page to manage the LDAP servers. You can add, edit, or delete a server, display server information in a printable format, move servers up and down in the list to change the search order, and test the server by authenticating a user with a valid username and password.

LDAP Authentication page elements

Element	Description
LDAP Authentication Server table	Displays all available LDAP servers.
Insert button	Opens the LDAP Authentication [Insert] page to configure up to 4 LDAP servers for user authentication.
Edit button	Opens the LDAP Authentication [Edit] page to allow changes to the provided fields or checkboxes.
Delete button	Deletes the selected LDAP server.
Report button	Displays the printable information of the selected LDAP server.
Move Up button	Moves a selected LDAP server up in the list to change the search order.
Move Down button	Moves a selected LDAP server down in the list to change the search order.
Test Server button	Opens the LDAP Authentication [Test] page to test the selected LDAP server by entering a valid user name and password. If authentication passes, the results are returned in the Status box. If authentication fails or the PMAC is unable to communicate with the LDAP server, the results are returned in the Error box

LDAP Authentication [Insert] page elements

Both, the **Insert** and the **Edit** buttons open this page.

The asterisk (*) preceding an element indicate that this information is mandatory.

Element	Description	Data Input Notes
*Hostname field	Unique case-insensitive name for the server.	Format: Valid IPv4 or IPv6 address or a valid hostname. Format: Case-insensitive. Range: 1-100-characters, alphanumeric [a-z, A-Z, 0-9], period (.), minus sign (-). The first character must be alpha.
Account Domain Name field	Domain name of the LDAP server.	Format: <name>.<tld> (for example, Oracle.com). Range: 1-20 characters, alphanumeric [a-z, A-Z, 0-9], period (.)
Account Domain Name Short field	The short version of the domain name listed above (ex. ORACLE).	Must be a capitalized version of the domain name without the extension. Range: 1-10 characters, alphanumeric [a-z, A-Z, 0-9]
*Port field	Port by which the LDAP servers can be accessed on the host machine.	Range: Integer with value between 0 and 65535 Default: 389
*Base DN field	Directory path of the user being authenticated.	Range = 1-100 characters alphanumeric [a-z, A-Z, 0-9]
Username field	Valid username used for account Domain Name lookups (not the user being authenticated).	
Password field	The password of the user DN used for account lookups.	Range: Restrictions depend on the LDAP server's settings.
Account Filter Format field	User account search filter.	Range: 1-100 characters, alphanumeric [a-z, A-Z, 0-9] Default: (&(objectClass=user)(sAMAccountName=%s))

Element	Description	Data Input Notes
*Account Canonical Form set of radio buttons	Canonical form for the provided username.	Format: Radio buttons Valid choices: • Traditional (for example, guest) • Backslash (for exaample, ORACLE\guest) • E-Mail (for example, guest@Oracle.com) Default: Backslash style
Referrals checkbox	Whether or not to follow referrals.	Default: unchecked (ignore)
Bind Requires DN checkbox	Whether the LDAP authentication bind requires a username in DN form	Default: unchecked (disabled)
OK button	Completes the action to create the LDAP server and returns user to the LDAP Authentication page.	
Apply button	Completes the action to create the LDAP server but remains on the page to allow for the configuration of another LDAP server.	
Cancel button	Cancels the current LDAP configuration and returns the user to the LDAP Authentication page.	

LDAP Authentication [Report] page elements

Element	Description
Print button	Opens the Print window to select a printer to print the LDAP server configuration information.
Save button	Saves the LDAP server configuration information to a text file.
Back button	Returns user to the LDAP Authentication page.

16

Files Management page

This section describes the PMAC status and management interfaces.

Note: Currently, only Files is supported.

Files Management page

The Files Management page is accessible on the GUI main menu using **Status and Manage** > **Files**.

Use this page to access files located locally on the PM&C server.

Files Management elements

The Files Management page contains the elements listed below.

Note: The Files Management page is updated every 30 seconds. If files are added to the PMAC File Management system, these files will eventually be displayed in the File Management page if the page remains displayed.

Table 16-1 Elements on the Files Management Page

Element	Description
Files list	A table that displays relevant information about files located locally on the PMAC server.

Table 16-1 (Cont.) Elements on the Files Management Page

Element	Description
Buttons	The following links are provided: **Delete** Provides a way to delete a selected files. You will be prompted prior to the file deletion. After you acknowledge the deletion, the files are deleted from the PMAC file management area. Becomes active only when one or more files are selected. **View** Provides a way to view a selected file. Becomes active only when one file is selected. **Note:** After a file is viewed, there is a single **Back** button which returns to the Files Management page with no files selected. **Download** Provides a way to download the selected file to the client side (PC) via the browser. The actual actions of the download are browser specific. Becomes active only when one file is selected.

Index

B

background task
  about delete operation, *6-9*
browser
  configuration, *4-5*

F

FRU
  report, *5-22*
FRU Information page, *5-22*

I

inventory
  enclosure information, *5-8*

P

password
  configure expiration, *13-21*
password *(continued)*
  parameters, *13-18*
  set, *13-19*
popups
  allow, *4-5*

R

report
  FRU, *5-22*
  RMS FRU, *5-22*
RMS FRU
  report, *5-22*
RMS FRU Information page, *5-22*

U

user account
  about administering, *13-3*
  disable, *13-7*
  enable, *13-7*