Oracle® Communications

DSR 5.0 Base Hardware and Software Installation Procedure

909-2282-001 Revision A

November 2013

ORACLE®

Oracle® Communications DSR 5.0 Base Hardware and Software Installation Procedure

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This document provides the methods and procedures used to configure the DSR 5.0 Management Server TVOE and PMAC, initialize the system's aggregation switches and enclosure switches, and perform the initial configuration of the DSR system's RMS and HP c-Class enclosure.

Following the execution of the subject document the DSR user will follow a DSR application procedure document (*909-2278-001*) to complete the DSR application specific configurations.

The procedures in this document should be executed **in order**. Skipping steps or procedures is not allowed unless explicitly stated.

Note: Before executing any procedures in this document, power must be available to each component, and all networking cabling is in place.[1]

The audience for this document includes Tekelec customers as well as the following groups:

- Software System
- Product Verification
- Documentation
- Customer Service including Software Operations and First Office Applications

[1] Network uplinks to the customer networking will be connected after the networking within the DSR equipment is established and verified.

1.1 References

External References

1. *909-2130-001 Initial Product Manufacture*
2. *909-2207-001 PM&C 5.0 Incremental Upgrade*
3. *909-2210-001 PM&C 5.x Disaster Recovery for HP c-Class*
4. *909-2249-001 Platform 6.5 Configuration Procedure*
5. *HP Solutions Firmware Upgrade Pack, 795-0000-2xx, v2.2.x (latest recommended, 2.2.4 minimum)*
6. *TR006683: NOAMP on HP DL380 Network Interconnect*
7. *TR006851: Platform 5.0 Generic HP c-Class Networking Interconnect*
8. *TR007133: DSR 5.x Network Interconnect: Topology 1 - L3-Agg*
9. *TR007134: DSR 5.x Network Interconnect: Topology 2 - L2-Agg*
10. *TR007135: DSR 5.x Network Interconnect: Topology 3 - L2-NoAgg-1Pair*
11. *TR007136: DSR 5.x Network Interconnect: Topology 4 - L2-NoAgg-2Pair*
12. *TR007137: DSR 5.x Network Interconnect: Topology 5 - L2-NoAgg-3Pairs-2SigNets*
13. *TR007138: DSR 5.x Network Interconnect: Topology 6 - L2-NoAgg-3Pairs-SegOAM&Sig*
14. *TR007139: DSR 5.x Network Interconnect: Topology 7 - NOs on RMS*
15. *WI006083: DSR Hardware Site Survey*

Refer to *A.1 Accessing Tekelec's Customer Support Site* to access the Tekelec documentation.

Internal References

Formal Peer Review Process, PD001866, v6.21, Nov 2008

1.2 Acronyms

An alphabetized list of acronyms used in the document:

Table 1: Acronyms

Acronym	Definition
BIOS	Basic Input Output System
BOM	Bill of Material
CA	Certificate Authority
CD	Compact Disk
CSR	Certificate Signing Request
DNS	Domain Name System
DSCP	Differentiated Services Code Point, a form of QoS

Acronym	Definition
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FMA	File Management Area
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering
iLO	Integrated Lights Out remote management port
IPFE	IP Front End
IE	Internet Explorer
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MP	Message Processor
MSA	Modular Smart Array
NAPD	Network Architecture Planning Diagram
NO	NOAM&P (Network Operations, Administration, Maintenance, and Provisioning)
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
PM&C	Platform Management & Configuration
RMS	Rack Mount Server
QOS	Quality of Service
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SO	SOAM (Site Operations, Administration, and Maintenance)
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VSP	Virtual Serial Port

1.3 Terminology

Multiple server types may be involved with the procedures in this manual. Therefore, most steps in the written procedures begin with the name or type of server to which the step applies. For example:

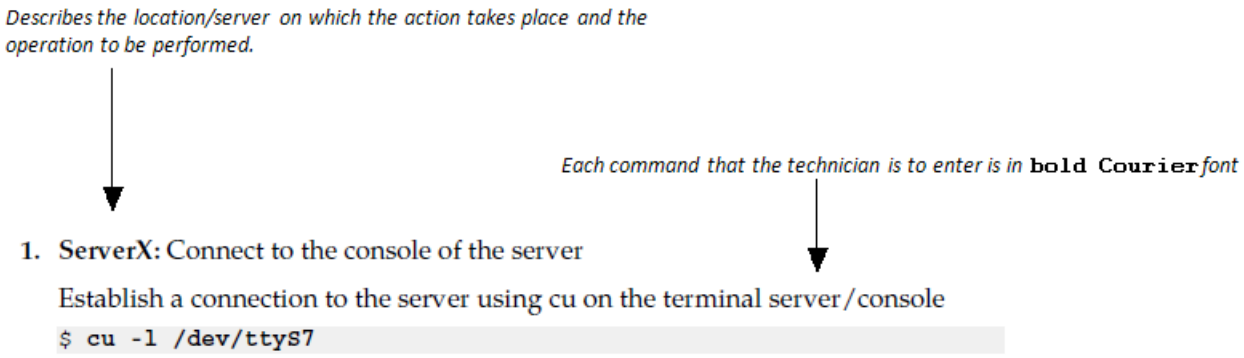


Figure 1: Example Of An Instruction That Indicates The Server To Which It Applies

Table 2: Terminology

Community String	An SNMP community string is a text string used to authenticate messages sent between a management station and a device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Domain Name System	A system for converting hostnames and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol
Management Server	An HP ProLiant DL 360/DL 380 server that has physical connectivity required to configure switches and may host the PM&C application or serve other configuration purposes.
NetBackup Feature	Feature that provides support of the Symantec NetBackup client utility on an application server.
Non-Segregated Network	Network interconnect where the control and management, or customer, networks utilize the same physical network.
PM&C	An application that supports platform-level management of Tekelec HP systems, such as the capability to manage and provision platform components of the system, so they can host applications.
Segregated Network	Network interconnect where the control and management, or customer, networks utilize separate physical networks.
Server	A generic term to refer to a server, regardless of underlying hardware, be it physical hardware or a virtual TVOE guest server.

Virtual PM&C	Additional term for PM&C - used in networking procedures to distinguish activities done on a PM&C guest and not the TVOE host running on the Management server.

1.4 Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)

  - **Brazil**

    Phone:

0-800-891-4341 (toll-free)

TAC Regional Support Office Hours:

8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

- **Chile**

  Phone:

  1230-020-555-5468

- **Colombia**

  Phone:

  01-800-912-0537

- **Dominican Republic**

  Phone:

  1-888-367-8552

- **Mexico**

  Phone:

  001-888-367-8552

- **Peru**

  Phone:

  0800-53-087

- **Puerto Rico**

  Phone:

  1-888-367-8552 (1-888-FOR-TKLC)

- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**
  - **India**

    Phone:

    +91-124-465-5098 or +1-919-460-2150

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays
  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Chapter 2

Acquiring Firmware

Topics:

2.1 Acquiring Firmware

Several procedures in this document pertain to the upgrading of firmware on various servers and hardware devices that are part of the Platform 6.5 configuration. The required firmware media and binaries are managed and distributed as part of the HP *Solutions Firmware Upgrade Pack 2.2.x*, released under Tekelec Part Number 795-0000-3*yy*[1] (2 USB media and 2 Documents) and 795-0000-4yy[1] (2 ISO files and 2 PDF files). The minimum firmware release required for Platform 6.5 is HP *Solutions Firmware Upgrade Pack 2.2.5* (PN: 795-0000-316 and 795-0000-416). However, if a firmware upgrade is needed, the current GA release of the HP Solutions Firmware Upgrade Pack must be used.

The HP *Solutions Firmware Upgrade Pack* contains multiple BOM items including media and documentation. This document only requires access to the media (USB media or ISO files) as well as the Release Notes [3] document. The *Upgrade Procedures* document is not used as the firmware upgrade procedures specific to this document are provided here.

The two pieces of required firmware media provided in the HP *Solutions Firmware Upgrade Kit 2.2.x* releases are:

- Tekelec's HP Service Pack for ProLiant (SPP) USB media or ISO file
- Tekelec's HP Misc. Firmware USB media or ISO file

Refer to the Release Notes of the target release of the HP Solutions Firmware Upgrade Pack [3] used to determine specific media part numbers to use and the specific firmware versions provided.

Platform 6.5 Servers and devices requiring possible firmware updates are:

- HP c7000 BladeSystem Enclosure Components:
- HP Rack Mount Servers (DL360 / DL380)
- HP External Storage Systems
  - MSA2012fc
  - D2200sb (Storage Blade)
  - D2220sb (Storage Blade)
  - D2700
  - P2000
- Cisco 4948/4948E/4948E-F Rack Mount Network Switches

[2] Where *yy* is a 2-digit number which increases with every new release.

Chapter 3

Install Overview

Topics:

This section contains the installation overview, and includes information about required materials, strategies, and SNMP configuration.

This section will configure the DSR base hardware systems (RMS and HP c-Class enclosure) (RMS and Blade IPM, Networking, Enclosure and PMAC Configuration). Following the execution of this document the DSR user will follow a DSR application procedure document (*909-2278-001*) to complete the DSR application specific configurations.

Note that IPM refers to installing either TVOE or TPD on the target system. TVOE is used when virtualization is needed (e.g., for the PMAC and NO/SO). TPD is used to the systems that do not require virtualization and for the Virtual Machines).

3.1 Required Materials

1. One (1) USB or ISO of TPD release (*872-2673-001*-6.5.0-82.17.0), or later shipping baseline as per Tekelec ECO. If a .usb file is provided, it should be used in the creation of a bootable USB media. For instructions on how to create a bootable USB, refer to Appendix K .
2. One (1) USB or ISO of PM&C release (*872-2586-101*-5.5.0-55.11.0), or later shipping baseline as per Tekelec ECO.
3. One (1) CD-ROM, USB, or ISO of TVOE release (*872-2525-101*-6.5.0_82.17.0), or later shipping baseline as per Tekelec ECO.
4. Passwords for users on the local system.
5. Access to the iLO Terminal or direct access to the server VGA port.
6. *HP Solutions Firmware Upgrade Pack, 795-0000-3xx (USB media) or 795-0000-4xx (ISO files), version 2.2.x (the latest must be used if an upgrade is to be performed, otherwise version 2.2.5 is the minimum)* A 1Gb or larger USB Flash Drive.
7. NAPD and all relevant configuration materials for ALL sites involved. This includes host IP addresses, site network element XML files, and netConfig configuration files.
8. DSR Media (*872-2526-101*-5.0.0)

The material for the list above can also be downloaded from Tekelec's secure website, located at *https://secure.tekelec.com/*

3.2 Installation Strategy

To ensure a successful application installation, carefully plan and assess all configuration materials and installation variables. After a customer site survey has been conducted, an installer can use this section to plan the exact procedure list that should be executed at each site.

The following list summarizes this process.

1. An overall installation requirement is established. This data that should be collected:
   - The total number of sites
   - The number of servers at each site and their role(s)
   - Determine whether the application's networking interface terminates on a Layer 2 or Layer 3 boundary
   - Establish the number of enclosures at each site (if any)
   - Determine if the application uses rack-mount servers or server blades
   - What time zone should be used across the entire collection of application sites
   - Will SNMP traps be viewed at the application level, or will an external NMS be used (or both)
2. A site survey is conducted to determine exact networking and site details. Additionally, IP networking options must be well understood, and IP address allocations collected from the customer, in order to complete switch configurations

3.3 SNMP Configuration

The network-wide plan for SNMP configuration should be decided upon before DSR installation proceeds. This section provides some recommendations for these decisions.

SNMP traps can originate from the following entities in a DSR installation:

- DSR Application Servers (NOAMP, SOAM, MPs of all types)
- DSR Auxiliary Components (OA, Switches, TVOE hosts, PMAC)

DSR application servers can be configured to:

1. Send all their SNMP traps to the NOAMP via merging from their local SOAM. All traps will terminate at the NOAMP and be viewable from the NOAMP GUI (entire network) and the SOAM GUI (site specific). This is the default configuration option.
2. Send all their SNMP traps to an external Network Management Station (NMS). The traps will NOT be seen at the SOAM OR at the NOAM. They will be viewable at the configured NMS(s) only.

Application server SNMP configuration is done from the NOAMP GUI, near the end of DSR installation. See the procedure list for details.

DSR Auxiliary components must have their SNMP trap destinations set explicitly. Trap destinations can be the NOAMP VIP, the SOAMP VIP, or an external (customer) NMS. The recommended configuration is as follows:

The following components:

- PMAC (TVOE)
- PMAC (App)
- OAs
- All Switch types (4948, 3020, 6120, 6125)
- TVOE for DSR Servers

Should have their SNMP trap destinations set to:

1. The local SOAM VIP
2. The customer NMS, if available

3.4 NTP Strategy

The following set of general principals capture the recommendations for NTP configuration of DSR.

Principle 1 - Virtual guests should not be used as NTP servers

Avoid specifying virtual guests as NTP references for other servers. Guest emulated clocks have been shown to result in poor NTP server behavior

Principle 2 - Virtual guests should synchronize to their virtual hosts

When virtualization is used in the product deployment, virtual guests should use their virtual hosts as their NTP references.

Principle 3 - Follow a topology based approach

MP servers should use their topology parents (SOAMs in a three tier topology), or if those parents are virtual guests, the enclosing virtual hosts should be used instead. See *Figure 2: Per Site NTP Topology* for clarification.

Similarly SOAM servers should use their topology parents (NOAMs), or if those parents are virtual guests, the enclosing virtual hosts should be used instead. See *Figure 2: Per Site NTP Topology* for clarification.

NOAMP and other A-Level servers should use a pool of reliable, customer provided references if the NOAMPs are implemented in hardware, otherwise they should sync to their virtual hosts.

Virtual hosts should always have NTP enabled and configured. Virtual hosts that contain A-Level guests, PMACs or other virtual product servers should synchronize to a reliable pool of customer references. Virtual hosts that contain B or C level guests should synchronize to the virtual hosts containing the parent topology guests.

Principle 4 - Provide a robust pool of sources

The pool of customer NTP server references should be of stratum 3 or above, accurate and highly reliable. If possible both local site server and backup remote site servers should be provided.

Principle 5 - Prefer local references

When references from multiple sites or networks are used on one server, the "prefer" keyword should be applied to the local references.

Principle 6 - Ensure connectivity

Care should be taken to ensure that all NTP references are reachable through the appropriate networking configuration. In particular firewall rules must be correctly specified to allow NTP clients to connect to their specified references.

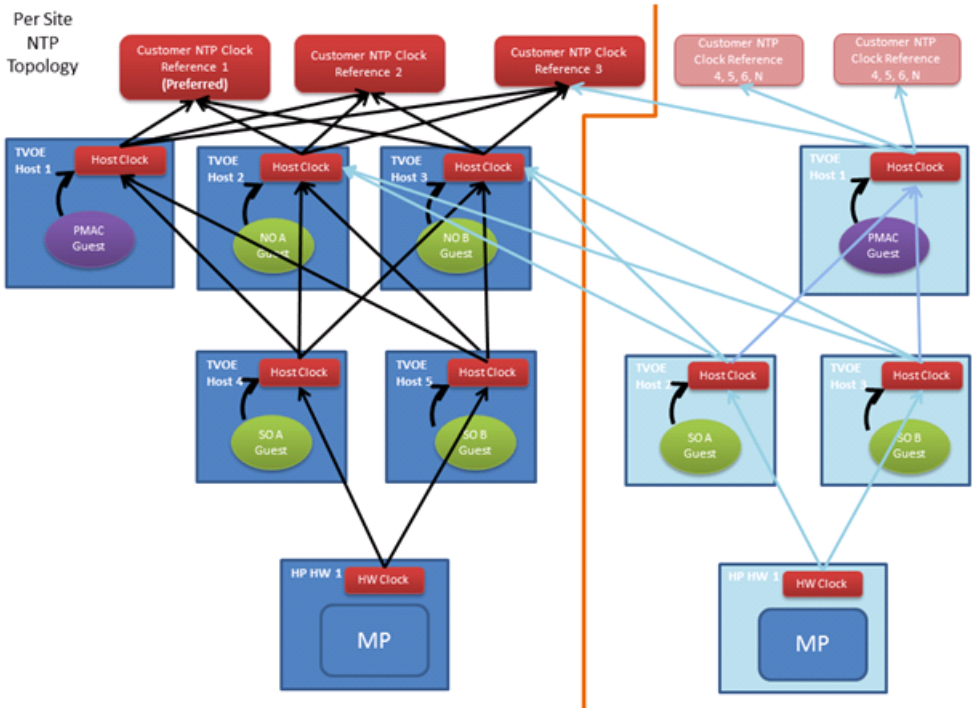


Figure 2: Per Site NTP Topology

3.5 Overview of DSR Networks

This table presents an overview of the networks configured and used by DSR at a site. Based on the deployment type/requirements, the networks could be physically or logically separated via VLANs.

Network Name	Default VLAN ID*	Routable	Description
Control	1	No	Network used by PMAC to IPM the servers/blades/VMs. Refer to the Hardware Site Survey for site specific information. (IPs are assigned via by the PMAC using DHCP)
Management	2	Yes	Network used for iLO interfaces, OAs, and enclosure switches. Also used to provide remote access to the TVOE and PMAC servers
XMI	3	Yes	Network used to provide access to the

Network Name	Default VLAN ID*	Routable	Description
			DSR entities (GUI, ssh), and for inter-site communication
IMI	4	No	Network used for intra-site communication
XSI-1	5	Yes	Network used for DSR signaling Traffic
XSI-2**	6	Yes	Network used for DSR signaling Traffic
XSI-3**	7	Yes	Network used for DSR signaling Traffic
XSI-4**	8	Yes	Network used for DSR signaling Traffic

* The VLAN ID assignments are site and deployment specific.

** Optional

Chapter 4

Software Installation Procedures

Topics:

This section contains the software installation procedures, including preparation and configuration information for a site.

The procedures in this section are expected to be executed in the order presented in this section.

If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* of this document.

Sudo

Platform 6.5 introduced a new non-root user 'admusr'. As a non-root user, many commands --when run as admusr-- now require the use of 'sudo'. Using sudo will require a password on the first command, as well as intermittently over a period of time. Therefore, if a prompt for the "`[sudo] password:`" appears, the user should re-enter the admusr login password.

Example:

```
[admusr@hostname ~]$ sudo <command>
[sudo] password for admusr: <ENTER
 PASSWORD HERE>
<command output omitted>
[admusr@hostname ~]$
```

4.1 Configure and IPM Management Server

Note: The Management Server is installed as a Virtual Host environment, and will host the PMAC application, and may host other DSR applications (as defined by the deployment configuration for the customer site).

Note: Depending on the deployment plan, a server may be IPM'ed with either TVOE (if virtualization is needed) or TPD (if no virtualization is needed)

4.1.1 Installing TVOE on the Management Server

Install the TVOE Hypervisor platform on the Management Server

The PM&C is not available to do an IPM of the TVOE management server. It is necessary to physically provide the TVOE media via a USB or optical.

Install TVOE onto the Management Server

Follow *4.1.1.1 IPM DL360 or DL380 Server* to IPM the management server with TVOE.

4.1.1.1 IPM DL360 or DL380 Server

This procedure provides instructions for configuring and IPMing the DL360 or DL380 server.

Needed material:

- TPD or TVOE installation media to be used for IPM.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

Configure and IPM the DL360 or DL380 server

Initial Product Manufacture: Follow Initial Product Manufacture Appendix D to configure and IPM the management server.

For a DL360 G6/G7 or DL380 G6/Gen8 server, the correct options to use for the IPM of the management server are:

```
TPDnoraid console=tty0 diskconfig=HPHW,force
```

4.1.2 Upgrade DL360 or DL380 Server Firmware

This procedure will upgrade the DL360 or DL380 server firmware. All servers should have SNMP disabled. Refer to Appendix J *Changing SNMP Configuration Settings for iLO*

The service Pack for ProLiant (SPP) installer automatically detects the firmware components available on the target server and will only upgrade those components with firmware older than what is on the current ISO.

Procedure Reference Tables:

Variable	Value
<ilo_IP>	Fill in the IP address of the iLO for the server being upgraded _____
<ilo_admin_user>	Fill in the username of the iLO's Administrator User _____
<ilo_admin_password>	Fill in the password for the iLO's Administrator User _____
<local_HPSPP_image_path>	Fill in the filename for the HP Support Pack for ProLiant ISO _____
<admusr_password>	Fill in the password for the admusr user for the server being upgraded _____

Needed Material:

- Tekelec's HP Service Pack for ProLiant (SPP) USB media or ISO file
- Tekelec's HP Misc Firmware USB media or ISO file (for errata updates is applicable)
- HP Solutions Firmware Upgrade Pack Release Notes [3]

Important Notes for this Procedure: The following procedure has some instructions meant for a production system in the field and you should be aware of the following notes regarding this procedure:

- Ignore references to the "Copy the ISO Images to the Workstation" procedure. Know that you must have the ISO files listed in the "Needed Material" section above.
- Ignore the <local_HPSUF_image_path> variable.
- For the "Update Firmware Errata" step check the HP Solutions Firmware Upgrade Pack Release Notes [3] to see if there are any firmware errata items that apply to the server being upgraded. If there is, there will be a directory matching the errata's ID in the /errata directory of the HP Misc Firmware ISO. The errata directories contain the errata firmware and a README file detailing the installation steps.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Local Workstation:** Insert the USB Flash Drive.
   If starting with the Tekelec USB media, insert the SPP USB media into a USB port on the server.
2. **Local Workstation:** Access the iLO Web GUI.
   Access the ProLiant Server iLO Web Login Page from an Internet Explorer ® session using the following URL:

```
https://<ilo_IP>/
```

3. **iLO Web GUI:** Login to iLO as an "administrator" user.

Username = **<ilo_admin_user>**

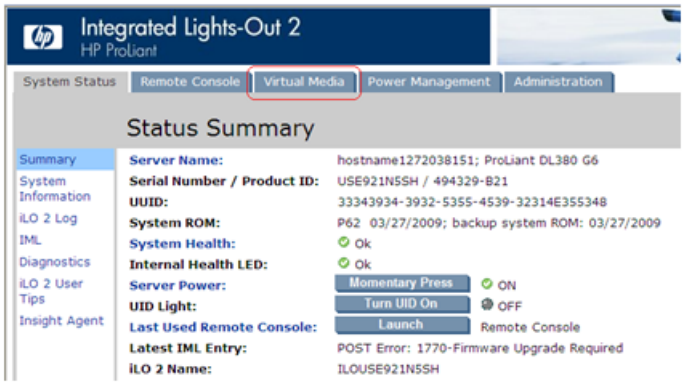
Password = **<ilo_admin_password>**

4. **Determine which iLO steps to take**
   a) If you are upgrading a G6 (iLO 2) server, continue at the next step.
   b) If you are upgrading a G7/Gen8 (iLO3/iLO4) server, continue at step 13.
5. **iLO 2 Web GUI:**

   If using SPP USB media plugged into the server, skip to step 10

   Select Virtual Media page.

   Click the **Virtual Media** tab from the System Summary page.

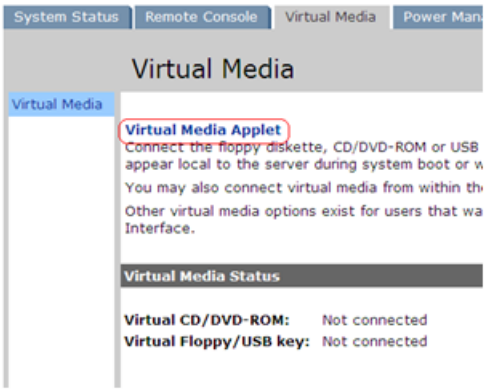


6. **iLO 2 Web GUI:**

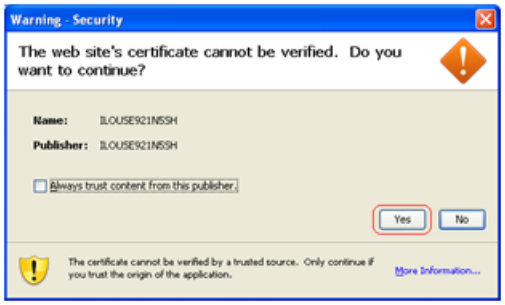
   Open the Virtual Media Applet .

   Click on the **Virtual Media Applet** link to launch the Virtual Media application

   The iLO GUI should open to the **Virtual Media** page.

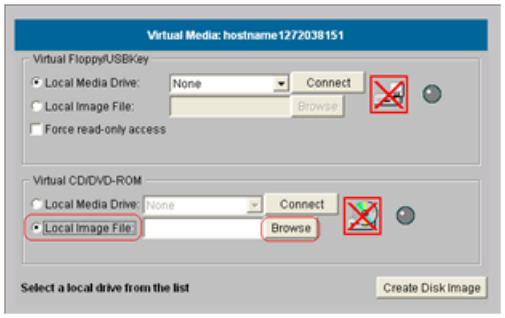


7. **iLO 2 Web GUI:** Acknowledge Security Warning.
   If a dialog similar to the one below is presented, click **Yes** to acknowledge the issue and proceed.



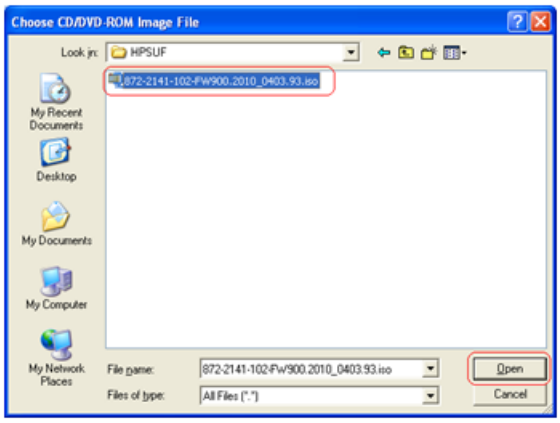
   If other warning dialogs are presented you may also acknowledge them as well to proceed to the Virtual Media applet.

8. **iLO 2 VM Applet:** Select the HP Support Pack for ProLiant ISO.
   In the Virtual CD/DVD-ROM Panel, select the **Local Image File** option and click the **Browse** button. Navigate to the *HP Smart Update Firmware* ISO file copied to the workstation in the Copy the ISO images to the workstation procedure.

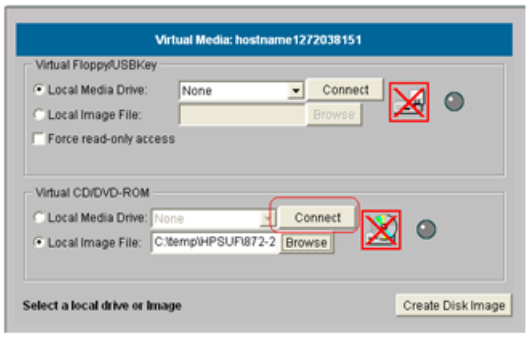


   Select ISO image file and click **Open**.

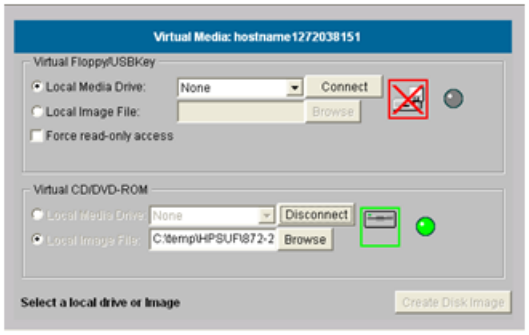
   Image File Name: <local_HPSPP_image_path> (See Copy the ISO images to the workstation)



9. **iLO 2 VM Applet:** Create Virtual Drive Connection.
   Click the **Connect** button to create a virtual DVD-ROM connection to the ISO image file.



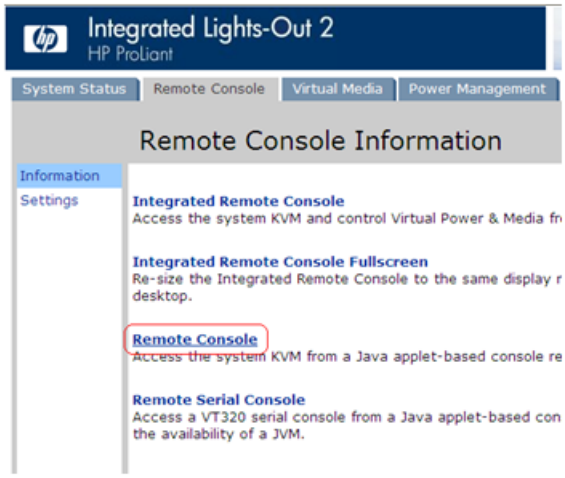
   When created the LED Light icon should be green.



   At this point, **DO NOT** close the applet but rather go back to the browser window containing the iLO Web GUI.

10. **iLO 2 Web GUI:** Access the Remote Console Page.
    At the ILO2 Web GUI, click on the **Remote Console** tab.

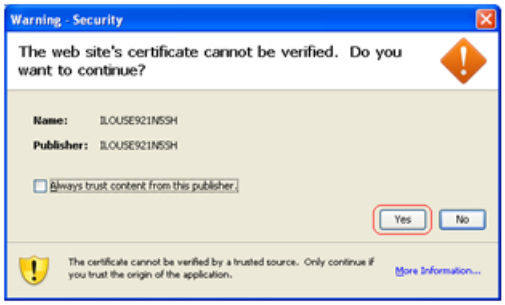
11. **iLO 2 Web GUI:** Launch the Remote Console Applet.
    On the Remote Console page, click on the **Remote Console** link to launch the console applet.



12. **iLO 2 - Java Security Prompt:** Acknowledge Security Warning

    If a dialog similar to the one below is presented, click **Yes** to acknowledge the issue and proceed.

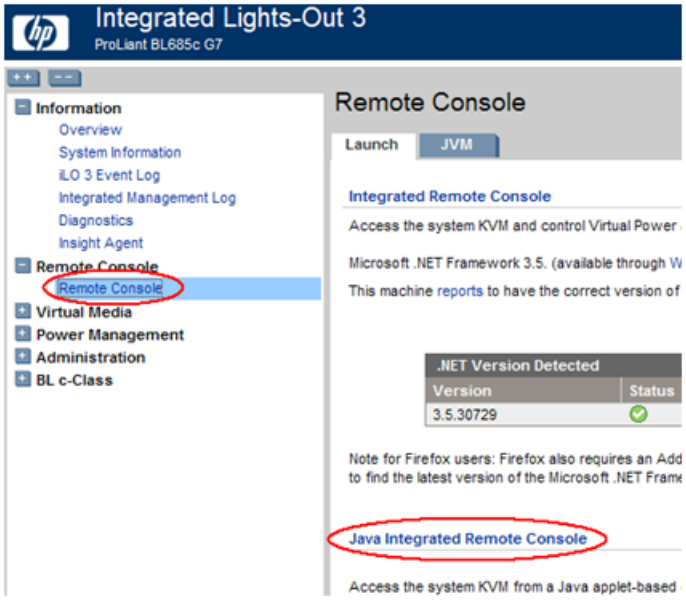
    Then skip to step 16.



    If other warning dialogs are presented you may also acknowledge them as well to proceed to the Java Integrated Remote Console applet.

13. **iLO3/iLO4 Web GUI:** Launch the Java Integrated Remote Console applet.

On the menu to the left navigate to the Remote Console page. Click on the Java Integrated Remote Console to open it.



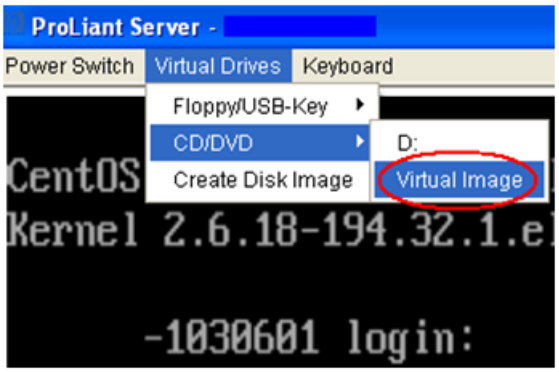
14. **iLO3/iLO4 - Java Security Prompt:** Acknowledge Security Warning.
If a dialog similar to the one below is presented, click **Yes** to acknowledge the issue and proceed.

If other warning dialogs are presented you may also acknowledge them as well to proceed to the Java Integrated Remote Console applet.

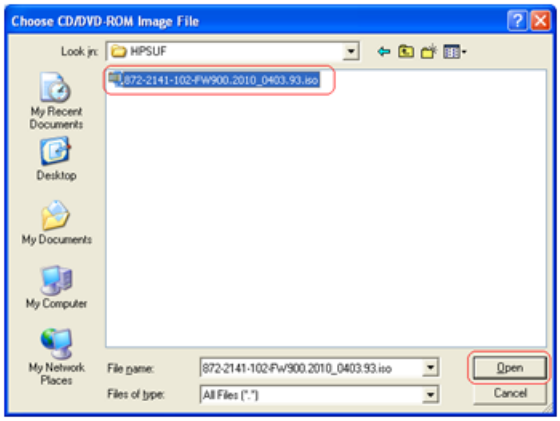
15. **iLO3/iLO4 - Remote Console:** Create Virtual Drive Connection

If using SPP USB media plugged into the server, skip to step 17

Click on the Virtual Drives drop down menu. Go to CD/DVD then click on Virtual Image.



Navigate to the *HP Support Pack for ProLiant ISO* ISO file copied to the workstation from the Copy the ISO images to the workstation procedure.



Select the ISO image file and click **Open**.

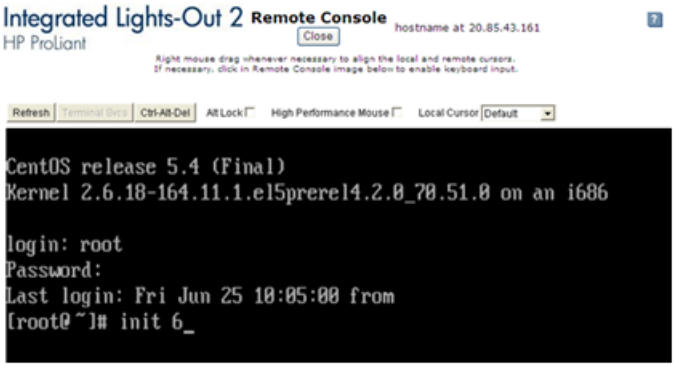
16. **iLO3/iLO4 - Remote Console:** Verify Virtual Image connection.
    At the bottom of the remote console window you should now see a green highlighted drive icon and "VirtualM" written next to it.

17. **Remote Console:** Reboot the server.
    Once the remote console application opens to the login prompt, login to the server as admusr.

```
localhost login: admusr
Password: <admusr_password>
```

Next, initiate server reboot by executing the following command:

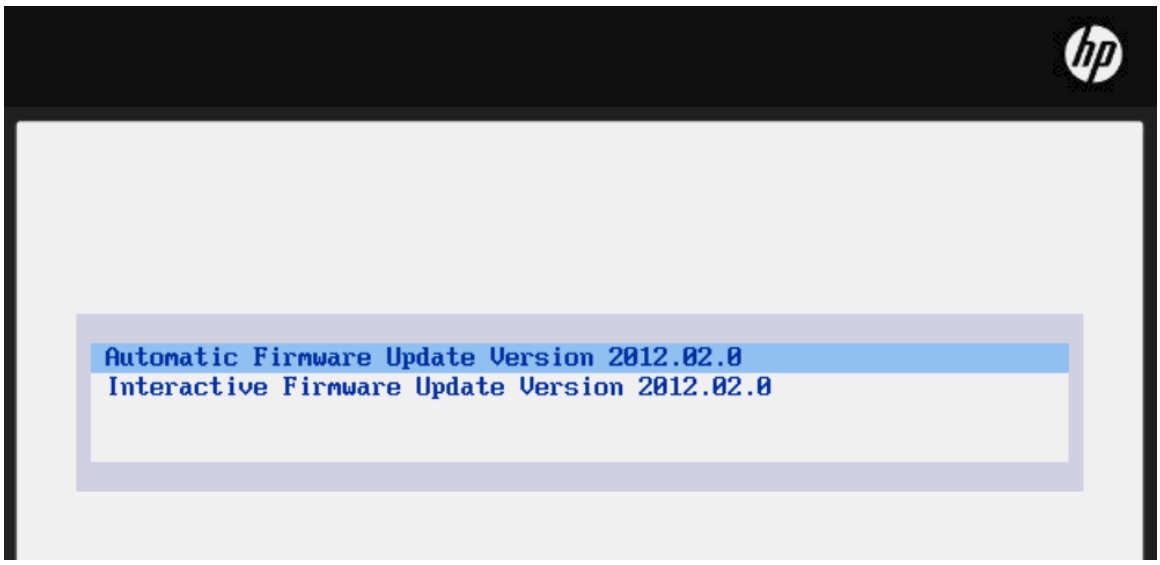
```
$ sudo init 6
```



18. **Remote Console:** Perform an unattended firmware upgrade.

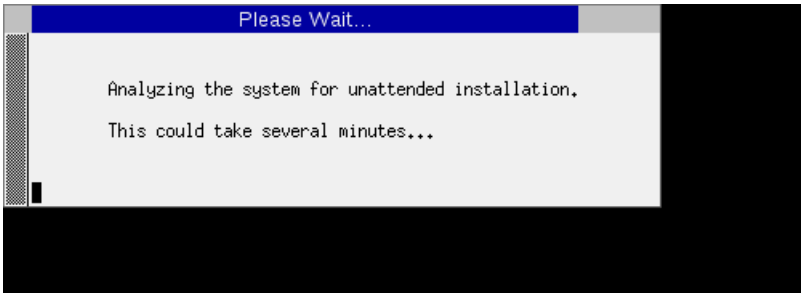
    The server will reboot into the *HP Support Pack for ProLiant ISO* ISO and present the following boot prompt.

    Press **[Enter]** to select the **Automatic Firmware Update** procedure.



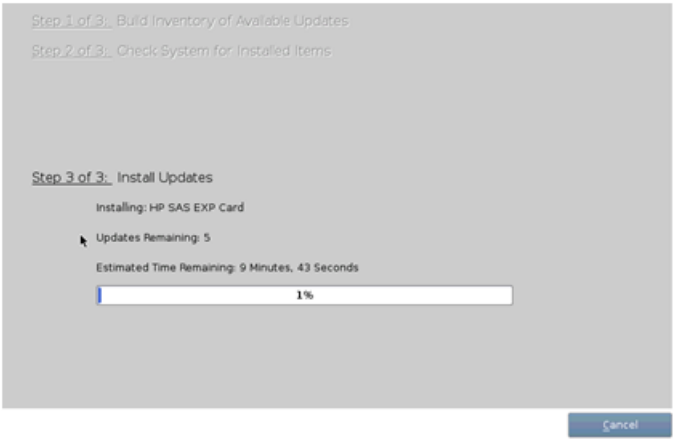
    If no key is pressed in 30 seconds the system will automatically perform an Automatic Firmware Update.

19. **Remote Console:** Analyze System.
    The firmware install will perform a system scan of the server in which it will identify all of the firmware components that are eligible for upgrade. This process may take up to 10 minutes and, during that time, the following screen is displayed on the console.



Note: No progress indication is displayed during the system scan and analysis stage. In about 10 minutes, the installation will automatically proceed to the next step.

20. **Remote Console:** Monitor Installation.
    Once analysis is complete, the installer will begin to upgrade the eligible firmware components. A progress indicator is displayed at this time, as shown below.



Note: If the iLO firmware is to be upgraded, it will be upgraded last. At this point the iLO2 session will be terminated and you will lose the remote console, virtual media and Web GUI connections to the server. This is expected and will not impact the firmware upgrade process.

21. **Local Workstation:** Clean up.
    Once the firmware updates have been completed the server will automatically be rebooted.
    - If you are upgrading a **G6 (iLO 2)** server; at this time you may close the remote console and virtual media applet windows and the iLO2 Web GUI browser session.
    - If you are upgrading a **G7/Gen8 (iLO3/iLO4)** server; closing the remote console window will disconnect the Virtual Image and you can close the iLO3/iLO4 Web GUI browser session.
    - If you are using SPP USB media plugged into the server you can now remove it.
22. **Local Workstation:** Verify server availability
    Wait 3 to 5 minutes and verify the server has rebooted and is available by gaining access to the login prompt.
23. **Update Firmware Errata:**
    Refer to the ProLiant Server Firmware Errata section to determine if this HP Solutions Firmware Update Pack contains additional firmware errata updates that should be applied to the server at this time.
24. **Remove the firmware Media:**

Remove the HP Smart Update Firmware DVD/USB media from the server drive, or USB port. Exit from the remote console.

25. **Repeat for all remaining RMSs:**
    Repeat this procedure for all remaining RMSs, if any.

4.1.3 Deploying Virtualized PM&C Overview

Deployment Procedure

Deploying a VM guest in the absence of a PM&C is a bit complicated. To facilitate this, the PM&C media will include a guest archive and a script that will deploy the running PMAC into a state where the Initialization process can begin.

- Install TVOE 2.5 on the management server via the ILO
- Create and configure the management bridge
- Determine if NetBackup Feature is enabled for this system. If enabled, install appropriate NetBackup client to the PM&C TVOE host.
- Attach PM&C media to the TVOE (CDR, USB)
- Mount the media
- Use the <mount-point>/upgrade/pmac-deploy script to create the VM and configure the guest on the first boot.
- Navigate browser to the management IP address of the deployed PM&C.
- Perform Initial Configuration.

What You Will Need -- Worksheet

Use the completed NAPD information to fill in the appropriate data in this Procedure's Reference tables. The following are provided to aid with the data collection for the TVOE management server and the PM&C Application hosted on the Management Server TVOE.

- Determine if the network configuration of this management server is Non-Segregated or Segregated.
- Determine the TVOE management server's required network interface, bond, and Ethernet device, and route data.
- Determine if the control network on the TVOE management server is to be tagged. If appropriate fill in the <control VLAN ID> value in the table, otherwise the control network is not tagged.
- Determine if the management network on the TVOE management Server is to be tagged. If appropriate fill in the <management_VLAN_ID> value in the table, otherwise the management network is not tagged.
- Determine the bridge name to be used on the TVOE management server for the management network. Fill in the <TVOE_Management_Bridge> value in the table.
- Determine if the NetBackup feature is enabled
  - Determine the NetBackup network on the TVOE management server is to be tagged. If appropriate fill in the <NetBackup_VLAN_ID> value in the table, otherwise the NetBackup network is not tagged.
  - Determine the bridge name to be used on the TVOE management server for the NetBackup network. Fill in the <TVOE_NetBackup_Bridge> value in the table.

- Determine if the NetBackup network is to be configured with jumbo frames. If appropriate fill in the <NetBackup_MTU_size> value in the table, otherwise the NetBackup network will use the default MTU size.
- If the PM&C NetBackup feature is enabled, and the backup service will be routed, with a source interface different than the management interface where the default route is applied, then define the route during PM&C initialization as a host route to the NetBackup server.

- The PM&C initialization profiles have been designed to configure the PM&C's networks and features. Profiles must identify interfaces. Existing profiles provided by PM&C use standard named interfaces (control, management). No vlan tagging is expected on the PM&C's interfaces, all tagging should be handled on the TVOE management server configuration.

Network Interface	DL360 (without HP NC364T 4pt Gigabit)	DL360 (with HP NC364T 4pt Gigabit in PCI Slot 2)	DL380	DL380 (with HP 4pt Gigabit in PCI Slot 1)	DL380 (with HP 4pt Gigabit in PCI Slot 3)
<ethernet_interface_1>	eth01	eth01	eth01	eth01	eth01
<ethernet_interface_2>	eth02	eth02	eth02	eth02	eth02
<ethernet_interface_3>		eth21	eth03	eth03	eth03
<ethernet_interface_4>		eth22	eth04	eth04	eth04
<ethernet_interface_5>		eth23		eth11	eth31

PM&C Interface Alias	TVOE Bridge Name	TVOE Bridge Interface
control	control	Fill in the appropriate value for this site (default is bond0): _____ <TVOE_Control_Bridge_Interface>
management	Fill in the appropriate value for this site: _____ <TVOE_Management_Bridge>	Fill in the appropriate value for this site: _____ <TVOE_Management_Bridge_Interface>
NetBackup	Fill in the appropriate value for this site: _____ <TVOE_NetBackup_Bridge>	Fill in the appropriate value for this site: _____ <TVOE_NetBackup_Bridge_Interface>

Fill in the appropriate value for this site:

Variable	Value	Description
<control_VLAN_ID>		For non-segregated networks, the control network may have a

Variable	Value	Description
		VLAN id assigned. In most cases, there is none.
<management_VLAN_ID>		For non-segregated networks, the management network will be on a tagged VLAN coming in on bond0
<mgmtVLAN_gateway_address>		Gateway address used for routing on the management network.
<NetBackup_server_IP>		The IP address of the remote NetBackup Server.
<NetBackup_VLAN_ID>		For non-segregated networks, the NetBackup network will be on a tagged VLAN coming in on bond0
<NetBackup_gateway_address>		Gateway address used for routing on the NetBackup network.
<NetBackup_network_ip>		The Network IP for the NetBackup network
<PMAC_NetBackup_netmask>		The IP netmask assigned to the PM&C for participation in the NetBackup network
<PMAC_NetBackup_ip_address>		The IP Address assigned to the PM&C for participation in the NetBackup network
<NetBackup_MTU_size>		If desired, the MTU size can be set to tune the NetBackup network traffic.
<management_server_mgmt_ip_address>		The TVOE Management Server's IP address on the management network.
<PMAC_mgmt_ip_address>		The PM&C Application's IP address on the management network.
<mgmt_netmask>		The IP netmask for the management network.
<PMAC_control_ip_address>		The PM&C Application's IP address on the control network.
<control_netmask>		The IP netmask for the control network.

Fill in the appropriate value for this site:

Network Bond Interface	Enslaved Interface 1	Enslaved Interface 2
bond0		
For Segregated Networks Only		
bond1		
bond2		Bonding used for abstraction only, not multiple interfaces

4.1.4 TVOE Network Configuration

1. **TVOE Management Server iLO:** Login to the management server on the remote console

   Login to iLo using application provided passwords via Appendix G *How to Access a Server Console using the iLO*

   Login to iLO in IE using password provided by application:

```
http://<management_server_iLO_ip>
```

   Click in the Remote Console tab and launch the Integrated Remote Console on the server.

   Click Yes if the Security Alert pops up.

2. **TVOE Management Server:** Verify the control network bond

   Note: The output below is for illustrative purposes only. It shows the control bond configured.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_Control_Bridge_Interface>
   Protocol: none
    On Boot: yes
 IP Address:
    Netmask:
Bonded Mode: active-backup
  Enslaving: <ethernet_interface_1> <ethernet_interface_2>
```

   If the bond has been configured, skip to the next step.

   Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

   Create control bond (<TVOE_Control_Bridge_Interface>).

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Control_Bridge_Interface>
--onboot=yes --type=Bonding --mode=active-backup --miimon=100
Interface <TVOE_Control_Bridge_Interface> added

$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_1>
--type=Ethernet --master=<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes
Interface <ethernet_interface_1> updated

$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_2>
--type=Ethernet --master-<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes
Interface <ethernet_interface_2> updated
```

3. **TVOE Management Server:** Verify the control network bridge

Note: The output below is for illustrative purposes only. It shows the control bridge configured.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=control
Bridge Name: control
    On Boot: yes
   Protocol: dhcp
 Persistent: yes
Promiscuous: no
     Hwaddr: 00:24:81:fb:29:52
        MTU:
Bridge Interface: bond0
```

If the bridge has been configured, skip to the next step.

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. Create control bridge (<TVOE_Control_Bridge>).

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_Control_Bridge>
--bootproto=dhcp --onboot=yes --bridgeInterfaces=<TVOE_Control_Bridge_Interface>
```

4. **TVOE iLO:** Create tagged control interface and bridge (optional)

   If you are using a tagged control network interface on this PMAC, then complete this step. Otherwise, proceed to the next step now.

```
$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control
--delBridgeInt=bond0
Interface bond0 updated
Bridge control updated
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Control_Bridge_Interface>
--onboot=yes
Interface <TVOE_Control_Bridge_Interface> created
$ sudo /usr/TKLC/plat/bin/netAdm set --device=<base_device_hosting_control_network>
 --onboot=yes
$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control
--bridgeInterfaces=<TVOE_Control_Bridge_Interface>
```

5. **TVOE Management Server:** Verify the tagged/non-segregated management network

   Note: This step only applies if the management network is tagged (non-segregated).

   Note: The output below is for illustrative purposes only. It shows the management bridge configured on a non-segregated network setup.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --device=bond0.2
      Protocol:  none
       On Boot:  yes
    IP Address:
       Netmask:
        Bridge:  Member of bridge management
```

   If the device has been configured, skip to the next step.

   Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

   Note: The example below illustrates a PM&C management server configuration in a Non-Segregated network, an un-tagged control network, and a tagged management network.

For this example created tagged device for management device.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface>
 --onboot=yes
Interface <TVOE_Management_Bridge_Interface> added
```

6. **TVOE Management Server:** Verify the untagged/segregated management network

   Note: This step only applies if the management network is untagged (segregated).

   Note: The output below is for illustrative purposes only. It shows the management bond configured on a segregated network setup.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_Management_Bridge_Interface>

      Protocol:  none
       On Boot:  yes
    IP Address:
       Netmask:
   Bonded Mode:  active-backup
     Enslaving:  <ethernet_interface_3> <ethernet_interface_4>
```

   If the bond has been configured, skip to the next step.

   Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface>
 --onboot=yes --type=Bonding --mode=active-backup --miimon=100
Interface <TVOE_Management_Bridge_Interface> added
$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_3>
--type=Ethernet --master=<TVOE_Management_Bridge_Interface> --slave=yes
--onboot=yes
Interface <ethernet_interface_3> updated
$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_4>
--type=Ethernet --master=<TVOE_Management_Bridge_Interface> --slave=yes
--onboot=yes
Interface <ethernet_interface_4> updated
```

7. **TVOE Management Server:** Verify the management bridge

   Note: The output below is for illustrative purposes only. It shows the management bridge configured on a non-segregated network setup.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=management
Bridge Name: management
    On Boot: yes
   Protocol: none
 IP Address: 10.240.4.86
    Netmask: 255.255.255.0
Promiscuous: no
     Hwaddr: 00:24:81:fb:29:52
        MTU:
Bridge Interface: bond0.2
```

   If the bridge has been configured, skip to the next step.

   Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

For this example created tagged device for management bridge.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_Management_Bridge>
 --address=<management_server_mgmtVLAN_IP> --netmask=<mgmtVLAN_netmask>
--onboot=yes --bridgeInterfaces=<TVOE_Management_Bridge_Interface>
```

8. **TVOE Management Server:** Verify the NetBackup network (if needed)

   If the NetBackup feature is not needed, skip to the next step.

   Note: The output below is for illustrative purposes only. It shows the **NetBackup** bridge is configured.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=netbackup
     Bridge Name: netbackup
         On Boot: yes
        Protocol: none
      IP Address: 10.240.6.2
         Netmask: 255.255.255.0
     Promiscuous: no
          Hwaddr: 00:24:81:fb:29:58
             MTU:
Bridge Interface: bond2
```

   If the bridge has been configured, skip to the next step.

   Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

   Note: The example below illustrates a TVOE management server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size.

   Note: The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs.

   Select **only one** of the following configurations:

   - Option 1: Create NetBackup bridge using a bond containing an untagged interface.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface>
--onboot=yes --type=Bonding --mode=active-backup --miimon=100
--MTU=<NetBackup_MTU_size>
Interface <TVOE_NetBackup_Bridge_Interface> added
$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_5>
--type=Ethernet --master=<TVOE_NetBackup_Bridge_Interface> --slave=yes --onboot=yes
 --MTU=<NetBackup_MTU_size>
Interface <ethernet_interface_5> updated
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>
 --bootproto=none --onboot=yes --MTU=<NetBackup_MTU_size>
--bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP>
 --netmask=<TVOE_NetBackup_Netmask>
```

   - Option 2: Create NetBackup bridge using an untagged native interface.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>
 --bootproto=none --onboot=yes --MTU=<NetBackup_MTU_size>
--bridgeInterfaces=<Ethernet_interface_5> --address=<TVOE_NetBackup_IP>
--netmask=<TVOE_NetBackup_Netmask>
```

- Option 3: Create NetBackup bridge using a tagged device.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface>
--onboot=yes
Interface <TVOE_NetBackup_Bridge_Interface> added
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>
 --onboot=yes --MTU=<NetBackup_MTU_size>
--bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP>
 --netmask=<TVOE_NetBackup_Netmask>
```

9. **TVOE Management Server:** Setup syscheck

   `syscheck` must be configured to monitor bond interfaces. Replace "**`bondedInterfaces`**" with "**`bond0`**" or "**`bond0,bond1`**" if segregated networks are used:

```
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES
--val=<bondedInterfaces>
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond –enable
$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond
```

   Note: The following is an example of the setup of syscheck with a single bond, bond0:

```
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=bond0
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable
$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond
```

   Note: The following is an example of the setup of syscheck with multiple bonds, bond0 and bond1:

```
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES
--val=bond0,bond1
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable
$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond
```

10. **TVOE Management Server:** Verify the default route

    Note: The output below is for illustrative purposes only. It shows the default route on the management bridge is configured.

```
$ sudo /usr/TKLC/plat/bin/netAdm query --route=default --device=management
Routes for TABLE: main and DEVICE: management
* NETWORK: default
  GATEWAY: 10.240.4.1
```

    If the route has been configured, skip to the next step.

    Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.

    For this example add default route on management network.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=default
--device=<TVOE_Management_Bridge> --gateway=<mgmt_gateway_address>
Route to <TVOE_Management_Bridge> added
```

11. **TVOE Management Server:** Verify the NetBackup route (optional)

    If the NetBackup network is a unique network for NetBackup data, verify the existence of the appropriate NetBackup route.

Note: The output below is for illustrative purposes only. It shows the route on the NetBackup bridge is configured.

If the NetBackup route is to be a network route, then:

```
$ sudo /usr/TKLC/plat/bin/netAdm query --route=net --device=<TVOE_NetBackup_Bridge>
Routes for TABLE: main and DEVICE: netbackup
* NETWORK: net
GATEWAY: 169.254.253.1
```

If the NetBackup route is to be a host route then:

```
$ sudo /usr/TKLC/plat/bin/netAdm query --route=host
--device=<TVOE_NetBackup_Bridge>
Routes for TABLE: main and DEVICE: netbackup
* NETWORK: host
GATEWAY: 169.254.253.1
```

If the route has been configured, skip to the next step.

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces (network devices, bonds, and bond enslaved devices) to configure.

For this example add network route on management network.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=<TVOE_Management_Bridge>
 --gateway=<NetBackup_gateway_address> --address=<NetBackup_network_IP>
--netmask=<TVOE_NetBackup_Netmask>
Route to <TVOE_NetBackup_Bridge> added
```

For this example add host route on management network.

Note: For the configuration of a host route, the <TVOE_NetBackup_Netmask> will be set to "255.255.255.255".

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=host --device=<TVOE_Management_Bridge>
 --gateway=<NetBackup_Server_IP> --address=<NetBackup_Server_IP>
--netmask=<TVOE_NetBackup_Netmask>
Route to <TVOE_NetBackup_Bridge> added
```

12. **TVOE Management Server:** Set hostname

```
$ sudo /bin/su - platcfg
```

1. Navigate to **Server Configuration** > **Hostname** and set the hostname.
2. Set TVOE Management Server hostname
3. Press OK.
4. Navigate out of Hostname

13. **TVOE Management Server:** set time zone and/or hardware clock

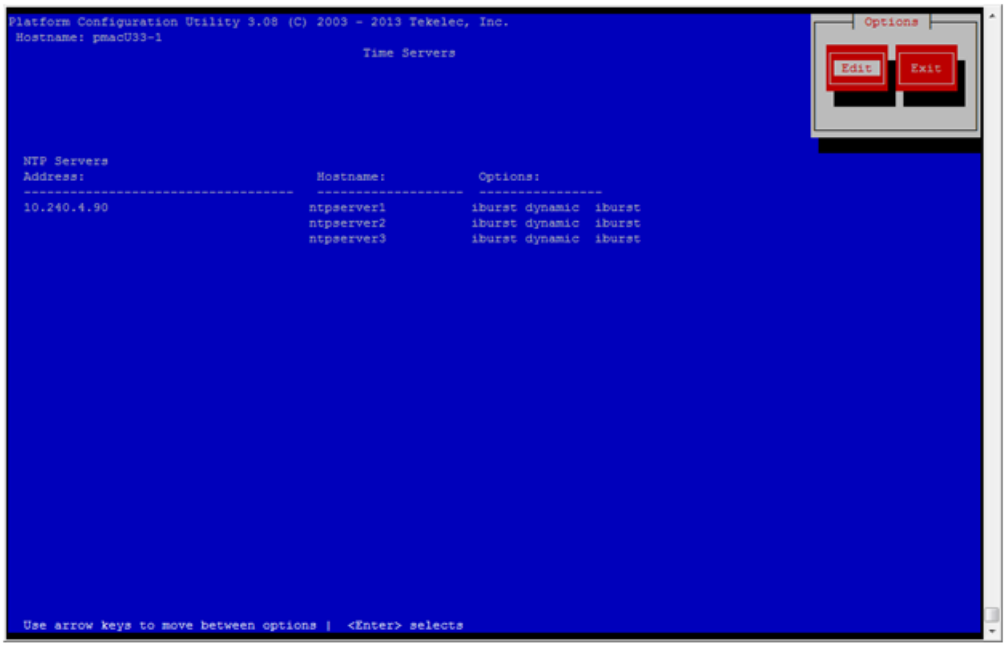
1. Navigate to **Server Configuration** > **Time Zone.**
2. Select Edit.
3. Set the time zone and/or hardware clock.
4. Press OK.
5. Navigate out of Server Configuration

14. This step will configure NTP servers for a server based on TPD.

1. **Server:** Login as platcfg

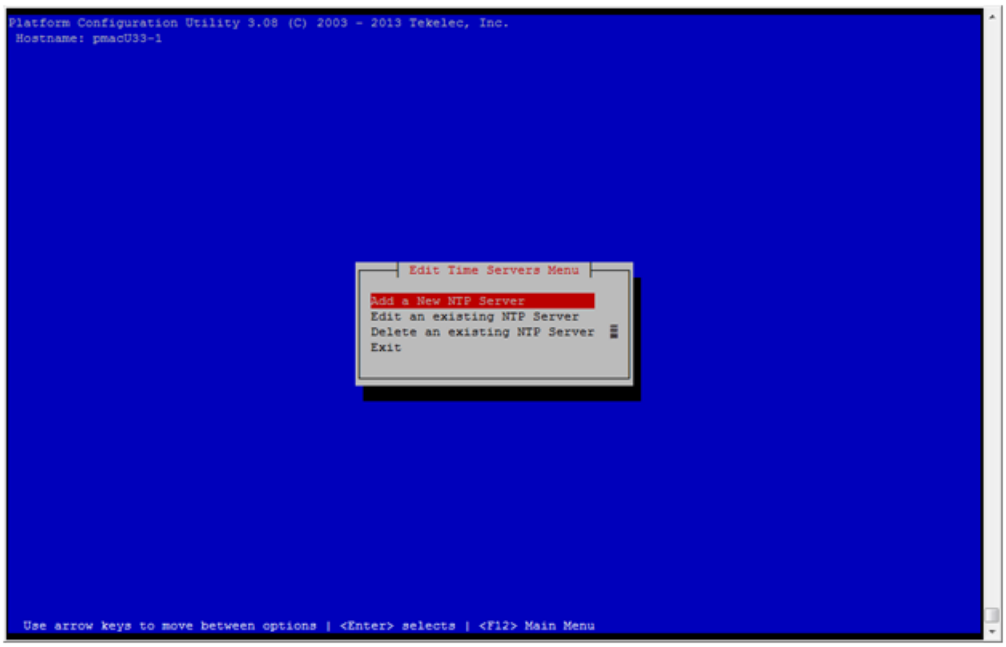
   Login as platcfg user on the server. The platcfg main menu will be shown.

2. **Server:** Navigate to Time Servers configuration page. Select the following menu options sequentially: **Network Configuration** > **NTP**. The 'Time Servers' page will now be shown, which shows the configured NTP servers and peers.



3. **Server:** Update NTP Information

   Select **Edit**. The **Edit Time Servers Menu** is displayed.



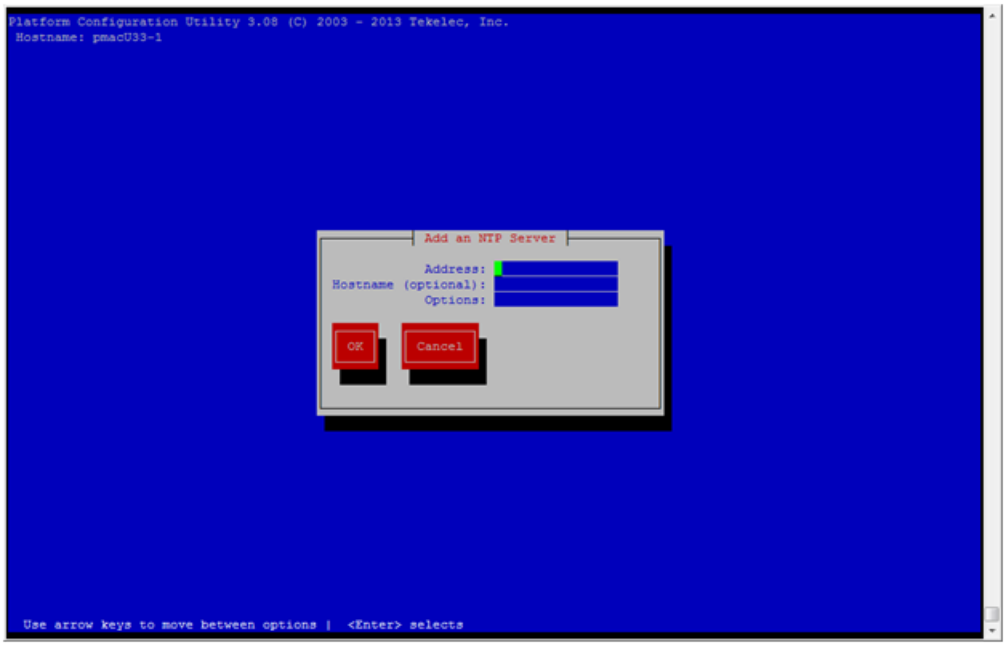
4. **Server:** Edit NTP Information

   Select the appropriate **Edit Time Servers Menu** option. When all Time Server actions are complete exit the **Edit Time Servers Menu**.

   a. **Adding an NTP Server**

      a. **Server:** If adding a new NTP server select **Add a New NTP Server**.

         The **Add an NTP Server** window is displayed.



      b. **Server:** Enter Appropriate data, and select **OK**

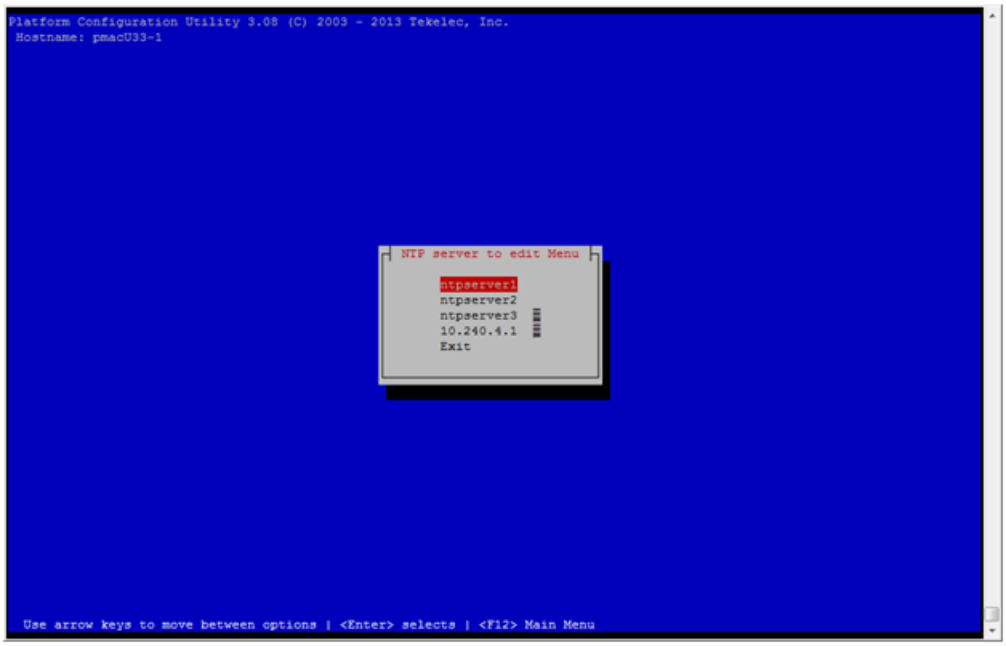
The NTP server is added. The **Edit Time Servers Menu** is displayed.

Note: The default NTP option is iburst. Additional NTP options are listed in the ntp.conf man page, some of the valid options are: burst, preferred, minpoll, and maxpoll.

b. Editing an NTP Server

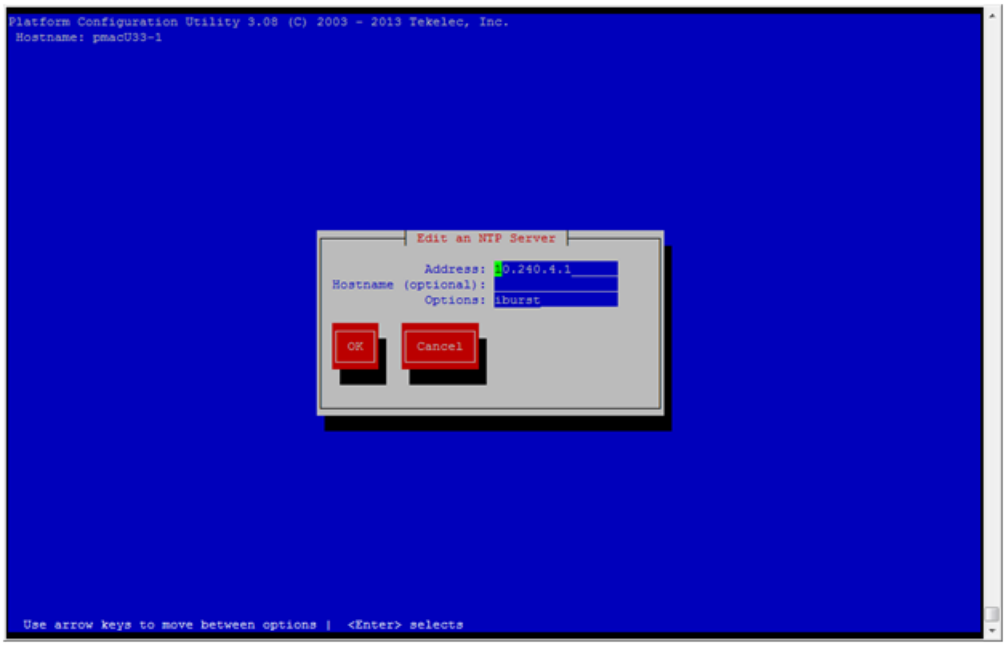
a. Server: If editing an existing NTP server select **Edit an existing NTP Server**.

The **NTP Server to edit Menu** window is displayed.



b. Server: Select appropriate NTP server.

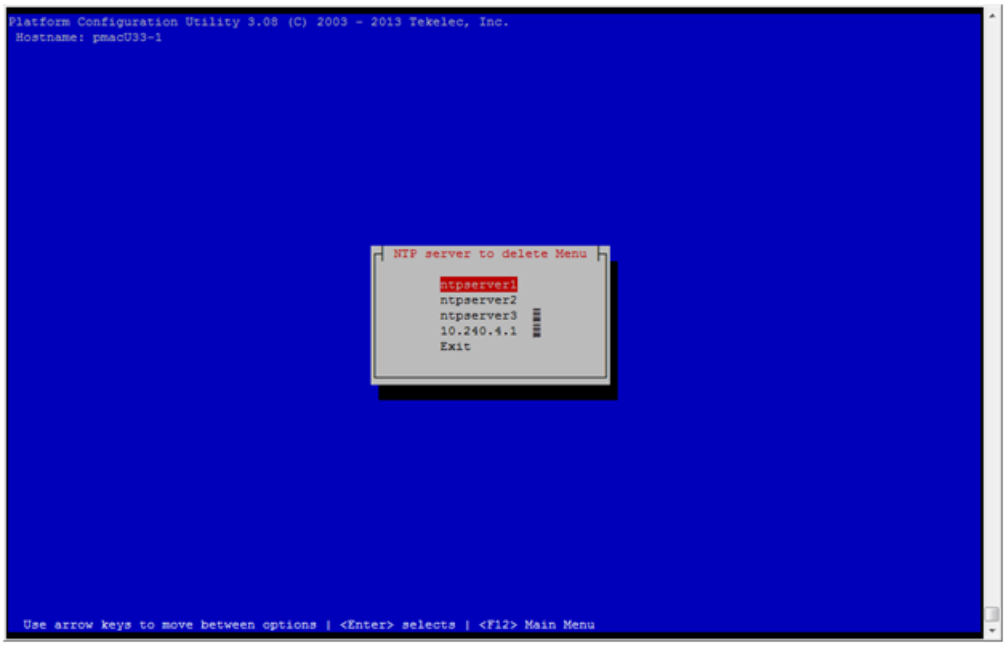
The **Edit an NTP Server** window is displayed.



c. **Deleting an existing NTP Server**

a. **Server:** If deleting an existing NTP server, select **Delete an existing NTP Server**.

The **NTP server to delete Menu** is displayed.



b. **Server:** Select appropriate NTP server.

The NTP server is deleted. The **Edit Time Servers Menu** is displayed.

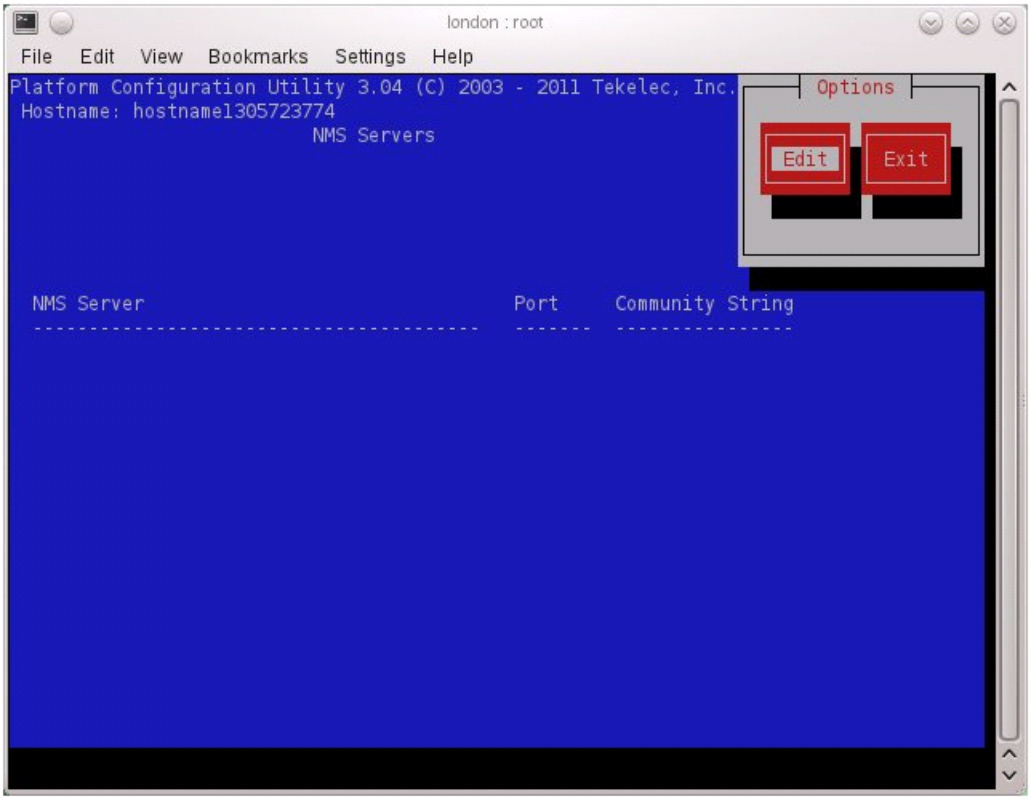
5. **Server:** Restart the NTP server
6. **Server:** Exit platcfg.

   Select **Exit** on each menu until platcfg has been exited.

15. This step will add an SNMP trap destination to a server based on TPD. All alarm information will then be sent to the NMS located at the destination.

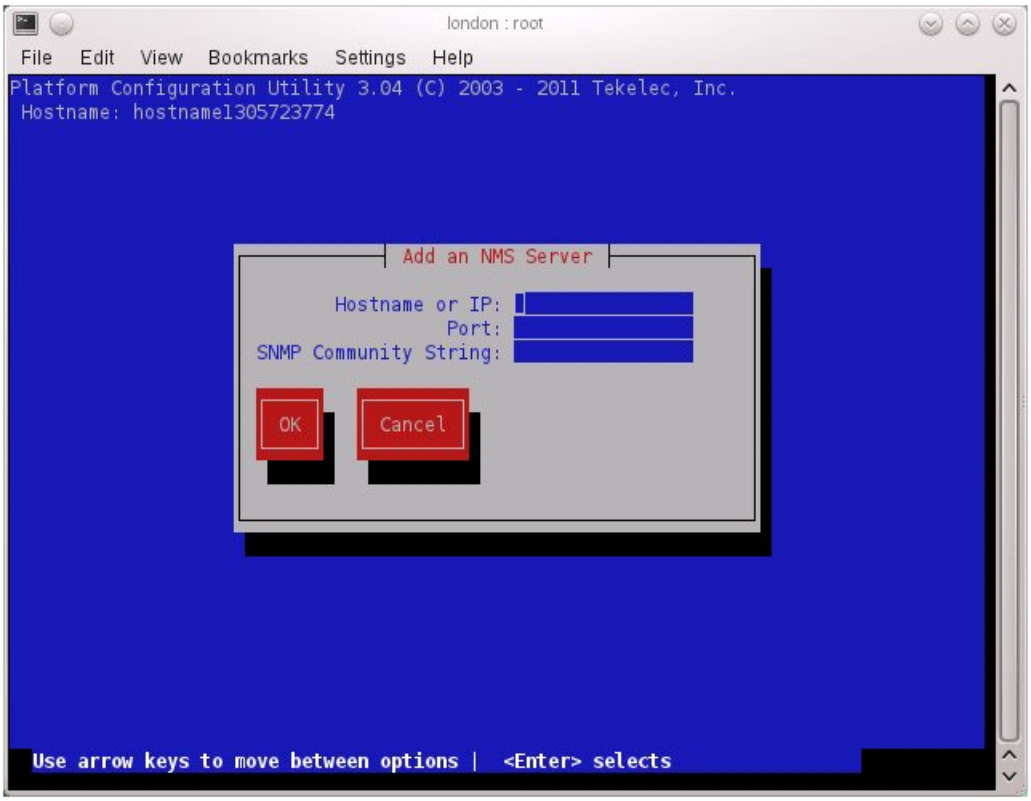
    1. **Server:** Login as platcfg user on the server. The platcfg main menu will be shown.
    2. **Server:** Navigate to NMS server configuration page.

       Select the following menu options sequentially: **Network Configuration** > **SNMP Configuration** > **NMS Configuration**. The 'NMS Servers' page will be shown, which displays all configured NMS servers for the server.



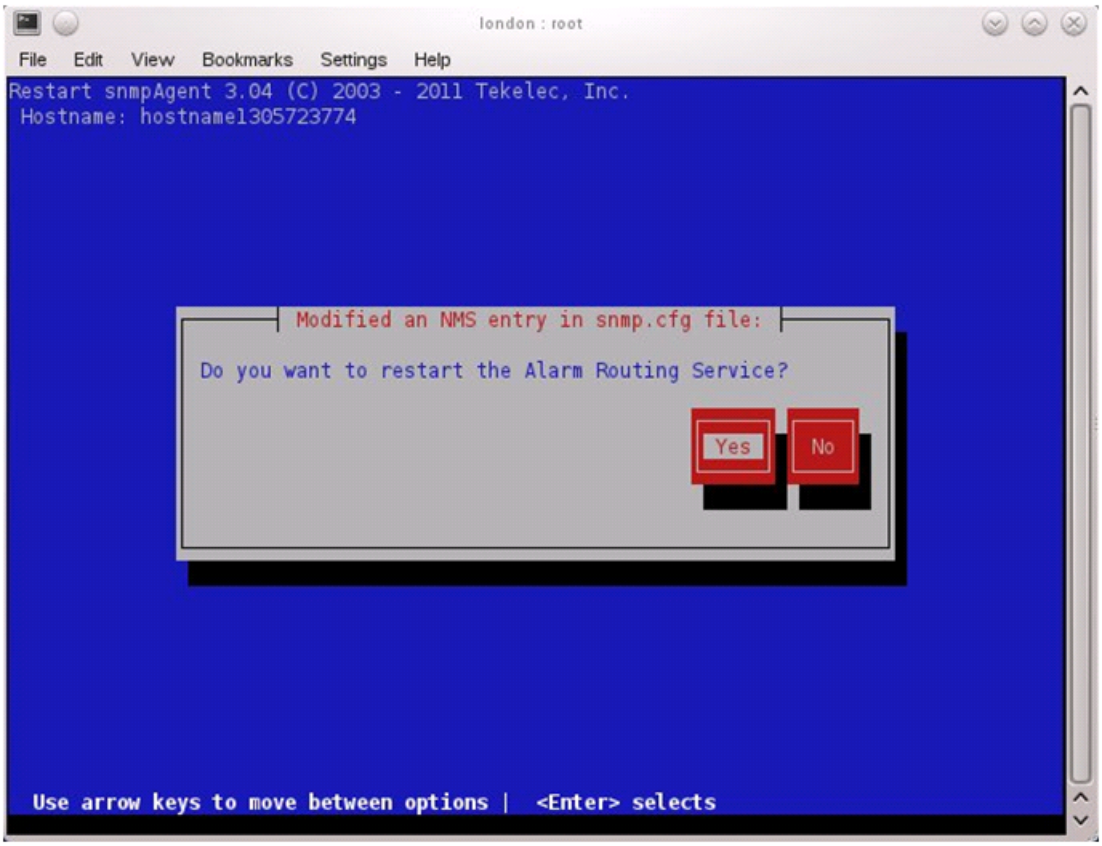
    3. **Server:** Add the SNMP trap destination.

       Select **Edit** and then choose **Add a New NMS Server**. The 'Add an NMS Server' page will be displayed.



Complete the form by entering in all information about the SNMP trap destination. Select **OK** to finalize the configuration.

The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialogue will then be presented.



Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented.

4. Select **Exit** on each menu until platcfg has been exited.

16. If NetBackup is configured in this system, this step will setup and install NetBackup Client on a TVOE host.

    Note: Once the NetBackup Client is installed on TVOE, the NetBackup Master should be configured to backup the following files from the TVOE host:

    - `/var/TKLC/bkp/*.iso`

    1. **TVOE Server:** Login as the admusr user
    2. **TVOE Server:** Open firewall ports for NetBackup using the following commands:

```
$ sudo ln -s /usr/TKLC/plat/share/netbackup/60netbackup.ipt
/usr/TKLC/plat/etc/iptables/
$ sudo /usr/TKLC/plat/bin/iptablesAdm reconfig
```

    3. **TVOE Server:** Enable platcfg to show the NetBackup Menu Items by executing the following commands:

```
$ sudo platcfgadm --show NBConfig
$ sudo platcfgadm --show NBInit
$ sudo platcfgadm --show NBDeInit
$ sudo platcfgadm --show NBInstall
```

```
$ sudo platcfgadm --show NBVerifyEnv
$ sudo platcfgadm --show NBVerify
```

4. Use the **vgguests** volume group in the following steps to create an LV and filesystem for the NetBackup client software.
   a. **Server:** Login as the admusr user.
   b. **Server:** Create a storageMgr configuration file that defines the LV to be created.

```
$ sudo echo "lv --mountpoint=/usr/openv --size=2G --name=netbackup_lv --vg=$VG"
 > /tmp/nb.lvm
```

   The above example uses the $VG as the volume group. Replace $VG with the desired volume group as specified by the application group.

   c. **Server:** Create the LV and filesystem by using storageMgr.

```
$ sudo /usr/TKLC/plat/sbin/storageMgr /tmp/nb.lvm
```

   This will create the LV, format it with a filesystem, and mount it under /usr/openv/. Example output is shown below:

```
Called with options: /tmp/nb.lvm
VG vgguests already exists.
Creating lv netbackup_lv.
Volume netbackup_lv will be created.
Success: Volume netbackup_lv was created.
Creating filesystem, this may take a while.
Updating fstab for lv netbackup_lv.
Configuring existing lv netbackup_lv.
```

   The LV for NetBackup has been created!

5. NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite is for the purpose of supporting Disaster Recovery at the customer site. This procedure provides instructions for installing or upgrading the Netbackup client software on an application server.

   See *B.3 Create NetBackup Client Config File* for more information.

   Disclaimer: Failure to install the NetBackup Client properly (i.e. by neglecting to execute this procedure) may result in the NetBackup Client being deleted during a Tekelec software upgrade.

   1. **Choose NetBackup Client Install Path:** There are two different ways to install NetBackup Client. The following is a guide to which method to use:
      - See *B.1 Netbackup Client Install/Upgrade with nbAutoInstall* for more information.
      - See *B.2 NetBackup Client Install/Upgrade with platcfg* for more information.

        Chosen Procedure: _____

      - **Execute the procedure chosen in Step 1**
      - **Application Console:** Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias.

Note: If NetBackup Client has successfully been installed then you can find the NetBackup server's hostname in the "/usr/openv/netbackup/bp.conf" file. It will be identified by the "SERVER" configuration parameter as is shown in the following output:

List NetBackup servers hostname:

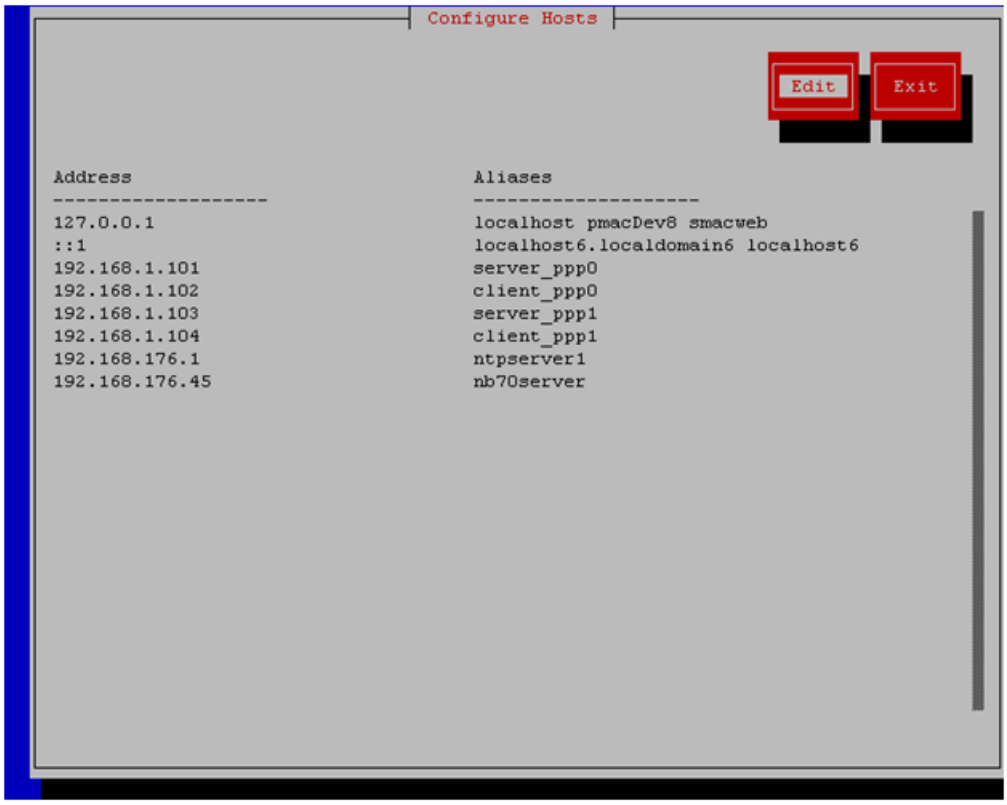
```
$ sudo cat /usr/openv/netbackup/bp.conf
SERVER = nb70server
CLIENT_NAME = pmacDev8
```

Note: : In the case of nbAutoInstall NetBackup Client may not yet be installed. For this situation the "/usr/openv/netbackup/bp.conf" cannot be used to find the NetBackup server alias.

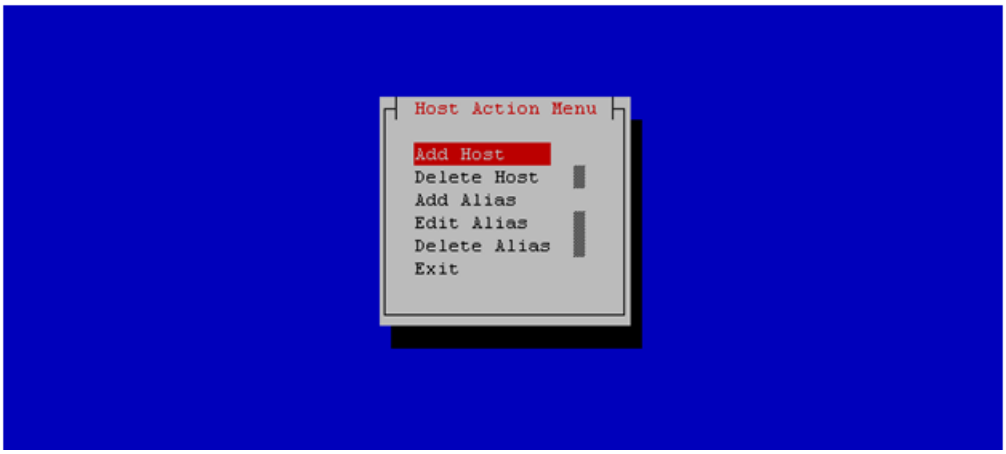
Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```
$ sudo su - platcfg
```

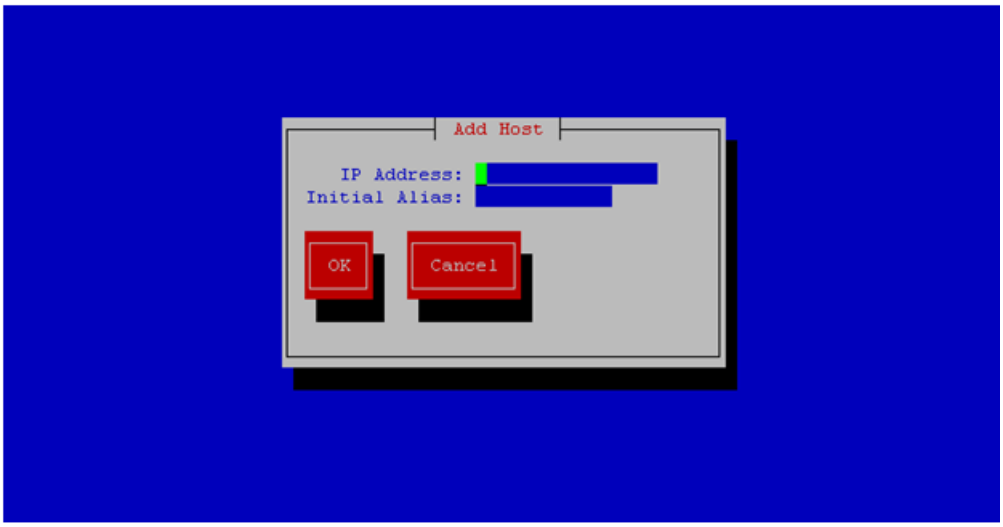
Navigate to **Network Configuration** > **Modify Hosts File**



Select **Edit**, the Host Action Menu will be displayed.



Select "**Add Host**", and enter the appropriate data



Select "**OK**", confirm the host alias add, and exit Platform Configuration Utility

- **Application Console:** Create a link for the application provided NetBackup client notify scripts to path on application server where NetBackup expects to find them.

  Note: Link notify scripts from appropriate path on application server for given application.

```
$ sudo mkdir -p /usr/openv/netbackup/bin/
$ sudo ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify
$ sudo ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify
```

- **Application Console**: Netbackup client software installation complete; if applicable return to calling procedure.

6. **TVOE Server:** Create softlinks for TVOE specific NetBackup notify scripts.

```
$ sudo ln -s /usr/TKLC/plat/sbin/bpstart_notify
/usr/openv/netbackup/bin/bpstart_notify
$ sudo ln -s /usr/TKLC/plat/sbin/bpend_notify /usr/openv/netbackup/bin/bpend_notify
```

17. **TVOE Management Server:** Verify server health

```
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
```

This command should return no output on a healthy system. If any alarms are reported, contact Customer Care Center.

18. **TVOE Management Server:** Ensure time set correctly.

a) Set time based on NTP Server

```
$ sudo /sbin/service ntpd stop
$ sudo /usr/sbin/ntpdate ntpserver1
$ sudo /sbin/service ntpd start
```

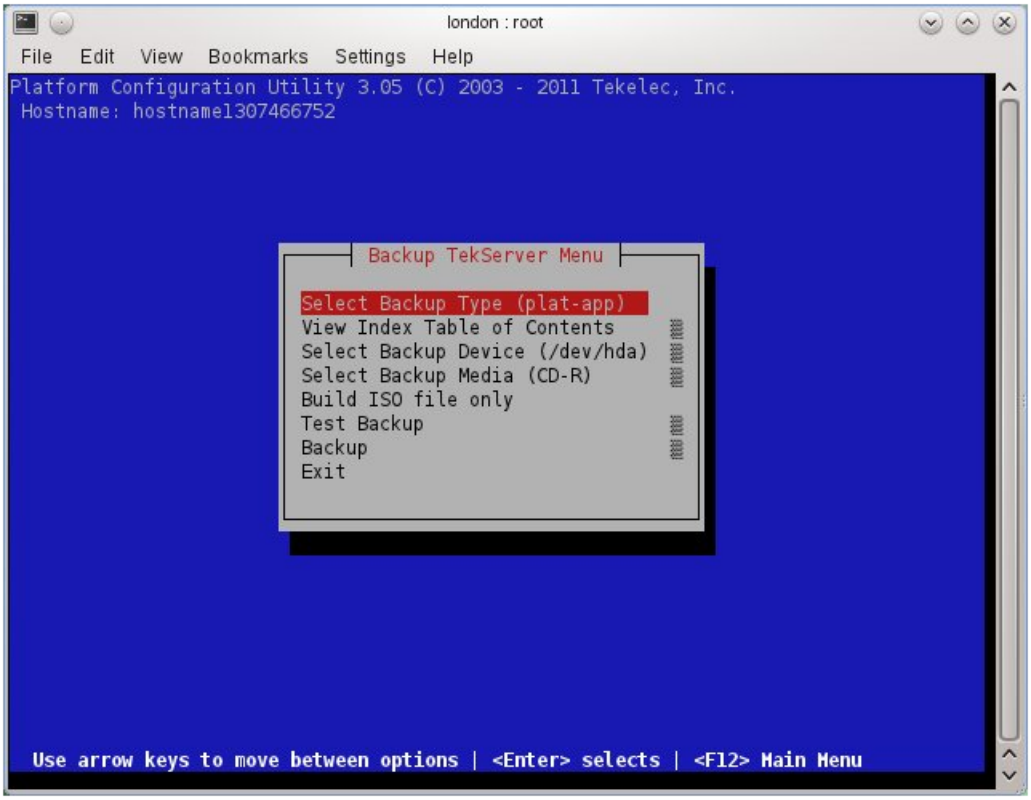
b) Reboot the server

```
$ sudo /sbin/init 6
```

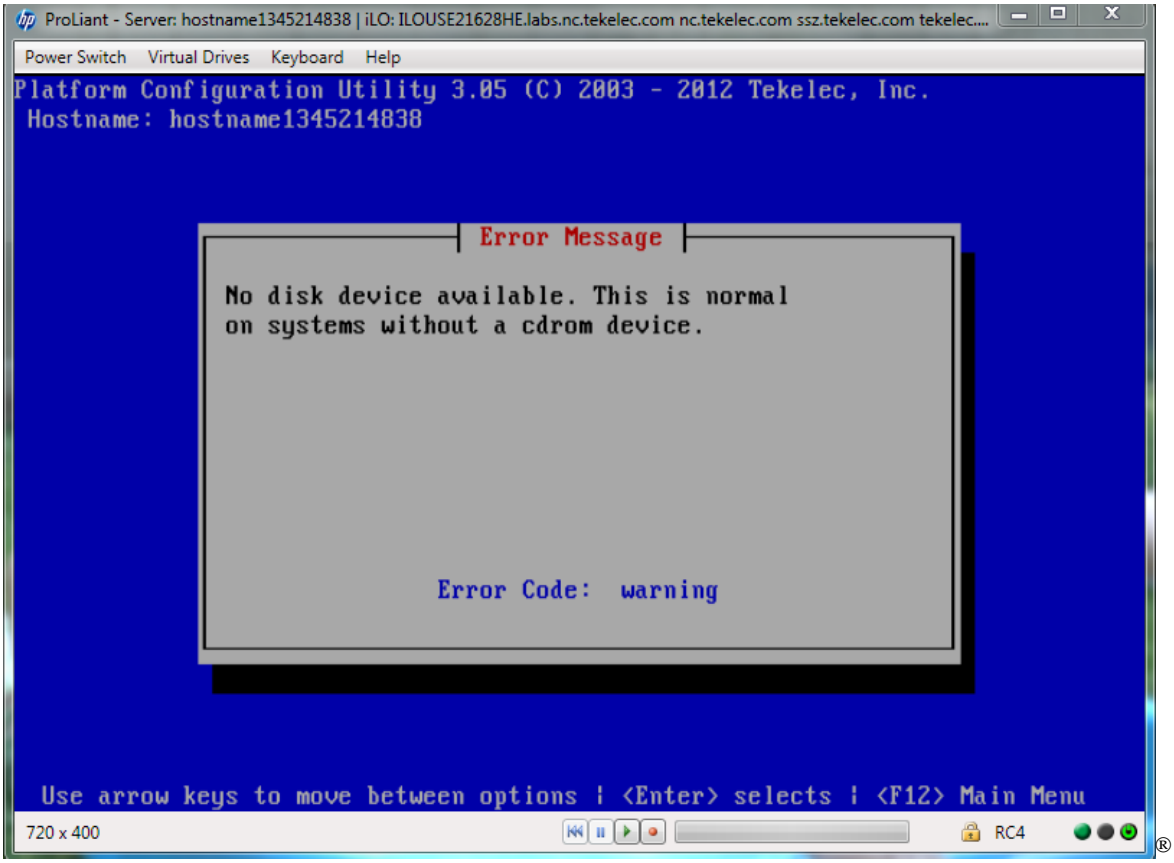
19. This step will backup system files which can be used at a later time to restore a failed system.

Note: The backup image is to be stored on a customer provided medium.

1. **TVOE Host:** Login as platcfg user. Select the following menu options sequentially: **Maintenance** > **Backup and Restore** > **Backup Platform (CD/DVD)**. The 'Backup TekServer Menu' page will now be shown.

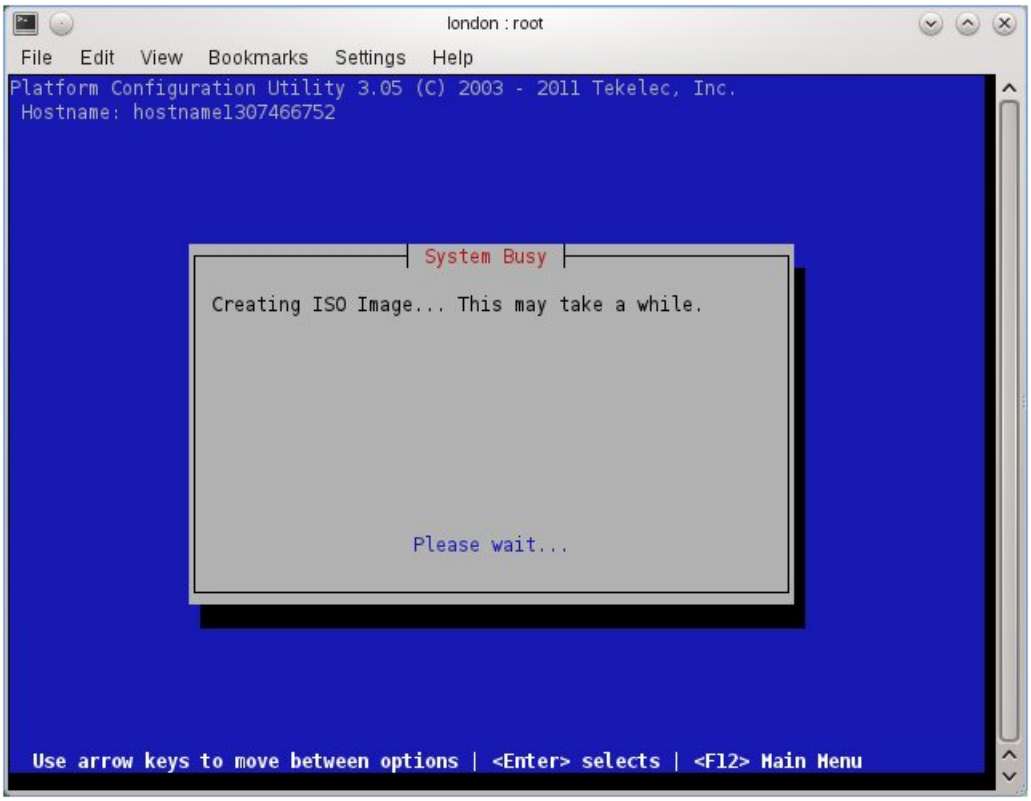


Note: If this operation is attempted on a system without a CD-ROM drive, the following message will appear:



2. **TVOE Host:** Build the backup ISO image. Select **Build ISO file only**. The following screen will display:

   Note: Creating the ISO image may happen so quickly that this screen may only appear for an instant.



After the ISO is created, platcfg will return to the Backup TekServer Menu as shown in step 2. The ISO has now been created and is located in the `/var/TKLC/bkp/` directory. An example filename of a backup file that was created is: "hostname1307466752-plat-app-201104171705.iso"

3. **TVOE Host:** Exit platcfg

   Select **Exit** on each menu until platcfg has been exited. The SSH connection to the TVOE server will be terminated.

4. **Customer Server:** Login to the customer server and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, execute the following command to copy the backup image to the customer system.

```
# scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/
```

   When prompted, enter the tvoexfer user password and press **Enter**.

   An example of the output looks like:

```
# scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/
tvoexfer@10.24.34.73's password:
hostname1301859532-plat-app-301104171705.iso     100% 134MB 26.9MB/s 00:05
```

   If the Customer System is a Windows system refer to Appendix E *Using WinSCP* Using WinSCP to copy the backup image to the customer system.

   The TVOE backup file has now been successfully placed on the Customer System.

4.2 Install PM&C

4.2.1 Deploy PM&C Guest

The **pmac-deploy** script is responsible for deploying a PM&C guest in the absence of a PM&C to create the guest and install the OS and application. This is all done a build-time and the system disk image is kept on the PM&C media, along with this script. Once the PM&C media is mounted, the **pmac-deploy** script can be found in the upgrade directory of the media.

1. **TVOE Management Server iLO:** Login to the management server on the remote console

   Login to iLo using application provided passwords via Appendix G *How to Access a Server Console using the iLO*

   ```
   http://<management_server_iLO_ip>
   ```

   Click in the Remote Console tab and launch the Integrated Remote Console on the server.

   Click Yes if the Security Alert pops up.

2. **TVOE Management Server:** Mount the PM&C media to the TVOE Management server.

   For a sample of mounting a DVD media:

   ```
   $ sudo /usr/TKLC/plat/bin/getCDROM DV-W28E-RW|sr0 /dev/sr0 $ sudo /bin/mount -t iso9660 /dev/sr0 /mnt/upgrade/
   ```

   For a sample of mounting a USB media

   ```
   $ sudo /bin/ls /media/*/*.iso
   /media/usb/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso
   $ sudo /bin/mount -o loop /media/usb/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso /mnt/upgrade
   ```

3. **TVOE Management Server:** Validate the PM&C media.

   Execute the self-validating media script:

   ```
   $ cd /mnt/upgrade/upgrade
   $ sudo .validate/validate_cd
   Validating cdrom...

   UMVT Validate Utility v2.2.2, (c)Tekelec, June 2012
   Validating <device or ISO>
   Date&Time: 2012-10-25 10:07:01
   Volume ID: tklc_872-2441-106_Rev_A_50.11.0
   Part Number: 872-2441-106_Rev_A
   Version: 50.11.0
   Disc Label: PMAC
   Disc description: PMAC
   The media validation is complete, the result is: PASS

   CDROM is Valid
   ```

   If the media validation fails, the media is not valid and should not be used.

4. **TVOE Management Server:** Using the pmac-deploy script, deploy the PM&C instance using the configuration detailed by the completed NAPD.

   For this example, deploy a PM&C without NetBackup feature

```
$ cd /mnt/upgrade/upgrade
$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name>
--controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address>
--controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge>
--managementIP=<PMAC_Management_ip_address>
--managementNM=<PMAC_Management_netmask>
--routeGW=<PMAC_Management_gateway_address>
--ntpserver=<TVOE_Management_server_ip_address>
```

   For this example, deploy a PM&C with the NetBackup feature. Deploying a PM&C with the NetBackup feature requires the "--netbackupVol" option, which creates a separate NetBackup logical volume on the TVOE host of PM&C. If the NetBackup feature's source interface is different than the management interface include the "--bridge" and the "--nic" as in the example below.

```
$ cd /mnt/upgrade/upgrade
$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name>
--controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address>
--controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge>
--managementIP=<PMAC_Management_ip_address>
--managementNM=<PMAC_Management_netmask>
--routeGW=<PMAC_Management_gateway_address>
--ntpserver=<TVOE_Management_server_ip_address>
--netbackupVol
--bridge=<TVOE_NetBackup_Bridge>
--nic=netbackup
```

```
$ cd /mnt/upgrade/upgrade
$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name>
--controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address>
--controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge>
--managementIP=<PMAC_Management_ip_address>
--managementNM=<PMAC_Management_netmask>
--routeGW=<PMAC_Management_gateway_address>
--ntpserver=<TVOE_Management_server_ip_address> --isoimagesVolSizeGB=20
```

   Note: If a mistake in the pmac-deploy is identified during this step the operator under the advisement of customer service can remove the guest with the following command:

```
$ sudo /usr/TKLC/plat/bin/guestMgr --remove <PMAC_Name>
```

5. The PM&C will deploy and boot. The management and control network will come up based on the settings that were provided to the pmac-deploy script.
6. **TVOE Management Server:** Unmount the media and remove.

```
$ cd /
$ sudo /bin/umount /mnt/upgrade
```

7. **TVOE Management Server:** Remove the PM&C Media

4.2.2 Setup PM&C

The steps in this section configure the PM&C application guest environment on the Management Server TVOE host. It also initializes the PM&C application. At the conclusion of this section, the PM&C application environment is sufficiently configured to allow configuration of system network assets associated with the Management Server.

1. **TVOE Management Server iLO:** Login to the management server on the remote console

   Login to iLo using application provided passwords via Appendix G *How to Access a Server Console using the iLO*

   ```
   http://<management_server_iLO_ip>
   ```

   Click in the Remote Console tab and launch the Integrated Remote Console on the server.

   Click Yes if the Security Alert pops up.

2. Login with PM&C admusr credentials

   Note: On a TVOE host, If you launch the virsh console, i.e., "$ **sudo /usr/bin/virsh console X**" or from the virsh utility "virsh # **console X"** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**ps -ef |grep virsh**", then kill the existing process "**kill -9 <PID>**". Then execute the "virsh console X" command. Your console session should now run as expected.

   Login using **virsh**, and wait until you see the login prompt. If a login prompt does not appear after the guest is finished booting, press **ENTER** to make one appear:

   ```
   $ sudo /usr/bin/virsh
   virsh # list

    Id    Name                           State
   ----------------------------------------------------
    4     pmacU17-1                      running

   virsh # console pmacU17-1

   [Output Removed]

   ######################
   1371236760: Upstart Job readahead-collector: stopping
   1371236767: Upstart Job readahead-collector: stopped
   ######################

   CentOS release 6.4 (Final)
   Kernel 2.6.32-358.6.1.el6prerel6.5.0_82.16.0.x86_64 on an x86_64

   pmacU17-1 login:
   ```

3. **TVOE Management Server iLO:** Login with PM&C admusr credentials

   Login to the TVOE as admusr using Appendix G *How to Access a Server Console using the iLO*

   Login to iLO in IE using password provided by application:

   ```
   http://<management_server_iLO_ip>
   ```

Click in the **Remote Console** tab and launch the Integrated Remote Console on the server.

Click **Yes** if the `Security Alert` pops up.

4. **TVOE Management Server iLO:** Login with PM&C admusr credentials

   Note: On a TVOE host, If you launch the virsh console, i.e., "$ **`sudo /usr/bin/virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**`ps -ef |grep virsh`**", then kill the existing process "**`kill -9 <PID>`**". Then execute the "virsh console X" command. Your console session should now run as expected.

   Login to PM&C console using virsh, and wait until you see the login prompt:

```
$ sudo /usr/bin/virsh
virsh # list
 Id    Name                           State
----------------------------------------------------
 4     pmacU17-1                      running

virsh # console pmacU17-1

[Output Removed]

pmacU17-1 login:
```

5. Verify the PM&C configured correctly on first boot.

   Run the following command (there should be no output):

```
$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/
$
```

6. Determine the TimeZone to be used for the PM&C

   Note: Valid time zones can be found on the server in the directory "/usr/share/zoneinfo". Only the time zones within the sub-directories (i.e. America, Africa, Pacific, Mexico, etc…..) are valid with platcfg.

7. Set the TimeZone

   Run:

```
$ sudo /usr/TKLC/smac/bin/set_pmac_tz.pl <timezone>
```

   For Example:

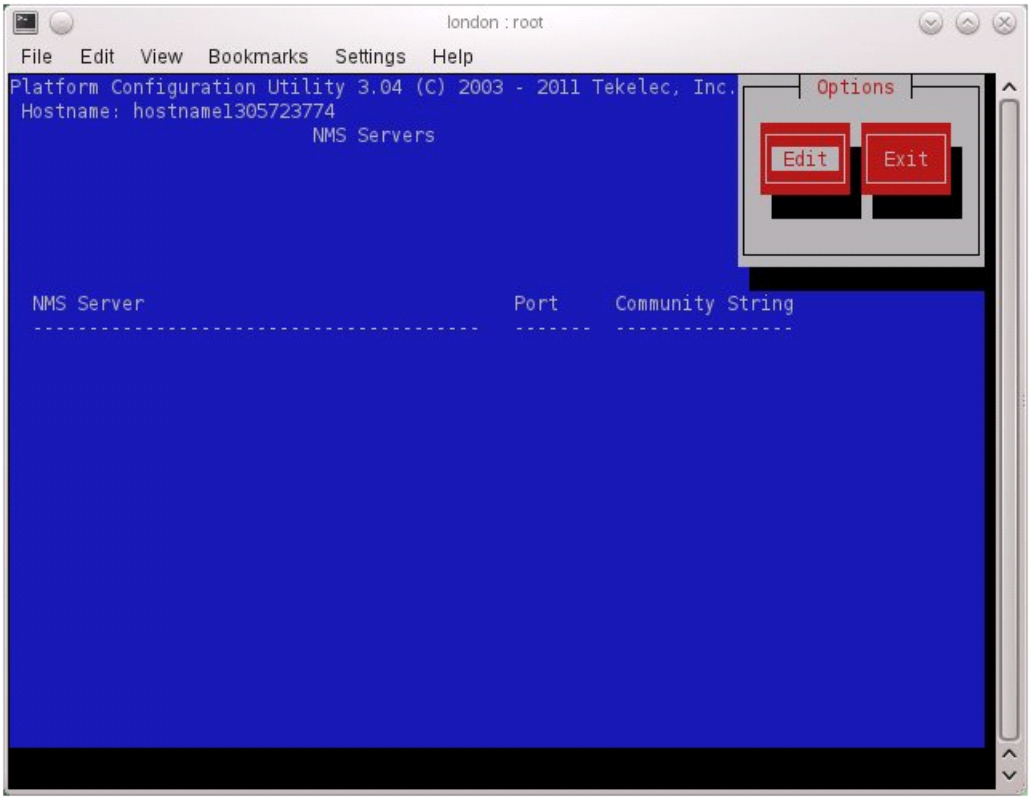
```
$ sudo set_pmac_tz.pl America/New_York
```

8. Verify the TimeZone has been updated

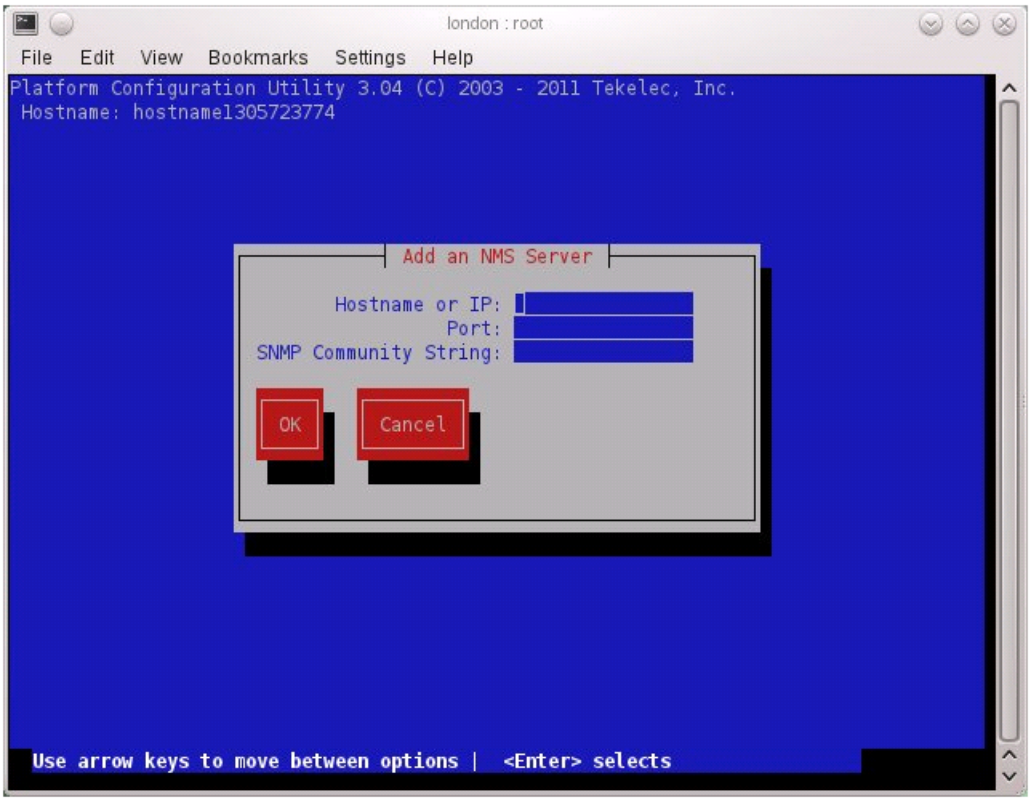
   Run:

```
$ sudo /bin/date
```

9. This step will add an SNMP trap destination to a server based on TPD. All alarm information will then be sent to the NMS located at the destination.
   1. **Server:** Login as platcfg user. Login as platcfg user on the server. The platcfg main menu will be shown.
   2. **Server:** Navigate to NMS server configuration page. Select the following menu options sequentially: **Network Configuration** > **SNMP Configuration** > **NMS Configuration**. The 'NMS Servers' page will be shown, which displays all configured NMS servers for the server.

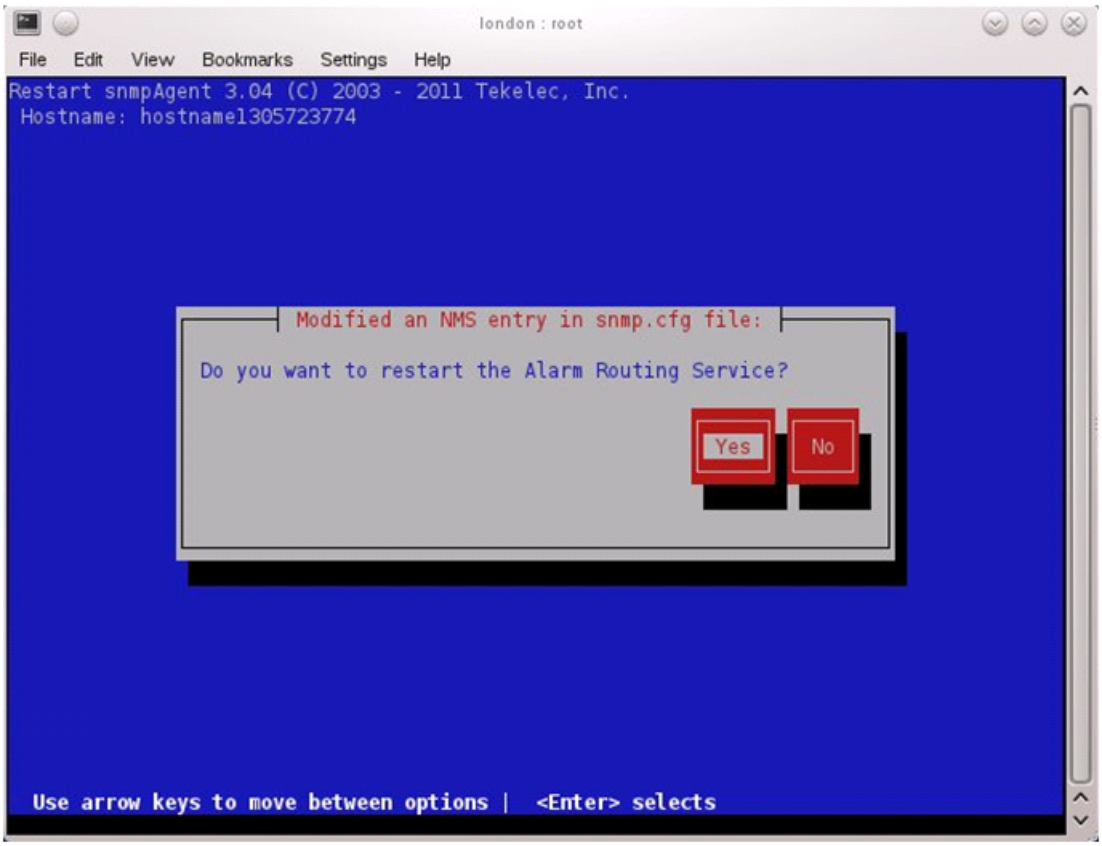


   3. **Server:** Add the SNMP trap destination. Select **Edit** and then choose **Add a New NMS Server**. The 'Add an NMS Server' page will be displayed.



Complete the form as follows: for "Hostname or IP" enter the Customer NMS server. For port, enter "162", for SNMP Community String, enter the customer defined string (if no customer defined string is provided, use "Tekelec"). Select **OK** to finalize the configuration. Repeat this to add the DSR SOAM VIP as an additional traps destination (for "Hostname or IP": use "DSR SOAM VIP", for port use "162" and for SNMP Community String "Tekelec"). Press **OK** again.

The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialogue will then be presented.



Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented.

4. **Server:** Exit platcfg. Select **Exit** on each menu until platcfg has been exited.

10. Gather and prepare configuration files that must be resident on the PM&C. These might be required to proceed with the Application installation after the PM&C has been deployed but before it has been initialized. These files are usually located within a given ISO on physical media (USB or CDROM).

    Note: This is an **optional** step only required if needed by an Application.

    a) Once the PM&C has completed rebooting, but prior to initializing, login to the PM&C as **admusr** using virsh on the management server iLO.
    b) Create any necessary destination subdirectories in the PM&C **`/usr/TKLC/smac/etc`** directory if not using an existing directory to transfer files.
    c) Make the media available to the TVOE Host server. Mount the media on the TVOE Host using one of the following methods:

        1. If the Application ISO is on a physical CDROM disk:

            a. Insert the disk into the CDROM drive of the TVOE Host Server.
            b. Determine the CDROM of the TVOE Host server by executing the following command:

```
$ sudo /usr/TKLC/plat/bin/getCDROM
```

Example: `/dev/sr0`

Note: sr0 is always designated as the CDROM device. There could be additional devices listed by the command if in use.

c. Make a temporary mount point and mount the optical media.

```
$ sudo /bin/mkdir /media/cdrom
$ sudo /bin/mount /dev/sr0 /media/cdrom
```

Note: Once mounted, this gives a direct path to the ISO on the CDROM device.

2. If using a USB Drive:

a. Insert the USB into an available USB slot on the TVOE Host server and execute the following command to determine its location and the ISO to be mounted:

```
$ sudo /bin/ls /media/*/*.iso
```

Example: **/media/sdd1/872-xxxx-104-5.0.0_50.8.0-application-x86_64.**

Note: The USB device is immediately added to the list of media devices once it is inserted into a USB slot on the TVOE Host server.

b. Note the device directory name under the media directory. This could be sdb1, sdc1, sdd1, sde1, depending on the USB slot the media was inserted into.

c. Loop mount the ISO to the standard TVOE Host mount point (if it is not already in use):

```
$ sudo /bin/mount -o loop /media/<device directory>/<ISO Name>.iso /mnt/upgrade
```

d) Execute the following commands on the PM&C guest to copy the required files from the TVOE host to the PM&C guest.

Wildcards can be used as necessary.

1. If the application is on a physical disk:

```
$ sudo /usr/bin/scp -r admusr@<TVOE_management_ip_address>:/media/cdrom/<path to
 files>/* /<path to destination directory>
```

2. If using a USB Drive:

```
$ sudo /usr/bin/scp -r admusr@<TVOE_management_ip_address>:/mnt/upgrade/<path to
 files>/* /<path to destination directory>
```

e) Remove the application media from the TVOE host:

1. If the application is on a physical disk:

```
$ sudo /bin/umount /media/cdrom
$ sudo /bin/rmdir /media/cdrom
```

2. If using a USB Drive:

```
$ sudo /bin/umount /mnt/upgrade
```

3. Remove application media, optical or USB, from the server.

11. Initialize the PM&C Application; run the following commands:

Note: If performing the setup on a Redundant PM&C do not initialize, skip this step and continue to step 1515.

```
$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --fileName=TVOE
Profile successfully applied.
$ sudo /usr/TKLC/smac/bin/pmacadm getPmacFeatureState
PMAC Feature State = InProgress
$ sudo /usr/TKLC/smac/bin/pmacadm addRoute --gateway=<mgmt_gateway_address>
--ip=0.0.0.0 --mask=0.0.0.0 --device=management
Successful add of Admin Route
$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig
Initialization has been started as a background task
```

12. Wait for the background task to successfully complete.

The command will show "IN_PROGRESS" for a short time.

Run the following command until a "COMPETE" or "FAILED" response is seen similar to the following:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
1: Initialize PM&C COMPLETE - PM&C initialized
Step 2: of 2 Started: 2012-07-13 08:23:55 running: 29 sinceUpdate: 47
taskRecordNum: 2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
```

Note: Some expected networking alarms may be present.

13. Perform a system healthcheck on PM&C

```
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
```

This command should return no output on a healthy system.

Note: An NTP alarm will be detected if the system switches are not configured.

```
$ sudo /usr/TKLC/smac/bin/sentry status
```

All Processes should be running, displaying output similar to the following:

```
PM&C Sentry Status
------------------

sentryd started: Mon Jul 23 17:50:49 2012
Current activity mode: ACTIVE
Process              PID     Status             StartTS          NumR
------------------ ------ ----------- ------------------------- ----
smacTalk           9039     running   Tue Jul 24 12:50:29 2012  2
smacMon            9094     running   Tue Jul 24 12:50:29 2012  2
```

```
hpiPortAudit       9137     running   Tue Jul 24 12:50:29 2012  2
snmpEventHandler   9176     running   Tue Jul 24 12:50:29 2012  2
eclipseHelp        9196     running   Tue Jul 24 12:50:30 2012  2


Fri Aug  3 13:16:35 2012
Command Complete.
```

14. Verify the PM&C application release

    Verify that the PM&C application Product Release is as expected.

    Note: If the PM&C application Product Release is not as expected, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

```
$ sudo /usr/TKLC/plat/bin/appRev
        Install Time: Fri Sep 28 15:54:04 2012
        Product Name: PMAC
     Product Release: 5.0.0_50.10.0
     Part Number ISO: 872-2441-905
     Part Number USB: 872-2441-105
Base Distro Product: TPD
Base Distro Release: 6.0.0_80.22.0
     Base Distro ISO: TPD.install-6.0.0_80.22.0-CentOS6.2-x86_64.iso
                  OS: CentOS 6.2
```

15. Logout of the virsh console

    Exit the virsh console session using Appendix I *How to Exit a Guest Console Session on an iLO*.

16. **Management Server iLO:** Exit the TVOE console.

    Run:

```
$ logout
```

    You may now close the iLO browser window.

4.2.3 Gather and Prepare Configuration Files

Use this procedure to gather and prepare configuration files that are required to proceed with the DSR 5.x installation.

Needed Material:

- HP Misc. Firmware DVD
- HP Solutions Firmware Upgrade Pack Release Notes [1]
- Application CD or ISO

If this procedure fails, contact the Tekelec Customer Care Center and ask for assistance.

Gather and prepare configuration files that must be resident on the PM&C. These might be required to proceed with the Application installation after the PM&C has been deployed but before it has been initialized. These files are usually located within a given ISO on physical media (USB or CDROM).

1. Once the PM&C has completed rebooting, but prior to initializing, log into the PM&C as admusr using virsh on the management server iLO.

2. Create any necessary destination subdirectories in the PM&C **/usr/TKLC/smac/etc** directory if not using an existing directory to transfer files.
3. Make the media available to the TVOE Host server. Mount the media on the TVOE Host using one of the following methods:
   a) If the Application ISO is on a physical CDROM disk:
      1. Insert the disk into the CDROM drive of the TVOE Host Server.
      2. Determine the CDROM of the TVOE Host server by executing the following command:

```
$ sudo /usr/TKLC/plat/bin/getCDROM
```

      Example:

      `/dev/sr0` (the physical Optical Drive for this server)

      `/dev/sr1` (Virtual Optical Drive)

      Note: sr0 is always designated as the CDROM device. There could be additional devices listed by the command if in use.

      3. Make a temporary mount point and mount the optical media.

```
$ sudo /bin/mkdir /media/cdrom
$ sudo /bin/mount /dev/sr0 /media/cdrom
```

      Note: Once mounted, this gives a direct path to the ISO on the CDROM device.

   b) If using a USB Drive:
      1. Insert the USB into an available USB slot on the TVOE Host server and execute the following command to determine its location and the ISO to be mounted:

```
$ sudo /bin/ls /media/*/*.iso
```

      Example: `/media/sdd1/872-2507-111-4.1.0_41.16.2-DSR-x86_64.iso`

      Note: The USB device is immediately added to the list of media devices once it is inserted into a USB slot on the TVOE Host server.

      2. Note the device directory name under the media directory. This could be sdb1, sdc1, sdd1, sde1, depending on the USB slot the media was inserted into.
      3. Loop mount the ISO to the standard TVOE Host mount point (if it is not already in use):

```
$ sudo /bin/mount -o loop /media/<device directory>/<ISO Name>.iso /mnt/upgrade
```

4. Execute the following commands on the PM&C guest to copy the required files from the TVOE host to the PM&C guest.

   Wildcards can be used as necessary.

   a) If the application is on a physical disk:

```
$ sudo /usr/bin/scp -r
admusr@<TVOE_management_ip_address>:/media/cdrom/upgrade/overlay/* /<path to
destination directory>
```

b) If using a USB Drive:

```
$ sudo /usr/bin/scp -r admusr@<TVOE_management_ip_address>:/mnt/upgrade/overlay/*
 /<path to destination directory>
```

5. Remove the application media from the TVOE host:
   a) If the application is on a physical disk:

```
$ sudo /bin/umount /media/cdrom
$ sudo /bin/rmdir /media/cdrom
```

   b) If using a USB Drive:

```
$ sudo /bin/umount /mnt/upgrade
```

   c) Remove the DSR 5.x application media, optical or USB, from the management server.

6. **Management server:** Copy IOS images into place (this will copy both the 4948E and 3020 IOS images into place).
   a) Insert the *Misc. Firmware* media into the CD or USB drive of the management server. For this step, be sure to use the correct IOS version specified by the *Firmware Upgrade Pack Release Notes[1].* Copy each IOS image called out by the release notes [1].
   b) If using a CDROM drive, mount it using the following command. If using a USB, skip this command as it will get auto-mounted:

```
# mount /dev/sr0 /media/cdrom
```

   c) Execute the following commands to copy the required files. Note that the **<PMAC Management_IP Address>** is the one used to deploy PM&C in procedure 4, step 3.

```
$ sudo /usr/bin/scp –p /media/cdrom/files/<4948E_IOS_image_filename> root@<PMAC
Management_IP Address>:/var/TKLC/smac/image
$ sudo /usr/bin/scp –p /media/cdrom/files/<3020(6120)_IOS_image_filename>
root@<PMAC Management_IP Address>:/var/TKLC/smac/image
```

   Note that If both 3020 and 6120 enclosure switches are present, make sure you copy the images for both type of switches by re-running the previous command.

   d) If using a CDROM drive, unmount it using the following command:

```
# umount /media/cdrom
```

   e) Remove the *Misc. Firmware* media from the drive.

4.3 Configure Aggregation Switches

4.3.1 Configure netConfig Repository

This procedure will configure the netConfig repository for all required services and for each switch to be configured.

At any time, you can view the contents of the netConfig repository by using one of the following commands:

- For switches, use the command: **sudo /usr/TKLC/plat/bin/netConfig --repo listDevices**
- For services, use the command: **sudo /usr/TKLC/plat/bin/netConfig --repo listServices**

Users returning to this procedure after initial installation should run the above commands and note any devices and/or services that have already been configured. Duplicate entries cannot be added; if changes to a repository entry are necessary, you must delete the original entry first:

- For switches, use the command: **sudo /usr/TKLC/plat/bin/netConfig --repo deleteDevice name=<device>**
- For services, use the command: **sudo /usr/TKLC/plat/bin/netConfig --repo deleteService name=<service>**

Terminology

The term 'netConfig server' refers to the entity where netConfig is executed. This may be a virtualized or physical environment. 'Management server' may also accurately describe this location but has been historically used to describe the physical environment while 'Virtual PM&C' was used to describe the virtualized netConfig server. Use of the term 'netConfig server' to describe dual scenarios of physical and virtualized environments will allow for future simplification of network configuration procedures.

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within "<>". Fill these worksheets out based on NAPD, and then refer back to these tables for the proper value to insert depending on your system type.

Variable	Value
<management_server_iLO_ip>	
<netConfig_server_mgmt_ip_address>	
<switch_backup_user>	admusr
<switch_backup_user_password>	See application documentation

For the first aggregation switch(4948, 4948E, or 4948E-F): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<device_model>	
<console_name>	

Variable	Value
<switch_console_password>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_mgmt_ip_address>	

For the second aggregation switch(4948, 4948E, or 4948E-F): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<device_model>	
<console_name>	
<switch_console_password>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_mgmt_ip_address>	

For each enclosure switch(6120XG, 6125G, or 3020): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<io_bay>	
<OA1_enX_ip_address>	X= the enclosure #
<OA_password>	

For each enclosure switch(6120XG, 6125G, or 3020): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	

Variable	Value
<switch_platform_password>	
<switch_enable_password>	
<io_bay>	
<OA1_enX_ip_address>	X= the enclosure #
<OA_password>	

1. **Management server iLO**: Log in and launch the integrated remote console. Follow *How to Access a Server Console using the iLO* to access the server console

   Follow Appendix G to log in to the management server iLO as admusr.

   a) On the management server, log in to iLO in IE using password provided by application: `http://<management_server_iLO_ip>`
   b) Click in the Remote Console tab and launch the Remote Console on the server.
   c) Click Yes if the Security Alert dialogue box is displayed.
   d) If not already done so, log in as admusr.

2. **Management Server**: Procedure pre-check

   If the installation is not designed for a virtual PM&C, log in to PM&C and go to *Step 4*.

   If there is a virtual PM&C, log in to the console of the virtual PM&C.

   - Verify virtual PM&C installation by issuing the following commands as admusr on the management server:

```
$ sudo /usr/bin/virsh list --all
Id Name State
----------------------------------
6 vm-pmac1A running
```

   - If this command provides no output, it is likely that a virtual instance of PM&C is not installed.
     - If there is a virtual PM&C, log in to the console of the virtual PM&C.
     - If the installation is not designed for a virtual PM&C, go to *Step 4*.
   - From the management server, log in to the console of the virtual PM&C instance found above.

     Example:

```
$ sudo /usr/bin/virsh console vm-pmac1A
Connected to domain vm-pmac1A
Escape character is ^]
<Press ENTER key>
CentOS release 6.2 (Final)
Kernel 2.6.32-220.7.1.el6prerel6.0.0_80.13.0.x86_64 on an x86_64
```

If the root user is already logged in, logout and log back in as admusr.

```
[root@pmac ~]# logout
```

```
vm-pmac1A login: admusr
Password:
Last login: Fri May 25 16:39:04 on ttyS4
```

- If this command fails, it is likely that a virtual instance of PM&C is not installed.
- If this is unexpected, refer to application documentation or contact *1.4 Customer Care Center*.

3. **netConfig Server:** Check that the switch templates directory exists:

```
$ /bin/ls -i /usr/TKLC/smac/etc/switch/xml
```

If the command returns an error:

```
ls: cannot access /usr/TKLC/smac/etc/switch/xml/: No such file or directory
```

Create the directory:

```
$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/xml
```

4. **netConfig Server**: Set up netConfig repository with necessary ssh information.

Use netConfig to create a repository entry that will use the ssh service. This command will provide the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> shown as the answer must be entered EXACTLY as they are shown here.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service
Service type? (tftp, ssh, conserver, oa) ssh
Service host? <netConfig_server_mgmt_ip_address>
Enter an option name <q to cancel>: user
Enter the value for user: <switch_backup_user>
Enter an option name <q to cancel>: password
Enter the value for password: <switch_backup_user_password>
Verify Password: <switch_backup_user_password>
Enter an option name <q to cancel>: q
Add service for ssh_service successful
$
```

To ensure that you entered the information correctly, use the following command and inspect the output, which will be similar to the one shown below.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service
Service Name: ssh_service
Type: ssh
Host: 10.250.8.4
Options:
password: C20F7D639AE7E7
user: admusr
$
```

5. **netConfig Server**: Set up netConfig repository with necessary tftp information.

Note: If there are no new Cisco (3020, 4948, 4948E or 4948E-F) switches to be configured, go to *Step 8*.

Use netConfig to create a repository entry that will use the tftp service. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service
Service type? (tftp, ssh, conserver, oa) tftp
Service host? <netConfig_server_mgmt_ip_address>
Enter an option name (q to cancel): dir
Enter a value for dir: /var/TKLC/smac/image/
Enter an option name(q to cancel): q
Add service for tftp_service successful
```

6. **netConfig Server**: Set up netConfig repository with necessary OA information.

   Note: If there are no new HP 6125G switches to be configured, go to *Step 8*.

   Use netConfig to create a repository entry that will use the OA service. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=oa_service_en<enclosure
 #>
Service type? (tftp, ssh, conserver, oa) oa
Service host? <OA1_enX_ip_address>
Enter an option name <q to cancel>: user
Enter the value for user: root
Enter an option name <q to cancel>: password
Enter the value for password: <OA_password>
Verify password:<OA_password>
Enter an option name <q to cancel>: q
Add service for oa_service successful
```

7. **Virtual PM&C**: Run conserverSetup command.

```
$ sudo /usr/TKLC/plat/bin/conserverSetup –s <management_server_mgmt_ip_address>
```

   You will be prompted for the platcfg credentials.

   An example:

```
[admusr@vm-pmac1A]$ sudo /usr/TKLC/plat/bin/conserverSetup -s
<management_server_mgmt_ip_address>
Enter your platcfg username, followed by [ENTER]:platcfg
Enter your platcfg password, followed by [ENTER]:<platcfg_password>
Checking Platform Revision for remote TPD installation...
The remote machine is running:
        Product Name: TPD
 Base Distro Release: 6.5.0_82.7.0
Checking Platform Revision for local TPD installation...
The local machine is running:
        Product Name: PMAC
 Base Distro Release: 6.0.0_80.17.0
Configuring switch 'switch1A_console' console server...Configured.
Configuring switch 'switch1B_console' console server...Configured.
Configuring iptables for port(s) 782...Configured.
```

```
Configuring iptables for port(s) 1024:65535...Configured.
Configuring console repository service...Configured.
bond0 interface: eth01
bond0 interface: eth02
```

- If this command fails, contact Tekelec *1.4 Customer Care Center*.
- Verify the output of the script.
- Verify that your Product Release is based on Tekelec Platform 6.5 (versions 6.5.x_x.x.x).
- Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.

8. **netConfig Server**: Set up netConfig repository with aggregation switch information.

   Note: If there are no new aggregation switches to be configured, go to *Step 9*.

   Use netConfig to create a repository entry for each switch. The initial command will prompt the user multiple times. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

   - The <device_model> can be 4948, 4948E, or 4948E-F depending on the model of the device. If you do not know, stop now and contact *1.4 Customer Care Center*.
   - The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor? Cisco
Device Model? <device_model>
Should the init oob adapter be added (y/n)? y
Adding consoleInit protocol for switch1A using oob...
What is the name of the service used for OOB access? console_service
What is the name of the console for OOB access? <console name>
What is the device console password? <switch_console_password>
Verify Password: <switch_console_password>
What is the platform access username? <switch_platform_username>
What is the platform user password? <switch_platform_password>
Verify Password: <switch_platform_password>
What is the device privileged mode password? <switch_enable_password>
Verify Password: <switch_enable_password>
Should the live network adapter be added (y/n)? y
Adding cli protocol for <hostname> using network...
What is the address used for network device access? <switch_mgmt_ip_address>
Should the live oob adapter be added (y/n)? y
Adding cli protocol for <hostname> using oob...
OOB device access already set: console_service
Device named switch1A successfully added.
```

   To check that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

   and check the output, which will be similar to the one shown:

```
$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>
Devices: Device: <switch_hostname> Vendor: Cisco Model: <device_model> Access:
Network: <enclosure_switch_IP> Access: OOB: Service: console_service Console:
<console_name> Init Protocol Configured Live Protocol Configured
$
```

Repeat this step for each 4948 / 4948E / 4948 E-F, using appropriate values for those switches.

9. **netConfig Server**: Set up netConfig repository with 3020 switch information.

   Note: If there are no new 3020s to be configured, go to *Step 10*.

   Use netConfig to create a repository entry for each 3020. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

   - If you do not know any of the required answers, stop now and contact *1.4 Customer Care Center*.
   - The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor? Cisco
Device Model? 3020

Should the init network adapter be added (y/n)? y

Adding netBootInit protocol for <switch_hostname> using network...
What is the address used for network device access? <enclosure_switch_ip>
What is the platform access username? <switch_platform_username>
What is the platform user password? <switch_platform_password>
Verify password: <switch_platform_password>

What is the device privileged mode password? <switch_enable_password>
Verify password: <switch_enable_password>


Should the init file adapter be added (y/n)? y

Adding netBootInit protocol for <switch_hostname> using file...
What is the name of the service used for TFTP access? tftp_service


Should the live network adapter be added (y/n)? y

Adding cli protocol for <switch_hostname> using network...
Network device access already set: <enclosure_switch_ip>

Device named <switch_hostname> successfully added.
```

To check that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

and check the output, which will be similar to the one shown below.

```
$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>
Device: <switch_hostname>
    Vendor:   Cisco
    Model:    <device_model>
    Access:   Network: <enclosure_switch_IP>
Access:   OOB:
Init Protocol Configured
Live Protocol Configured
```

Repeat this step for each 3020, using appropriate values for those 3020s.

10. **netConfig Server**: Set up netConfig repository with 6120XG switch information.

    Note: If there are no 6120XGs to be configured, stop and continue with the appropriate switch configuration procedure.

    Use netConfig to create a repository entry for each 6120XG. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

    - If you do not know any of the required answers, stop now and contact *1.4 Customer Care Center*.
    - The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor? HP
Device Model? 6120

Should the init network adapter be added (y/n)? y

Adding sshInit protocol for <switch_hostname> using network...
What is the address used for network device access? <enclosure_switch_ip>
What is the platform access username? <switch_platform_username>
What is the platform user password? <switch_platform_password>
Verify password: <switch_platform_password>

What is the device privileged mode password? <switch_enable_password>
Verify password: <switch_enable_password>


Should the live network adapter be added (y/n)? y

Adding cli protocol for <switch_hostname> using network...
Network device access already set: <enclosure_switch_ip>



Should the live oob adapter be added (y/n)? n



Device named <switch_hostname> successfully added.
```

    To check that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

    and check the output, which will be similar to the one shown:

```
$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>
Devices:
Device: <switch_hostname>
Vendor: HP
Model: 6120
FW Ver: 0
Access: Network: <enclosure_switch_IP>
Init Protocol Configured
Live Protocol Configured
$
```

    Repeat this step for each 6120, using appropriate values for those 6120s.

11. **netConfig Server:** Set up netConfig repository with 6125G switch information.

    Note: If there are no 6125Gs to be configured, stop and continue with the appropriate switch configuration procedure.

    Use netConfig to create a repository entry for each 6125G. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.

    - If you do not know any of the required answers, stop now and contact *1.4 Customer Care Center*
    - The device name must be 20 characters or less.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname>
--reuseCredentials
Device Vendor? HP
Device Model? 6125
Should the live network adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using network...
What is the address used for network device access? <enclosure_switch_ip>
What is the platform access username? <switch_platform_username>
What is the platform user password? <switch_platform_password>
Verify password: <switch_platform_password>
What is the device privileged mode password? <switch_platform_password>
Verify password: <switch_platform_password>
Should the live oob adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using oob...
What is the name of the service used for OOB access? oa_service_en<enclosure #>
What is the name of the console for OOB access? <io_bay>
What is the device console password? <switch_platform_password>
Verify password: <switch_platform_password>

Should the init oob adapter be added (y/n)? y

Adding consoleInit protocol for <switch_hostname> using oob...
OOB device access already set: oa_service

Device named 6125G_IOBAY3 successfully added.
```

To check that you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
```

and check the output, which will be similar to the one shown:

```
$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>
Device: <switch_hostname>
Vendor: HP
Model: 6125
FW Ver:   0


Access: Network: <enclosure_switch_IP>
Access:   OOB:
Service: oa_service
Console: <io_bay>
Init Protocol Configured
Live Protocol Configured
$
```

4.3.2 Configure Cisco 4948/4948E/4948E-F aggregation switches (PM&C installed)(netConfig)

This procedure will configure 4948/4948E/4948E-F switches with an appropriate IOS and configuration from a single management server and virtual PM&C for use with the c-Class or RMS platform.

Procedure Reference Tables:

Steps within this procedure may refer to variable data indicated by text within "<>". Refer to this table for the proper value to insert depending on your system type.

Variable	Serial Port
<switch1A_serial_port>	ttyS4
<switch1B_serial_port>	ttyS5

Fill in the appropriate value from [3].

Variable	Cisco 4948	Cisco 4948E	Cisco 4948E-F
<IOS_image_file>			
<PROM_image_file>			

Fill in the appropriate value for this site:

Variable	Value
<switch_platform_username>	See referring application documentation
<switch_platform_password>	See referring application documentation
<switch_console_password>	See referring application documentation
<switch_enable_password>	See referring application documentation
<management_server_mgmt_ip_address>	
<pmac_mgmt_ip_address>	
<switch_mgmtVLAN_id>	
<switch1A_mgmtVLAN_ip_address>	
<mgmt_Vlan_subnet_id>	
<netmask>	
<switch1B_mgmtVLAN_ip_address>	
<switch_Internal_VLANS_list>	
<management_server_mgmtInterface>	
<management_server_iLO_ip>	
<customer_supplied_ntp_server_address>	

Variable	Value
<platcfg_password>	Refer to TR006061 for this value
<management_server_mgmtInterface>	Value gathered from NAPD
<switch_backup_user>	admusr
<switch_backup_user_password>	Check application documentation

Note: The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.

Note: Uplinks must be disconnected from the customer network prior to executing this procedure. One of the steps in this procedure will instruct when to reconnect these uplink cables. Refer to the application appropriate schematic or procedure for determining which cables are used for customer uplink.

Needed Material:

- Tekelec's HP Misc. Firmware USB media or ISO file
- HP Solutions Firmware Upgrade Pack Release Notes [3]
- Template xml files on the application media.

Note: Filenames and sample command line input/output throughout this section do not specifically reference the 4948E-F. Template settings are identical between the 4948E and 4948E-F. The original 4948 switch -- as opposed to the 4948E or the 4948E-F is referred to simply by the model number 4948. Where all three switches are being referred to, this will be made clear by reference to '4948 / 4948E / 4948 E-F' switches.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Virtual PM&C**: Run conserverSetup command.

```
$ sudo /usr/TKLC/plat/bin/conserverSetup –s <management_server_mgmt_ip_address>
```

You will be prompted for the platcfg credentials.

An example:

```
[admusr@vm-pmac1A]$ sudo /usr/TKLC/plat/bin/conserverSetup -s
<management_server_mgmt_ip_address>
Enter your platcfg username, followed by [ENTER]:platcfg
Enter your platcfg password, followed by [ENTER]:<platcfg_password>
Checking Platform Revision for remote TPD installation...
The remote machine is running:
        Product Name: TPD
 Base Distro Release: 6.5.0_82.7.0
Checking Platform Revision for local TPD installation...
The local machine is running:
        Product Name: PMAC
 Base Distro Release: 6.0.0_80.17.0
Configuring switch 'switch1A_console' console server...Configured.
Configuring switch 'switch1B_console' console server...Configured.
Configuring iptables for port(s) 782...Configured.
Configuring iptables for port(s) 1024:65535...Configured.
Configuring console repository service...Configured.
bond0 interface: eth01
bond0 interface: eth02
```

- If this command fails, contact Tekelec *1.4 Customer Care Center*.
- Verify the output of the script.
- Verify that your Product Release is based on Tekelec Platform 6.5 (versions 6.5.x_x.x.x).
- Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.

2. **Virtual PM&C:** Verify the IOS image is on the system. If the appropriate image does not exist, copy the image to the PM&C.

   Determine if the IOS image for the 4948/4948E/4948E-F is on the PM&C.

```
$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file>
```

   If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by the Firmware Upgrade Pack Release Notes *[3]*

3. **Virtual PM&C:** Get IOS image and PROM information on the switches.

   Note: ROM & PROM are intended to have the same meaning for this procedure

   Connect to switch1A, check the IOS and PROM version.

   Connect serially to switch1A by issuing the following command.

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
switch1A_console
Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ec?' for help]
Press Enter
Switch> show version | include image
System image file is "bootflash:cat4500-ipbasek9-mz.122-53.SG2.bin"
Switch> show version | include ROM
ROM: 12.2(31r)SGA1
System returned to ROM by reload
```

   Note: If the console command fails, contact Tekelec Customer Care Center.

   Note the IOS image & ROM version for comparison in a following step.

```
To exit from the console, enter <ctrl-e><c><.> and you will be returned to the
server prompt.
```

   Connect to switch1B, check the IOS and PROM version.

   Connect serially to switch1B by issuing the following command:

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
switch1B_console
Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ec?' for help]
Press Enter
Switch> show version | include image
System image file is "bootflash:cat4500-ipbasek9-mz.122-53.SG2.bin"
Switch> show version | include ROM
ROM: 12.2(31r)SGA1
System returned to ROM by reload
```

   Note: If the console command fails, contact Tekelec Customer Care Center.

Note the IOS image & ROM version for comparison in a following step.

```
 To exit from the console, enter <ctrl-e><c><.> and you will be returned to the
server prompt.
```

4. **Virtual PM&C:** Determine if switch IOS and/or PROM upgrade is required.

   Compare the IOS and PROM version from previous step with the version specified in the *HP Solutions Firmware Upgrade Pack* for the switch model being used.

   Check the version from the previous step against the version from the release notes referenced. If the versions are different, or if the IOS version from the previous step does not have "k9" in the name, then an upgrade is necessary. Check below for the appropriate action.

   FOLLOW ONE OF THESE CHOICES:

   - If switch1A or both switches require an upgrade, then continue to the next step.
   - If switch1B requires an upgrade, skip to step 16.
   - If neither switch requires an upgrade, then skip to step 18.

5. **Virtual PM&C:** Verify IOS & PROM images on the system. If the appropriate image does not exist, copy the image to the PM&C and upload the switch.

   Determine if the IOS & PROM images for the 4948/4948E/4948E-F is on the PM&C.

```
$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file>
$ /bin/ls -i /var/TKLC/smac/image/<PROM_image_file>
```

   If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by the Firmware Upgrade Pack Release Notes *[3]*

6. **Virtual PM&C**: Modify PM&C Feature to allow TFTP.

   Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:

```
$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
 --enable=1
$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
```

   Note: This may take up to 60 seconds to complete.

7. **Virtual PM&C -> Management Server:** Manipulate host server physical interfaces.

   Note: On a TVOE host, If you launch the virsh console, i.e., "# **`virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**`ps -ef |grep virsh`**", then kill the existing process "**`kill -9 <PID>`**". Then execute the "virsh console X" command. Your console session should now run as expected.

   Exit from the virtual PM&C console by following the instructions in Appendix I *How to Exit a Guest Console Session on an iLO*. This will return the terminal to the server prompt.

   If upgrading the IOS or PROM on switch1A:

Ensure that the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface by performing the following commands:

```
$ sudo /sbin/ifup <ethernet_interface_1>
$ sudo /sbin/ifdown <ethernet_interface_2>
$ sudo /sbin/ip addr show <management_server_mgmtInterface> | grep inet
```

The command output should contain the IP address of the variable **<management_server_mgmt_ip_address>**

If upgrading the IOS or PROM on switch1B:

Ensure that the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface by performing the following commands:

```
$ sudo /sbin/ifup <ethernet_interface_2>
$ sudo /sbin/ifdown <ethernet_interface_1>
$ sudo /sbin/ip addr show <management_server_mgmtInterface> | grep inet
```

The command output should contain the IP address of the variable **<management_server_mgmt_ip_address>**

Connect to the Virtual PMAC by logging into the console of the virtual pmac instance found in procedure 3.1.1 Step 2.

```
$ sudo /usr/bin/virsh console vm-pmac1A
```

8. **Virtual PM&C:** Attach to switch console.

   If upgrading the firmware on switch1A, connect serially to switch1A by issuing the following command as admusr on the PM&C server:

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
switch1A_console
Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ec?' for help]
Press Enter
```

   If the switch is not already in enable mode ("switch#" prompt) then issue the "**enable**" command, otherwise continue with the next step.

```
Switch> enable
Switch#
```

   If upgrading the firmware on switch1B, connect serially to switch1B by issuing the following command as admusr on the PM&C server:

```
$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg
switch1B_console
Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ec?' for help]
Press Enter
```

If the switch is not already in enable mode ("switch#" prompt), then issue the "**enable**" command, otherwise continue with the next step.

```
Switch> enable
Switch#
```

9. **Virtual PM&C (switch console session):** Configure ports on the 4948/4948E/4948E-F switch. To ensure connectivity, ping the management server's management vlan ip address from the switch.

   Platform version specific to be on the management vlan:

```
Switch# conf t
```

If upgrading the firmware on switch1A, use these commands:

```
Switch(config)# vlan <switch_mgmtVLAN_id>
Switch(config-vlan)# int vlan <switch_mgmtVLAN_id>
Switch(config-if)# ip address <switch1A_mgmtVLAN_ip_address> <netmask>
Switch(config-if)# no shut
Switch(config-if)# int gi1/40
```

If upgrading the firmware on switch1B, use these commands:

```
Switch(config)# vlan <switch_mgmtVLAN_id>
Switch(config-vlan)# int vlan <switch_mgmtVLAN_id>
Switch(config-if)# ip address <switch1B_mgmtVLAN_ip_address> <netmask>
Switch(config-if)# no shut
Switch(config-if)# int gi1/40
```

If the model is 4948, execute these commands:

```
Switch(config-if)# switchport trunk encap dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree portfast trunk
Switch(config-if)# end
Switch# write memory
```

If the model is 4948E or 4948E-F, execute these commands:

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree portfast trunk
Switch(config-if)# end
Switch# write memory
```

Now issue ping command:

Note: The ip address**<pmac_mgmt_ip_address>** should be in the reference table at the beginning of this procedure.

```
Switch# ping <pmac_mgmtVLAN_ip_address>
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to <pmac_mgmt_ip_address>, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round trip min/avg/max = 1/1/4 ms
```

If ping is not successful , double check that the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact Customer Care Center.

10. **Virtual PM&C (Switch console session):** Upgrade PROM

    If upgrading the PROM, continue, otherwise skip to Step 13.

```
Switch# copy tftp: bootflash:
Address or name of remote host []? <pmac_mgmt_ip_address>

Source filename []? <PROM_image_file>
Destination filename [<PROM_image_file>]? [Enter]
Accessing tftp://<pmac_mgmt__ip_address>/<PROM_image_file>...
Loading <PROM_image_file> from <pmac_mgmt__ip_address> (via Vlan2): !!!!!! [OK –
 45606 bytes]

45606 bytes copied in 3.240 secs (140759 bytes/sec)
Switch#
```

11. **Virtual PM&C (Switch console session):** Reload the switch

```
Switch# reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm] [Enter]
=== Boot messages removed ===
```

    Type **[Control-C]** when *Type control-C to prevent autobooting* is displayed on the screen.

12. **Virtual PM&C (Switch console session):** Upgrade PROM

```
rommon 1 > boot bootflash:<PROM_image_file>

=== PROM upgrade messages removed ===

System will reset itself and reboot within few seconds....
```

13. **Virtual PM&C (Switch console session):** Verify Upgrade

    The switch will reboot when the firmware upgrade completes. Allow it to boot up. Wait for the following line to be printed:

```
Press RETURN to get started!
Would you like to terminate autoinstall? [yes]: [Enter]
Switch> show version | include ROM
ROM: 12.2(31r)SGA1
System returned to ROM by reload
```

    Review the output and look for the ROM version. Verify that the version is the desired new version. If the switch does not boot properly or has the wrong ROM version, contact Tekelec Customer Care.

14. **Virtual PM&C (switch console session):** Upload the IOS to the switch and verify.

    On the switch, copy the IOS file over to the switch by issuing the following command sequence:

```
Switch> en
Switch# copy tftp: bootflash:
Address or name of remote host []? <pmac_mgmt_ip_address>
Source filename []? <IOS_image_file>
Destination filename [<IOS_image_file>]? Enter
```

Press Enter here, you do NOT want to change the filename.

```
Accessing tftp://<pmac_mgmt_ip_address>/<IOS_image_file>...
Loading <IOS_image_file> from <pmac_mgmt_ip_address> (via Vlan2):
!!!!!! [OK – 45606 bytes]
45606 bytes copied in 3.240 secs (140759 bytes/sec)

Switch# dir bootflash:
Directory of bootflash:/
1 -rwx 17779888 May 11 2011 02:25:23 -05:00
<IOS_image_file>
2 -rwx 17779888 May 11 2011 02:25:23 -05:00
<OLD_IOS_image_file>
60817408 bytes total (43037392 bytes free)
```

15. **Virtual PM&C (switch console session):** Set the active IOS image and config-register from the switch console session that was established.

    Set the active IOS image:

```
Switch# conf t
Switch(config)# boot system flash bootflash:<ios_image_file>
Switch(config)# no boot system flash bootflash:<OLD_IOS_image_file>
Switch(config)# config-register 0x2102
Switch(config)# end
Switch# write memory
Switch#
```

    Verify the changes:

```
Switch# show run | include boot
boot-start-marker
boot system flash bootflash: <ios_image_file>
boot-end-marker

Switch# show version | include register
Configuration register is 0xXXXX (will be 0x2102 at next reload)

Switch# reload
Proceed with reload? [confirm]
```

    Wait until the switch reloads, then issue the following command to ensure the switch is at the appropriate IOS version:

```
Switch> show version | include image
System image file is <IOS_image_file>"
```

    Note: You might see an additional prompt:

```
System Config has been modified. Save? [yes|no] no
```

    If the switch is not at the appropriate version, stop here and contact Customer Care Center. If it is, move on to the next step.

16. **Virtual PM&C (switch console session):** Delete any other IOS images if there are multiple IOS images on the switch, delete the unused images.

```
Switch>en
Switch# show bootflash:
-#- --length-- -----date/time------ path
1 25771102 Jan 20 2012 08:20:08 <ios_image_file>
2 16332568 Jan 24 2012 18:54:44 <OLD_IOS_image>

Switch# delete /force /recursive bootflash:<OLD_IOS_image>
```

Repeat this command until the only file on the switch is <ios_image_file>

Execute the following to remove remaining vlan data and reset the config register.

```
Switch# conf t
Switch(config)# config-register 0x2101
Switch(config)# no vlan 2-4094
Switch(config)# end
```

Note: There might be a switch message saying some default vlans will not be deleted, it is ok to ignore this.

To exit from console, enter **<ctrl-e><c><.>** and you will be returned to the server prompt.

17. **Virtual PM&C:** Repeat for switch1B, if determined to be needed.

Repeat *Step 7* - *Step 16* for switch1B, then continue to the next step.

18. **Virtual PM&C**: Modify PM&C Feature to disable TFTP.

Disable the DEVICE.NETWORK.NETBOOT feature.

```
$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
 --enable=0
$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
```

Note: This may take up to 60 seconds to complete.

19. **Virtual PM&C**: Reset switches to factory defaults.

Connect serially to both switch1A and switch1B as outlined in *Step 7*, and reload each switch by performing the following commands:

```
Switch# write erase
Switch# reload
```

Wait until the switch reloads, then exit from console, enter **<ctrl-e><c><.>** and you will be returned to the server prompt. Wait for the first switch to finish before repeating this process for the second switch.

Note: There might be messages from the switch, if asked to confirm, press enter. If asked yes or no, type in '**no**' and press enter.

20. **Virtual PM&C:**

Verify the initialization xml template file and configuration xml template file is present on the system and is the correct version for the system.

```
$ sudo /bin/more /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml
$ sudo /bin/more /usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml
$ sudo /bin/more /usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml
```

If either file does not exist, copy the files onto the virtual pmac from the application media using application provided procedures. .

21. **Virtual PM&C:** Modify switch1A_4948_4948E_init.xml and switch1B_4948_4948E_init.xml files for information needed to initialize the switch.

    Update the init.xml files for all values preceded by a dollar sign. For example, if a value has $some_variable_name, that value will be modified and the dollar sign must be removed during the modification.

    When done editing the file, save and exit to return to the command prompt.

22. **Virtual PM&C:** Modify `4948_4948E_configure.xml` for information needed to configure the switches.

    Update the configure.xml file for all values preceded by a dollar sign. For example, if a value has $some_variable_name, that value will be modified and the dollar sign must be removed during the modification.

    When done editing the file, save and exit to return to the command prompt.

23. **Virtual PM&C:** Initialize each switch

    Initialize switch1A by issuing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml
$
```

    Note: This step takes about 2-3 minutes to complete.

    Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.

    A successful completion of netConfig will return the user to the prompt.

    Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname

Hostname: switch1A

$
```

    Note: If this command fails, stop this procedure and contact Customer Care Center

    Initialize switch1B by issuing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml
$
```

Note: This step takes about 2-3 minutes to complete.

Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.

A successful completion of netConfig will return the user to the prompt.

Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname

Hostname: switch1B

$
```

Note: If this command fails, stop this procedure and contact Customer Care Center

24. **Virtual PM&C -> Management Server:** Manipulate host server physical interfaces for switch1B.

    Exit from the virtual pmac console, by entering **< ctrl-] >** and you will be returned to the server prompt.

    Ensure that the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface by performing the following commands:

```
$ sudo /sbin/ifup <ethernet_interface_2>
$ sudo /sbin/ifdown <ethernet_interface_1>
$ sudo /sbin/ip addr show <management_server_mgmtInterface> | grep inet
```

    The command output should contain the IP address of the variable

    <management_server_mgmt_ip_address>

    Connect to the Virtual PMAC by logging into the console of the virtual pmac instance found in procedure 3.1.1 Step 2.

```
$ sudo /usr/bin/virsh console vm-pmac1A
```

    Note: On a TVOE host, If you launch the virsh console, i.e "# virsh console X" or from the virsh utility "virsh # console X" command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "ps -ef |grep virsh", then kill the existing process "kill -9 <PID>". Then execute the "virsh console X" command. Your console session should now run as expected.

25. **Virtual PM&C:** Verify switch configuration

    Ping each of the switches' SVI (router interface) addresses to verify switch configuration.

```
# /bin/ping <switch1A_mgmtVLAN_IP>
# /bin/ping <switch1B_mgmtVLAN_IP>
```

26. **Virtual PM&C:** Verify the switch is using the proper IOS image per Platform version.

Issue the following commands to verify the IOS release on each switch:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A listFirmware
Image: cat4500-ipbasek9-mz.122-53.SG2.bin
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B listFirmware
Image: cat4500-ipbasek9-mz.122-53.SG2.bin
```

27. **Management Server**: Ensure both interfaces are enabled on the TVOE host.

    Exit from the virtual PM&C console by following the instructions in Appendix I *How to Exit a Guest Console Session on an iLO*. This will return the terminal to the server prompt.

    Ensure that the interfaces of the server connected to switch1A and switch1B are up by performing the following commands:

```
$ sudo /sbin/ifup <ethernet_interface_1>
$ sudo /sbin/ifup <ethernet_interface_2>
```

28. **Cabinet:** Connect network cables from customer network

    Attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports.

    Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active

29. **Virtual PM&C:** Verify access to customer network

    Verify connectivity to the customer network by issuing the following command:

```
$ /bin/ping <customer_supplied_ntp_server_address>
PING ntpserver1 (10.250.32.51) 56(84) bytes of data.
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms
```

30. **Cabinet:** Connect network cables from customer network

    Attach switch1B customer uplink cables and detach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports.

    Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.

31. **Virtual PM&C:** Verify access to customer network

    Verify connectivity to the customer network by issuing the following command:

```
$ /bin/ping <customer_supplied_ntp_server_address>
PING ntpserver1 (10.250.32.51) 56(84) bytes of data.
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms
64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms
```

32. **Cabinet:** Connect network cables from customer network

    Re-attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports.

    Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active

33. **Management Server:** Restore the TVOE host back to its original state.

    Exit from the virtual PM&C console by following the instructions in Appendix I *How to Exit a Guest Console Session on an iLO*. This will return the terminal to the server prompt.

    Restore the server networking back to original state:

```
$ sudo /sbin/service network restart
```

34. Perform *F.2 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* for each switch configured in this procedure.

4.4 Configure PM&C

4.4.1 Configure NetBackup Feature

If the PM&C application will be configured with the optional NetBackup feature and the NetBackup client will be installed on this server execute the following procedure with the appropriate NetBackup feature data, otherwise continue with next procedure.

4.4.1.1 Configure PM&C application

Configuration of the PM&C application is typically performed using the PM&C GUI. This procedure defines application and network resources. At a minimum, you should define network routes and DHCP pools. Unlike initialization, configuration is incremental, so you may execute this procedure to modify the PM&C configuration.

Note: The installer must be knowledgeable of the network and application requirements. The final step will configure and restart the network and the PM&C application; network access will be briefly interrupted.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **PM&C GUI:** Load GUI and navigate to the Configuration view

   Open web browser and enter:

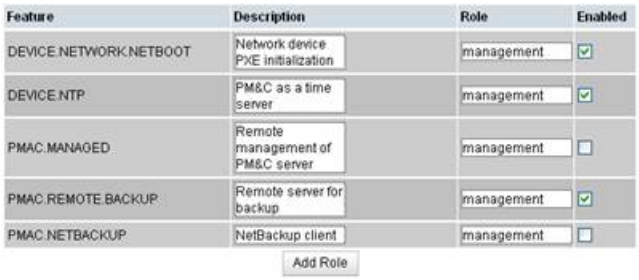
```
https://<pmac_management_network_ip>
```

   Login as pmacadmin user.

Navigate to **Main Menu** > **Administration** > **PM&C Configuration**.

2. **PM&C GUI:** Configure optional features

   If NetBackup is to be used, enable the NetBackup feature. Otherwise use the selected features as is. The following image is for reference only:



   The "**Enabled**" checkbox selects the desired features. The "**Role**" field provides a drop-down list of known network roles that the feature may be associated with. The "**Description**" may be edited if desired.

   If the feature should be applied to a new network role (e.g. "**NetBackup**"), click on the "**Add Role**" button. Enter the name of the new role and click on "**Add**". (Note: role names are not significant, they are only used to associate features with networks). The new role name will appear in the "**Role**" drop-down field for features.

   When done, click on the "**Apply**" button. This foreground task will take a few moments, and then refresh the view with an Info or Error notice to verify the action. To discard changes, just navigate away from the view.

3. **PM&C GUI:** Reconfigure PM&C networks

Note: The Network reconfiguration enters a tracked state. After you click on "**Reconfigure**", you should use a "**Cancel**" button to abort.

Click on "**Network Configuration**" in the navigation pane, and follow the wizard through the configuration task.

1. Click on "**Reconfigure**" to display the "**Network**" view. The default "**management**" and "**control**" networks should be configured correctly. Networks may be added, deleted or modified from this view. They are defined with IPv4 dotted-quad addresses and netmasks. When complete, click on "**Next**".
2. On the "**Network Roles**" view, you may change the role of a network. Network associations can be added (e.g. "**NetBackup**") or deleted. You cannot add a new role since roles are driven from features. When complete, click on "**Next**".
3. On the "**Network Interfaces**" view, you may add or delete interfaces, and change the IP address within the defined network space. If you add a network (again, e.g. "**NetBackup**"), the "**Add Interface**" view is displayed when clicking on "**Add**". This view provides an editable drop-down field of known interfaces. You may add a new device here if necessary. The Address must be an IPv4 host address in the network. When complete, click on "**Next**".
4. On the "**Routes**" view, you may add or delete route destinations. The initial PM&C deployment does not define routes. Most likely you will want to add a default route - the route already exists, but this action defines it to PM&C so it may be displayed by PM&C. Click on "**Add**". The Add Route view provides an editable drop-down field of known devices. Select the egress device for the route. Enter IPv4 dotted-quad addresses and netmask for the route destination, and next-hop gateway. Then click on "**Add Route**". When complete, click on "**Next**".
5. On the "**DHCP Ranges**" view, you will need to define DHCP pools used by servers that PM&C manages. Click on the "**Add**" button. Enter the starting and ending IPv4 address for the range on the network used to control servers (by default, the "**control**" network). Click on "**Add DHCP Range**". Only one range per network may be defined. When all pools are defined, click on "**Next**".
6. The "**Configuration Summary**" provides a view of your reconfigured PM&C. Click "**Finish**" to launch the background task that will reconfigure the PM&C application. A Task and Info or Error notice is displayed to verify your action.
7. Verify your reconfiguration task completes. Navigate to: **Main Menu** > **Task Monitoring**. As the network is reconfigured, you will have a brief network interruption. From the Background Task Monitoring view, verify the "**Reconfigure PM&C**" task succeeds.

4. **PM&C GUI:** Set the PM&C Application GUI Site Settings

   Navigate to **Main Menu** > **Administration** > **GUI Site Settings**

   Set the "**Site name**" to a descriptive name, and set the "**Welcome Message**" that is displayed upon login.

5. **PM&C**: Perform PM&C application backup.

```
$ sudo /usr/TKLC/smac/bin/pmacadm backup
PM&C backup been successfully initiated as task ID 7
$
```

Note: The backup runs as a background task. To check the status of the background task use the PM&C GUI Task Monitor page, or issue the command " **pmaccli getBgTasks** ". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".

Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

6. **PM&C:** Verify the Backup was successful

   Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

   The output of pmaccli getBgTasks should look similar to the example below:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
2: Backup PM&C COMPLETE - PM&C Backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:
2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
::
```

7. **PM&C:** Save the PM&C backup

   The PM&C backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PM&C backup to an appropriate remote server.

4.4.2 Install and Configure NetBackup Client on PM&C

If the PM&C application will be configured with the optional NetBackup feature and the NetBackup client will be installed on this server execute the following procedure with the appropriate NetBackup feature data, otherwise continue with next procedure.

4.4.2.1 PM&C NetBackup Client Installation and Configuration

This procedure provides instructions for installing and configuring the Netbackup client software on a PM&C application.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **PM&C GUI:** Verify the PM&C application guest has been configured with "NetBackup" virtual disk.

   Execute *B.4 Configure PM&C application guest NetBackup virtual disk*.

2. **TVOE Management Server iLO:** Login with PM&C admusr credentials

   Login to iLo using application provided passwords via Appendix G *How to Access a Server Console using the iLO*

Login to iLO in IE using password provided by application:

```
http://<management_server_iLO_ip>
```

Click in the **Remote Console** tab and launch the Integrated Remote Console on the server.

Click **Yes** if the `Security Alert` pops up.

3. **TVOE Management Server iLO:** Login with PM&C admusr credentials

   Note: On a TVOE host, If you launch the virsh console, i.e., "$ **`sudo /usr/bin/virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**`ps -ef |grep virsh`**", then kill the existing process "**`kill -9 <PID>`**". Then execute the "virsh console X" command. Your console session should now run as expected.

   Login to PM&C console using virsh, and wait until you see the login prompt:

```
$ sudo /usr/bin/virsh
virsh # list
 Id    Name                           State
----------------------------------------------------
 4     pmacU17-1                      running

virsh # console pmacU17-1

[Output Removed]

pmacU17-1 login:
```

4. **PM&C:** Perform *B.5 Application NetBackup Client Install/Upgrade Procedures*.

   Note: The following data is required to perform the *B.5 Application NetBackup Client Install/Upgrade Procedures*:

   - The PM&C is a 64 bit application; the appropriate Netbackup client software versions are 7.1 and 7.5.
   - The PM&C application NetBackup user is "NetBackup"; see appropriate documentation for password.
   - The paths to the PM&C application software NetBackup notify scripts are:
     - `/usr/TKLC/smac/sbin/bpstart_notify`
     - `/usr/TKLC/smac/sbin/bpend_notify`
   - For the PM&C application the following is the NetBackup server policy files list:
     - `/var/TKLC/smac/image/repository/*.iso`
     - `/var/TKLC/smac/backup/backupPmac*.pef`

   After executing the *B.5 Application NetBackup Client Install/Upgrade Procedures*, the NetBackup installation and configuration on the PM&C application server is complete.

   Note: At the NetBackup Server the NetBackup policy(ies) can now be created to perform the NetBackup backups of the PM&C application.

4.5 HP C-7000 Enclosure Configuration

Note: This section will apply if the installation includes one or more HP C-7000 Enclosures. It will use the HP Onboard Administrator user interfaces (insight display, and OA GUI) to configure the enclosure settings.

4.5.1 Configure Initial OA IP

This procedure will set initial IP address for Onboard Administrator in location OA Bay 1 (left as viewed from rear) and Bay 2, using the front panel display.

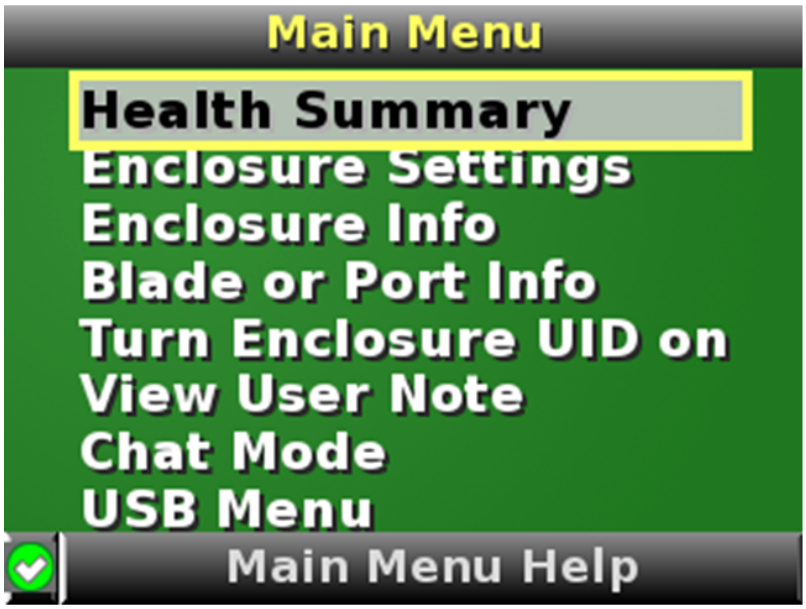
Note: The enclosure should be provisioned with two Onboard Administrators. This procedure needs to be executed only for OABay 1, regardless of the number of OA's installed in the enclosure.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

Configure OA's IP

Configure OA Bay1 IP address using insight display on the front side of the enclosure.

You will see following:



Navigate to **Enclosure Settings** and press **OK**.

Navigate to the **OA1 Ipv4** and press **OK**. Navigate again to the **OA1 Ipv4** and press **OK**.

On the **OA1 Network Mode** screen choose **static** and press **OK**.

On the **OA1 IP address** screen fill in **IP**, **mask** and **gateway**. Press **OK** and then press **Accept All**.

Navigate to "**OA2 Ipv4**" on the Insight display and repeat the above steps to assign the IP parameters of OA2.

4.5.2 Configure initial OA settings via configuration wizard

This procedure will configure initial OA settings using a configuration wizard. This procedure should be used for initial configuration only and should be executed when the Onboard Administrator in OA Bay 1 (left as viewed from rear) is installed and active.

Note: The enclosure should be provisioned with two Onboard Administrators. Note that the OA in Bay 2 will automatically acquire it's configuration from the OA in Bay 1 once the configuration is complete.

Note: This procedure should be used for initial configuration only. Follow Appendix H to learn how to correctly replace one of the Onboard Administrators.

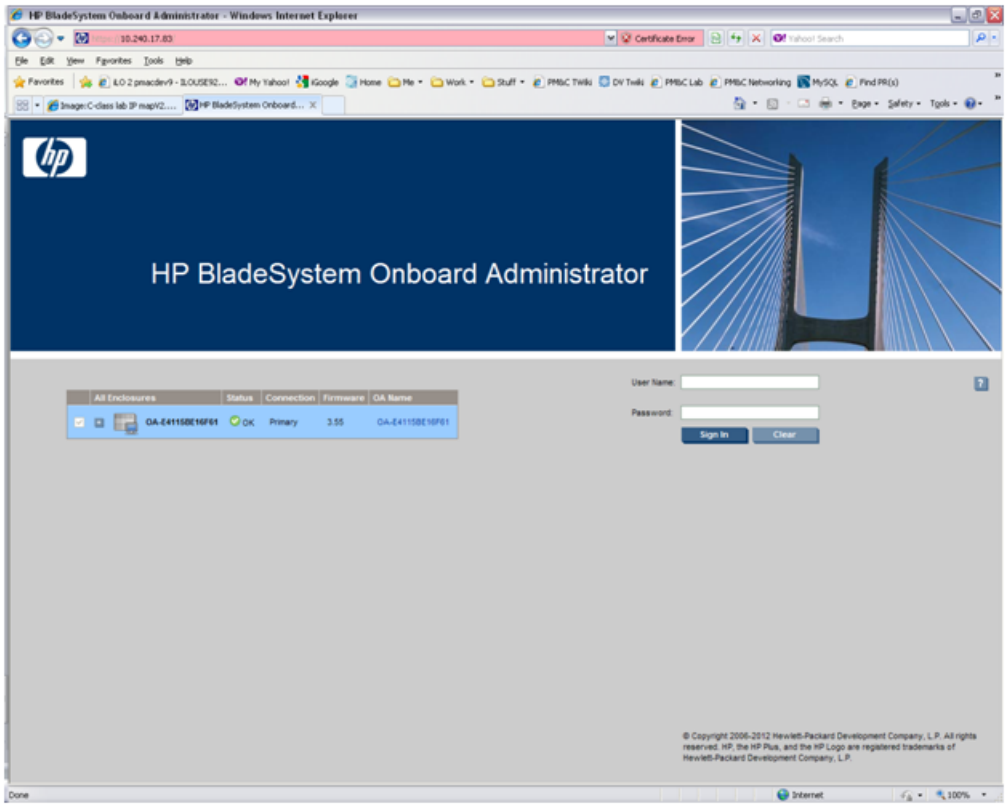
Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **OAGUI:** Login

   Open your web browser and navigate to the OA Bay1 IP address assigned in *4.5.1 Configure Initial OA IP*.

```
http://<OA1_ip>
```

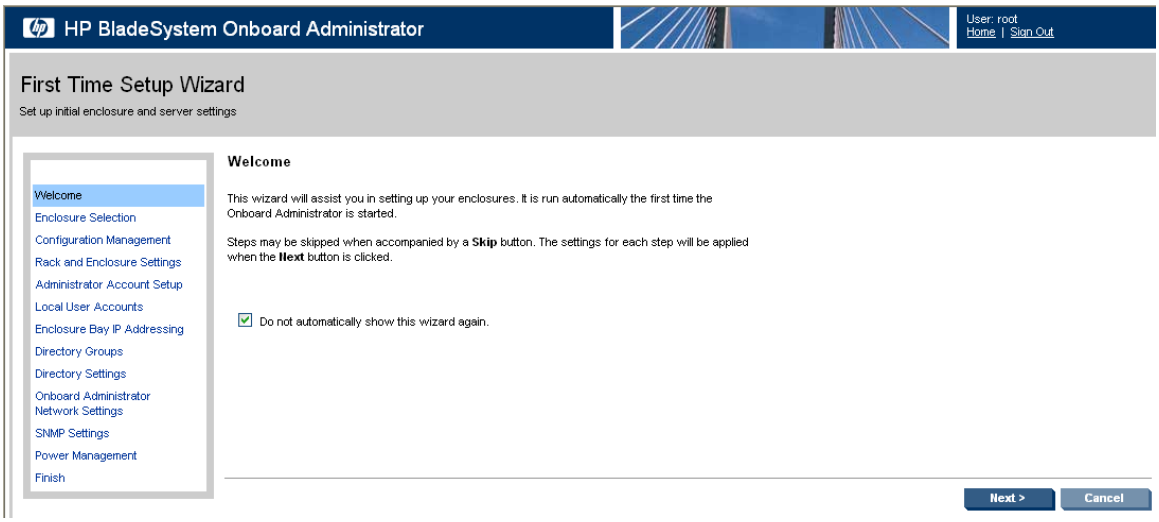
   You will see following:



   Login as an administrative user. Original password is on paper card attached to each OA.

2. **OAGUI:** Run First Time Setup wizard

You will see the main wizard window:



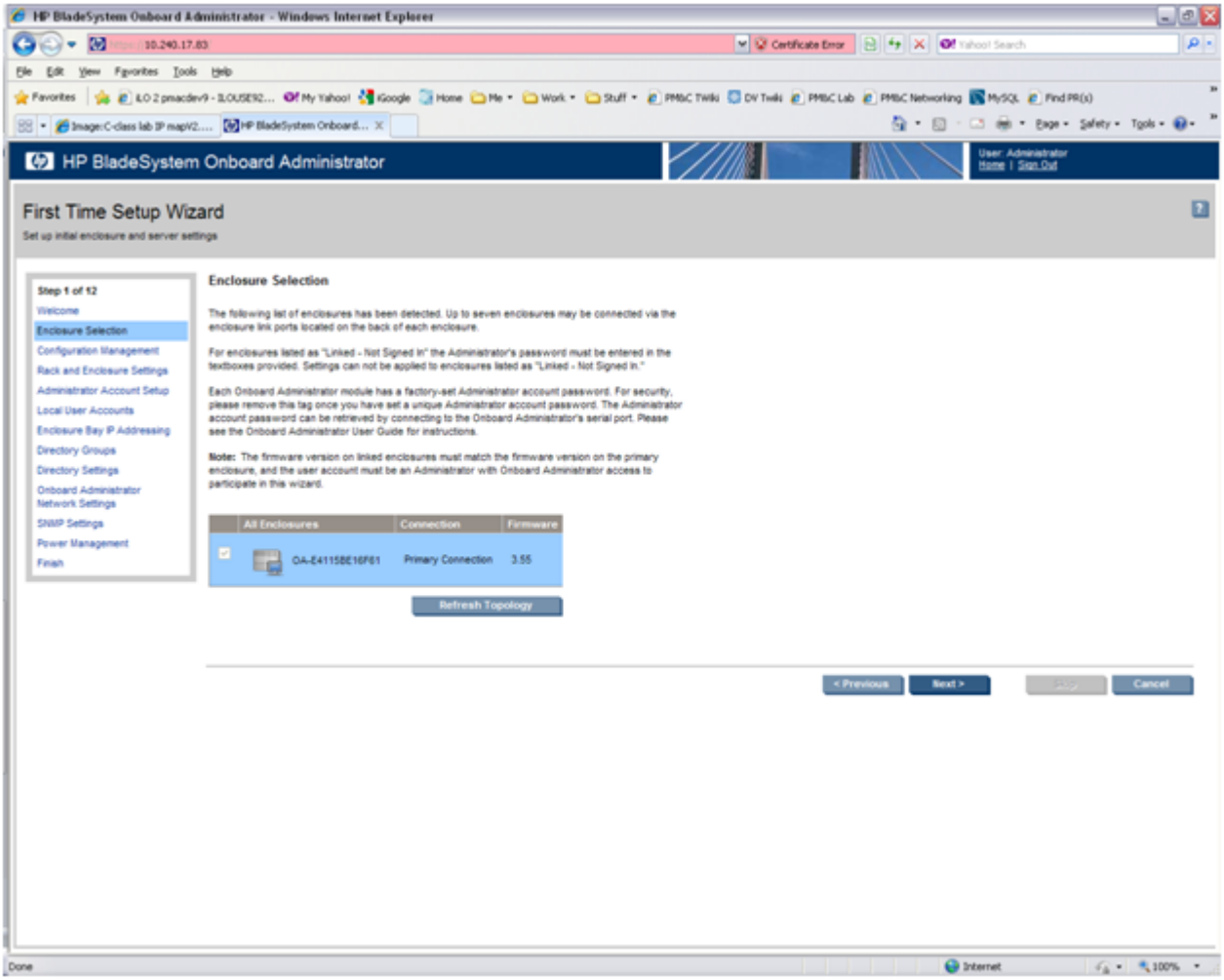
Note: If needed Navigate to **Wizards > First Time Setup** to get to the screen above.

Click on **`Next`** to choose enclosure you want to configure.

You will see **Rack and Enclosure Settings**:

3. **OAGUI:** Select enclosure

   Choose enclosure:



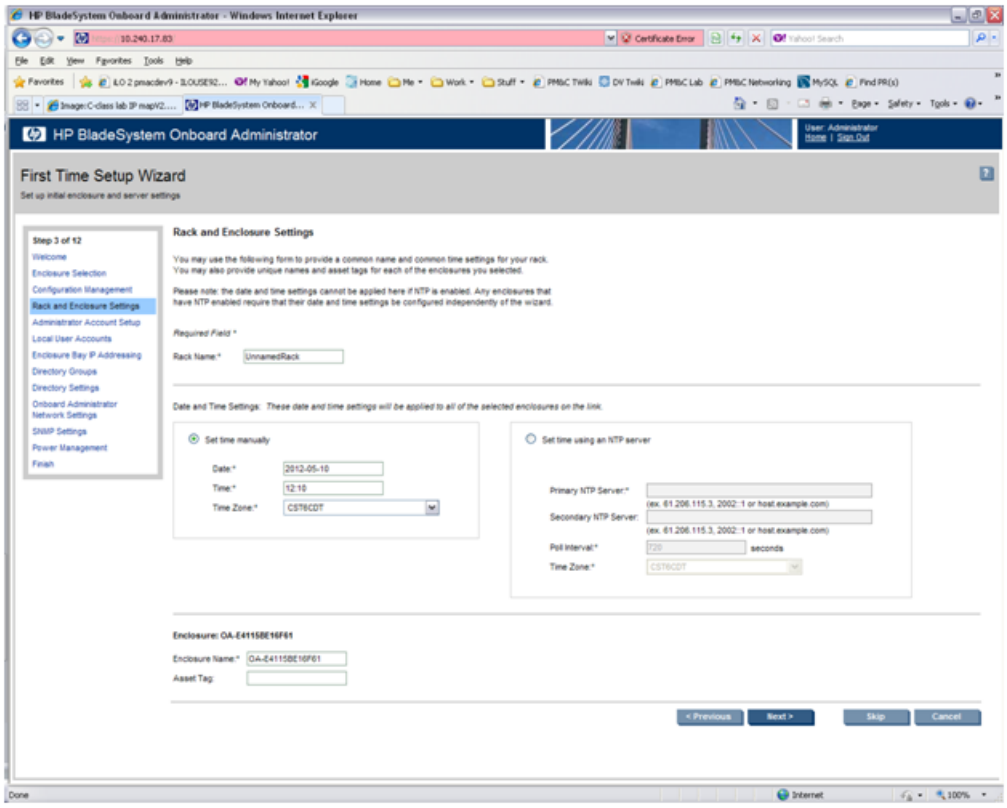
Click on **Next**.

4. **OAGUI:** Skip Configuration Management

   You will see **`Configuration Management.`** Skip this step. Click **Next**.

5. **OAGUI:** Rack and Enclosure Settings

   You should see this screen:



Fill in **Rack Name** in format **`xxx_xx.`**

Fill in **Enclosure name** in format **`<rack name>_<position>`**

Example:

```
Rack Name: 500_03
Enclosure Name: 500_03_03
```

Note: Enclosure positions are numbered from 1 at the bottom of the rack to 4 at the top.

Check **Set time using an NTP server** item and fill in **Primary NTP server** (which is recommended to be set to the **<customer_supplied_ntp_server_address>**).

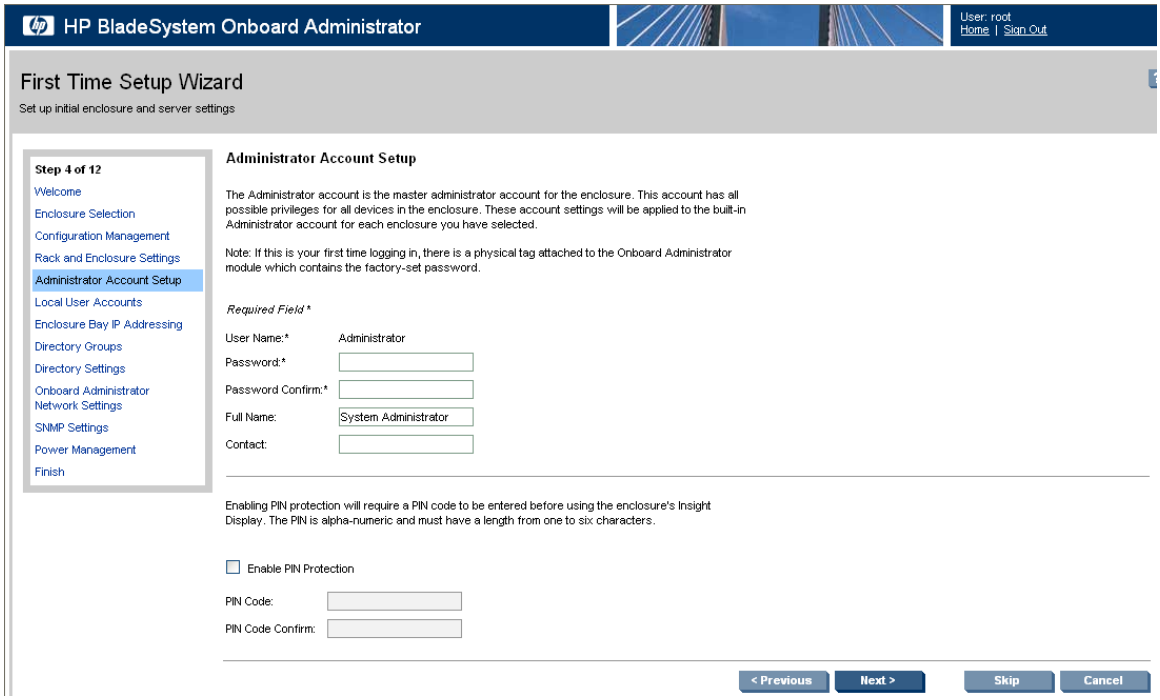
Set **Poll interval** to **720**.

Set **Time Zone** to UTC if customer does not have any specific requirements.

Click on **Next**.

6. **OAGUI:** Change administrator password

   You can see `Administrator Account Setup`:



Change Administrator's password (refer to application documentation) and click on **Next**.

7. **OAGUI:** Create pmacadmin and admusr user.

   On the **`Local User Accounts`** screen click on **New** to add **`pmacadmin`** user.

   You will see **`User Settings`** screen. Fill in **User Name** and **Password**. **Privilege Level** set to **Administrator**. Refer to the application documentation for the password.

   Verify that all of the blades have been checked before proceeding to check the checkbox for **Onboard Administrator Bays** under the `User Permissions` section.

   Then click on **Add User**.

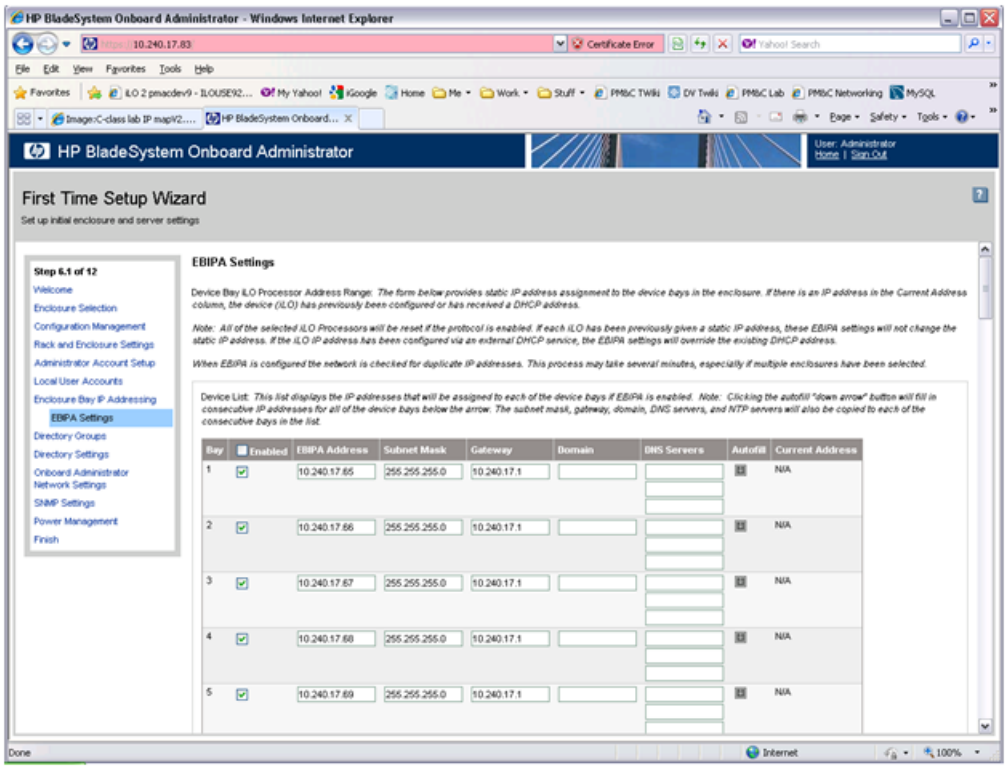
   In the same way create the **admusr** user.

   Then click on **Next**.

8. **OAGUI:** EBIPA settings

   On the **`EBIPA Settings`** (Enclosure Bay IP Addressing) screen click on **Next** to continue or **Skip** if you have already done it. If you pressed **Skip**, go to Step 9 of this procedure.

   Note: Setting up the EBIPA addresses is required.



Go to the Device List section of the EBIPA Settings Screen (at the top).

Fill in the iLO IP, Subnet Mask and Gateway fields for Device Bays 1-16.

Do not fill in the iLO IP, subnet Mask or Gateway fields for Device Bays 1A-16A and 1B-16B

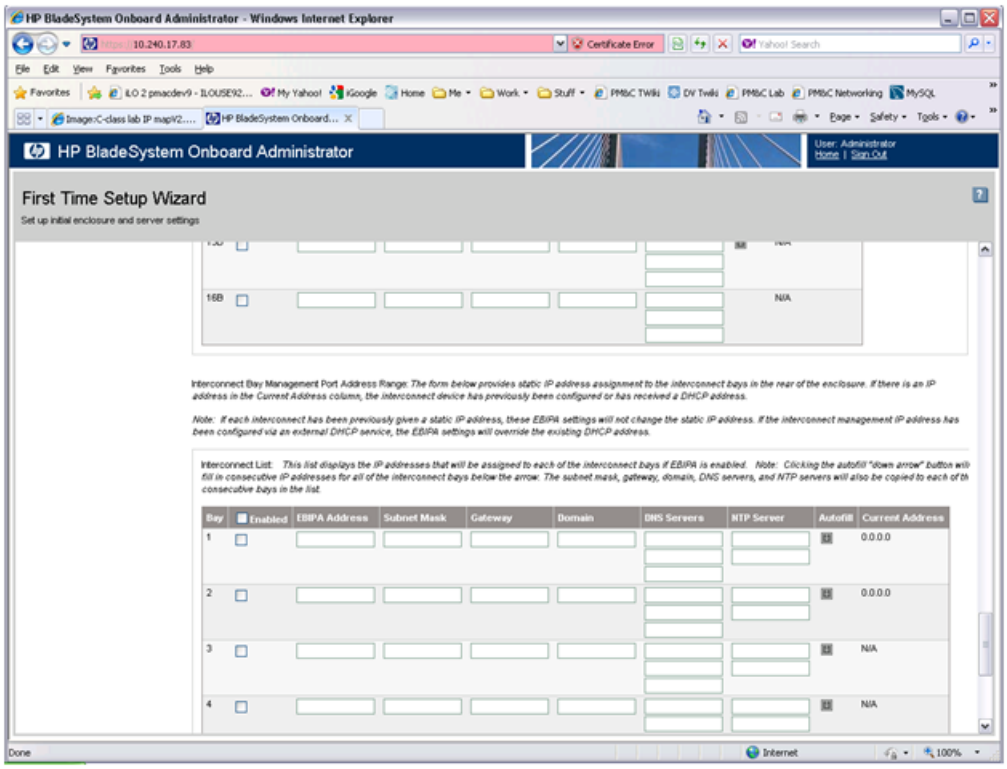
Note: Bays 1A-16A and 1B-16B are used for double-density blades (f.e. BL2x220c) which are not supported in this release.

Click Enabled on each Device Bay 1 through 16 that is in use.

Note: Any unused slots should have an ip address assigned, but should be disabled

Note: Do not use autofill as this will fill the entries for the Device Bays 1A through 16B

Scroll down to the Interconnect List (below Device Bay 16B)



Fill in the EBIPA Address, Subnet Mask and Gateway fields for each Interconnect Bay in use. Click Enable on each Interconnect Bay in use.

By clicking **Next** you will apply those settings. System may restart devices such as interconnect devices or iLOs to apply new addresses. After finishing check the IP addresses to ensure that apply was successful.

9. **OAGUI:** Skip Directory Groups step

   To skip Directory Groups step, click **Next**.

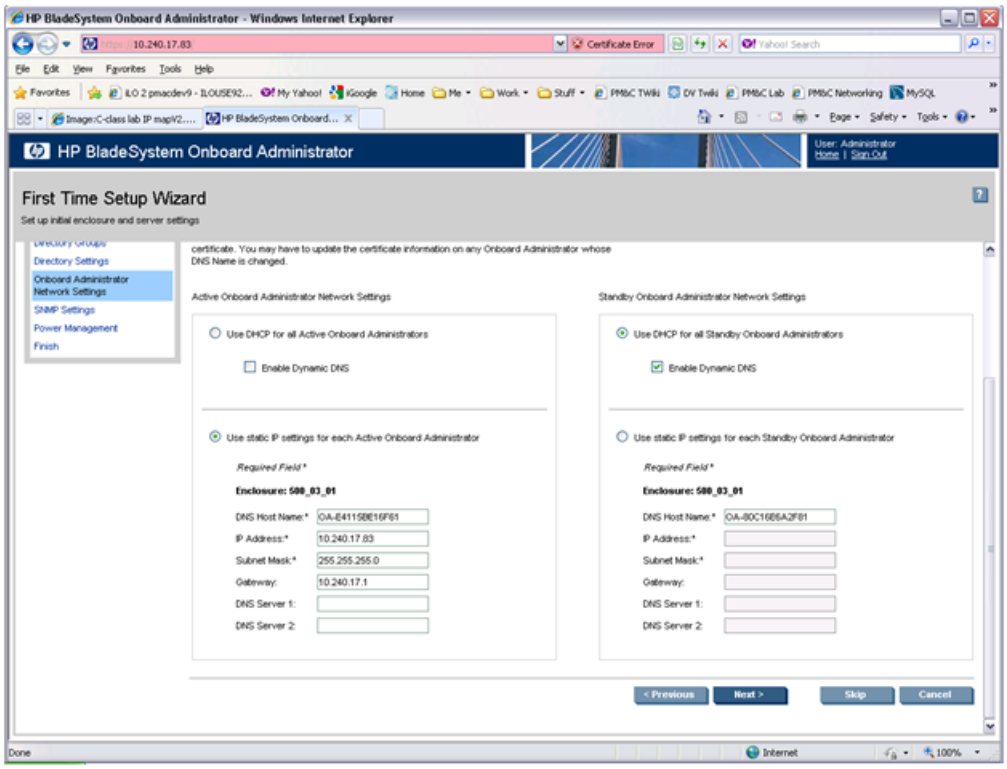
10. **OAGUI:** Skip Directory Settings step

    To skip `Directory Settings` step, click **Next**.

11. **OAGUI:**OA network settings

    On the **`Onboard Administrator Network Settings`** tab you can assign or modify the IP address and the other network settings for the Onboard Administrator(s).

    The **`Active Administrator Network Settings`** pertain to the active OA (OA Bay 1 location during initial configuration). If the second Onboard Administrator is present, the **`Standby Onboard Administrator Network Settings`** will be displayed as well. Click on "Use static IP settings for each Standby Onboard Administrator". Fill in the IP Address, Subnet mask and Gateway for the Standard OA.

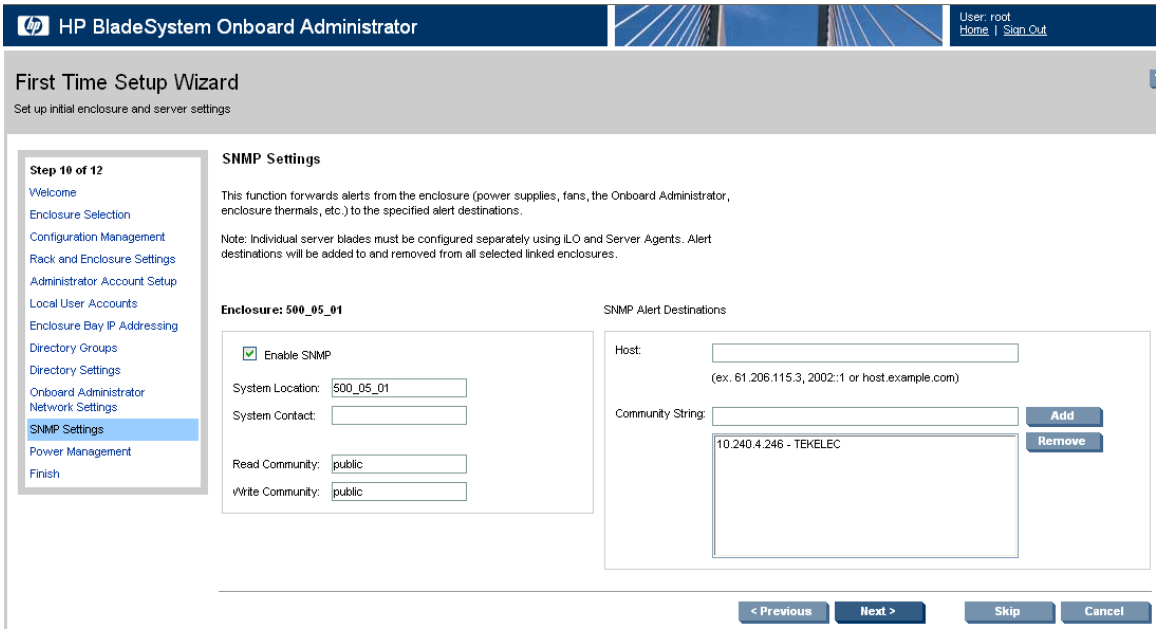


Click on **Next**.

Note: If you change the IP address of the active OA, you will be disconnected. Then you will have to close your browser and sign in again using the new IP address.

12. **OAGUI:**SNMP Settings

    Mark **Enable SNMP**.



Fill in **System Location** that is equal to **`Enclosure name`** you have filled in Step 5.

Do not set **`Read Community`** and **`Write Community`**.

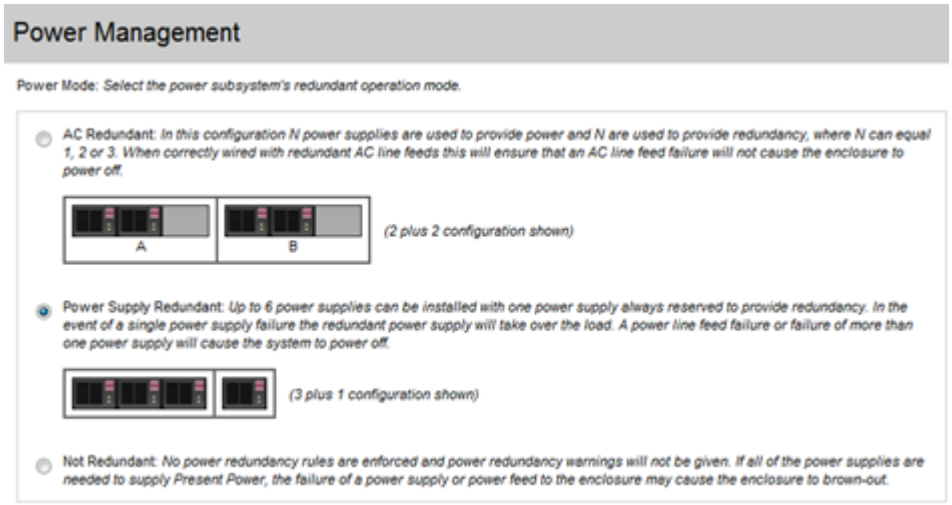
Note: This step does not set an SNMP Trap Destination, to do that see section *4.5.6 Add SNMP trap destination on OA.*.

Click on **Next**.

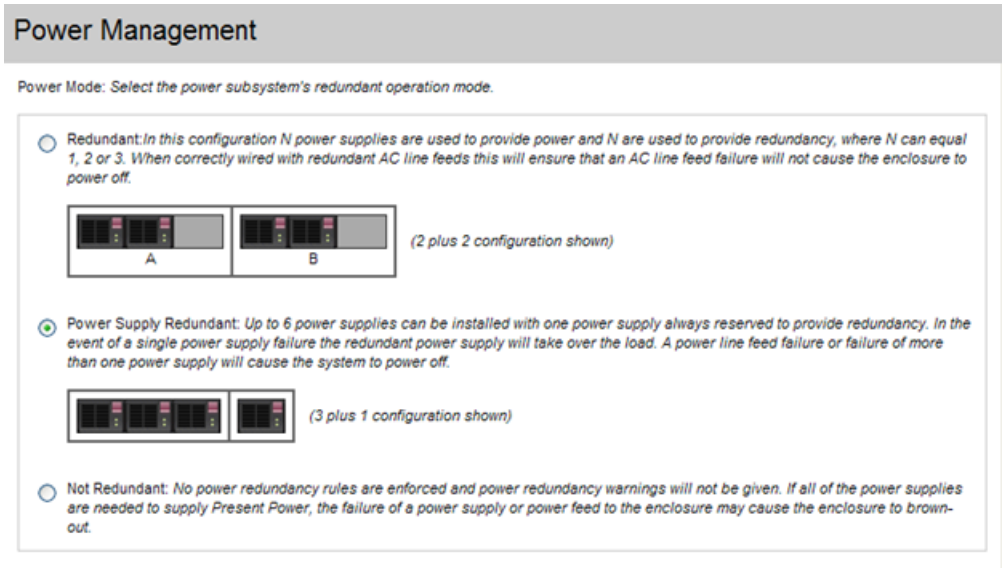
13. **OA GUI:** Power Management

    The Power Mode setting on the Power Management screen must be configured for power supply redundancy. The first available setting on the Power Management screen will be either "AC Redundant" or "Redundant" depending on whether the Enclosure is powered by AC or DC. In either case, select the **second** radio button, "Power Supply Redundant".

    AC-powered Enclosures:



DC-powered Enclosures:



For all other settings on the Power Management screen, leave the default settings unchanged.

Click on **Next**.

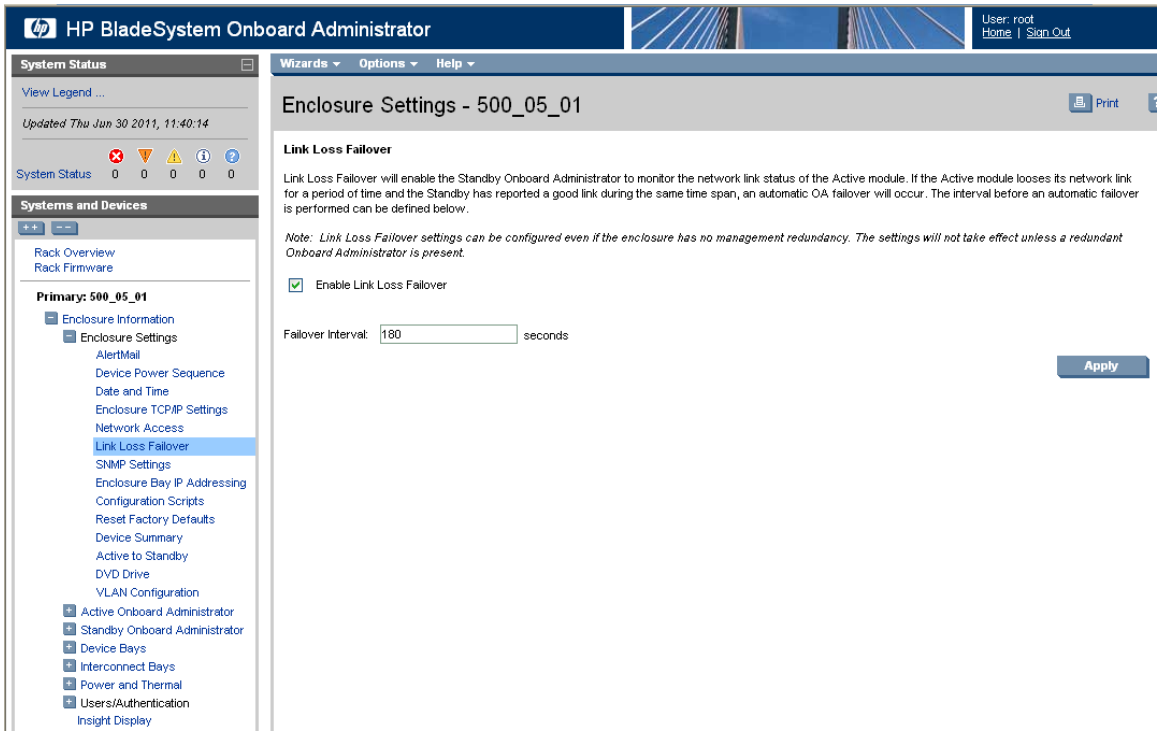
14. **OAGUI:** Finish First Time Setup Wizard

    Click on **Finish**.

    Note: If only one OA has been configured, skip the following step.

15. **OAGUI:** Set Link Loss Failover

    Navigate to **Enclosure Information > Enclosure Settings > Link Loss Failover**



Check the **`Enable Link Loss Failover`** and specify **`Failover Interval`** to be **`180`** seconds.

Click **Apply**.

4.5.3 Configure OA Security

This procedure will disable telnet access to OA.

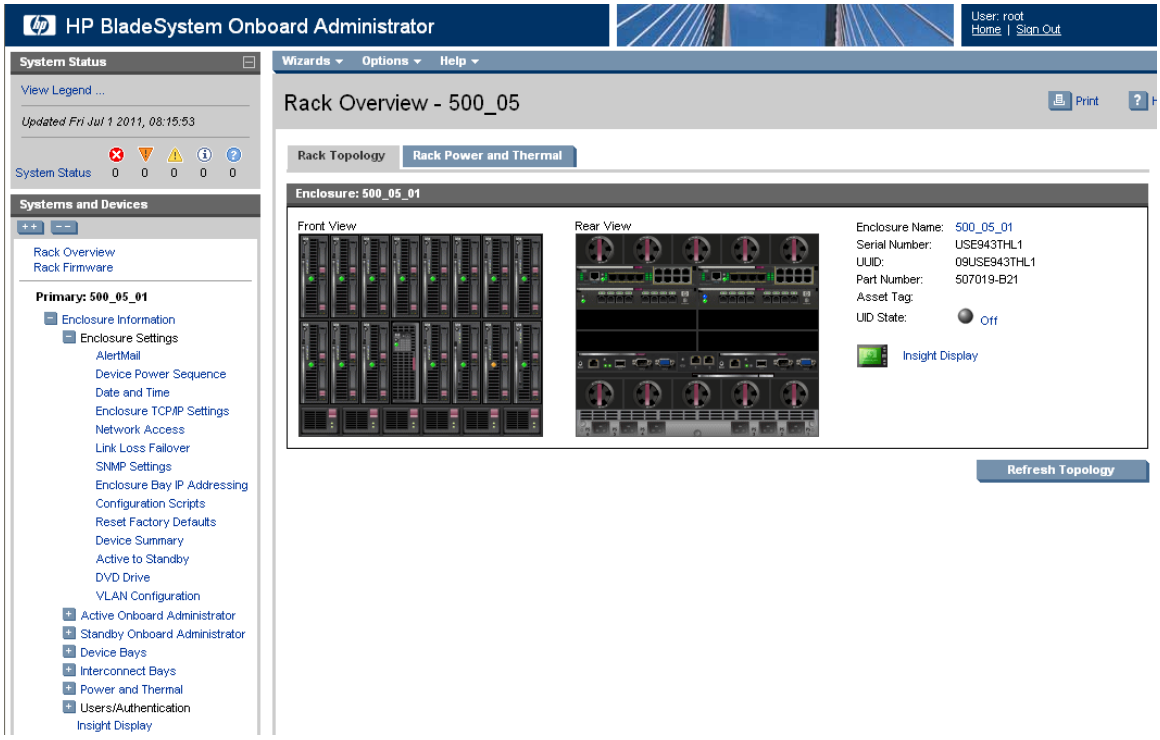
Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Active OAGUI:** Login

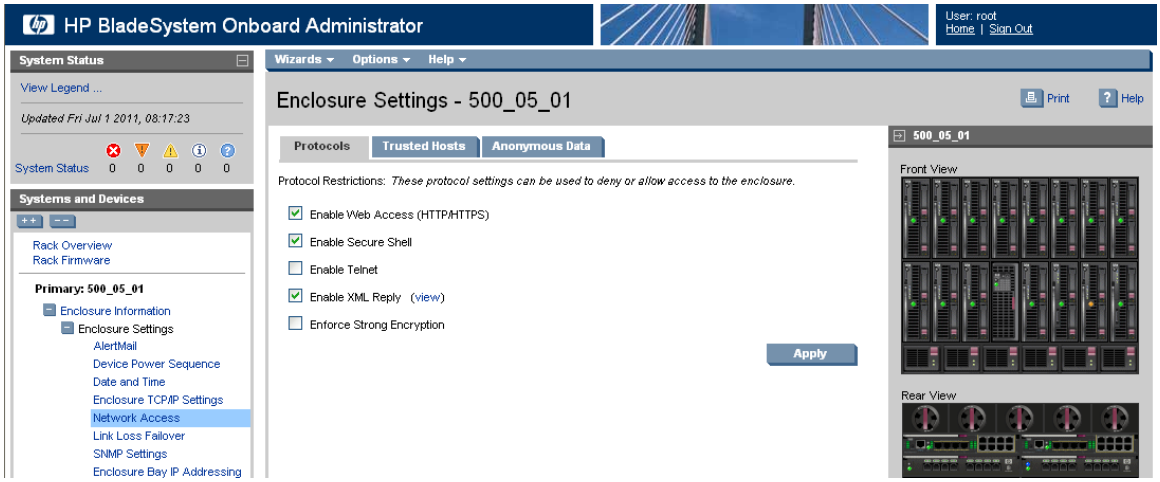
   Navigate to the IP address of the active OA, using (*Determining which Onboard Aministrator is Active*). Login as an administrative user.

2. **OAGUI:** Disable telnet

   Navigate to **Enclosure Information** > **Enclosure Settings** > **Network Access**



Then uncheck the **`Enable Telnet`**



Click on **Apply**.

4.5.4 Upgrade or Downgrade OA Firmware

This procedure will update the firmware on the OA's.

Needed material:

- Tekelec's HP Misc. Firmware USB media or ISO file
- HP Solutions Firmware Upgrade Pack Release Notes [3]

Note: The enclosure should be provisioned with two Onboard Administrators. This procedure will install the same firmware version on both Onboard Administrators.

Note: This procedure should be used to upgrade or downgrade firmware or to ensure both OA's have the same firmware version. When the firmware update is initiated, the standby OA is automatically updated first.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. Execute section 4.10.2.1 "Adding ISO Images to the PM&C Image Repository" to add the HP Misc FW ISO.
2. **OAGUI:** Login

   Navigate to the IP address of the active OA, using Appendix C (*Determining which Onboard Administrator is Active*). Login as an administrative user.

3. **OA GUI:** Check OA firmware versions.

   In the left navigation area, navigate to **Enclosure Information** > **Active Onboard Administrator** > **Firmware Update**

   Examine the **`Firmware Version`** shown in the **`Firmware Information table`**. Verify the version meets the minimum requirement specified by Release Notes [3] and that the firmware versions match for both OA's. If it is so the firmware does not need to be changed. Skip the rest of this procedure.

4. Save All OA Configuration

   If one of the two OAs has a later version of firmware than the version provided by the HP Solutions Firmware Upgrade Pack 795-000-2xx [3], this procedure will downgrade it to that version. A firmware downgrade can result in the loss of OA configuration. Before proceeding, ensure that you have a record of the initial OA configuration necessary to execute the following OA configuration procedures, as required by the customer and application:

   1. *4.5.1 Configure Initial OA IP*
   2. *4.5.2 Configure initial OA settings via configuration wizard*
   3. *4.5.3 Configure OA Security*
   4. *4.5.6 Add SNMP trap destination on OA.*

5. **OAGUI:** Initiate OAfirmware upgrade

   If the firmware needs to be upgraded, click on **Firmware Update** in the left navigation area.

   Enter the appropriate URL in the bottom text box labeled "Image URL". The syntax is:

```
https://<PM&C_Management_Network_IP>/TPD/<HPFW_mount_point>/files/<OA_firmware_version>.bin
```

   For example:

```
https://10.240.4.198/TPD/HPFW--872-2488-XXX--HPFW/files/hpoa300.bin
```

   Check the **Force Downgrade** box if present.

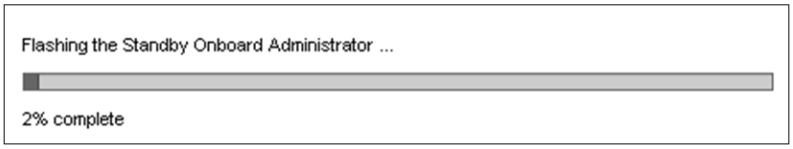
   Click **Apply**

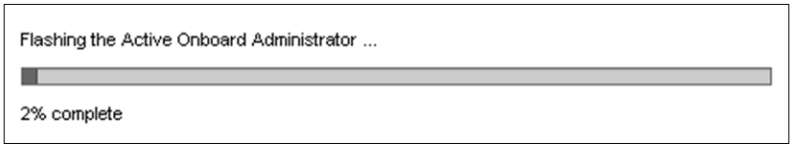
   If a confirmation dialog is displayed, click "**OK**".

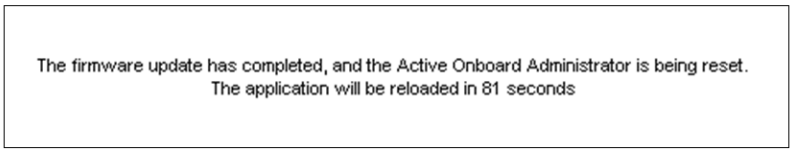
   Note: The upgrade may take up to 25 minutes.

6. **OAGUI:** Observe OAfirmware upgrade progress

   You should observe the following updates during the upgrade.







7. **OAGUI:** Reload the HPOAapplication

   The upgrade is complete when the following is displayed:

   Clear your browser's cache and click to reload the application . The login page should appear momentarily.

8. **OAGUI:** Verify the firmware upgrade

   Login to the OA again. It may take few minutes before the OA is fully functional and accepts the credentials.

   In the left navigation area, navigate to **Enclosure Information** > **Active Onboard Administrator** > **Firmware Update**

   Examine the **`Firmware Version`** shown in the **`Firmware Information table`**. Verify the firmware version information is correct.

9. **OA GUI:** Check/re-establish OA configuration

   Ensure that all OA configuration established by the following procedures is still intact after the firmware update. Re-establish any settings by performing the procedure(s):

1. *4.5.1 Configure Initial OA IP*
2. *4.5.2 Configure initial OA settings via configuration wizard*
3. *4.5.3 Configure OA Security*
4. *4.5.6 Add SNMP trap destination on OA.*

4.5.5 Store OA Configuration on Management Server

This procedure will backup OA settings on the management server .

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

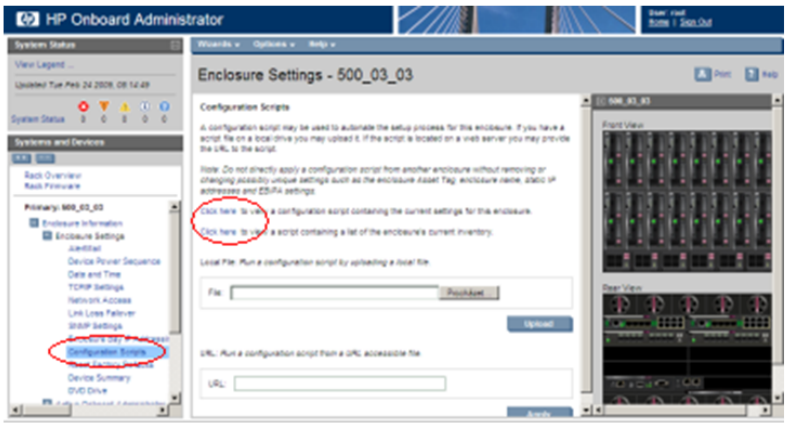
1. **OAGUI:** Login

   Navigate to the IP address of the active OA, using Appendix C (*Determining which Onboard Administrator is Active*). Login as root.

2. **OAGUI:** Store configuration file

   Navigate to the **Enclosure Information** > **Enclosure Settings** > **Configuration scripts**

   On the **`Configuration script`** open the first configuration file (current settings for enclosure):



   Store this file on local disk.

   For example:

   Press **`ctrl+s`**, choose file name, path, and as type choose text file.

   f.e. you may choose the following syntax for the configuration file name:

   `<enclosure ID>_<timetag>.conf`

3. **PM&C:** Backup configuration file

   Do the following to backup the file on the PM&C:

   Under directory **`/usr/TKLC/smac/etc`** you can create your own subdirectory structure. Login to management server via ssh as admusr and create the target directory:

```
$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/OA_backups/OABackup
```

Next, copy the configuration file to the created directory.

For unix users:

```
# scp ./<cabinet_enclosure_backup file>.conf \
admusr@<pmac_management_network_ip>:/var/TKLC/home/admusr
```

Windows users: Refer to Appendix A (*Using WinSCP*) to copy the file to the management server.

Now, on the PM&C, move the configuration file to the OA Backup folder that you created under /usr/TKLC/smac/etc:

```
$ sudo /bin/mv /var/TKLC/home/admusr/<cabinet_enclosure_backup file>.conf
/usr/TKLC/smac/etc/OA_backups/OABackup
```

4. **PM&C:** Perform PM&C application backup to capture the OA backup

```
$ sudo /usr/TKLC/smac/bin/pmacadm backup
PM&C backup been successfully initiated as task ID 7
$
```

Note: The backup runs as a background task. To check that status of the background task use the PM&C GUI Task Monitor page, or issue the command "$ **sudo /usr/TKLC/smac/bin/pmaccli getBgTasks**". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".

Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

5. **PM&C:** Verify the Backup was successful

Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

The output of pmaccli getBgTasks should look similar to the example below:

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
2: Backup PM&C COMPLETE - PM&C Backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:
 2 Server Identity:
Physical Blade Location:
Blade Enclosure:
Blade Enclosure Bay:
Guest VM Location:
Host IP:
Guest Name:
TPD IP:
Rack Mount Server:
IP:
Name:
::
```

6. **PM&C**: Save the PM&C backup

If the NetBackup feature has not been configured for this PM&C, or the Redundant PM&C is not configured in this system, the PM&C backup must be moved to a remote server. Transfer, (sftp, scp, rsync, or preferred utility), the PM&C backup to an appropriate remote server.

7. **OAGUI:** Log out

   Log out from the OA by pressing **Sign Out** at the top-right corner.

4.5.6 Add SNMP trap destination on OA.

This procedure will add an SNMP trap destination from the Onboard Administrator.

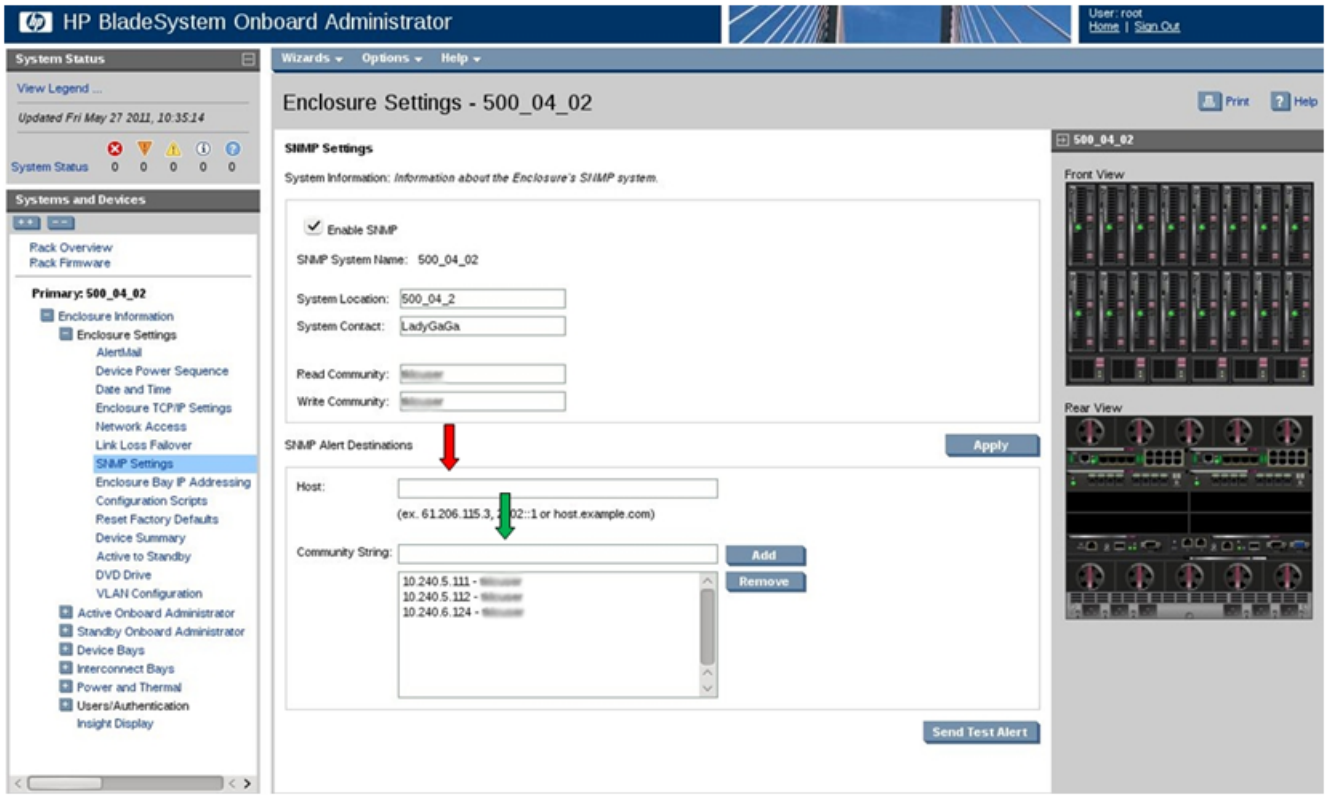
1. **Active OA GUI:** Login

   Navigate to the IP address of the active OA. Use *Appendix C: Determining which Onboard Administrator is Active* to determine the active OA. Login as an administrative user.

2. **OA GUI:** Add SNMP trap destination

   Navigate to **Enclosure Information** > **Enclosure Settings** > **SNMP Settings**.

Type the host destination information into the 'Host:' box (indicated by the red arrow in the following figure). Additionally, type the community string to the 'Community String:' box (indicated by the green arrow in the following figure). Finally, click the **Add** button to the trap destination to the configuration.



The SNMP trap destination has now been added to the configuration and should show up in the list of configured destinations. Click **Apply** to activate the configuration. The following progress meter may appear.

When the progress meter disappears, the configuration has been applied.

4.6 Enclosure Switches Firmware Update

If the enclosure switches used are Cisco 3020, execute procedure *4.6.1.1 Upgrade 3020 Switch IOS Firmware*.

If the switches used are HP 6120XG, execute procedure *4.6.2.1 Upgrade HP 6120XG Switch Firmware*.

If the switches used are HP 6125G, execute procedure *4.6.3.1 Upgrade 6125G Switch Firmware*.

4.6.1 Cisco 3020 Switch Firmware Update

4.6.1.1 Upgrade 3020 Switch IOS Firmware

This procedure will describe the steps how to upgrade IOS firmware for the 3020 switches.

Needed material:

- Tekelec's HP Misc. Firmware USB media or ISO file
- HP Solutions Firmware Upgrade Pack Release Notes [3]
- Application specific documentation (documentation that referred to this procedure)

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Virtual PM&C**: Login as admusr to the Virtual PM&C server.

   Then verify prerequisite network reachability with the following command:

   ```
   $ /bin/ping -w3 <mgmtVLAN_gateway_address>
   ```

2. **Virtual PM&C**: Copy the appropriate version of Cisco 3020 IOS firmware, as specified by the HP Solutions Firmware Upgrade Pack Release Notes [3], from the HP Misc Firmware ISO or DVD to the /home/admusr directory.

   Then check to make sure it is present in the /home/admusr directory:

   ```
   $ /bin/ls -i /home/admusr
   ```

   The output of the command should show the appropriate 3020 IOS firmware file among the files listed. Example:

   ```
   cbs30x0-ipbasek9-tar.122-58.SE1.tar
   ```

   Then copy the Cisco 3020 IOS firmware file to the /var/TKLC/smac/image directory:

   ```
   $ sudo /bin/cp /home/admusr/<3020_IOS_Firmware_File> /var/TKLC/smac/image/
   ```

   Then check to make sure it is present in the /var/TKLC/smac/image directory:

   ```
   $ /bin/ls -i /var/TKLC/smac/image
   ```

3. **Virtual PM&C**: Create and edit a file named "network-confg" in the /var/TKLC/smac/image directory by entering the following command:

   ```
   $ sudo /usr/bin/vim /var/TKLC/smac/image/network-confg
   ```

4. **Virtual PM&C**: Once in the "vim" editor modify the "network-confg" file to contain only the following lines:

   ```
   enable secret passtemp
   line vty 0 15
   password passtemp
   transport input telnet
   ```

Once the contents of the "network-confg" file match the above lines save the file and exit the "vim" editor.

5. **Virtual PM&C**: Use the **cat** command to check that the "network-confg" file was created and edited successfully.

```
$ /bin/cat /var/TKLC/smac/image/network-confg
enable secret passtemp
line vty 0 15
password passtemp
transport input telnet
```

The output above should be seen.

6. **Virtual PM&C**: Verify network reachability to the 3020 switch by using this command:

```
$ /bin/ping -w3 <enclosure_switch_IP>
```

7. **Virtual PM&C**: Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:

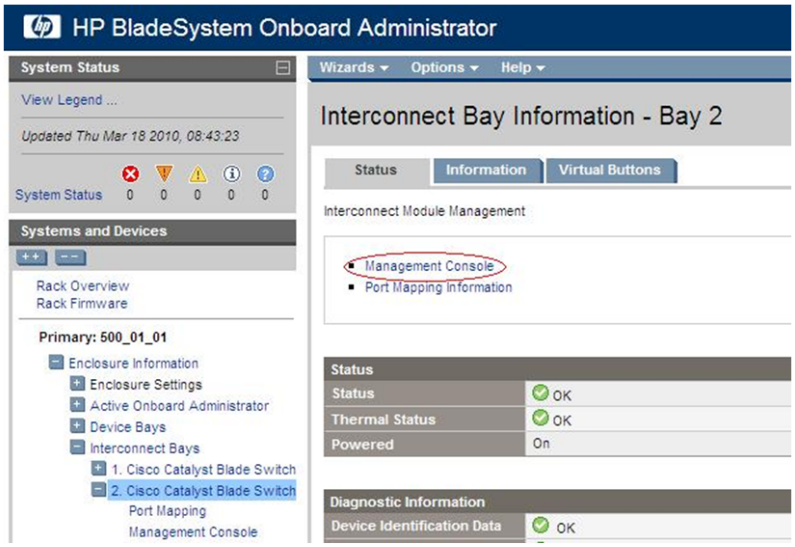
```
$  sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
 --enable=1
Successful Edit of Admin Feature
$

$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
Platform has been successfully reset

NOTE: If you change the enabled features, restart sentry
$
```

Note: This may take up to 60 seconds to complete. The "restart sentry" note can be ignored.

8. **OAGUI:** Login to the OA GUI and click on the interconnect bay for the 3020 to be configured on the Rear View image of the middle pane.

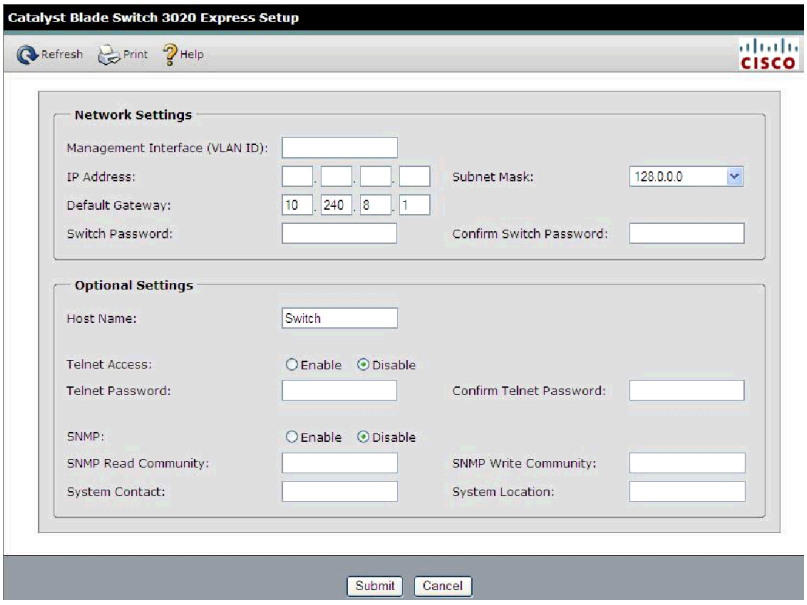
Alternatively, on the left pane, one could expand **`Interconnect Bays`**, then click on the Cisco 3020 to be upgraded.

a) Then click on **Management Console**.

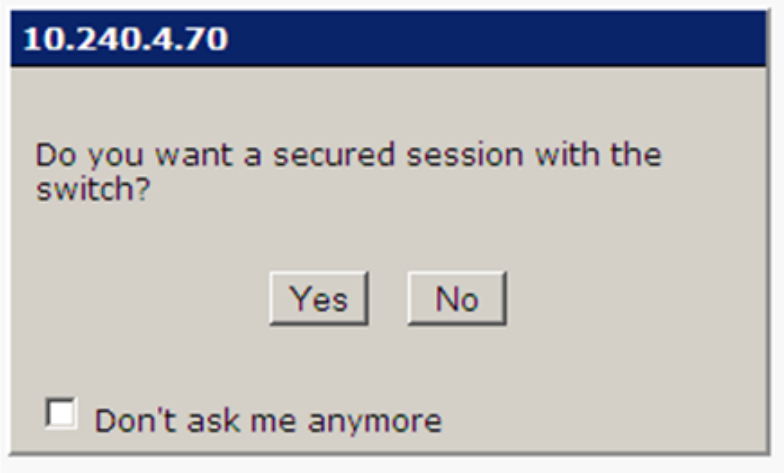


b) A new page will be opened. If asked for a username and password, leave the username blank and use the appropriate password provided by the application documentation. Then click **OK**.

c) If prompted with the "Express Setup" screen, click **Refresh**.

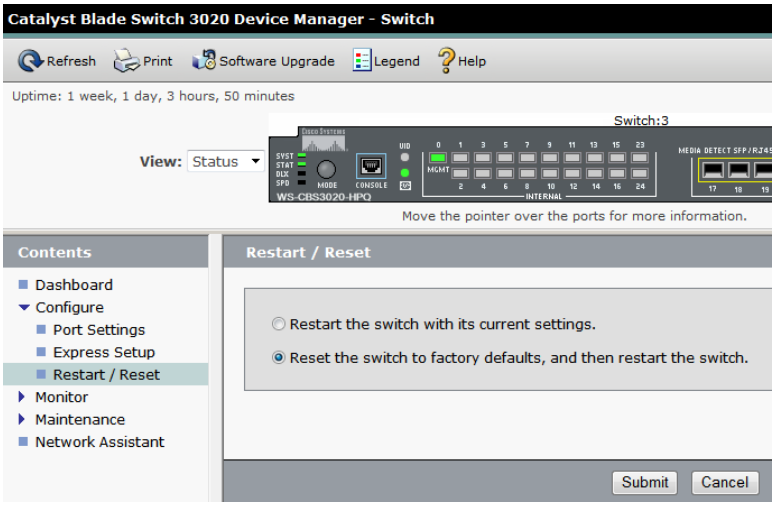


d) If prompted with "`Do you want a secured session with the switch?`", click on **No**.



Then a new Catalyst Blade Switch 3020 Device Manager will be opened.

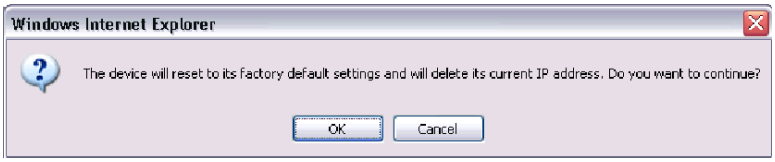
9. **OA GUI**: Restore switch to factory defaults.
   a) Navigate to **Configure** > **Restart/Reset**.



b) Click the radio button that says "Reset the switch to factory defaults, and then restart the switch".

c) Then click the "Submit" button.

A pop-up window will appear that looks like this:



d) Click OK and the switch will be reset to factory defaults and reloaded.

10. **3020 Switch CLI**: Use telnet to connect to the command line interface of the 3020 switch once it has had time to restart and acquire the configuration from the "network-confg" file.

Then login and enter enabled mode:

```
User Access Verification

Password:passtemp
Switch>en
Password:passtemp
Switch#
```

11. **3020 Switch CLI**: Begin the firmware download:

```
Switch#archive download-sw /overwrite /force-reload
tftp://<pmac_mgmtVLAN_ip_address>/<cisco_3020_IOS_firmware_file>
```

Example:

```
Switch#archive download-sw /overwrite /force-reload
tftp://10.240.34.10/cbs30x0-ipbasek9-tar.122-58.SE1.tar
```

The firmware download will take several minutes. The following is some of the output that will be seen during the upgrade:

```
Loading cbs30x0-ipbasek9-tar.122-58.SE1.tar from 10.240.34.10 (via FastEthernet0):
 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
[OK - 16455680 bytes]

Loading cbs30x0-ipbasek9-tar.122-58.SE1.tar from 10.240.34.10 (via FastEthernet0):
 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
examining image...
extracting info (110 bytes)
extracting cbs30x0-ipbasek9-mz.122-58.SE1/info (390 bytes)
extracting info (110 bytes)

System Type:             0x00000000
  Ios Image File Size:   0x00D59A00
  Total Image File Size: 0x00FB1A00
  Minimum Dram required: 0x08000000
  Image Suffix:          ipbasek9-122-58.SE1
  Image Directory:       cbs30x0-ipbasek9-mz.122-58.SE1
  Image Name:            cbs30x0-ipbasek9-mz.122-58.SE1.bin
  Image Feature:         IP|LAYER_3|SSH|3DES|MIN_DRAM_MEG=128

Old image for switch 1: same as image to overwrite
  Image to be installed already exists...will be removed before download.

Deleting `flash:cbs30x0-ipbasek9-mz.122-58.SE1' to create required space
Extracting images from archive into flash...
cbs30x0-ipbasek9-mz.122-58.SE1/ (directory)
extracting cbs30x0-ipbasek9-mz.122-58.SE1/cbs30x0-ipbasek9-mz.122-58.SE1.bin
(13988491 bytes)
```

Skipping many lines beginning with "extracting".

The following output will be seen once the firmware installation is done and the switch is reloaded into the new firmware image:

```
Installing (renaming): `flash:update/cbs30x0-ipbasek9-mz.122-58.SE1' ->
                                        `flash:/cbs30x0-ipbasek9-mz.122-58.SE1'
New software image installed in flash:/cbs30x0-ipbasek9-mz.122-58.SE1

All software images installed.
Requested system reload in progress...
Switch#
```

12. **3020 Switch CLI**: Use telnet to connect to the command line interface of the 3020 switch once it has had time to restart and acquire the configuration from the "network-confg" file.

    Then login and enter enabled mode:

```
User Access Verification

Password:passtemp
Switch>en
Password:passtemp
Switch#
```

13. **3020 Switch CLI**: Check the installed IOS firmware version to verify the upgrade completed:

```
Switch#show version
```

After scrolling to the bottom of the output produced by this command, the following will be seen or similar:

```
SW Version            SW Image
----------            ----------
12.2(58)SE1           CBS30X0-IPBASEK9-M
```

Make sure the "SW Version" column matches the appropriate version indicated in the HP Solutions Firmware Upgrade Pack Release Notes [3] and that the "SW Image" column includes the wording "IPBASEK9".

Once the installed IOS version is verified, exit the telnet connection to the switch:

```
Switch#exit
```

14. **Virtual PM&C**: Disable the DEVICE.NETWORK.NETBOOT feature with the management role to stop tftp traffic:

```
$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
 --enable=0
Successful Edit of Admin Feature
$

$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
Platform has been successfully reset
NOTE: If you change the enabled features, restart sentry
$
```

Note: This may take up to 60 seconds to complete. The "restart sentry" note can be ignored.

15. **Virtual PM&C**: Clean up the network-confg and 3020 IOS firmware files, answering "yes" when prompted.

    The 3020 IOS filename used is an example. Make sure to remove any 3020 IOS firmware files present.

```
$ sudo /bin/rm /var/TKLC/smac/image/network-confg
rm: remove regular file `/var/TKLC/smac/image/network-confg'?yes

$ sudo /bin/rm /var/TKLC/smac/image/cbs30x0-ipbasek9-tar.122-58.SE1.tar
rm: remove regular file
`/var/TKLC/smac/image/cbs30x0-ipbasek9-tar.122-58.SE1.tar'?yes
```

16. **OA GUI**: Perform *Step 8* and *Step 9* again, using "passtemp" as the password if prompted, to reset the 3020 back to factory defaults now that the firmware has been upgraded.
17. **Virtual PM&C**: Make sure this procedure has been run for all 3020 switches to be upgraded.

4.6.2 HP 6120XG Switch Firmware Update

4.6.2.1 Upgrade HP 6120XG Switch Firmware

This procedure describes the steps how to upgrade firmware for the 6120XG switches.

Needed material:

- Tekelec's HP Misc. Firmware USB media or ISO file

- HP Solutions Firmware Upgrade Pack Release Notes [3]
- WinSCP
- SSH client (eg. PuTTY)

1. **Local Workstation:**

   Copy the appropriate version of HP 6120XG firmware, as specified by the *HP Solutions Firmware Upgrade Pack Release Notes*[3]

2. **6120XG Switch:** Login

   Login to the switch as *manager* via ssh (accepting switch's key if prompted):

```
login as: manager
```

   Press any key to continue as prompted by the switch

3. **6120XG Switch:** Enter global configuration

```
Switch# config
```

4. **6120XG Switch:** Find current firmware version and compare to release notes

```
Switch(config)# show version
Image stamp:    /sw/code/build/vern(Z 14 zin t4b)
                Sep 23, 2010 16:48:29
                z.14.12
                31
Boot Image:     Secondary
```

   Record the firmware version (z.14.12 in this case) and the current Boot Image location being used (Secondary in this case). Compare the firmware version currently being used to the latest version specified in the HP *Solutions Firmware Upgrade Pack Release Notes* [3]. Continue with this upgrade procedure if necessary.

   Whatever Boot Image is being used, the opposite one will be upgraded. So in this case, since the Secondary Boot Image is being used, the Primary Boot image will be upgraded.

5. **6120XG Switch:** Record current firmware version of boot image to be upgraded.

   Record the current version of the Boot Image to be upgraded. This will be used to compare after upgrading the success of the upgrade. (Primary Image in this case).

```
Switch(config)#    show flash
Image              Size(Bytes)Date   Version
-------            -----------  -------- --------
Primary Image      : 7595562    8/17/10  z.14.09
Secondary Image    : 7732899    9/23/10  z.14.12

Boot Rom Version   : z.14.09
Default Boot       : Secondary
```

6. **6120XG Switch:** Make sure Secure Copy is enabled.

```
Switch(config)# show ip ssh
SSH Enabled           : Yes                          Secure Copy enabled : Yes
  TCP Port Number     : 22                             Timeout (sec)     : 120
  Host Key Type       : RSA                            Host Key Size     : 2048
```

```
  Ciphers :
  MACs    :

  Ses Type    | Source IP                                              Port
  --- ------- + ------------------------------------------------------ ------
  1   console |
. . . .
```

Look at the output of **show ip ssh**. If `Secure Copy Enabled = Yes`, then continue to the next step. If **Secure Copy Enabled = No**, then perform the command below:

```
Switch(config)# ip ssh filetransfer
Tftp and auto-tftp have been disabled.
Switch(config)#
```

Enter show ip ssh again to make sure Secure Copy has been enabled.

7. **6120XG Switch:** Open the event log.

   Go into the switch's menu interface and type "**y**" to save the configuration

```
Switch(config)# menu
Do you want to save current configuration [y/n/^C]? y
```

Select:

```
4. Event Log
```

Then select:

```
End
```

Keep this terminal window open.

8. **Local Workstation:**

   Configure WinSCP to work with the 6120XG. (These directions are applicable to WinSCP versions 4.27 to 5.14. Other versions may have these options in different locations).

   - Open WinSCP on your local workstation.
   - Click on “Preferences” in the list on the left.
   - Select the “Commander” interface (click on the circle next to it)
   - Then click on the **Preferences…** button.
   - In “Transfer settings”, uncheck “Preserve timestamp”.
   - In “Endurance” settings, set the “Enable transfer resume/…” option to “Disable”.
   - Click the **OK** button.
   - Click on “Session” in the list on the left.

9. **Local Workstation:**

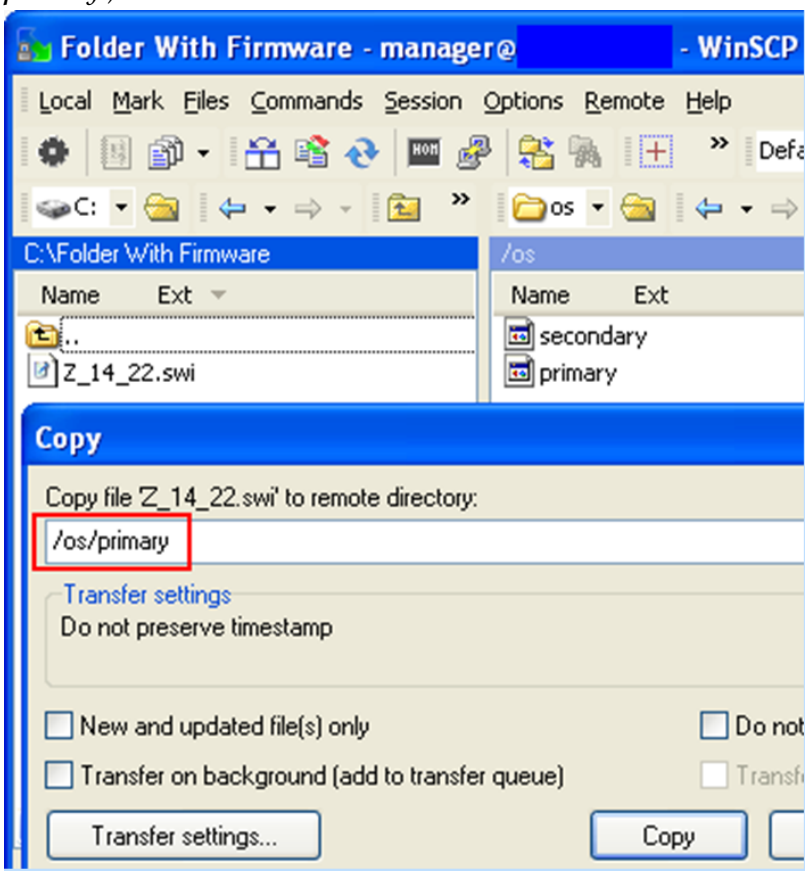
   - With WinSCP still on the "Session" screen, enter the 6120XG's **<switch_ip_address>** under ***Host name*** and **manager** as the **User name**.
     - If using **netConfig:** enter **<platform_username>** for the **User name** and **<platform_password>** for the **Password**.

- If using **SwitchConfig**: enter **manager** for the **User name** and **<switch_manager_password>** for the **Password.**

- Leave the ***Port number*** at ***22***
- Leave ***File protocol*** at ***SFTP***, and if present, select the checkbox next to ***Allow SCP fallback***.
- Click the **Login** button.
- If prompted to "add host key to the cache", click the **Yes** button

10. **Local Workstation:** Copy the new firmware to the switch Boot Image to be updated

- Once WinSCP logs into the switch, in the left window, find the firmware file that was copied to the local workstation in *Step 1*.
- In the right window on the switch, open the folder labeled "**os**"
- Drag the firmware file on the left to the window on the right.
- A copy window pop up with "**/os/*.***" written will appear. Replace *.* with either ***primary*** or ***secondary*** depending on which boot image is being upgraded. (in this example it would be ***primary***).



- Click the **Copy** button.

11. **6120XG Switch:** Go back to the Event Log on the SSH session with the switch.

Go back to the switch ssh window where the ***Event Log*** is open. If the connection has timed out, redo *Step 2*, *Step 3*, and *Step 6*. Watch for the following log event (it can take a few minutes):

```
update: Primary Image updated
```

In this example, the Primary Image is being updated. If the user were updating the Secondary Image, it would say "Secondary" instead of "Primary".

12. 6120XG Switch: Get Back to the Command Line Interface (CLI).

Now that the "updated" message has appeared, select:

```
Back
```

Then select:

```
5. Command Line (CLI)
Switch(config)#
```

13. 6120XG Switch: Check the firmware version.

Run the **show flash** command to make sure the Image being updated has the correct firmware version. (in this example ***Primary Image*** has changed to ***z.14.22***)

```
Switch(config)# show flash
Image       Size(Bytes)Date   Version
-------           -------------   --------    --------
Primary Image   : 7732899         10/21/10    z.14.22
Secondary Image : 7193633         06/23/10    z.14.12
Boot Rom Version: z.14.09
Default Boot    : Secondary
```

14. 6120XG Switch: Reboot into the new firmware.

Now reboot the switch into the new Boot Image. (***primary*** in this example). If the ***Secondary Image*** has been updated, replace "primary" with "secondary" in the command below:

```
Switch(config)# boot system flash primary
Device will be rebooted, do you want to continue [y/n]? y
```

15. 6120XG Switch: Log back in.

Once the switch has rebooted, log back into the switch as *manager* via ssh.

```
login as: manager
Press any key to continue as prompted by the switch.

Switch#
```

16. 6120XG Switch: Re-enter global configuration.

```
Switch# config
```

17. 6120XG Switch: Make sure the switch has booted properly into the new firmware image.

Run the **show version** command. Make sure the new firmware version is displayed.

```
Switch(config)# show version
Image stamp:/sw/code/build/vern(Z_14_zin_t4b)
             Oct 21 2010 16:48:29
             Z.14.22
             31
Boot Image:   Primary
```

18. **6120XG Switch:** Verify the "Default Boot" has changed.

    Run the **show flash** command, checking to make sure the image that was upgraded has been set as the "default Boot". (**Primary** in this example).

```
6120XG_IOBAY1# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 7798047   03/07/12 Z.14.32
Secondary Image : 7732899   10/21/10 Z.14.22
Boot Rom Version: Z.14.09
Default Boot    : Primary
```

4.6.3 HP 6125G Switch Firmware Update

4.6.3.1 Upgrade 6125G Switch Firmware

This procedure will describe the steps to upgrade firmware for the 6125G switches.

Needed Materials

- Tekelec's HP Misc. Firmware USB media or ISO file
- HP Solutions Firmware
- Upgrade Pack Release Notes [3]
- WinSCP
- SSH client (for example, PuTTY)

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Local Workstation:** Copy the appropriate version of 6125G firmware, as specified by the HP Solutions Firmware Upgrade Pack Release Notes [3], to the local workstation.
2. **Active OA CLI:** Log in to the active Onboard Administrator via ssh (accepting the OA's key if prompted).

```
login as: <OA_Admin_User>
--------------------------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
--------------------------------------------------------------------------
Firmware Version: 3.70
Built: 10/01/2012 @ 17:53
OA Bay Number:  2
OA Role:       Active
root@10.240.8.6's password: <OA_Admin_Password>

OA>
```

3. **Active OA CLI:** Connect to the serial console of the 6125G switch to be upgraded. Setup netConfig repository with necessary ssh information.

```
OA> connect interconnect <iobay_number>
```

Use the number of the IO bay the switch is in to complete the command, which will be similar to the one shown below.

```
OA> connect interconnect 1
NOTICE: This pass-thru connection to the integrated I/O console
is provided for convenience and does not supply additional access
control.  For security reasons, use the password features of the
integrated switch.

Connecting to integrated switch 4 at 9600,N81...
Escape character is '<Ctrl>_' (Control + Shift + Underscore)

Press [Enter] to display the switch console:
```

Press the "Enter" button, as needed, to continue to the 6125G switch serial console.

```
<6125G Blade Switch>
```

4. **6125G CLI:** Check current firmware version.

```
<6125G Blade Switch> display boot-loader
 Slot 1
The current boot app is:  flash:/6125-cmw520-r2105.bin
The main boot app is:     flash:/6125-cmw520-r2105.bin
The backup boot app is:   flash:/6125-cmw520-r2105.bin
```

If the "current boot app" and the "main boot app" are already at the version specified by the HP Solutions Firmware Upgrade Pack Release Notes [3], then the switch is up to date and the rest of this procedure can be skipped. Otherwise, continue to *Step 5*.

5. **6125G CLI:** Enable DHCP for the switch's management interface.

```
<6125G Blade Switch> system-view
[6125G Blade Switch] interface M-Ethernet 0/0/0
[6125G Blade Switch-M-Ethernet0/0/0] ip address dhcp-alloc
[6125G Blade Switch-M-Ethernet0/0/0] quit
[6125G Blade Switch]
```

6. **6125G CLI:** Set up the local user.

```
[6125G Blade Switch] local-user plat
New local user added.
[6125G Blade Switch-luser-plat] password simple passtemp
[6125G Blade Switch-luser-plat] authorization-attribute level 3
[6125G Blade Switch-luser-plat] service-type ssh terminal
[6125G Blade Switch-luser-plat] quit
[6125G Blade Switch]
```

7. **6125G CLI**: Set up SSH and SFTP.

```
[6125G Blade Switch] ssh server enable
Info: Enable SSH server.
[6125G Blade Switch] sftp server enable
Info: Enable SFTP server.
[6125G Blade Switch] ssh user plat service-type all authentication-type password
[6125G Blade Switch] public-key local create rsa
Warning: The local key pair already exist.
```

```
Confirm to replace them? [Y/N]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:  (Press Enter)
Generating Keys...
+++++
++++++++++++
++++
+++++++
```

Note: Answer 'y' if prompted to replace an existing local key pair

8. **6125G CLI**: Set up the user interfaces.

```
[6125G Blade Switch] user-interface aux 0
[6125G Blade Switch-ui-aux0] authentication-mode scheme
[6125G Blade Switch-ui-aux0] quit
[6125G Blade Switch] user-interface vty 0 7
[6125G Blade Switch-ui-vty0-7] authentication-mode scheme
[6125G Blade Switch-ui-vty0-7] user privilege level 3
[6125G Blade Switch-ui-vty0-7] quit
[6125G Blade Switch] quit
<6125G Blade Switch>
```

9. **6125G CLI:** Display the management interface information to determine its IP address.

```
<6125G Blade Switch> display interface M-Ethernet 0/0/0 brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
M-E0/0/0             UP   UP       10.240.8.10
```

Note: The Main IP address that the management interface has acquired via DHCP. This IP address will be used in the following steps. In this example, it is 10.240.8.10.

10. **Local Workstation:** Open and configure WinSCP. (These directions are applicable to WinSCP versions 4.27 to 5.14. Other versions may have these options in different locations.)
    - Open WinSCP on your local workstation.
    - Click on Preferences in the list on the left.
    - Select the Commander interface (click on the circle next to it).
    - Then, click on the **Preferences…** button.
    - In Transfer settings, uncheck Preserve timestamp.
    - In Endurance settings, set the Enable transfer resume/… option to Disable.
    - Click the **OK** button.
    - Click on Session in the list on the left.

11. **Local Workstation:** Connect to the 6125 with WinSCP via SFTP.
    - With WinSCP still on the Session screen, make sure SFTP is selected under File Protocol.
    - Leave the port number at 22.
    - Enter the 6125G's IP address under Host name. This is the IP address noted in *Step 9*.
    - Enter plat under User name.

- Enter passtemp under Password.
- Click the **Login** button. If prompted to add host key to the cache, click the **Yes** button.

12. **Local Workstation:** Copy the new firmware to the switch.
    - After WinSCP logs into the switch, in the left window, locate the firmware file that was copied to the local workstation in *Step 1*.
    - Drag the firmware file from the left to the window on the right.
    - When the Copy window appears, click on the **Copy** button and wait for the firmware file to finish copying to the switch.
    - Visually check that the new firmware file now appears in the right window after the copy is complete.
    - Close WinSCP.
13. **Local Workstation:** Log in to the 6125G.
    If you have disconnected from the 6125G CLI and/or the OA, return to the 6125G CLI by performing *Step 2* and *Step 3*. Then return to this step.

```
Login authentication

Username: plat
Password: passtemp
<6125G Blade Switch>
```

14. **6125G CLI:** Load the new firmware file as the main flash image. Make sure to use the correct firmware file name that you copied to the switch.

```
<6125G Blade Switch> boot-loader file flash:/6125-cmw520-r2105.bin slot 1 main
```

    Enter "Y" when asked to continue.

```
This command will set the boot file of the specified board. Continue? [Y/N]: Y
  The specified file will be used as the main boot file at the next reboot on
slot 1!
```

15. **6125G CLI:** Reboot the switch to run the new firmware version. Enter Y to save the configuration when prompted.

```
<6125G Blade Switch> reboot
 Start to check configuration with next startup configuration file, please
wait.........DONE!
 This command will reboot the device. Current configuration will be lost, save
current configuration? [Y/N]: Y
```

    When prompted about the file name leave it blank and press **Enter**.

```
Please input the file name(*.cfg)[flash:/config.cfg]
(To leave the existing filename unchanged, press the enter key):
 Validating file. Please wait....
 The current configuration is saved to the active main board successfully.
 Configuration is saved to device successfully.
```

When prompted to continue with the reboot, enter **Y**.

```
This command will reboot the device. Continue? [Y/N]:Y
#Apr 26 13:43:23:098 2000 6125G Blade Switch DEVM/1/REBOOT:
 Reboot device by command.

%Apr 26 13:43:23:190 2000 6125G Blade Switch DEVM/5/SYSTEM_REBOOT: System is
rebooting now.
```

16. 6125G CLI: Press the **Enter** key when prompted after the reboot is complete and login to the 6125G.

```
Press ENTER to get started.

Login authentication
Username: plat
Password: passtemp
<6125G Blade Switch>
```

17. 6125G CLI: Verify that the new firmware is both the "current boot app" and the "main boot app".

```
<6125G Blade Switch> display boot-loader
 Slot 1
The current boot app is:  flash:/6125-cmw520-r2105.bin
The main boot app is:     flash:/6125-cmw520-r2105.bin
The backup boot app is:   flash:/6125-cmw520-r2105.bin
```

18. 6125G CLI: Reset the 6125G to a default state.

Clear the RSA key.

```
<6125G Blade Switch> system-view
System View: return to User View with Ctrl+Z.

[6125G Blade Switch] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]: Y

[6125G Blade Switch] quit
```

Reset the configuration to defaults.

```
<6125G Blade Switch> reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]: Y
Configuration file in flash is being cleared.
Please wait ...

MainBoard:
 Configuration file is cleared.
```

Reboot the switch.

```
<6125G Blade Switch> reboot
 Start to check configuration with next startup configuration file, please
wait.........DONE!
```

Do not save the configuration. Enter "N" when prompted.

```
 This command will reboot the device. Current configuration will be lost, save
current configuration? [Y/N]: N
```

Enter "Y" when asked to continue.

```
 This command will reboot the device. Continue? [Y/N]:Y
#Apr 26 13:43:23:098 2000 6125G Blade Switch DEVM/1/REBOOT:
 Reboot device by command.
```

19. **6125G CLI:** After the reboot is complete, exit the 6125G CLI by pressing (Ctrl + Shift + Underscore).

    Then enter "D" to disconnect when prompted.

```
Press ENTER to get started.
------------------------------------------------------------------------
Command: D)isconnect, C)hange settings, send B)reak, E)xit command mode X)modem
send > D
------------------------------------------------------------------------

OA>
```

    Make sure this procedure has been run for all 6125G switches to be upgraded.

4.7 Enclosure and Blades Setup

4.7.1 Add Cabinet and Enclosure to the PM&C system inventory

This procedure provides the instructions for adding a cabinet and an enclosure to the PM&C system inventory.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **PM&C GUI:** Login

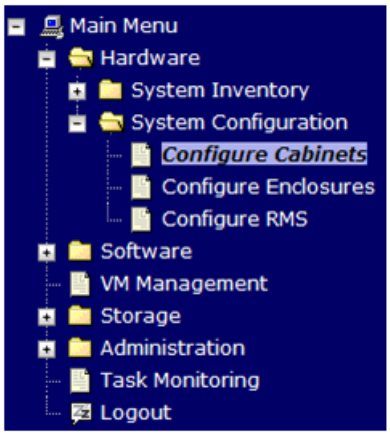
   Open your web browser and enter:

```
https://<pmac_management_network_ip>
```

   Login as the pmacadmin user.

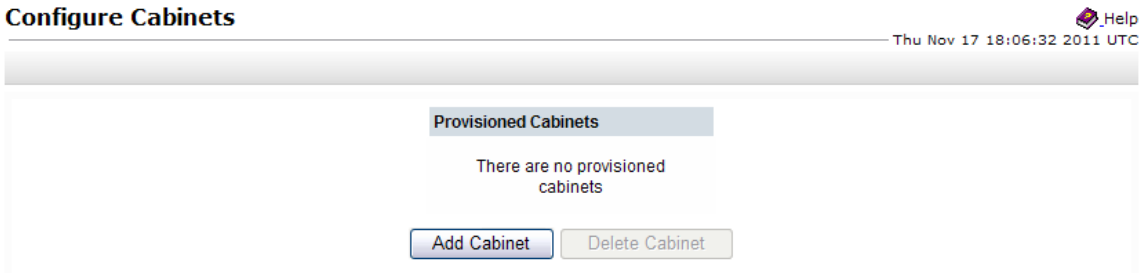
2. **PM&C GUI:** Navigate to Configure Cabinets

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Cabinets**.



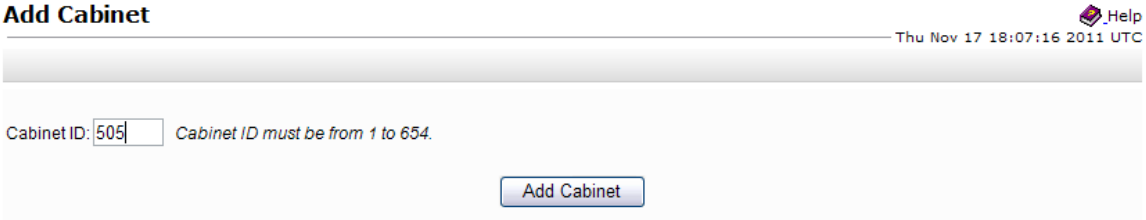
3. **PM&C GUI:** Add Cabinet

   On the **`Configure Cabinets`** panel, press the **Add Cabinet** button



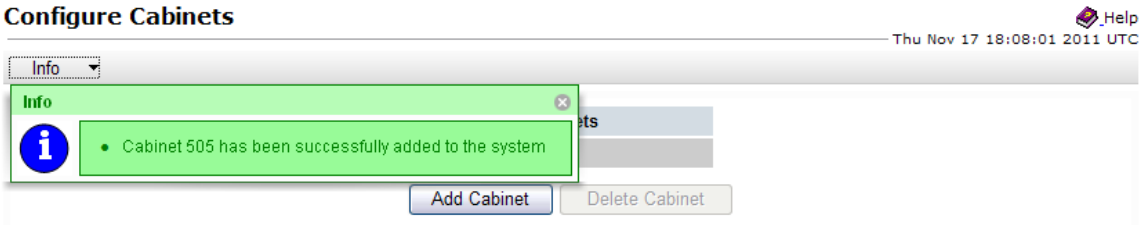
4. **PM&C GUI:** Enter Cabinet ID

   Enter the **`CabinetID`** and press the **Add Cabinet** button.

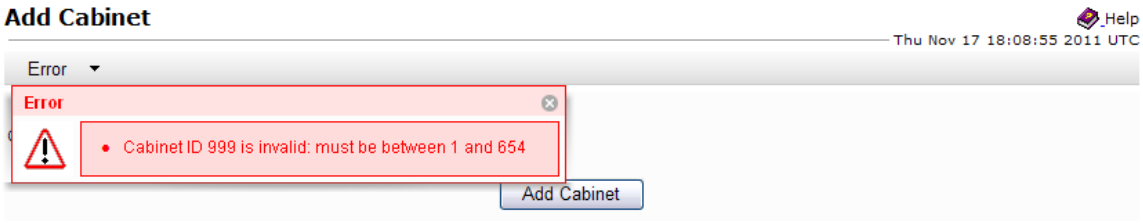


5. **PM&C GUI:** Check errors

   If no error is reported to the user you will see the following:

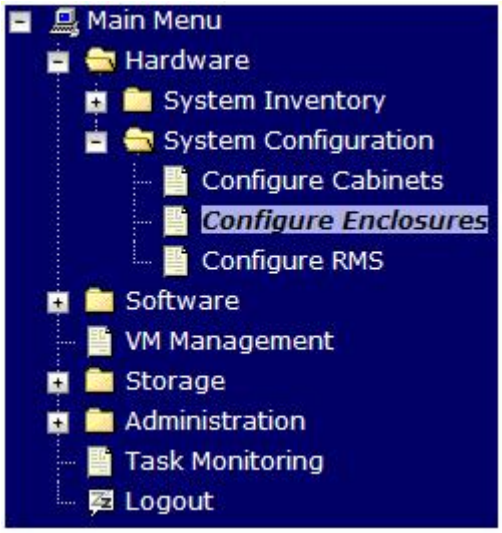


   Or you will see an error message:



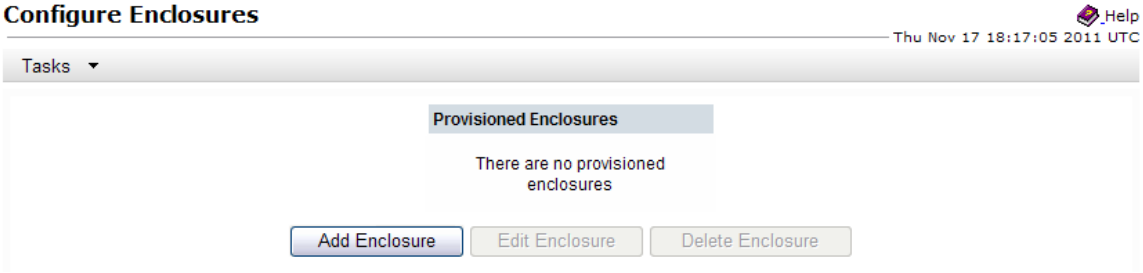
6. **PM&C GUI:** Navigate to Configure Enclosures

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure Enclosures**.



7. **PM&C GUI:** Add Enclosure

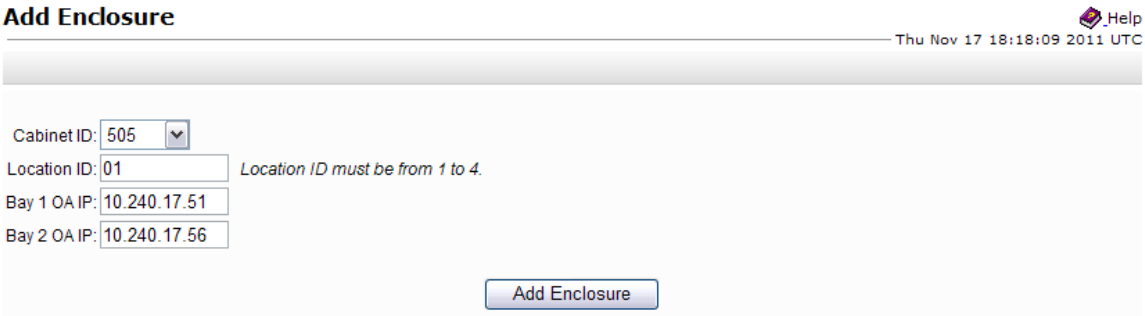
   On the **`Configure Enclosures`** panel, press the **Add Enclosure** button



8. **PM&C GUI:** Provide Enclosure Details

   On the **`Add Enclosure`** panel, enter the **`Cabinet ID`**, **`Location ID`**, and two **`OA IP`** addresses (the enclosure's active and standby OA).

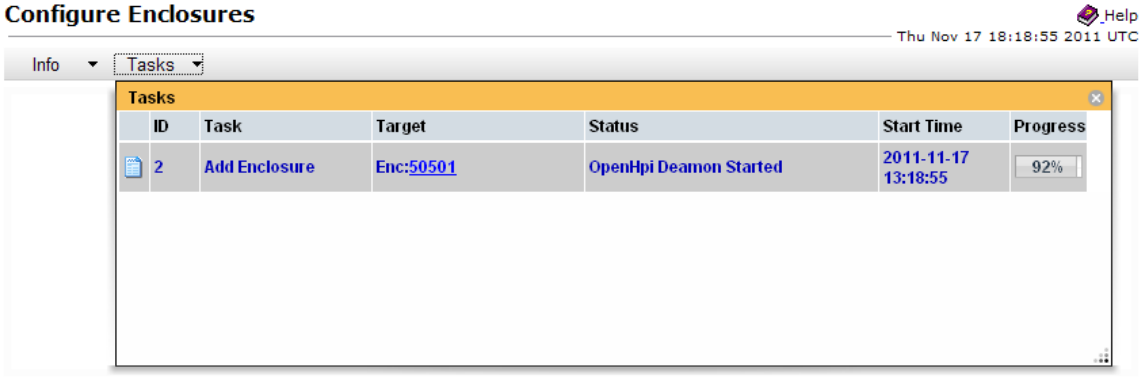
   Then click on **Add Enclosure**.



Note: Location ID is used to uniquely identify an enclosure within a cabinet. It can have a value of 1, 2, 3, or 4. The cabinet ID and location ID will be combined to create a globally unique ID for the enclosure (for example, an enclosure in cabinet 502 at location 1, will have an enclosure ID of 50201).

9. **PM&C GUI:** Monitor Add Enclosure

   The Configure Enclosures page is then redisplayed with a new background task entry in the Tasks table. This table can be accessed by pressing the **Tasks** button located on the toolbar under the Configure Enclosures heading.



When the task is complete and successful, its text will change to green, and its Progress column will indicate "100%".

4.7.2 Configure Blade Server iLO Password for Administrator Account

This procedure will change the blade server iLO password for Administrator account for blade Servers in an enclosure.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **PM&C:** Log into the PM&C as admusr using ssh.
2. **PM&C:** Create xml file

In **/usr/TKLC/smac/html/public-configs** create an xml file with information similar to the following example. Change the Administrator password field only as instructed by the application.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admusr" PASSWORD="<iLo admusr password>">
<USER_INFO MODE="write">
<ADD_USER USER_NAME="admusr" USER_LOGIN="admusr" PASSWORD="<iLo admusr password>">
<ADMIN_PRIV value="Yes"/>
<REMOTE_CONS_PRIV value ="Yes"/>
<RESET_SERVER_PRIV value ="Yes"/>
<VIRTUAL_MEDIA_PRIV value ="Yes"/>
<CONFIG_ILO_PRIV value ="Yes"/>
</ADD_USER>
</USER_INFO>
<USER_INFO MODE="write">
<MOD_USER USER_LOGIN="Administrator">
<PASSWORD value="<iLo Administrator password>"/>
</MOD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

Save this file as **change_ilo_admin_passwd.xml**

3. **OA shell:** Login to the active OA

   Log into OA via ssh as root user.

```
login as: root

------------------------------------------------------
WARNING: This is a private system.  Do not attempt to login unless you are an
authorized user.  Any authorized or unauthorized access and use may be moni-
tored and can result in criminal or civil prosecution under applicable law.
------------------------------------------------------

Firmware Version: 3.00
Built: 03/19/2010 @ 14:13 OA
  Bay
 Number:  1 OA
 Role:       Active
admusr@10.240.17.51's password:
```

   If the **OA Role** is not **Active,** login into the other OA the enclosure system

4. **OA shell:** Run hponcfg

   Run the following command:

```
> hponcfg all https://<pmac_ip>/public-configs/change_ilo_admin_passwd.xml
```

5. **OA shell:** Check the output

   Observe the output for error messages and refer to the **HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide** for troubleshooting

6. **OA shell:** Logout

   Logout from the OA

7. **PM&C:** Remove temporary file

   On the PM&C remove the configuration file you created. This is done for security reasons, so that no one can reuse the file:

```
$ sudo /bin/rm –rf /usr/TKLC/smac/html/public-configs/change_ilo_admin_passwd.xml
```

4.8 Configure Enclosure Switches

If the enclosure switches used are Cisco 3020, execute procedure *4.8.1.1 Configure Cisco 3020 switch (netConfig)*.

If the switches used are HP 6120XG, execute procedure *4.8.2.1 Configure HP 6120XG switch (netConfig)*.

If the enclosure switches used are HP6125G, execute procedure .

4.8.1 Configure Cisco 3020 Switches

4.8.1.1 Configure Cisco 3020 switch (netConfig)

This procedure will configure 3020 switches from the PM&C server using templates included with an application.

If the aggregation switches are provided by Tekelec, then the Cisco 4948/4948E/4948E-F switches must be configured using *4.3.2 Configure Cisco 4948/4948E/4948E-F aggregation switches (PM&C installed)(netConfig)* If the aggregation switches are provided by the customer, the user must ensure that the customer aggregation switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Tekelec or the customer, contact Tekelec Technical Services and ask for assistance.

This procedure requires that no IPM activity is occurring or will occur during the execution of this procedure.

Needed materials:

- HP Misc. Firmware DVD
- HP Solutions Firmware Upgrade Pack Release Notes [3]
- Application specific documentation (documentation that referred to this procedure)
- Template xml files in an application ISO on an application CD.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Virtual PM&C:** Prepare for switch configuration

   Login as admusr to the PM&C, then run:

```
$ /bin/ping -w3 <mgmtVLAN_gateway_address>
```

2. **Virtual PM&C:** Verify network connectivity to 3020 switches

For each 3020 switch, verify network reachability.

```
$ /bin/ping -w3 <enclosure_switch_IP>
```

3. **Virtual PM&C**: Modify PM&C Feature to allow TFTP.

   Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:

```
$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
 --enable=1
$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
```

   Note: This may take up to 60 seconds to complete.

4. **Virtual PM&C:** Verify the template xml files are in existence.

   Verify the initialization xml template file and configuration xml template file is present on the system and is the correct version for the system.

   Note: The XML files prepared in advanced with the NAPD can be used as an alternative.

```
$ /bin/more /usr/TKLC/smac/etc/switch/xml/3020_init.xml
$ /bin/more /usr/TKLC/smac/etc/switch/xml/3020_configure.xml
```

   If either file does not exist, copy the files from the application media into the directory shown above.

   If 3020_init.xml file exists, page through the contents to verify it is devoid of any site specific configuration information other than the device name. If the template file is appropriate, then skip the remainder of this step and continue with the next step.

   If 3020_configure.xml file exists, page through the contents to verify it is the appropriate file for the this site and edited for this site. All network information is necessary for this activity. If the template file is appropriate, then skip the remainder of this step and continue with the next step.

5. **Virtual PM&C:** Modify 3020 xml files for information needed to configure the switch.

   Update the 3020_init.xml file for the values noted in the next sentence. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$some_variable_name** will need to be modified, removing the dollar sign and the less than, greater than sign. When done editing the file, save and quit.

   Update the 3020_configure.xml file for the values noted in the next sentence. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$some_variable_name** will need to be modified, removing the dollar sign and the less than, greater than sign. When done editing the file, save and quit.

```
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_init.xml
```

```
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_config.xml
```

6. **Virtual PM&C/OA GUI:** Reset switch to factory defaults

   Note: Do not wait for the switch to finish reloading before proceeding to the next step. After completing step 6 by initiating the reload, proceed to *Step 7*.

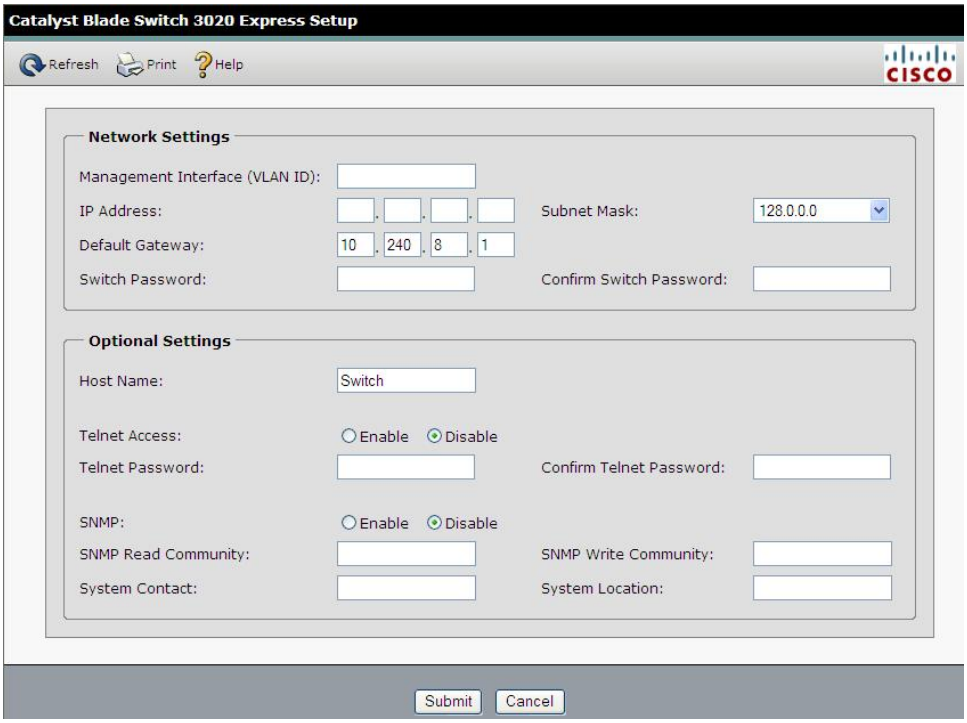
If the switch has been previously configured using netConfig or previous attempts at initialization have failed, use netConfig to reset the switch to factory defaults by executing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> setFactoryDefault
```

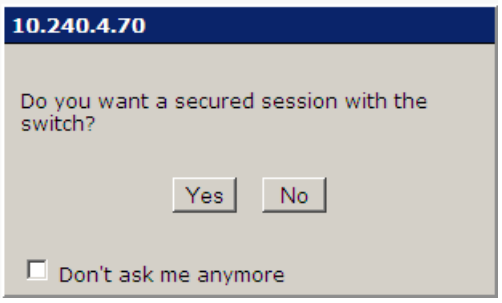
If the above command failed, use Internet Explorer to navigate to <enclosure_switch_ip_address>.

A new page will be opened. If you are asked for a username and password, leave the username blank and use the appropriate password provided by the application documentation. Then click **OK**.

If you are prompted with the "Express Setup" screen, click **Refresh**.

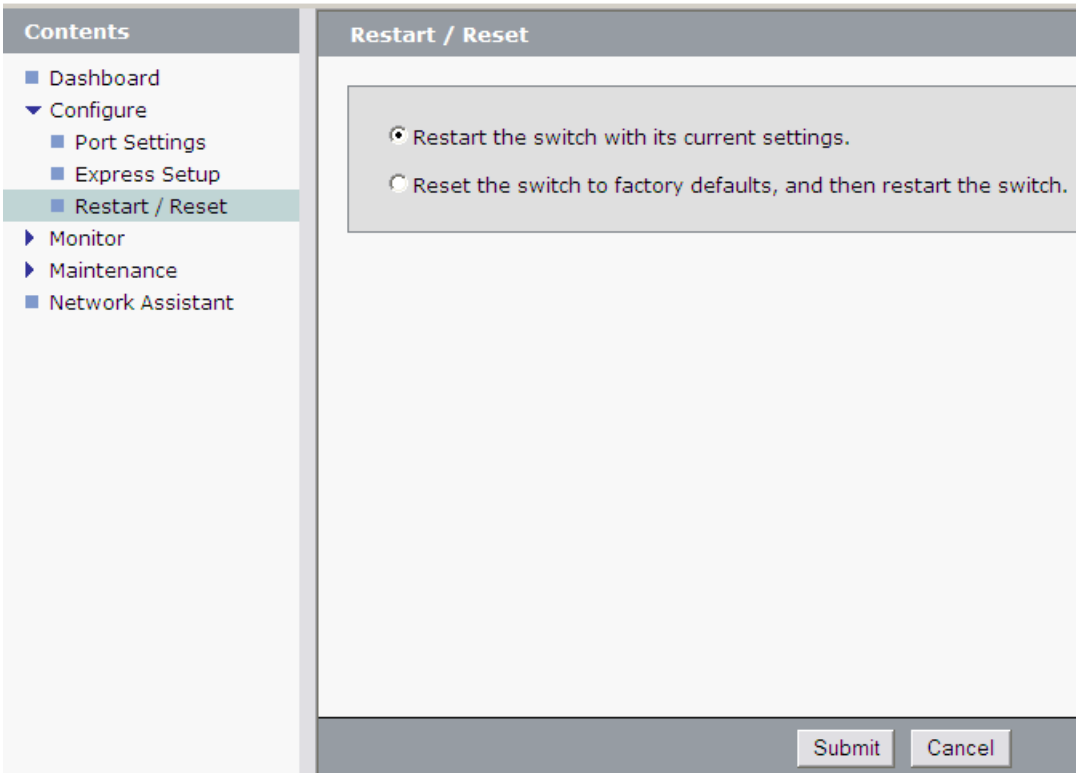


If you are prompted with "Do you want a secured session with the switch?", click on **No**.



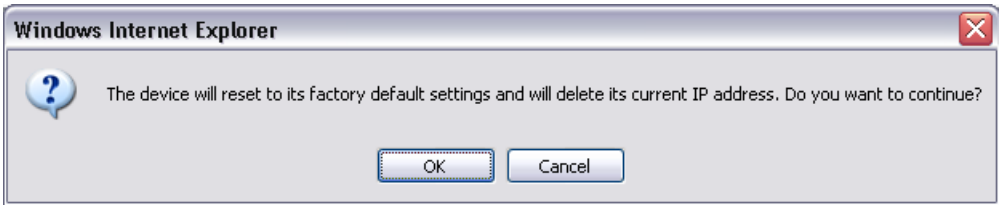
Then a new Catalyst Blade Switch 3020 Device Manager will be opened.

Navigate to **Configure** > **Restart/Reset**.



Click the circle that says "Reset the switch to factory defaults, and then restart the switch". Then click the "**Submit**" button.

A pop-up window will appear that looks like this:



Click OK and the switch will be reset to factory defaults and reloaded.

7. **Virtual PM&C:** Remove the old ssh key and Initialize the switch

   Remove the old ssh key:

```
$ sudo /usr/bin/ssh-keygen -R <enclosure_switch_ip>
```

   The following command must be entered at least 60 seconds and at most 5 minutes after the previous step is completed.

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/3020_init.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/3020_init.xml
Waiting to load the configuration file...
loaded.
```

```
Attempting to login to device...
Configuring....
```

Note: This step takes about 4-5 minutes to complete, it is imperative that you wait until returned to the command prompt. **DO NOT PROCEED UNTIL RETURNED TO THE COMMAND PROMPT**.

Check the output of this command for any errors. A successful completion of netConfig will return the user to the prompt. Due to strict host checking and the narrow window of time in which to perform the command, this command is prone to user error. Most issues are corrected by returning to the previous step and continuing. If this step has failed for a second time, stop the procedure and contact the Customer Care Center.

8. **Virtual PM&C:** Reboot the switch using netConfig

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> reboot save=no
```

Wait 2-3 minutes for the switch to reboot. Verify it has completed rebooting and is reachable by pinging it.

```
$ /bin/ping <enclosure_switch_IP>
From 10.240.8.48 icmp_seq=106 Destination Host Unreachable
From 10.240.8.48 icmp_seq=107 Destination Host Unreachable
From 10.240.8.48 icmp_seq=108 Destination Host Unreachable
64 bytes from 10.240.8.13: icmp_seq=115 ttl=255 time=1.13 ms
64 bytes from 10.240.8.13: icmp_seq=116 ttl=255 time=1.20 ms
64 bytes from 10.240.8.13: icmp_seq=117 ttl=255 time=1.17 ms
```

9. **Virtual PM&C:** Configure the switches

Configure both switches by issuing the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/3020_configure.xml
Processing file: /usr/TKLC/smac/etc/switch/xml/3020_configure.xml
$
```

Note: This step takes about 2-3 minutes to complete

Check the output of this command for any errors. If the file fails to configure the switch, please review/troubleshoot the file first. If troubleshooting is unsuccessful, stop this procedure and contact Customer Care Center.

A successful completion of netConfig will return the user to the prompt.

10. **Virtual PM&C:** Verify switch configuration

To verify the configuration was completed successfully, execute the following command and review the configuration:

```
# sudo /usr/TKLC/plat/bin/netConfig showConfiguration --device=<switch_name>
Configuration:  = (
   Building configuration...

   Current configuration : 3171 bytes
   !
   ! Last configuration change at 23:54:24 UTC Fri Apr 2 1993 by plat
   !
```

```
   version 12.2

<output removed to save space >

   monitor session 1 source interface Gi0/2 rx
   monitor session 1 destination interface Gi0/1 encapsulation replicate
   end

   )
```

Return to step 4 and repeat for each 3020 switch.

11. Virtual PM&C: Modify PM&C Feature to disable TFTP.

    Disable the DEVICE.NETWORK.NETBOOT feature:

```
$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT
 --enable=0
$  sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
```

    Note: This may take up to 60 seconds to complete.

12. Perform *F.2 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)* for each switch configured in this procedure

4.8.2 Configure HP 6120XG Switches

4.8.2.1 Configure HP 6120XG switch (netConfig)

This procedure will configure the HP 6120XG switches from the PM&C server & the command line interface using templates included with an application.

Needed materials:

- HP Misc. Firmware DVD
- HP Solutions Firmware Upgrade Pack Release Notes [3]
- Application specific documentation (documentation that referred to this procedure)
- Template xml files in an application ISO on an application CD.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Virtual PM&C:** Prepare for switch configuration

   If the aggregation switches are provided by Tekelec, login to the management server, then run:

```
$ /bin/ping -w3 <switch1A_mgmtVLAN_address>
$ /bin/ping -w3 <switch1B_mgmtVLAN_address>
$ /bin/ping -w3 <switch_mgmtVLAN_VIP>
```

   If the aggregation switches are provided by the customer, login to the management server, then run:

```
$ /bin/ping -w3 <mgmtVLAN_gateway_address>
```

2. **Virtual PM&C:** Verify network connectivity to 6120XG switches

For each 6120XG switch, verify network reachability.

```
$ /bin/ping -w3 <enclosure_switch_IP>
```

3. **Virtual PM&C:** Restore switch to factory defaults

   If the 6120XG switch has been configured prior to this procedure, clear out the configuration using the following command:

```
$ /usr/bin/ssh manager@<enclosure_switch_IP>
Switch# config
Switch(config)# no password all
Password protection for all will be deleted, continue [y/n]? y
Switch(config)# end
Switch# erase startup-config
Configuration will be deleted and device rebooted, continue [y/n]? y
(switch will automatically reboot, reboot takes about 120-180 seconds)
```

   Note: You may need to press [ENTER] twice. You may also need to use previously configured credentials.

   If the above procedures fails, log in via telnet and reset the switch to manufacturing defaults. If the above ssh procedures fails, log in via telnet and reset the switch to manufacturing defaults

```
$ /usr/bin/telnet <enclosure_switch_IP>
Switch# config
Switch(config)# no password all (answer yes to question)
Password protection for all will be deleted, continue [y/n]? y
Switch(config)# end
Switch# erase startup-config
(switch will automatically reboot, reboot takes about 120-180 seconds)
```

   Note: The console connection to the switch must be closed, or the initialization (step 8) will fail.

4. **Virtual PM&C:** Copy switch configuration template from media to the tftp directory.

   Copy switch initialization template and configuration template from the media to the tftp directory.

```
$ sudo /bin/cp -i /<path to media>/6120XG_init.xml /usr/TKLC/smac/etc/switch/xml
$ sudo /bin/cp -i /<path to media>/6120XG_[single,LAG]Uplink_configure.xml
/usr/TKLC/smac/etc/switch/xml
$ sudo /bin/cp -i
/usr/TKLC/plat/etc/TKLCnetwork-config-templates/templates/utility/addQOS_trafficTemplate_6120XG.xml
 /usr/TKLC/smac/etc/switch/xml
```

   - Where **[single,LAG]** are variables for either one of 2 files-see the following:
     - `6120XG_SingleUplink_configure.xml` is for one uplink per enclosure switch topology
     - `6120XG_LAGUplink_configure.xml` is for LAG uplink topology

5. **Virtual PM&C:** verify the switch configuration file template in the tftp directory

   Verify the switch initialization template file and configuration file template are in the correct directory.

```
$ /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/*6120XG*.xml
-rw-r--r-- 1 root root 1955 Feb 16 11:36
/usr/TKLC/smac/etc/switch/xml/6120XG_init.xml
-rw-r--r-- 1 root root 1955 Feb 16 11:36
```

```
/usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml
-rw-r--r-- 1 root root 702 Sep 10 10:33 addQOS_trafficTemplate_6120XG.xml
```

6. **Virtual PM&C:** Edit the switch configuration file template for site specific information

   Edit the switch initialization file and switch configuration file template for site specific addresses, VLAN IDs, and other site specific content. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$<some_variable_name>** will need to be modified, removing the dollar sign and the less than, greater than sign.

```
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6120XG_init.xml
$ sudo /bin/vi
/usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml
$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml
```

7. **Virtual PM&C:** Apply include-credentials command to the switch

   Login to the switch using SSH

```
$ /usr/bin/ssh manager@<enclosure_switch_IP>
Switch# config
Switch(config)# include-credentials
```

   If prompted, answer yes to both questions.

   Log out of the switch.

```
Switch(config)# logout
Do you want to log out [y/n]? y
Do you want to save current configuration [y/n/^C]?  y
```

   Continue to the next step.

8. **Virtual PM&C:** Initialize the switch

   Initialize the switch

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/6120XG_init.xml
```

   This could take up to 2-3 minutes.

   Note: Upon successful completion of netConfig, the user will be returned to the PM&C command prompt. If netConfig fails to complete successfully, contact Tekelec Customer Service

9. **Virtual PM&C:** Configure the switch

   Configure the switch

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml
```

   This could take up to 2-3 minutes.

   Note: Upon successful completion of netConfig, the user will be returned to the PM&C command prompt. If netConfig fails to complete successfully, contact Tekelec Customer Service

10. **Virtual PM&C:** Apply QoS Settings

Apply the QoS traffic template settings.

```
$ sudo /usr/TKLC/plat/bin/netConfig
--file=/usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml
```

Note: The switch will reboot after this command. This step will take 2-5 minutes.

11. **Virtual PM&C:** Verify proper configuration of HP 6120XG switches

    Once each HP 6120XG has finished booting from the previous step, verify network reachability and configuration.

```
$ /bin/ping -w3 <enclosure_switch_IP>
$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP>
<switch_platform_username>@<enclosure_switch_IP>'s password:
<switch_platform_password>
Switch# show run
```

    Inspect the output of `show run`, and ensure that it is configured as per site requirements.

12. **Virtual PM&C:** Repeat steps for each HP 6120XG

    For each HP 6120XG, repeat steps 3-12.

13. Perform *F.1 Backup HP (6120XG, 6125G) Enclosure Switch* for each switch configured in this procedure.

4.9 Server Blades Installation Preparation

4.9.1 Upgrade Blade Server Firmware

This procedure will provide the steps to upgrade the firmware on the Blade servers.

The HP Support Pack for ProLiant installer automatically detects the firmware components available on the target server and will only upgrade those components with firmware older than what is on the current ISO.

Needed Materials:

- Tekelec's HP Service Pack for ProLiant (SPP) USB media or ISO file
- Tekelec's HP Misc Firmware USB media or ISO file (for errata updates is applicable)
- HP Solutions Firmware Upgrade Pack Release Notes [3]
- USB Flash Drive (1GB or larger) if not starting with Tekelec USB media

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

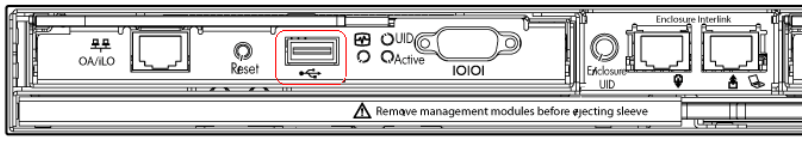
1. **Local Workstation:** When starting with ISO files, Prepare the USB Flash Drive

   Copy the HP Support Pack for ProLiant ISO to the USB Flash Drive.

   If starting with Tekelec USB media this is unnecessary, continue to the next step.

2. Insert USB Flash Drive

Insert the USB Flash Drive with the HP Support Pack for ProLiant ISO into the USB port of the Active OA Module.



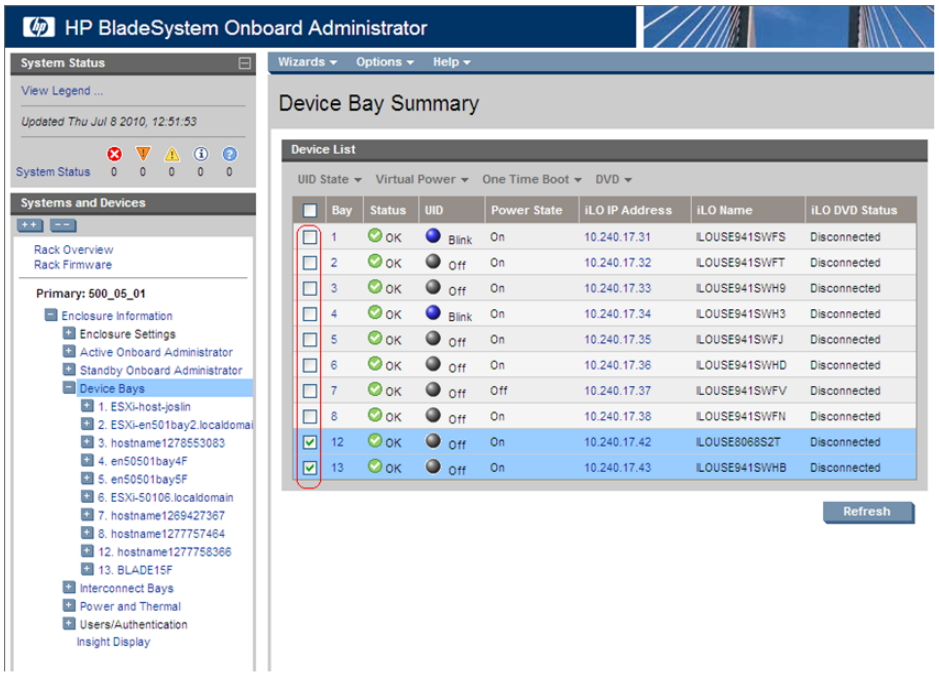
3. **Active OAGUI:** Login

   Navigate to the IP address of the active OA, using Appendix C (*Determining which Onboard Aministrator is Active*). Login as an administrative user.

4. **OA Web GUI:** Access the Device Summary page

   On the left pane, expand the **Device Bays** node to display the **Device Bay Summary** window.

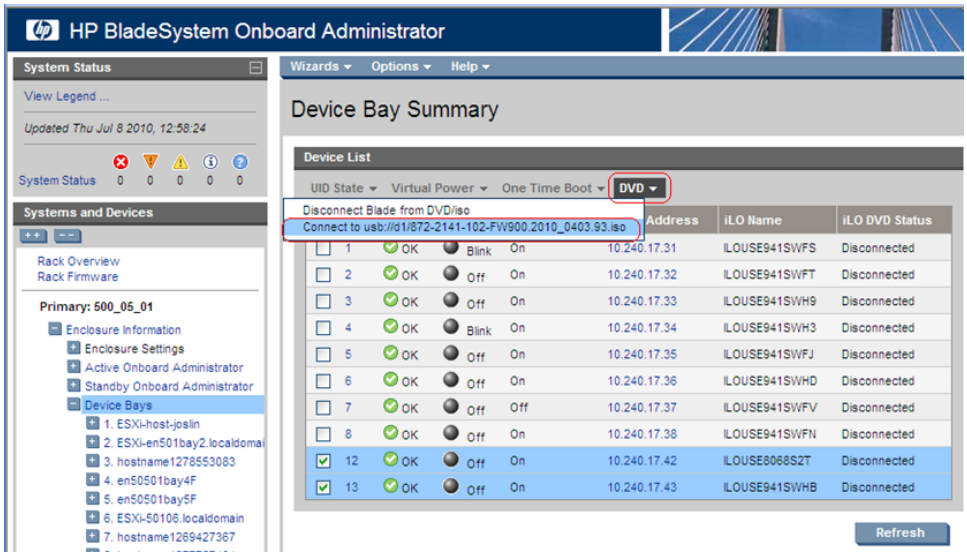
   Select the individual blades to be upgraded by clicking and enabling the corresponding UID checkbox.



Note: A maximum of 8 blades should be upgraded concurrently at one time. If the c7000enclosure has more than 8 blades they will need to be upgraded in multiple sessions.

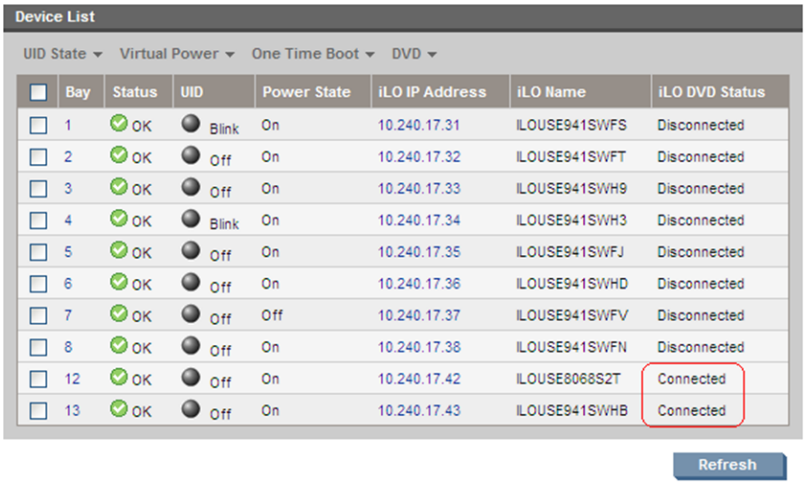
5. **OA Web GUI:** Connect to USB Drive

   Once the blades are selected, connect them to the ISO on the USB Drive, by selecting the **Connect to usb…** item from the **DVD** menu.



6. **OA Web GUI:** Verify Drive Connection

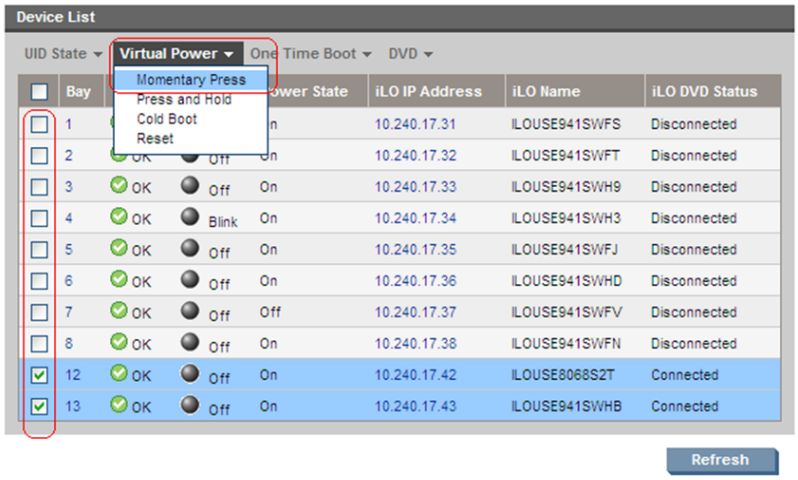
   Once each blade has mounted the ISO media the **`Device List`** table should indicate an **`iLO DVD Status`** as **`Connected`** for each blade that was previously selected.



Note: The **Refresh** button may need to be clicked in order to see the current status of all blades.

7. **OA Web GUI:** Power Down Blades

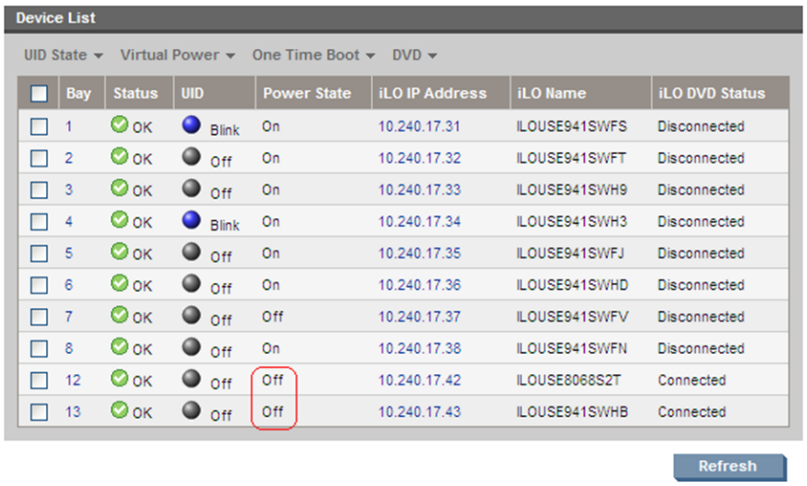
   If needed, reselect the UID checkbox for each blade to be upgraded and then select the **Momentary Press** option under the **`Virtual Power`** menu.



When prompted click the **OK** button to confirm the action.

8. **OA Web GUI:** Verify Power Down

   The power down sequence can take several minutes to complete. When it completes the **`Device List`** table will indicate the **`Power State`** of each select blade to be **`Off`**.



Note: The **Refresh** button may need to be clicked in order to see the current status of all blades.

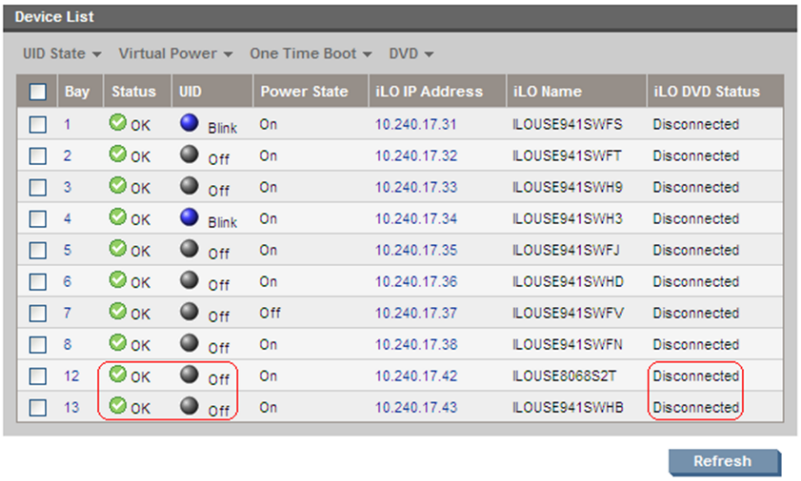
9. **OA Web GUI:** Initiate Firmware Upgrade

   To power the blades back on and begin the automated firmware upgrade process, repeat Steps 7 and 8 this time being sure the **`Power State`** indicates **`On`** for each selected blade.

10. **OA Web GUI:** Monitor Firmware Upgrade

    From this point on each blade will boot into an automated firmware upgrade process that will last between 20 to 25 minutes. During this time all feedback is provided through the UID lights. While the update process is running, the UID light blinks.

The UID lights will not blink until the server fully boots and the firmware upgrades have started to be applied. If no upgrades are needed the UID lights will not blink, but the server will still reboot and the iLO DVD will disconnected after completion.



Upon a successful firmware upgrade, the **`Device List`** table will list each blade with a **Status** of **`OK, UID`** of **`Off`** and the **`iLO DVD Status`** as **`Disconnected`**. At this time the blades will automatically be rebooted.

Note: Make sure all blades have disconnected before continuing. If any blades are still connected after their UIDs have stopped blinking and Status=OK, disconnect them manually by selecting **Disconnect Blade from DVD/ISO from** the DVD menu. If the UID led is solid, a failure has occurred during the firmware upgrade. Use the iLO's integrated remote console or a kvm connection to view the error.

If necessary, repeat Steps 4 through 10 for the remaining blades in the enclosure to be upgraded. Proceed to the next step.

11. Remove USB Flash Drive

The USB flash drive may now safely be removed from the Active OA module.

12. Update Firmware Errata

Check the HP Solutions Firmware Upgrade Pack Release Notes [3] to see if there are any firmware errata items that apply to the server being upgraded.

If there is, there will be a directory matching the errata's ID in the /errata directory of the HP Misc Firmware ISO. The errata directories contain the errata firmware and a README file detailing the installation steps.

4.9.2 Confirm/Upgrade Blade Server BIOS Settings

This procedure will provide the steps to confirm and update the BIOS boot order on the blade servers. All servers should have SNMP disabled. Refer to Appendix J *Changing SNMP Configuration Settings for iLO*

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

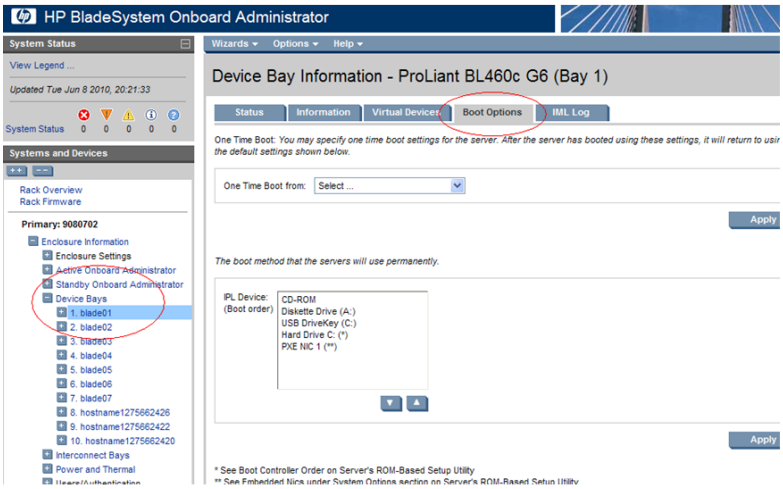
1. **Active OAGUI:** Login

   Navigate to the IP address of the active OA, using Appendix C (*Determining which Onboard Administrator is Active*). Login as an administrative user.

2. **Active OAGUI:** Navigate to device Bay Settings

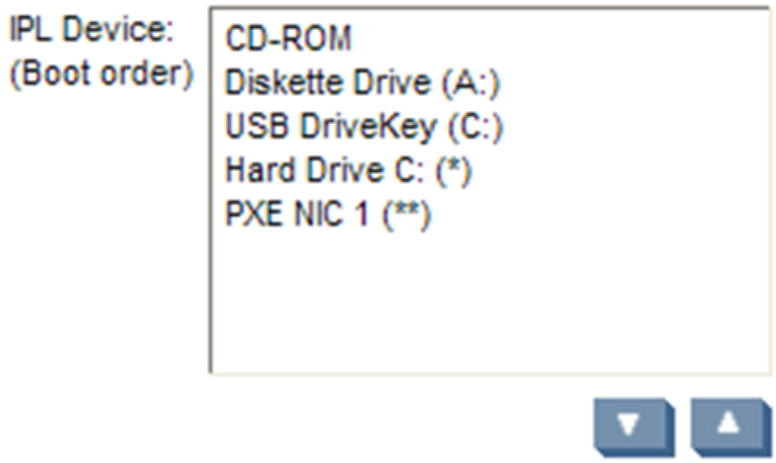
   Navigate to **Enclosure Information** > **Device Bays** > **<Blade 1>**

   Click on **Boot Options** tab.



3. **Active OAGUI:** Verify/update Boot device Order

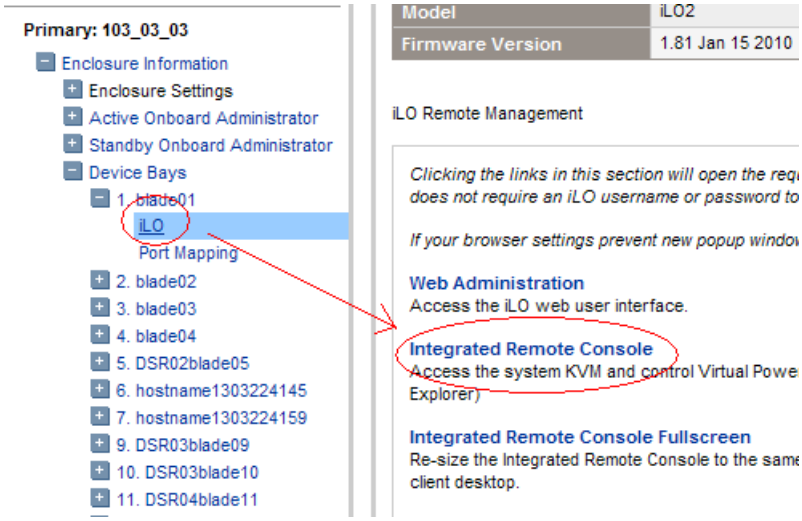
   Verify that the Boot order is as follows. If it is not, use the up and down arrows to adjust the order to match the picture below, then click on **Apply**



4. **OA:** Access the Blade iLO

   Navigate to **Enclosure Information** > **Device Bays** > **<Blade 1>** > **iLO**

   Click on **Integrated Remote Console**



   This will launch the iLO interface for that blade. If this is the first time the iLO is being accessed, you will be prompted to install an addon to your web browser, follow the on screen instructions to do so.

5. **OA:** Restart the blade and access the BIOS

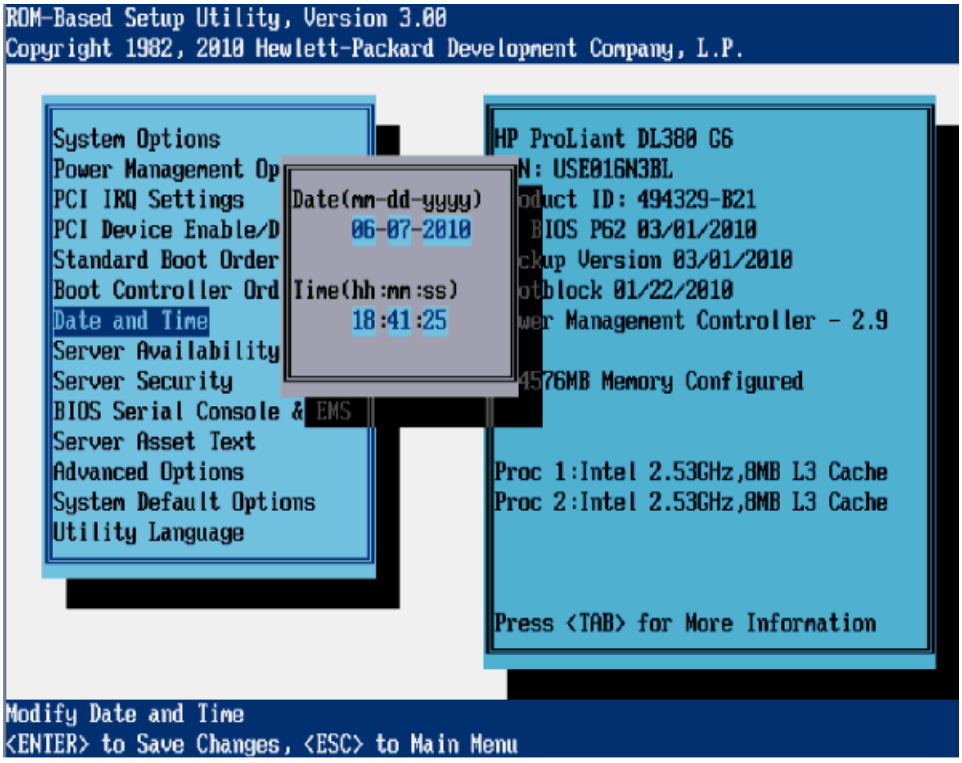
   You might be prompted with a certificate security warning, just press continue.

   Once a prompt is displayed, login onto the blade using the "admusr" username.

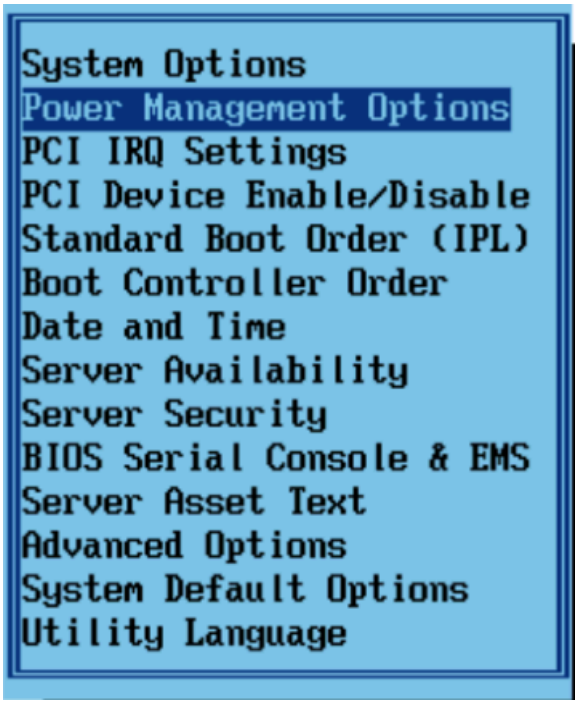
   Once logged in, Reboot the server (using the "reboot" command) and after the server is powered on, as soon as you see <F9=Setup> in the lower left corner of the screen, press **F9** to access the BIOS setup screen.

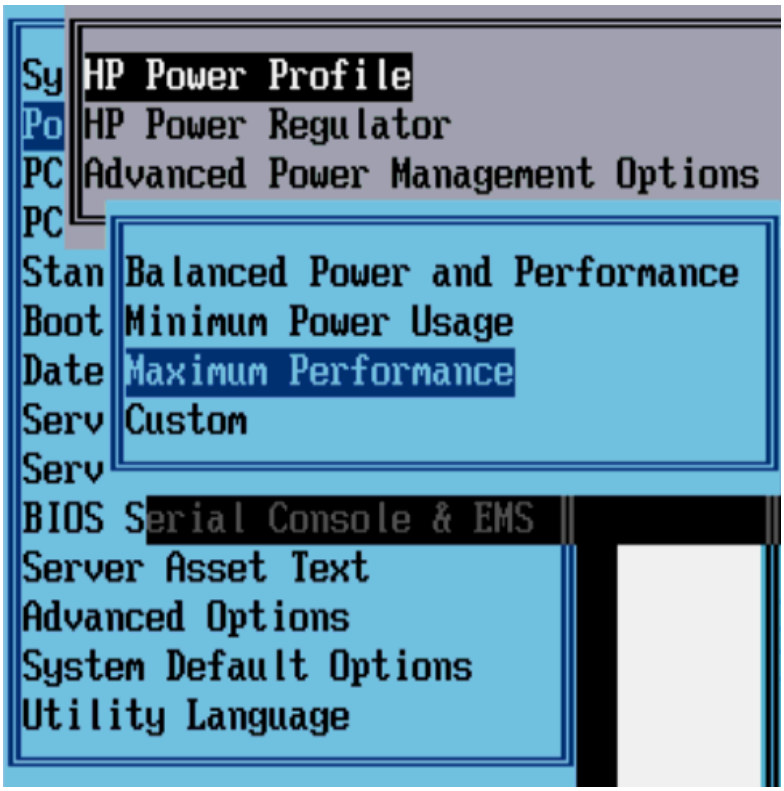
6. **OA:** Updated BIOS settings

1. Scroll to **Date and Time** and press **Enter**
2. Set current date, set current UTC time and press **Enter**



3. Go back to the main menu by pressing **<ESC>** and scroll down to **Power Management Options** and press **Enter**
4. Select **HP Power Profile** and press **Enter**
5. Scroll down to **Maximum Performance** and press **Enter**





6. Press **<ESC>** twice to return to exit the BIOS setup screen and **F10** to confirm, exiting the utility
7. The blade will reboot afterwards

7. **Active OAGUI:** Repeat for the remaining blades

   Repeat Steps 2 through 6 for the remaining blades. Once done, exit out of the OA GUI.

4.10 Installing TVOE on Rack Mount Server(s)

Note: This procedure is specific to RMS servers that will be managed by PMAC, and do not yet have a TVOE environment configured. It requires that the RMS server is on the PMAC control network (i.e., it is able to receive a DHCP IP address from PMAC on the 192.168.1.0 network).

This is an "IPM" activity for a server that will be a Virtual Host.

4.10.1 Add Rack Mount Server to the PM&C System Inventory

This procedure provides instructions to add a rack mount server to the PM&C system inventory.

Prerequisite:

- *4.4.1.1 Configure PM&C application* has been completed.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

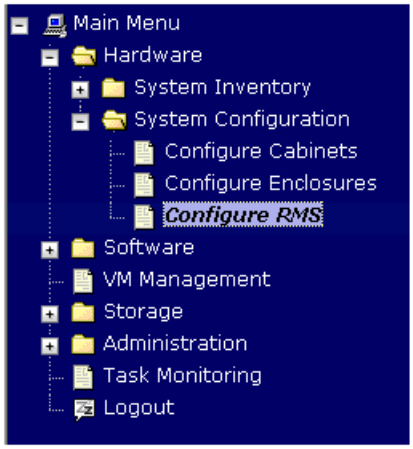
1. **PM&C GUI:** Login

   Open web browser and enter:

   ```
   https://<pmac_management_network_ip>
   ```

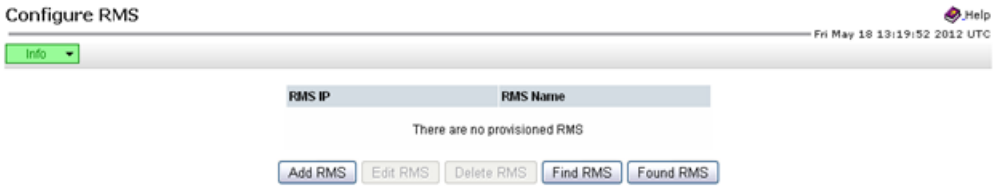
2. **PM&C GUI:** Configure RMS

   Navigate to **Main Menu** > **Hardware** > **System Configuration** > **Configure RMS**

3. **PM&C GUI:** Add RMS

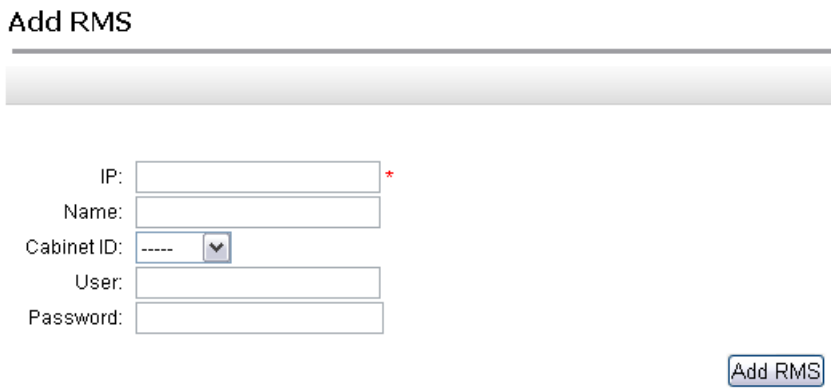
   On the Configure RMS panel, click the Add RMS button.



4. **PM&C GUI:** Enter information

   Enter the IP Address of the rack mount server management port (iLO). All the other fields are optional.

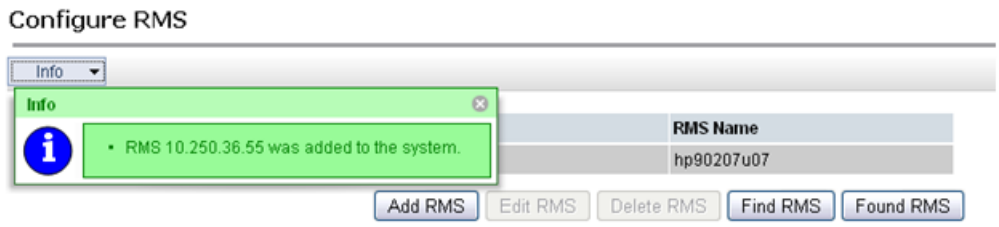
   Then click on the **Add RMS** button.



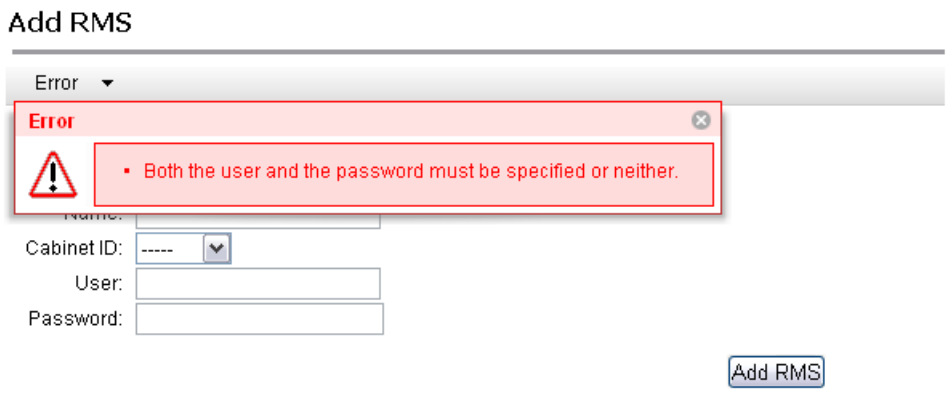
   Note: The PM&C contains default credentials for the rack mount server management port (not to be confused with OS or Application credentials), however if you know the default credentials will not work then enter the valid credentials for the rack mount server management port.

5. **PM&C GUI:** Check errors

   If no error is reported to the user you will see the following:

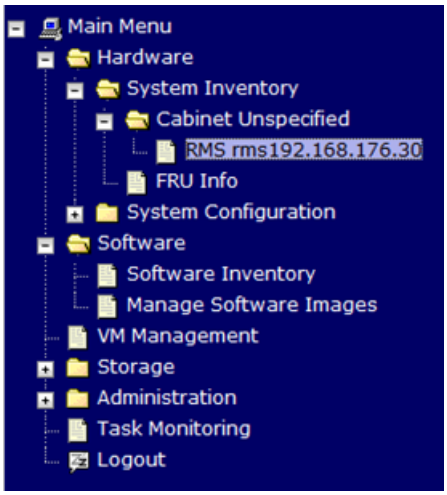


   Or you will see an error message:

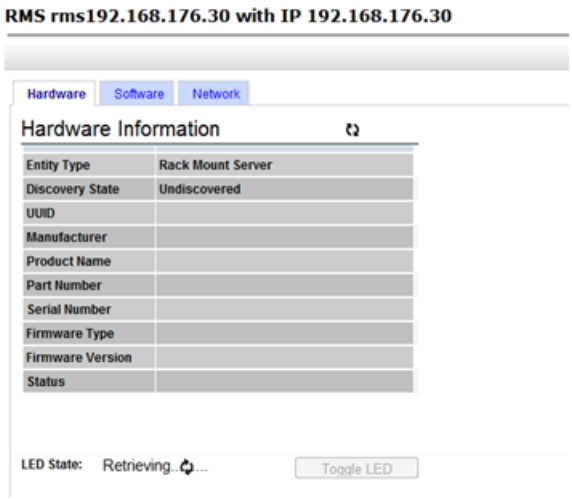


6. **PM&C GUI:**Verify RMS discovered

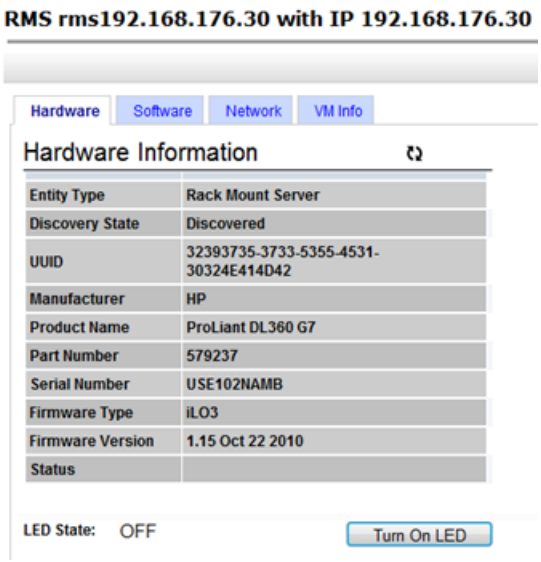
   Navigate to **Main Menu** > **Hardware** > **System Inventory** > **Cabinet xxx** > **RMS yyy** Where **xxx** is the cabinet id selected when adding RMS (or "unspecified") and **yyy** is the name of the RMS.



   The RMS inventory page is displayed.



Periodically refresh the hardware information using the double arrow to the right of the title "Hardware Information" until the "Discovery state" changes from "Undiscovered" to "Discovered". If "Status" displays an error, contact the Customer Care Center for assistance by referring to the *1.4 Customer Care Center* section of this document.



4.10.2 Add ISO Image to the PM&C Repository

If the Rack Mount Server (RMS) is to be configured as a TVOE hosting application guests execute this procedure using the applicable TVOE ISO as the image to add, otherwise continue to next procedure.

4.10.2.1 Adding ISO Images to the PM&C Image Repository

Note: If the ISO image has already been added to the PM&C Software Inventory in a previous procedure, skip this procedure.

This procedure provides the steps for adding ISO images to the PM&C repository.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. Make the image available to PM&C

   There are three ways to make an image available to PM&C:

   - Insert the CD containing an iso image into the removable media drive of the PM&C server.
   - Attach the USB device containing the ISO image to a USB port of the Management Server.
   - Use sftp to transfer the iso image to the PM&C server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
     - cd into the directory where your ISO image is located (not on the PM&C server)
     - Using sftp, connect to the PM&C management server

```
> sftp pmacftpusr@<pmac_management_network_ip>
> put <image>.iso
```

     - After the image transfer is 100% complete, close the connection

```
> quit
```

   Refer to the documentation provided by application for pmacftpusr password.

2. **PM&C GUI:** Login

   Open web browser and enter:

```
https://<pmac_management_network_ip>
```

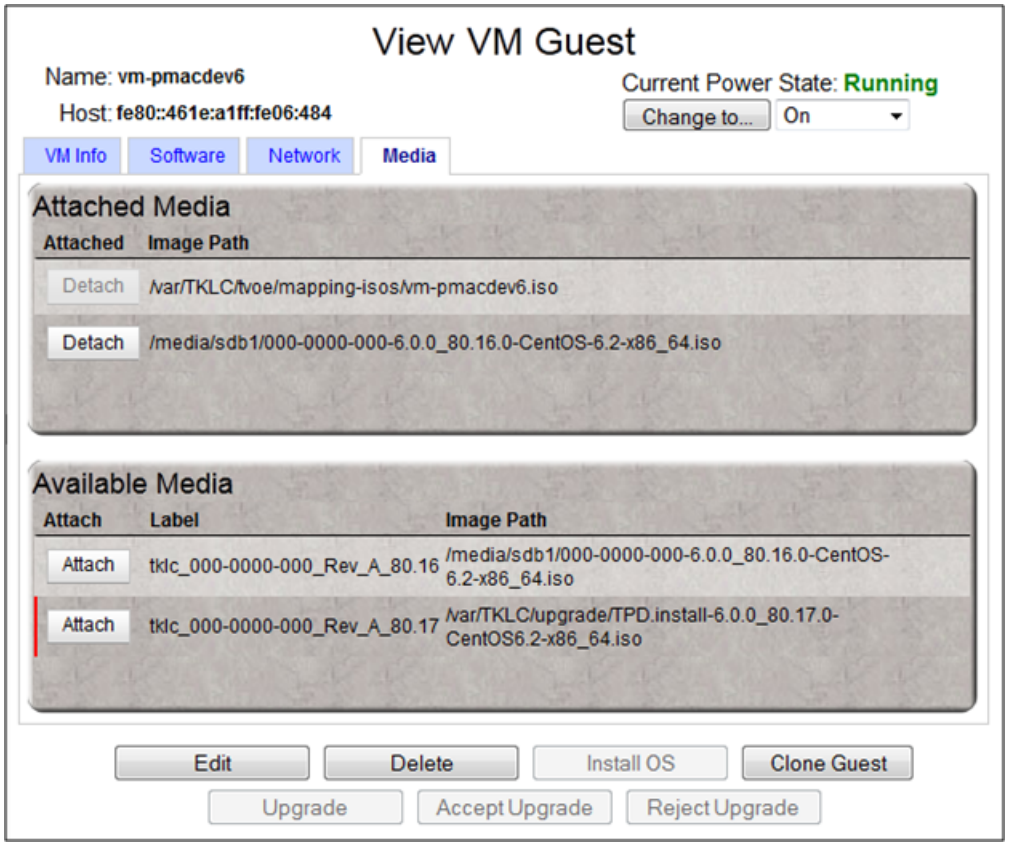
   Login as pmacadmin user.

3. **PM&C GUI:** Attach the software image to the PM&C guest

   If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step.

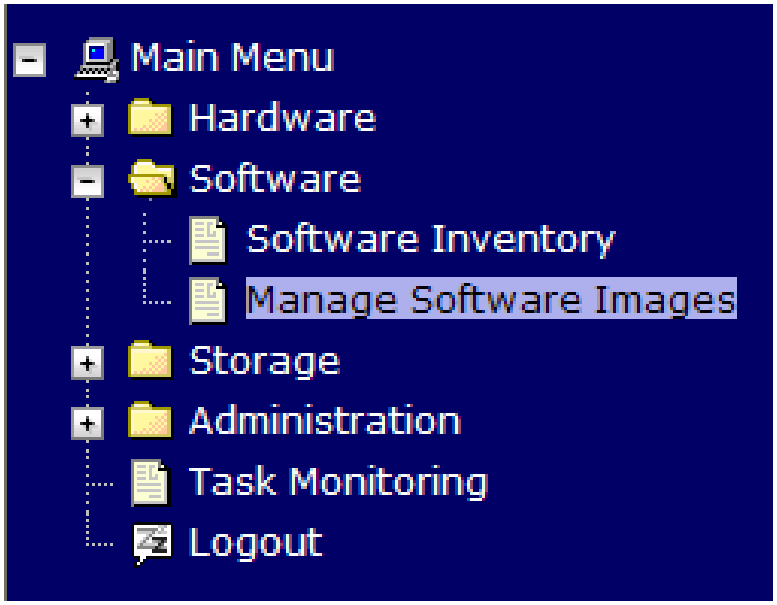
   In the PM&C GUI, navigate to **Main Menu** > **VM Management.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab.

   Under the **Media** tab, find the ISO image in the "**Available Media**" list, and click its "**Attach**" button. After a pause, the image will appear in the "**Attached Media**" list.



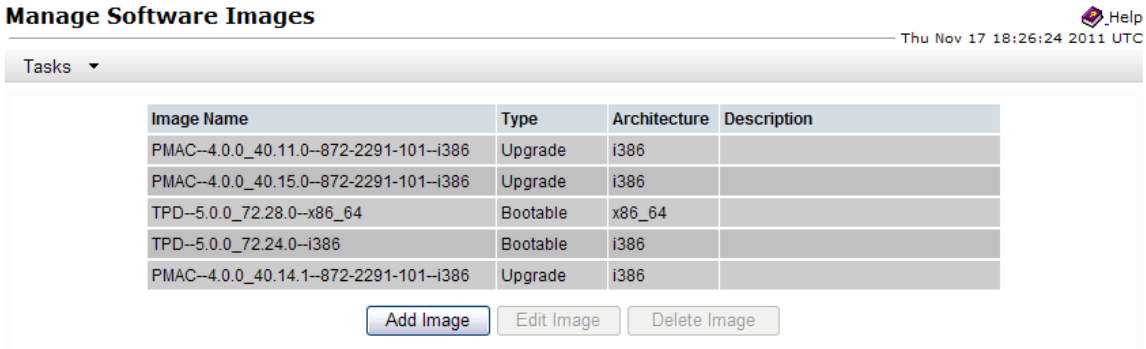
4. **PM&C GUI:** Navigate to Manage Software Images

   Navigate to **Main Menu** > **Software** > **Manage Software Images**



5. **PM&C GUI:**Add image

Press the **Add Image** button .



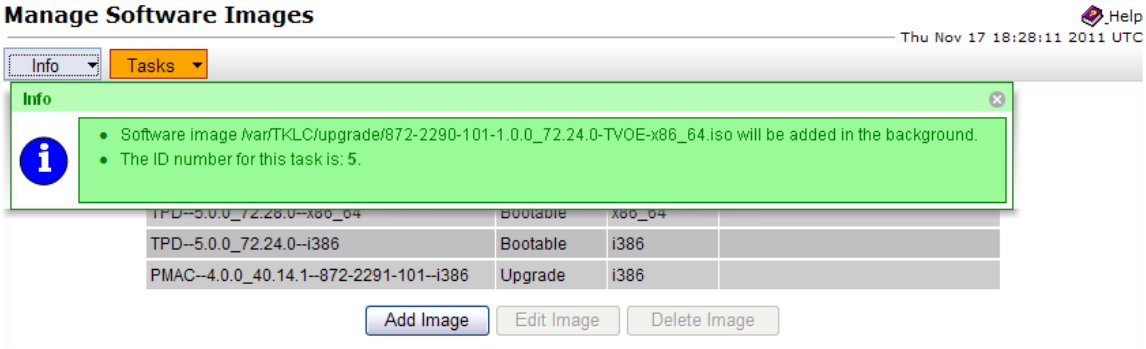
6. **PM&C GUI:** Add the ISO image to the PM&C image repository.
   Select an image to add:

   - If in Step 1 the image was transferred to PM&C via sftp it will appear in the list as a local file "/var/TKLC/...".
   - If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number.

   Enter an appropriate image description and press the **Add New Image** button.

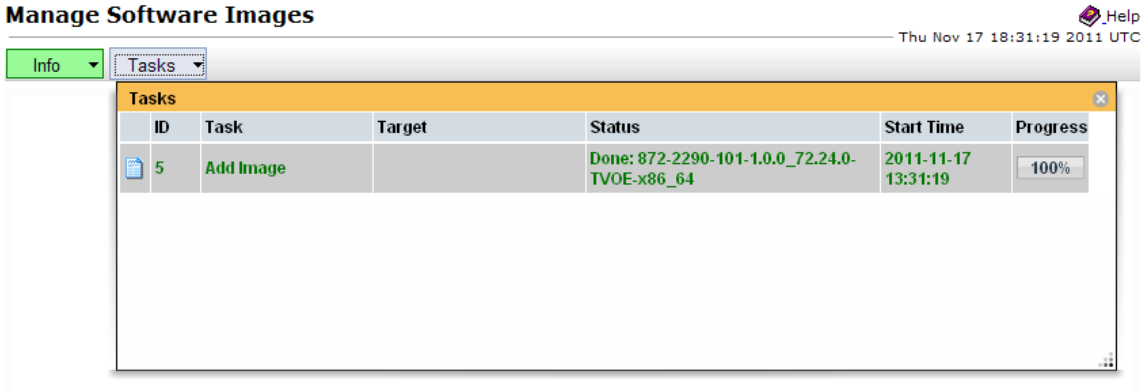
7. **PM&C GUI** Monitor the Add Image status

The `Manage Software Images` page is then redisplayed with a new background task entry in the table at the bottom of the page:



8. **PM&C GUI** Wait until the Add Image task finishes

   When the task is complete, its text changes to green and its Progress column indicates "100%". Check that the correct image name appears in the Status column:



9. **PM&C GUI:** Detach the image from the PM&C guest

   If the image was supplied on CD or USB, return to the PM&C guest's "**Media**" tab used in Step 3, locate the image in the "**Attached Media**" list, and click its "**Detach**" button. After a pause, the image will be removed from the "**Attached Media**" list. This will release the virtual device for future use.

   Remove the CD or USB device from the Management Server.

   Note: If there are additional ISO images to be provisioned on the PM&C, repeat the procedure with the appropriate ISO image data.

4.11 Initial Product Manufacture of Application Server

The PM&C application is capable of installing bootable software on an application server, RMS or blade server, provisioned on the PM&C through the execution of adding the RMS or the enclosure. The following procedure provides the steps necessary to IPM (either TPD or TVOE) an application server. The appropriate is required to be added to the PM&C repository for this procedure to proceed.

4.11.1 IPM Servers Using PM&C Application

This procedure provides the steps for installing TPD using an image from the PM&C image repository.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **PM&C GUI:** Login

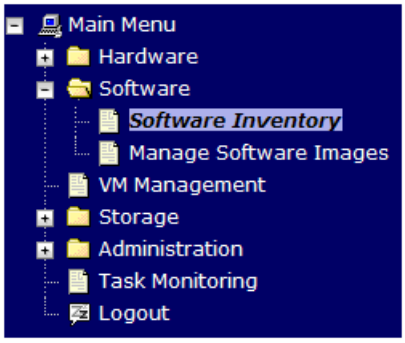
   If needed, open web browser and enter:

   ```
   https://<pmac_management_network_ip>
   ```

   Login as the pmacadmin user.

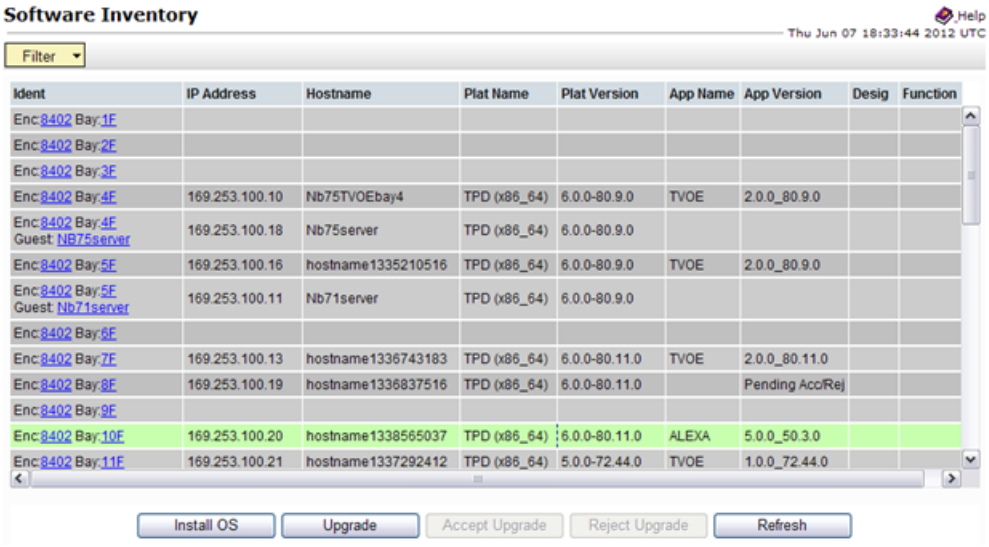
2. **PM&C GUI:** Navigate to the Software Inventory

   Navigate to **Main Menu** > **Software** > **Software Inventory**.



3. **PM&C GUI:** Select Servers

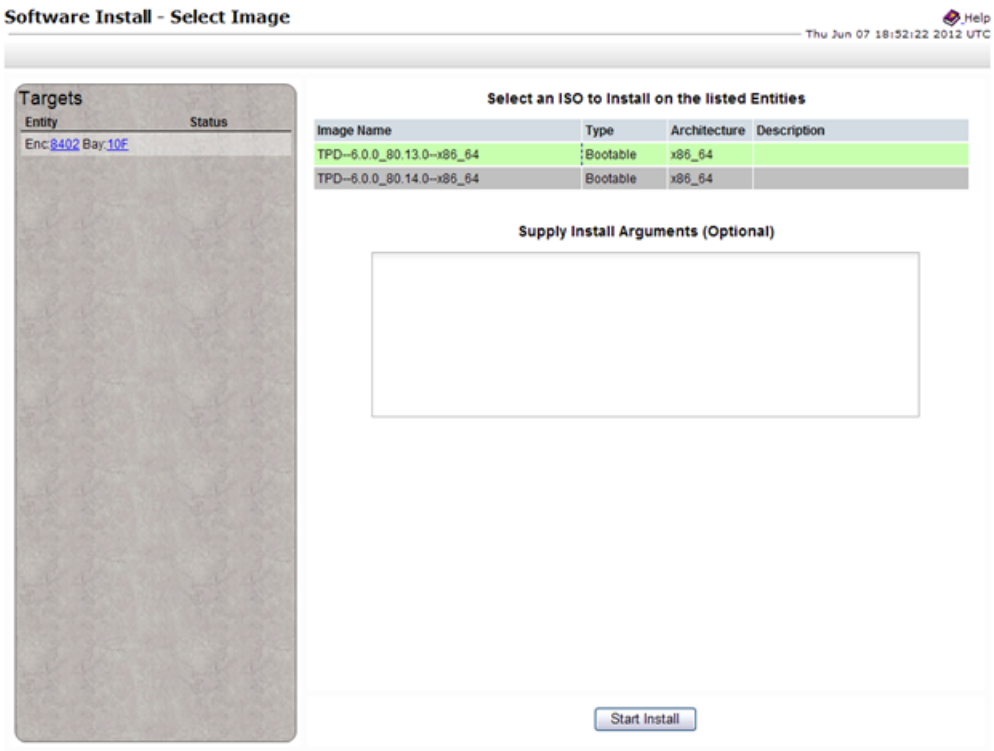
   Select the servers you want to IPM. If you want to install the same OS on more than one server, you may select multiple servers by individually clicking multiple rows. Selected rows will be highlighted in green.



Press the **Install OS** button.

4. **PM&C GUI:** Select Image

   The left side of the screen displays the servers to be affected by the OS installation. From the list of available bootable images on the right side of the screen, select the OS image to install on the selected servers.



5. **PM&C GUI:** Supply Install Arguments (Optional)

   Install arguments can be supplied by entering them into the text box displayed under the list of bootable images. These arguments will be appended to the kernel line during the IPM process. If no install arguments need to be supplied for the OS being installed, leave the install arguments text box empty.

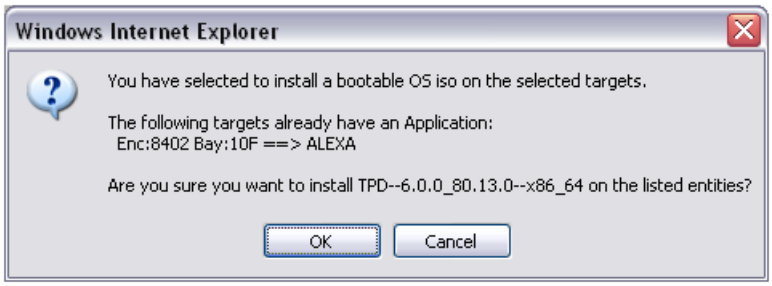
   Note: The valid arguments for a TPD IPM are listed in Appendix D.

6. **PM&C GUI:** Start Install

   Press the **Start Install** button.

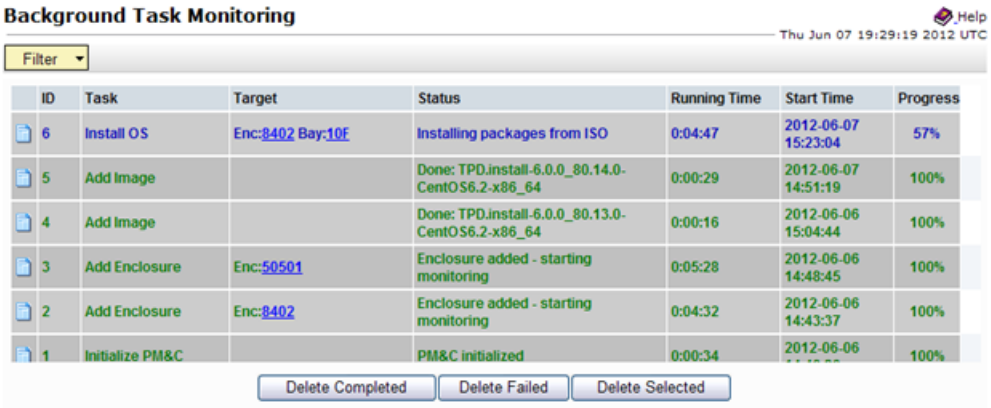
7. **PM&C GUI:** Confirm OS Install

   Press the **OK** button to proceed with the install.



8. **PM&C GUI:** Monitor Install OS

   Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Install OS background task. A separate task will appear for each server affected.



   When the task is complete and successful, its text will change to green and its Progress column will indicate "100%".

   Note: Repeat this procedure for additional RMS servers with appropriate data.

Appendix A

Accessing Tekelec Customer Support Site

Topics:

A.1 Accessing Tekelec's Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at *www.adobe.com*.

1. Log into the *Tekelec Customer Support* site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Appendix B

NetBackup Procedures (Optional)

Topics:

B.1 Netbackup Client Install/Upgrade with nbAutoInstall

Executing this procedure will enable TPD to automatically detect when a Netbackup Client is installed and then complete TPD related tasks that are needed for effective Netbackup Client operation. With this procedure, the Netbackup Client install (pushing the client and performing the install) is the responsibility of the customer and is not covered in this procedure.

Note: If the customer does not have a way to push and install Netbackup Client, then use *B.2 NetBackup Client Install/Upgrade with platcfg*.

Note: It is required that this procedure is executed before the customer does the Netbackup Client install.

1. **Follow Tekelec Provided Workarounds**

   Follow Tekelec provided procedures to prepare the server for Netbackup Client install using nbAutoInstall.

2. **Enable nbAutoInstall:**

   Execute the following command:

   ```
   $ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable
   ```

   The server will now periodically check to see if a new version of Netbackup Client has been installed and will perform necessary TPD configuration accordingly.

   At any time, the customer may now push and install a new version of Netbackup Client.

3. Return to calling procedure if applicable.

B.2 NetBackup Client Install/Upgrade with platcfg

Executing this procedure will push and install NetBackup Client via platcfg menus.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Application server iLO:** Login and launch the integrated remote console

   Log in to iLO in IE using password provided by application

   ```
   http://<management_server_iLO_ip>
   ```

   Click in the **Remote Console** tab and launch the **Integrated Remote Console** on the server.

   Click **Yes** if the `Security Alert` pops up.

2. **TVOE Application Server iLO:** If the application is a guest on a TVOE host: Log in with application admusr credentials. If the application is not a guest on a TVOE host continue to step 3.

   Note: On a TVOE host, If you launch the virsh console, i.e., "# **`virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the

TVOE host. Exit out of the "virsh console", then run "**`ps -ef |grep virsh`**", then kill the existing process "**`kill -9 <PID>`**". Then execute the "virsh console X" command. Your console session should now run as expected.

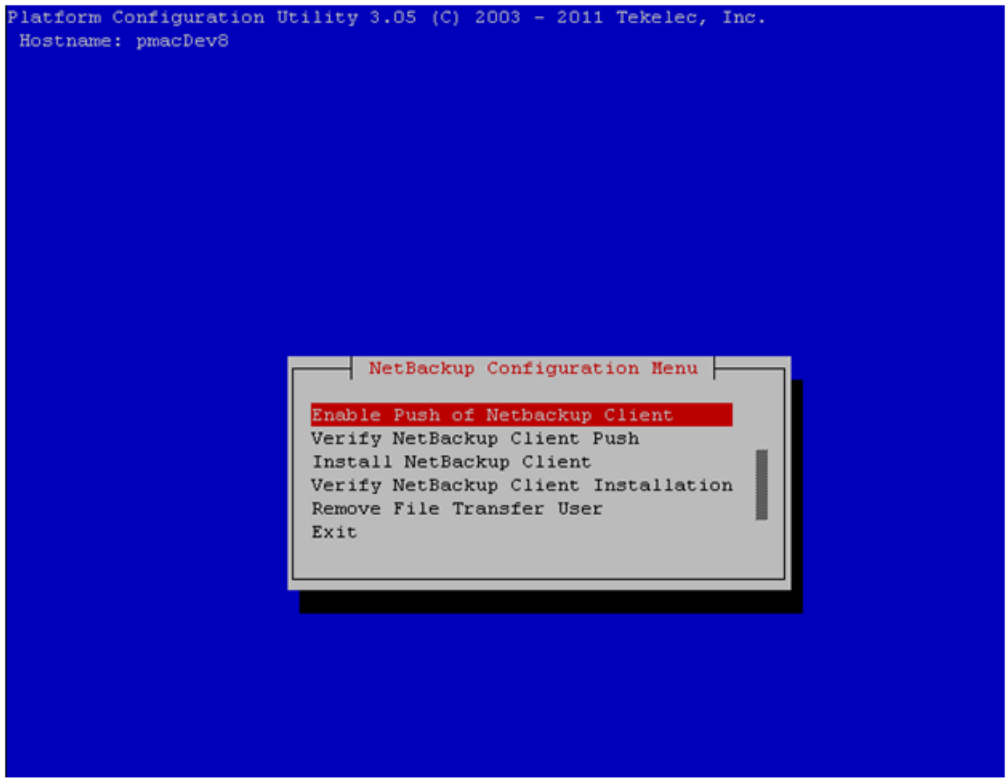
Login to application console using virsh, and wait until you see the login prompt:

```
$ virsh
virsh $ list --all
Id Name State
----------------------------------
13 myTPD running
20 applicationGuestName running

virsh $ console applicationGuestName
[Output Removed]
Starting ntdMgr: [ OK ]
Starting atd: [ OK ]
'TPD Up' notification(s) already sent: [ OK ]
upstart: Starting tpdProvd...
upstart: tpdProvd started.
CentOS release 6.2 (Final)
Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.14.0.x86_64 on an x86_64
applicationGuestName login:
```

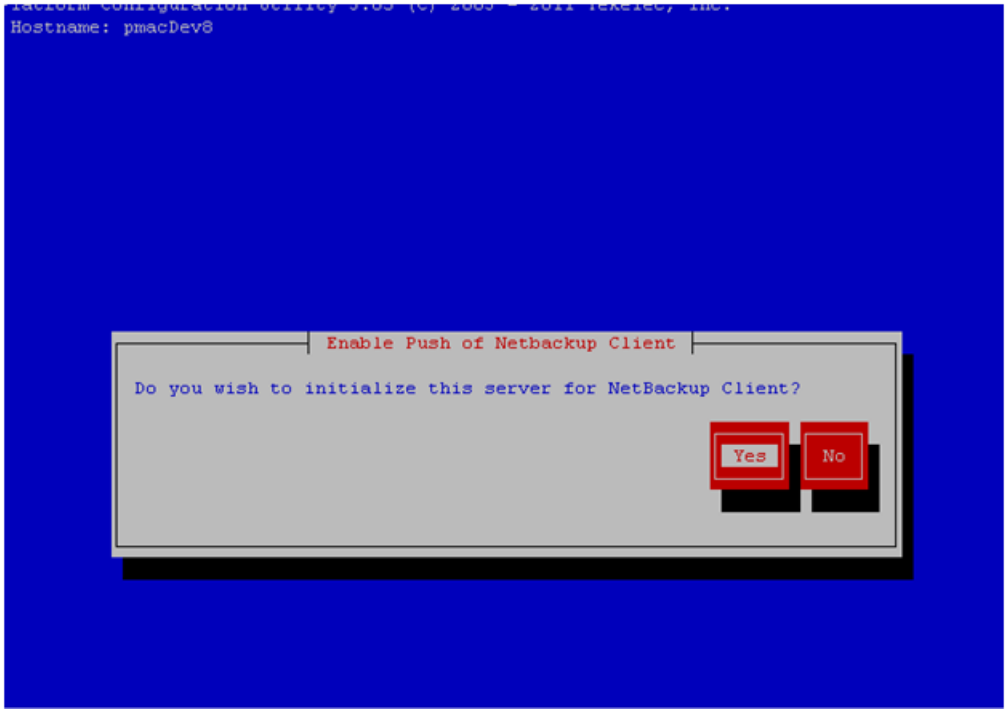
3. **Application Console**: Configure NetBackup Client on application server

```
$ sudo su - platcfg
```

Navigate to **NetBackup Configuration**

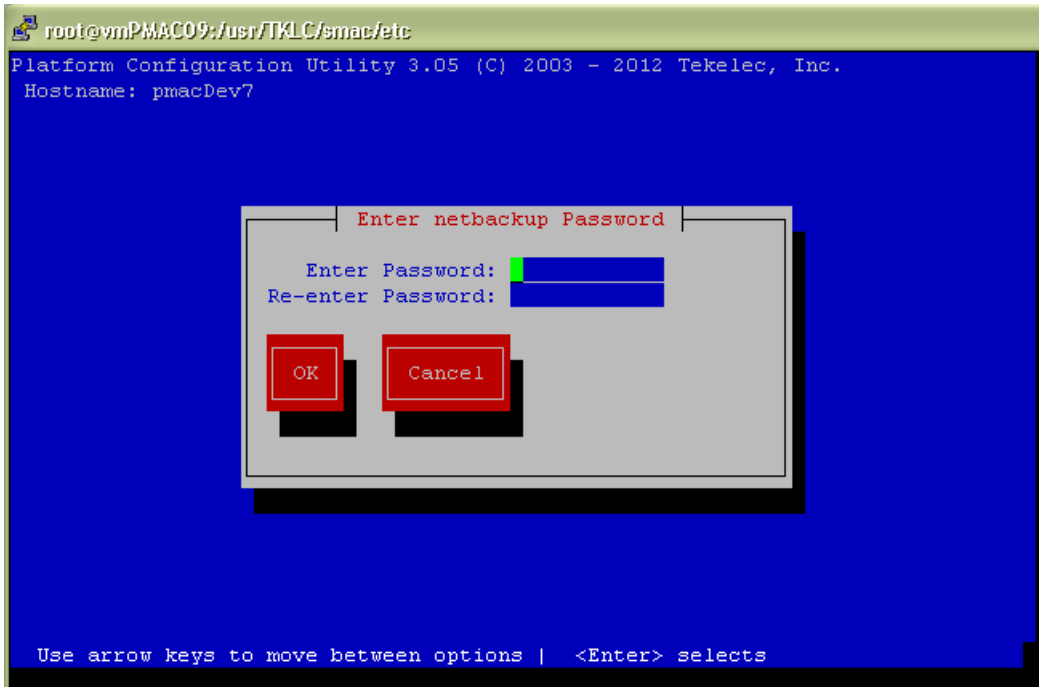


4. **Application Console**: Enable Push of NetBackup Client
   Navigate to **NetBackup Configuration** > **Enable Push of NetBackup Client**

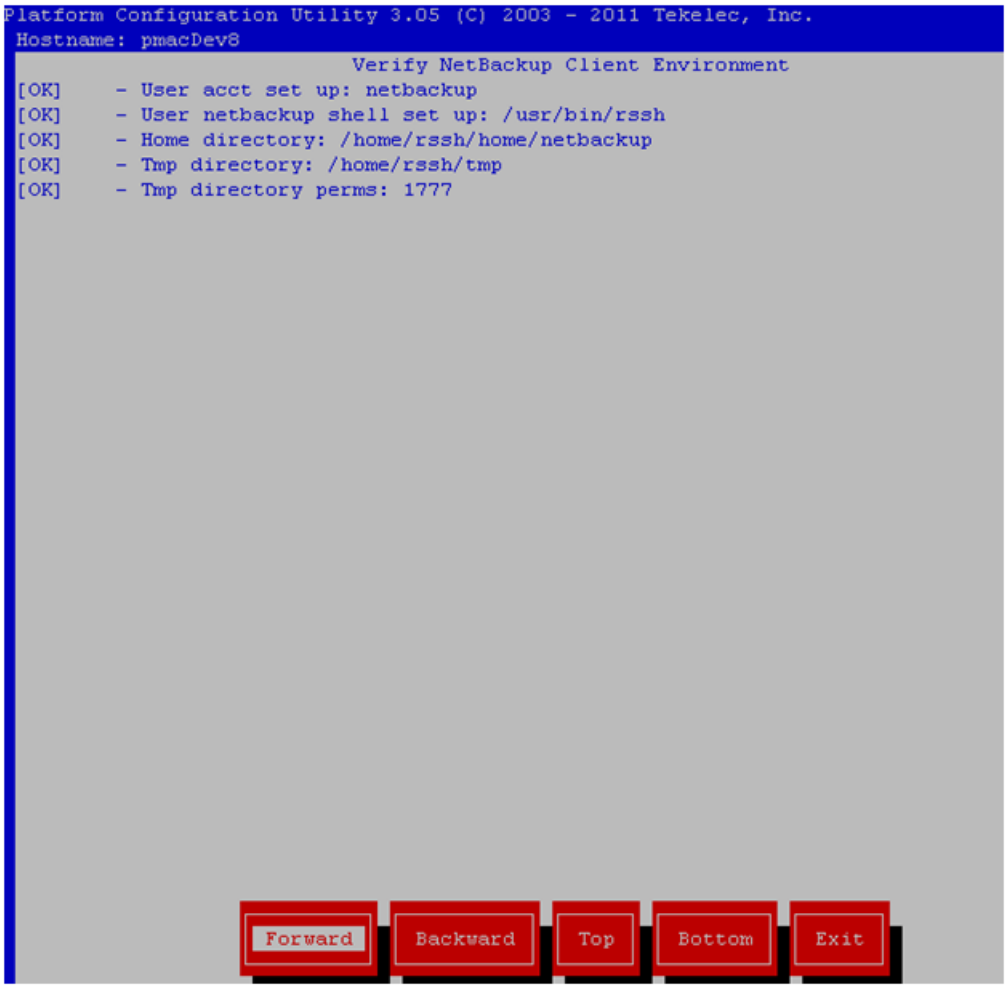


   Select **Yes** to initialize the server and enable the Netbackup client software push.

5. **Application Console** Enter NetBackup password and select OK.



6. If the version of NetBackup is greater than 7.5.0.0, follow the Tekelec provided procedure for the version of NetBackup that is being pushed.
7. **Application Console**: Verify Netbackup client software push is enabled.
   Navigate to **NetBackup Configuration** > **Verify NetBackup Client Push**



Verify list entries indicate "**OK**" for Netbackup client software environment.

Select "**Exit**" to return to NetBackup Configuration menu.

8. **NetBackup server:** Push appropriate Netbackup client software to application server

   Note: The NetBackup server is not an application asset. Access to the NetBackup server, and location path of the Netbackup client software is under the control of the customer. Below are the steps that are required on the NetBackup server to push the Netbackup client software to the application server. These example steps assume the NetBackup server is executing in a Linux environment.

   Note: The backup server is supported by the customer, and the backup utility software provider. If this procedural STEP, executed at the backup utility server, fails to execute successfully, STOP and contact the Customer Care Center of the backup and restore utility software provider that is being used at this site.

   Log in to the NetBackup server using password provided by customer:

   Navigate to the appropriate Netbackup client software path:

Note: The input below is only used as an example.

```
$ sudo cd /usr/openv/netbackup/client/Linux/6.5
```

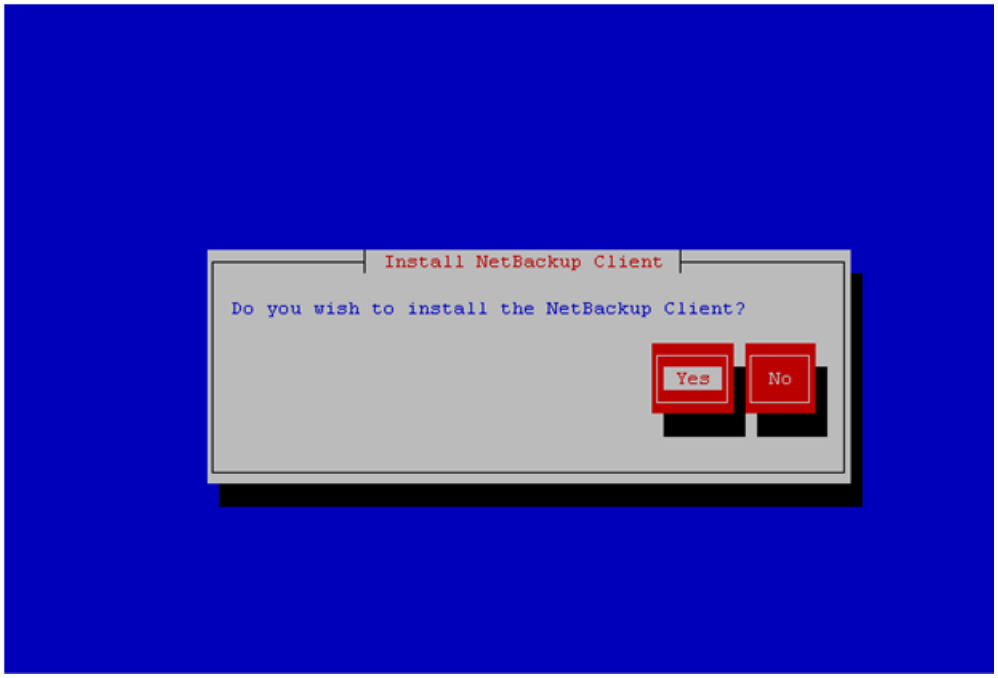
Execute the sftp_to_client NetBackup utility using the application IP address and application NetBackup user;

```
$ ./sftp_to_client 10.240.17.101 netbackup
Connecting to 10.240.17.101...
The authenticity of host '10.240.17.101 (10.240.17.101)' can't be established.
RSA key fingerprint is 9a:e6:fc:55:16:3b:94:b2:7d:9f:30:b2:3c:e6:65:a9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.240.17.101' (RSA) to the list of known hosts.
netbackup@10.240.17.101's password:

sftp completed successfully.
```

Enter application server NetBackup user password; the following NetBackup software output is expected but may vary from this example, **observe the sftp completed successfully**:

```
The root user on 10.240.17.101 must now execute the command
"sh /tmp/bp.15030/client_config [-L]".  The optional argument, "-L",
is used to avoid modification of the client's current bp.conf file.
#
```

9. **Application Console:** Install Netbackup client software on application server.
   Navigate to **NetBackup Configuration** > **Install NetBackup Client**

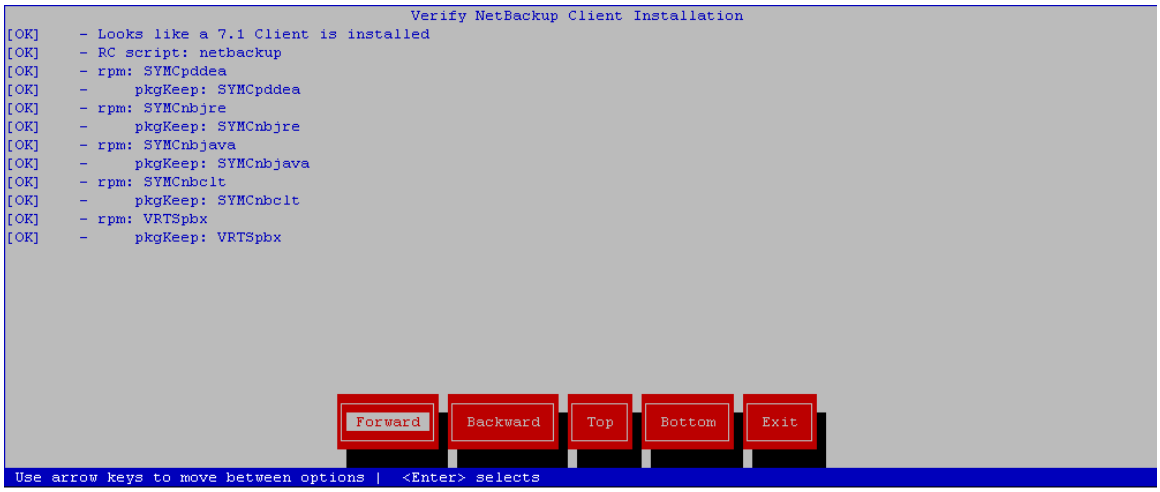


   Select **Yes** to install the Netbackup client software.

   Select "**Exit**" to return to NetBackup Configuration menu.

10. **Application Console:** Verify Netbackup client software installation on the application server.

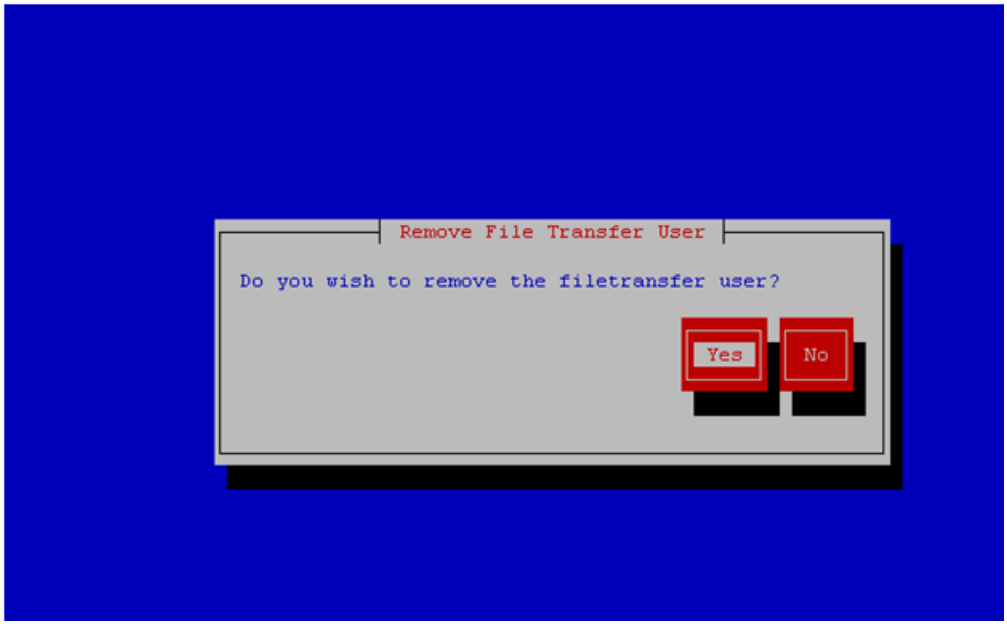
Navigate to **NetBackup Configuration** > **Verify NetBackup Client Installation**.



Verify list entries indicate "OK" for Netbackup client software installation.

Select "Exit" to return to NetBackup Configuration menu.

11. **Application Console:** Disable Netbackup client software transfer to the application server.
    Navigate to **NetBackup Configuration** > **Remove File Transfer User**



Select "Yes" to remove the NetBackup file transfer user from the application server.

12. **Application Console:** Verify that the server has been added to the `/usr/openv/netbackup/bp.conf` file

```
$ sudo cat /usr/openv/netbackup/bp.conf
CLIENT_NAME = 10.240.34.10
SERVER = NB71server
```

13. **Application server iLO:** Exit platform configuration utility (platcfg)
14. Return to calling procedure if applicable.

B.3 Create NetBackup Client Config File

This procedure will copy a NetBackup Client config file into the appropriate location on the TPD based application server. This config file will allow a customer to install previously unsupported versions of NetBackup Client by providing necessary information to TPD.

The contents of the config file should be provided by Tekelec. Contact Tekelec if you are attempting to install an unsupported version of NetBackup Client.

1. **Server:** Create NetBackup Client Config File

   Create the NetBackup Client config file on the server using the contents that were previously determined. The config file should be placed in the /usr/TKLC/plat/etc/netbackup/profiles directory and should follow the following naming conventions:

   NB$ver.conf

   Where $ver is the client version number with the periods removed. For the 7.5 client the value of $ver would be 75 and the full path to the file would be:

   `/usr/TKLC/plat/etc/netbackup/profiles/NB75.conf`

   Note: The config files must start with "NB" and must have a suffix of ".conf". The server is now capable of installing the corresponding NetBackup Client.

   The server is now capable of installing the corresponding NetBackup Client.

2. **Server:** Create NetBackup Client config file script.

   Create the NetBackup Client config script file on the server using the contents that were previously determined. The config script file should be placed in the /usr/TKLC/plat/etc/netbackup/scripts directory. The name of the NetBackup Client config script file should be determined from the contents of the NetBackup Client config file. As an example for the NetBackup 7.5 client the following is applicable:

   NetBackup Client config:

```
/usr/TKLC/plat/etc/netbackup/profiles/NB75.conf
```

   NetBackup Client config script:

```
/usr/TKLC/plat/etc/netbackup/scripts/NB75
```

B.4 Configure PM&C application guest NetBackup virtual disk

1. **PM&C GUI:** Determine if the PM&C application guest is configured with a "NetBackup" virtual disk.

   Navigate to "**Virtual Machine Management**" view and select the PM&C application guest from the "**VM Entities**" list.

2. **PM&C GUI:** Determine if the "Virtual Disks" list contains the "NetBackup" device.

   If the "NetBackup" device exists for the PM&C application guest then return to the procedure that invoked this procedure. Otherwise continue with this procedure.

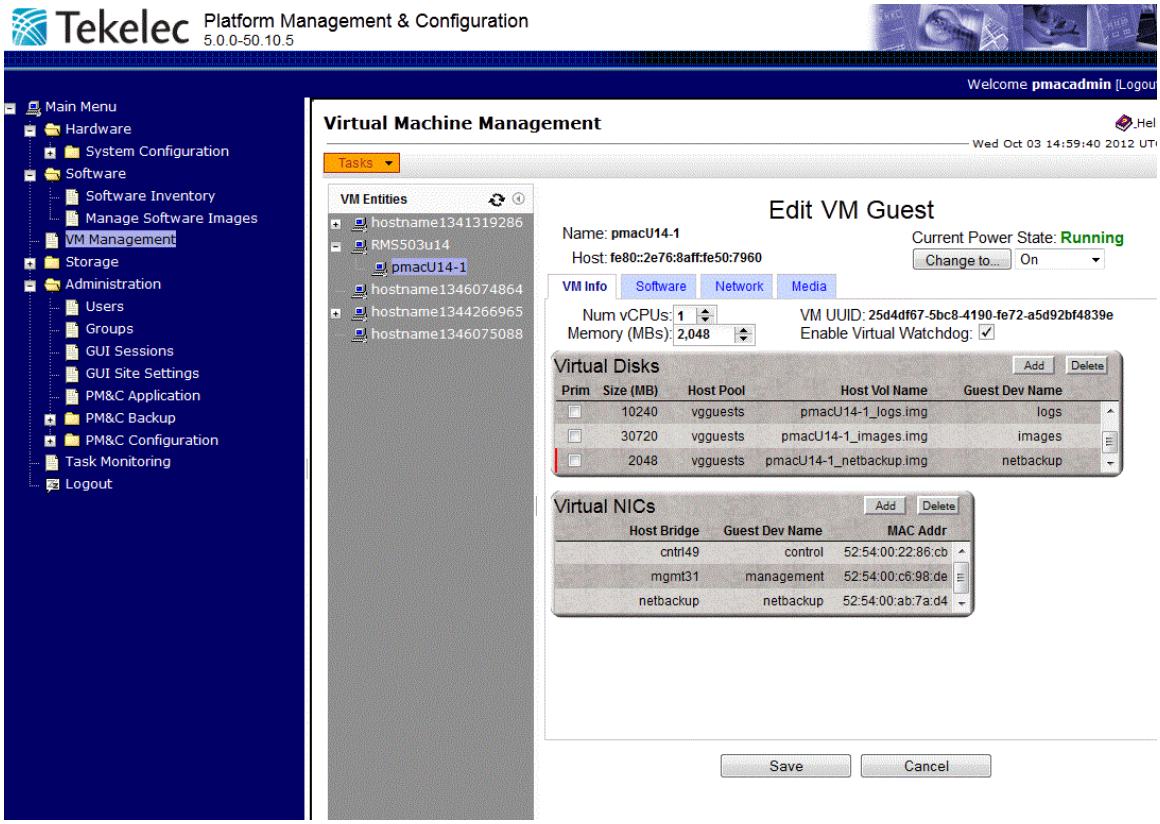
3. **PM&C GUI:** Edit the PM&C application guest to add the "NetBackup" virtual disk.

   Click "Edit" and enter the following data for the new NetBackup virtual disk.

   - Size (MB): "2048"
   - Host Pool: "vgguests"
   - Host Vol Name: "<pmacGuestName>_netbackup.img"
   - Guest Dev Name: "NetBackup"

   Note: The "Guest Dev Name" must be set to "isoimages" for the PM&C application to mount the appropriate host device. The <pmacGuestName> variable should be set to this PM&C guest's name to create a unique volume name on the TVOE host of the PM&C.

4. **PM&C GUI:**Verify the new NetBackup virtual disk data and save.



5. **PM&C GUI:** Confirm the PM&C application guest edit.

   A confirmation dialog will be presented with the message, "Changes to the PMAC guest: <pmacGuestName> will not take effect until after the next power cycle. Do you wish to continue?". Click "OK" to continue.

6. **PM&C GUI:** Confirm the Edit VM Guest task has completed successfully.

   Navigate to the Background Task Monitoring view. Confirm the guest edit task has completed successfully.

7. **TVOE Management server iLO:** Shutdown the PM&C application guest.

   Note: In order to configure the PM&C application with the new NetBackup virtual disk the PM&C application guest needs to be shut down and restarted. Refer to *PM&C 5.0 Incremental Upgrade, 909-2207-01, Appendix F. Shutdown PM&C Guest* .

8. **TVOE Management Server iLO:** Start the PM&C application guest.

   Note: In order to configure the PM&C application with the new isoimages virtual disk the PM&C application guest needs to be shut down and restarted.

   Using virsh utility on TVOE host of PM&C guest, start the PM&C guest. Query the list of guests until the PM&C guest is "running".

```
$ sudo /usr/bin/virsh
virsh # list --all
Id Name State
----------------------------------
20 pmacU14-1 shut off

virsh # start pmacU14-1
Domain pmacU14-1 started

virsh # list --all
Id Name State
----------------------------------
20 pmacU14-1 running
```

9. Return to the procedure that invoked this procedure.

B.5 Application NetBackup Client Install/Upgrade Procedures

NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite is for the purpose of supporting Disaster Recovery at the customer site. This procedure provides instructions for installing or upgrading the Netbackup client software on an application server.

Disclaimer: Currently only the NetBackup 7.1 and NetBackup 7.5 clients are supported. If the NetBackup Client that is being installed is not supported, contact customer support for guidance on creating a config file that will allow for install of unknown NetBackup Clients. *B.3 Create NetBackup Client Config File* can be used once the contents of the config are known.

Disclaimer: Failure to install the NetBackup Client properly (i.e., by neglecting to execute this procedure) may result in the NetBackup Client being deleted during a Tekelec software upgrade.

1. **Choose NetBackup Client Install Path**

   There are two different ways to install NetBackup Client. The following is a guide to which method to use:

   - If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools then use *B.1 Netbackup Client Install/Upgrade with nbAutoInstall*. This is not common and if the answer to the previous question is not known then do not use *B.1 Netbackup Client Install/Upgrade with nbAutoInstall*.
   - If you don't use *B.1 Netbackup Client Install/Upgrade with nbAutoInstall*, use *B.2 NetBackup Client Install/Upgrade with platcfg*.

   Chosen Procedure: _____

2. **Execute the procedure chosen in Step 1**
3. **Application Console:** Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias.

   Note: If NetBackup Client has successfully been installed then you can find the NetBackup server's hostname in the "/usr/openv/netbackup/bp.conf" file. It will be identified by the "SERVER" configuration parameter as is shown in the following output:

   List NetBackup servers hostname:

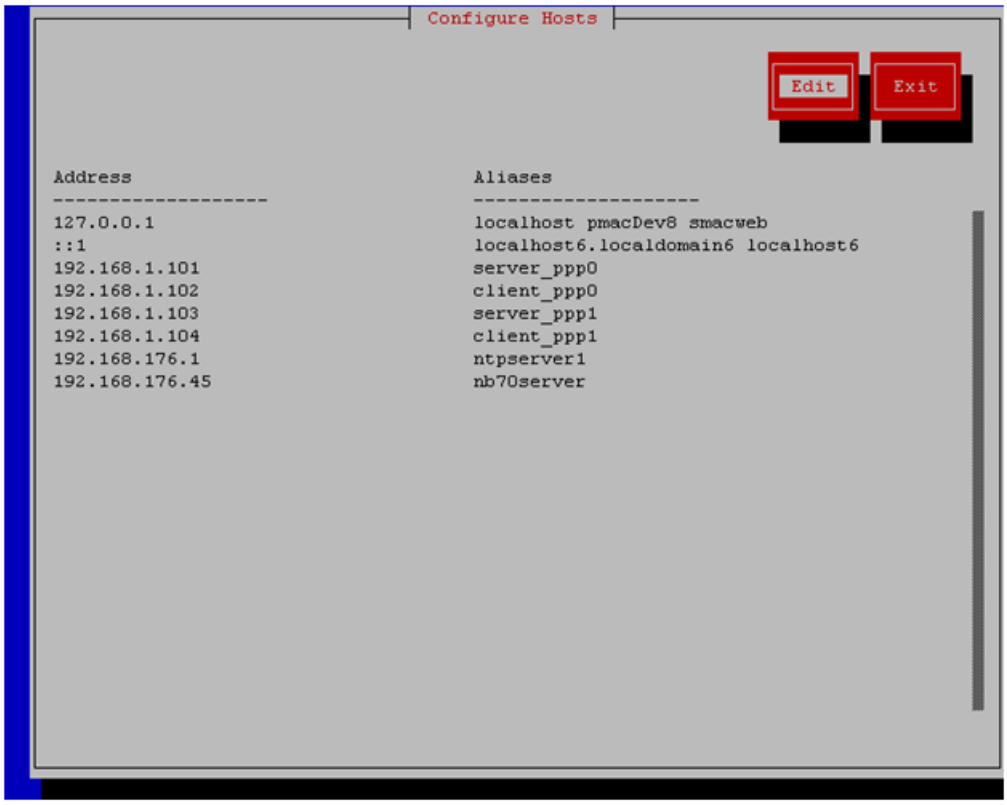
```
$ sudo cat /usr/openv/netbackup/bp.conf
SERVER = nb70server
CLIENT_NAME = pmacDev8
```

   Note: : In the case of nbAutoInstall NetBackup Client may not yet be installed. For this situation the "/usr/openv/netbackup/bp.conf" cannot be used to find the NetBackup server alias.

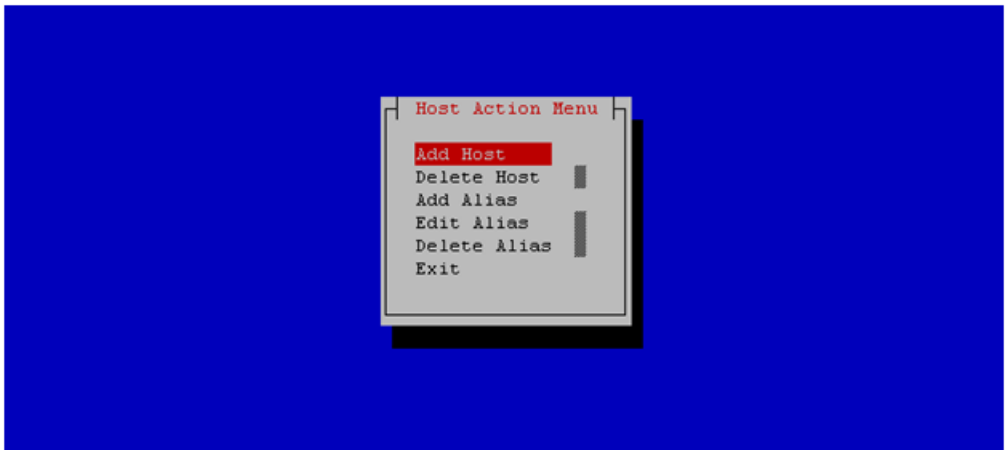
   Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```
$ sudo su - platcfg
```

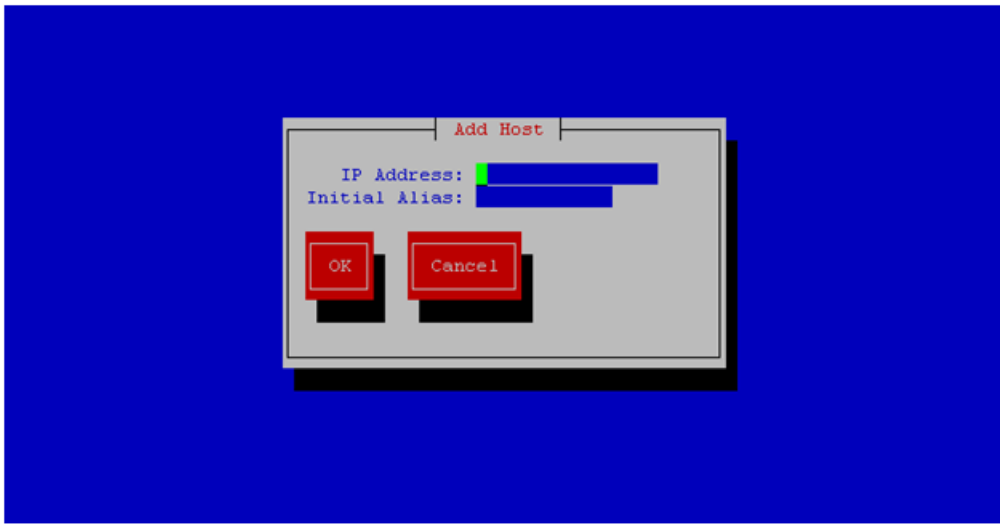
   Navigate to **Network Configuration** > **Modify Hosts File**



Select **Edit**, the Host Action Menu will be displayed.



Select "**Add Host**", and enter the appropriate data



Select "**OK**", confirm the host alias add, and exit Platform Configuration Utility

4. **Application Console:** Create a link for the application provided NetBackup client notify scripts to path on application server where NetBackup expects to find them.

   Note: Link notify scripts from appropriate path on application server for given application.

```
$ sudo mkdir -p /usr/openv/netbackup/bin/
$ sudo ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify
$ sudo ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify
```

5. **Application Console**: Netbackup client software installation complete; if applicable return to calling procedure.

B.1 Netbackup Client Install/Upgrade with nbAutoInstall

Executing this procedure will enable TPD to automatically detect when a Netbackup Client is installed and then complete TPD related tasks that are needed for effective Netbackup Client operation. With this procedure, the Netbackup Client install (pushing the client and performing the install) is the responsibility of the customer and is not covered in this procedure.

Note: If the customer does not have a way to push and install Netbackup Client, then use *B.2 NetBackup Client Install/Upgrade with platcfg*.

Note: It is required that this procedure is executed before the customer does the Netbackup Client install.

1. **Follow Tekelec Provided Workarounds**

   Follow Tekelec provided procedures to prepare the server for Netbackup Client install using nbAutoInstall.

2. **Enable nbAutoInstall:**

Execute the following command:

```
$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable
```

The server will now periodically check to see if a new version of Netbackup Client has been installed and will perform necessary TPD configuration accordingly.

At any time, the customer may now push and install a new version of Netbackup Client.

3. Return to calling procedure if applicable.

B.2 NetBackup Client Install/Upgrade with platcfg

Executing this procedure will push and install NetBackup Client via platcfg menus.

Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center by referring to the *1.4 Customer Care Center* section of this document.

1. **Application server iLO:** Login and launch the integrated remote console

   Log in to iLO in IE using password provided by application

   ```
   http://<management_server_iLO_ip>
   ```

   Click in the **Remote Console** tab and launch the **Integrated Remote Console** on the server.

   Click **Yes** if the `Security Alert` pops up.

2. **TVOE Application Server iLO:** If the application is a guest on a TVOE host: Log in with application admusr credentials. If the application is not a guest on a TVOE host continue to step 3.

   Note: On a TVOE host, If you launch the virsh console, i.e., "# **`virsh console X`**" or from the virsh utility "virsh # **`console X"`** command and you get garbage characters or output is not quite right, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit out of the "virsh console", then run "**`ps -ef |grep virsh`**", then kill the existing process "**`kill -9 <PID>`**". Then execute the "virsh console X" command. Your console session should now run as expected.

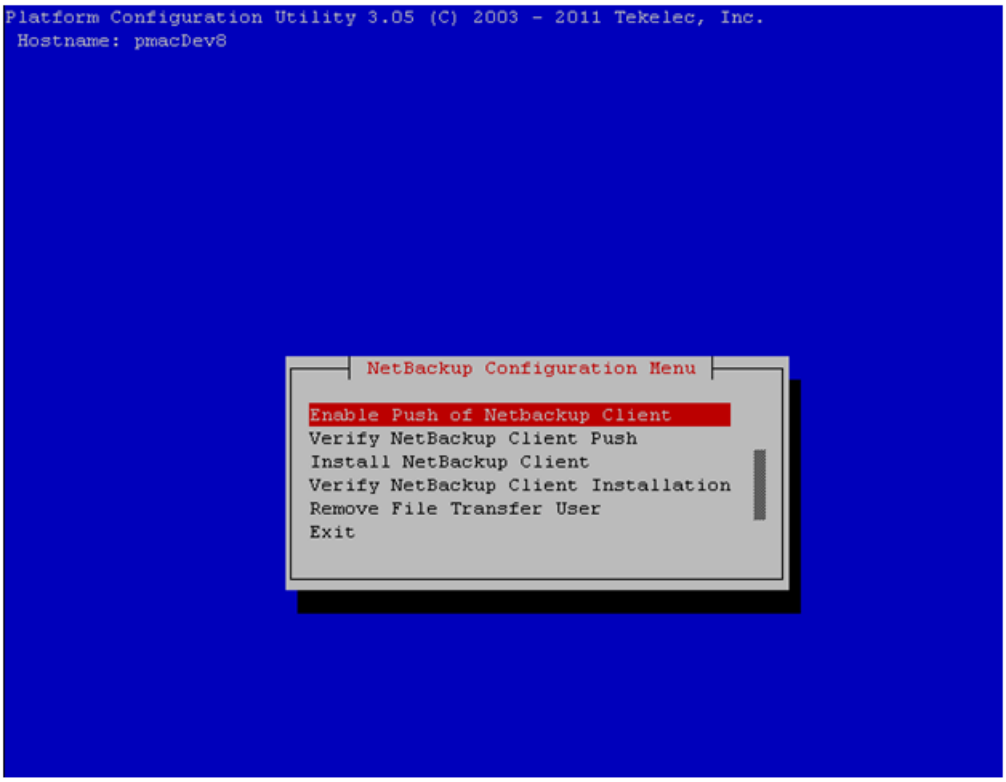
   Login to application console using virsh, and wait until you see the login prompt:

```
$ virsh
virsh $ list --all
Id Name State
----------------------------------
13 myTPD running
20 applicationGuestName running

virsh $ console applicationGuestName
[Output Removed]
Starting ntdMgr: [ OK ]
Starting atd: [ OK ]
'TPD Up' notification(s) already sent: [ OK ]
upstart: Starting tpdProvd...
upstart: tpdProvd started.
CentOS release 6.2 (Final)
Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.14.0.x86_64 on an x86_64
applicationGuestName login:
```

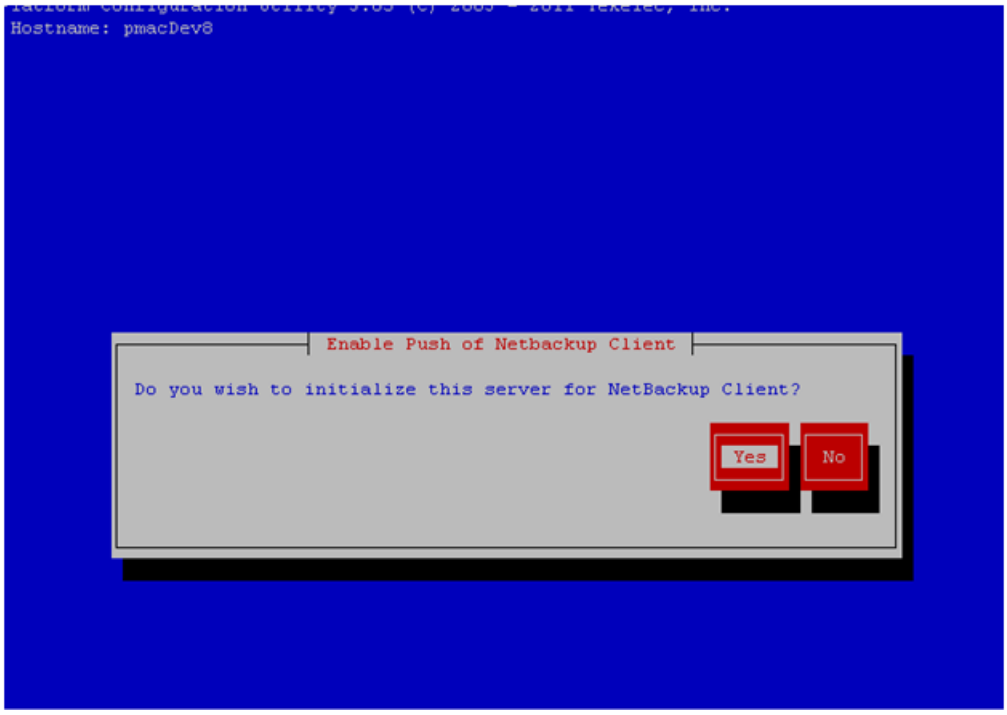
3. **Application Console**: Configure NetBackup Client on application server

```
$ sudo su - platcfg
```

   Navigate to **NetBackup Configuration**

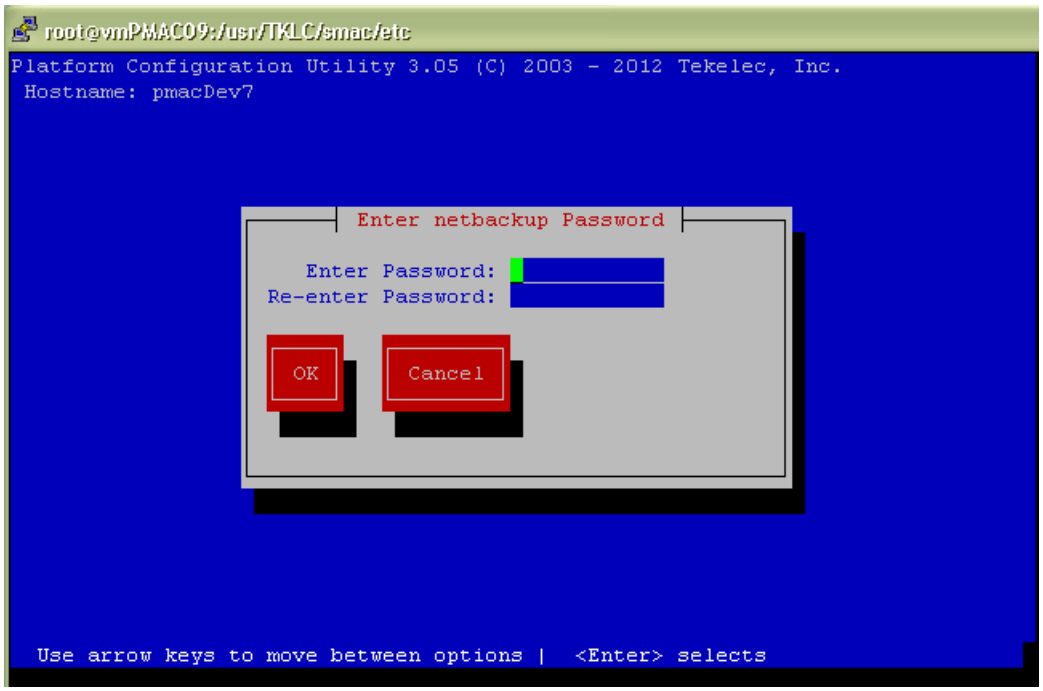


4. **Application Console**: Enable Push of NetBackup Client
   Navigate to **NetBackup Configuration** > **Enable Push of NetBackup Client**



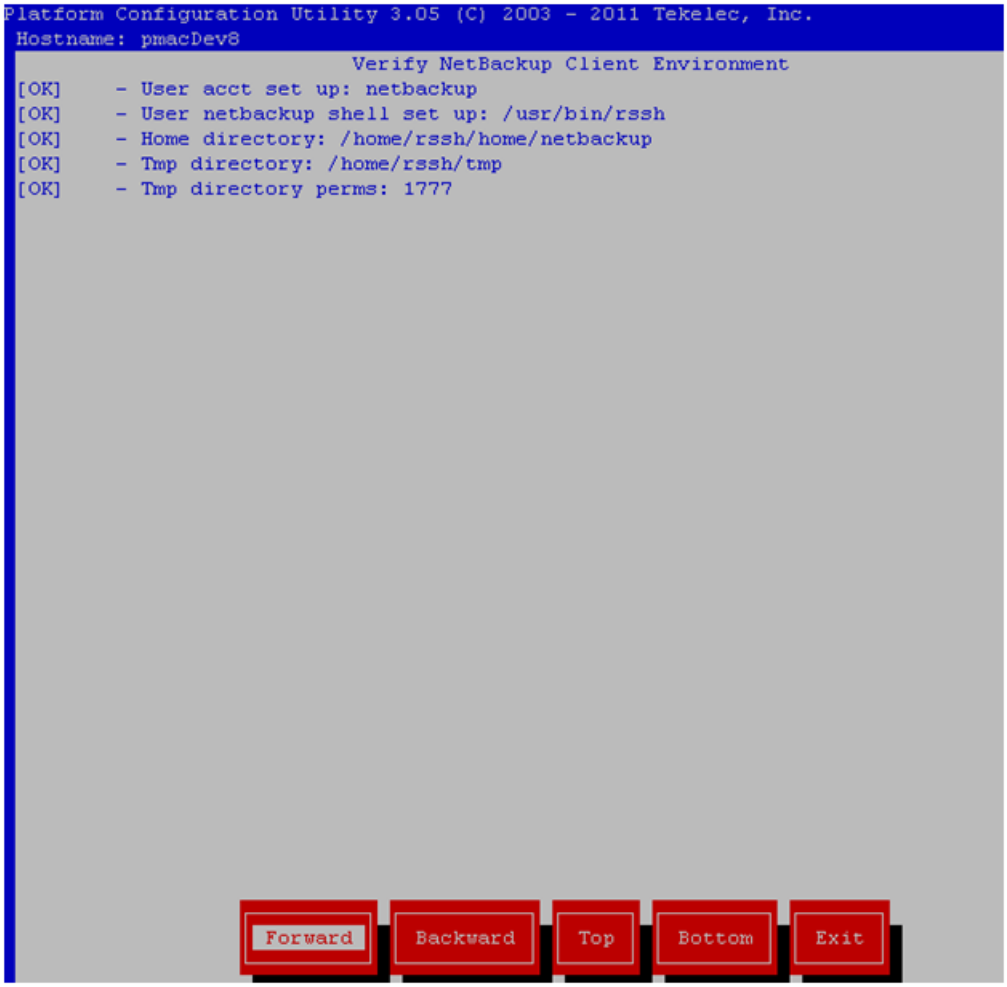
Select **Yes** to initialize the server and enable the Netbackup client software push.

5. **Application Console** Enter NetBackup password and select OK.



6. If the version of NetBackup is greater than 7.5.0.0, follow the Tekelec provided procedure for the version of NetBackup that is being pushed.
7. **Application Console**: Verify Netbackup client software push is enabled.

Navigate to **NetBackup Configuration** > **Verify NetBackup Client Push**



Verify list entries indicate "**OK**" for Netbackup client software environment.

Select "**Exit**" to return to NetBackup Configuration menu.

8. **NetBackup server:** Push appropriate Netbackup client software to application server

   Note: The NetBackup server is not an application asset. Access to the NetBackup server, and location path of the Netbackup client software is under the control of the customer. Below are the steps that are required on the NetBackup server to push the Netbackup client software to the application server. These example steps assume the NetBackup server is executing in a Linux environment.

   Note: The backup server is supported by the customer, and the backup utility software provider. If this procedural STEP, executed at the backup utility server, fails to execute successfully, STOP and contact the Customer Care Center of the backup and restore utility software provider that is being used at this site.

   Log in to the NetBackup server using password provided by customer:

   Navigate to the appropriate Netbackup client software path:

Note: The input below is only used as an example.

```
$ sudo cd /usr/openv/netbackup/client/Linux/6.5
```

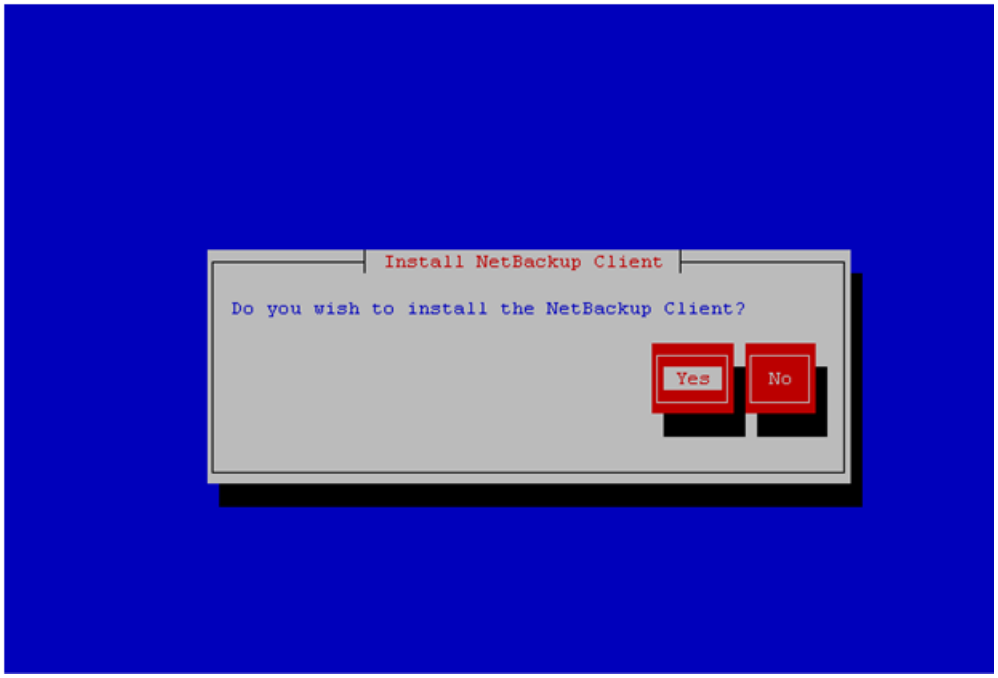
Execute the sftp_to_client NetBackup utility using the application IP address and application NetBackup user;

```
$ ./sftp_to_client 10.240.17.101 netbackup
Connecting to 10.240.17.101...
The authenticity of host '10.240.17.101 (10.240.17.101)' can't be established.
RSA key fingerprint is 9a:e6:fc:55:16:3b:94:b2:7d:9f:30:b2:3c:e6:65:a9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.240.17.101' (RSA) to the list of known hosts.
netbackup@10.240.17.101's password:

sftp completed successfully.
```

Enter application server NetBackup user password; the following NetBackup software output is expected but may vary from this example, **observe the sftp completed successfully**:

```
The root user on 10.240.17.101 must now execute the command
"sh /tmp/bp.15030/client_config [-L]".  The optional argument, "-L",
is used to avoid modification of the client's current bp.conf file.
#
```

9. **Application Console:** Install Netbackup client software on application server.
   Navigate to **NetBackup Configuration** > **Install NetBackup Client**

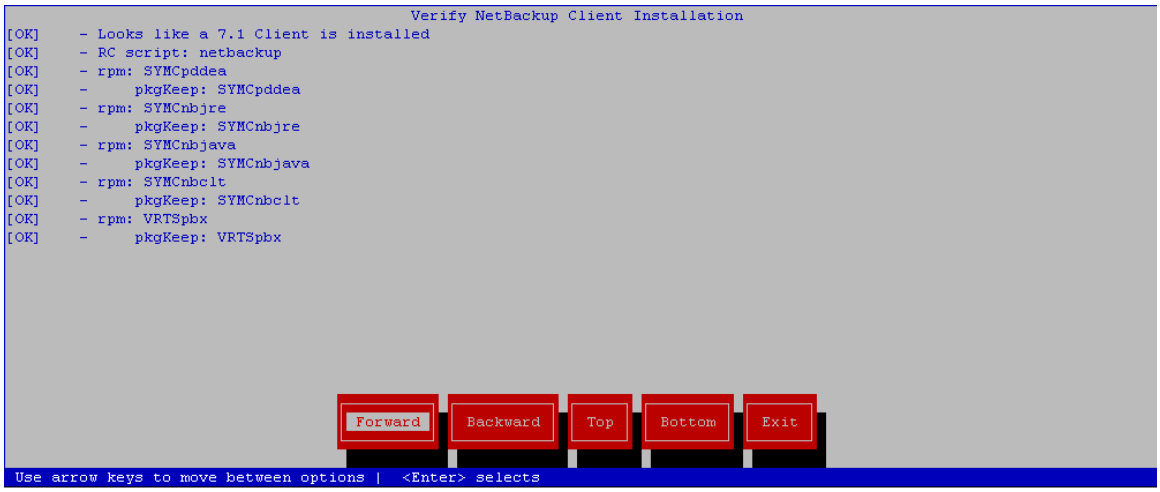


   Select **Yes** to install the Netbackup client software.

   Select "**Exit**" to return to NetBackup Configuration menu.

10. **Application Console:** Verify Netbackup client software installation on the application server.

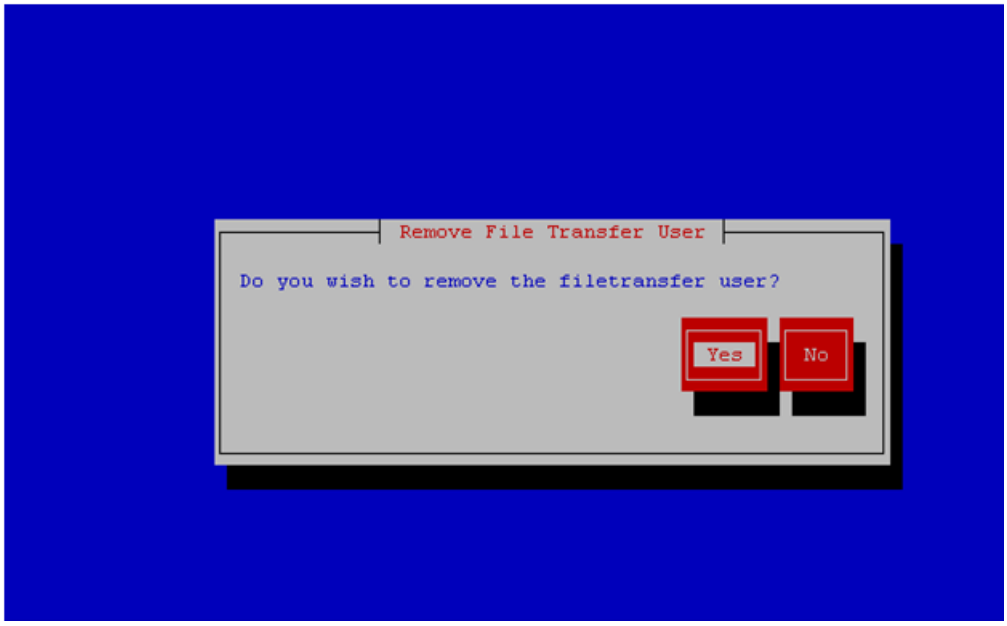
Navigate to **NetBackup Configuration** > **Verify NetBackup Client Installation**.



Verify list entries indicate "OK" for Netbackup client software installation.

Select "Exit" to return to NetBackup Configuration menu.

11. **Application Console:** Disable Netbackup client software transfer to the application server.
    Navigate to **NetBackup Configuration** > **Remove File Transfer User**



Select "Yes" to remove the NetBackup file transfer user from the application server.

12. **Application Console:** Verify that the server has been added to the `/usr/openv/netbackup/bp.conf` file

```
$ sudo cat /usr/openv/netbackup/bp.conf
CLIENT_NAME = 10.240.34.10
SERVER = NB71server
```

13. **Application server iLO:** Exit platform configuration utility (platcfg)
14. Return to calling procedure if applicable.

Appendix C

Worksheet: netConfig Repository

Topics:

C.1 Worksheet: netConfig Repository

For each additional enclosure switch(6120XG, 6125XG, or 3020):

Variable	Value
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	

Variable	Value
<switch_platform_password>	
<switch_enable_password>	
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_hostname>	
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<OA1_enX_ip_address>	X=the enclosure #
<OA password>	
<io_bay>	

Appendix D

Initial Product Manufacture of Server

Topics:

Note: This section is specific to RMS Servers.

D.1 Setting Server's CMOS clock

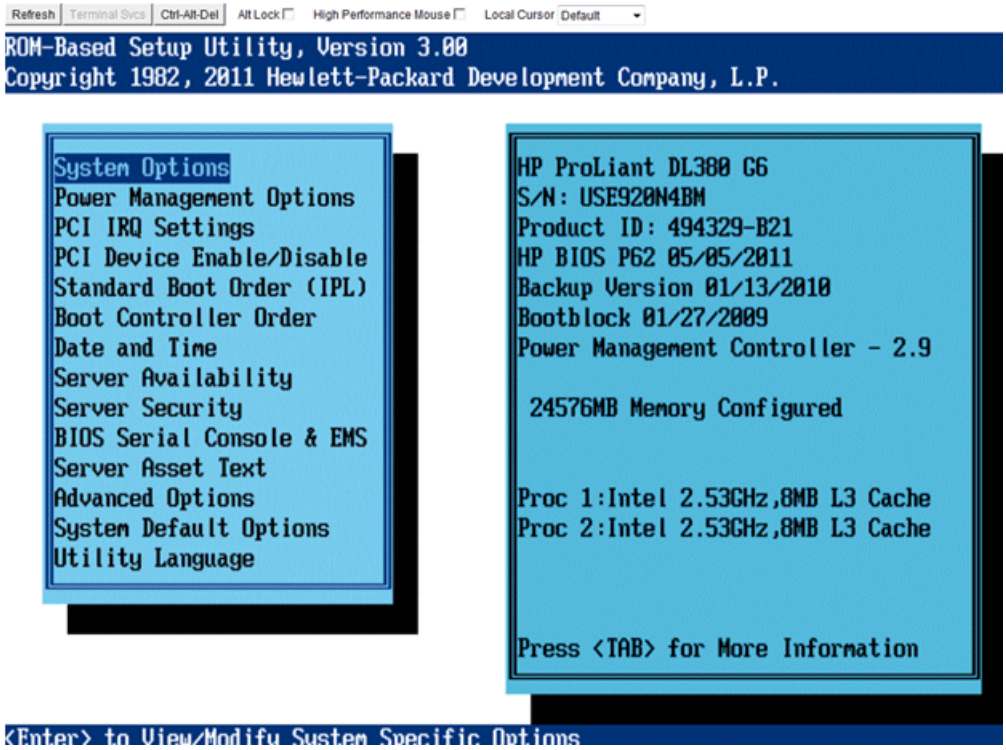
The date and time in the server's CMOS clock **MUST** be set **correctly** before running the IPM procedure. There are a number of different ways to set the server's CMOS clock.

Note: The IPM installation process managed by PM&C for blade servers automatically sets the server's CMOS clock, so there is no need to set the server CMOS clock when using PM&C.

D.2 Configure the RMS Server BIOS Settings

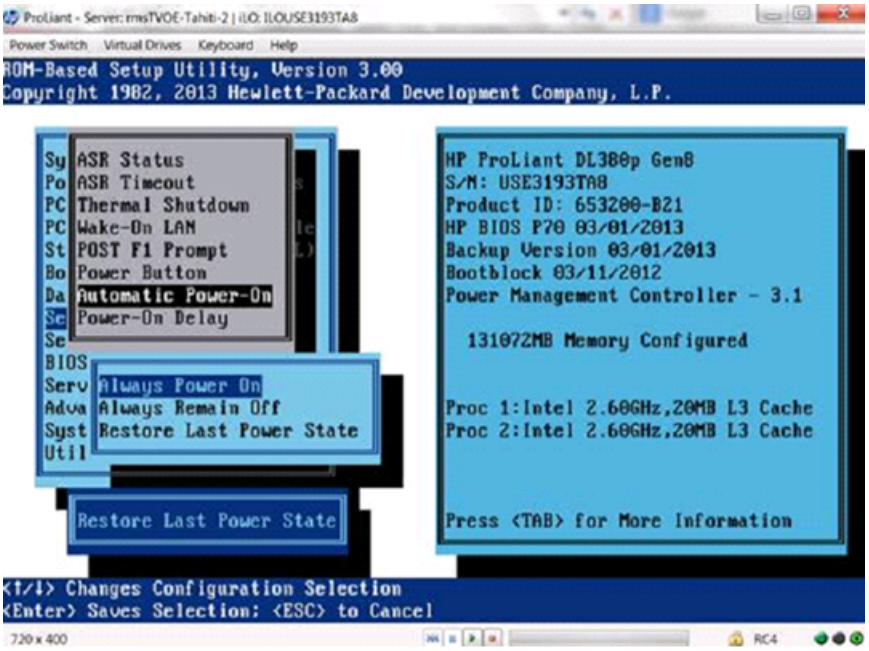
DL360/380 Server: Access the Server BIOS

a) Reboot the server and after the server is powered on, as soon as the <F9=Setup> in the lower left corner of the screen is visible, press **F9** to access the BIOS setup screen.

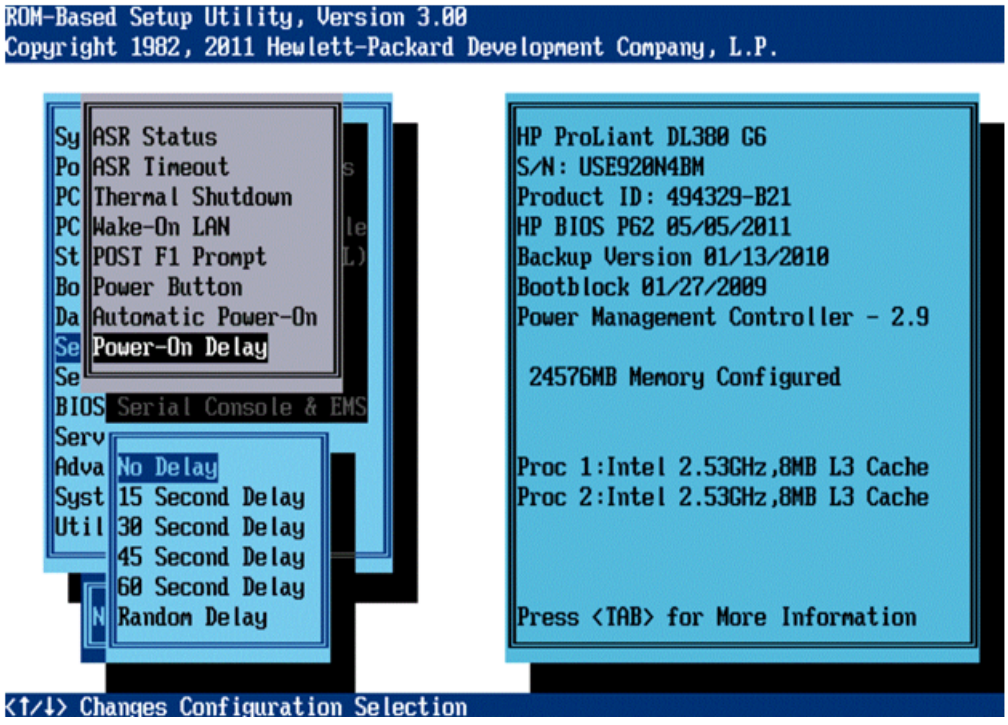


b) Select **Server Availability**

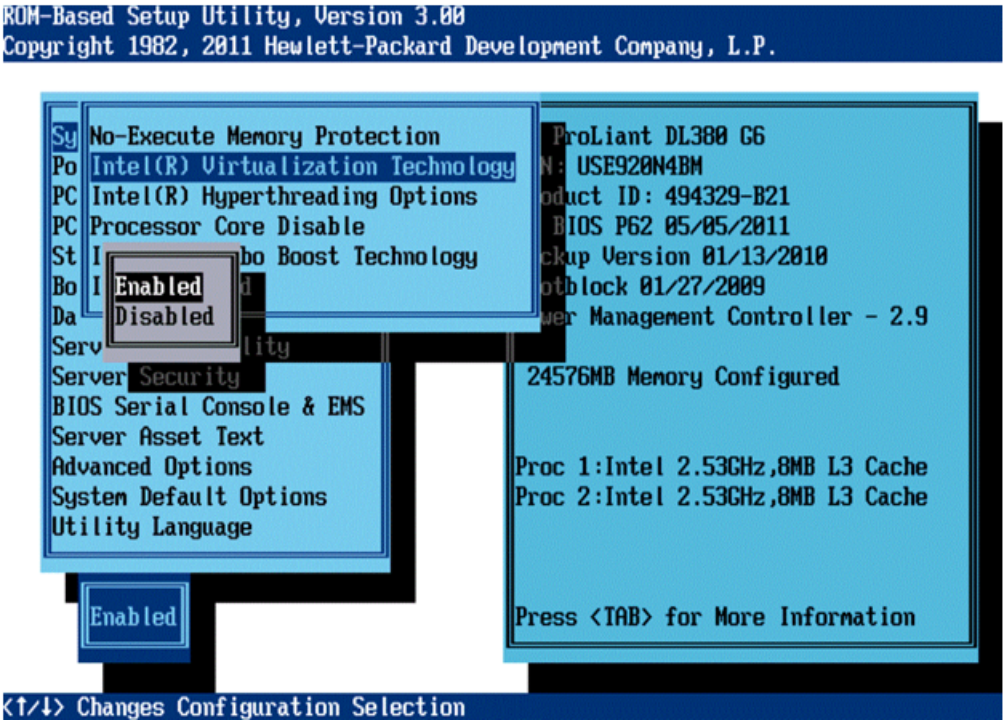
c) If applicable, Change "Automatic Power-On" to **Always Power On** (Gen8 servers) or **Enabled** (G6, G7 servers).



d) Change "Power-On Delay" to **No Delay**



e) Press **<ESC>** once
f) Select **System Options**
g) Select **Processor Options**
h) Change "Intel® Virtualization Technology" to **Enabled**



i) *If available,* select **Serial Port Options** and press **Enter**

1. Press **Enter** to select **Embedded Serial Port** and change it to **COM2** and press **Enter**
2. Press **Enter** to select **Virtual Serial Port** and change it to **COM1** and press **Enter**
3. Press **<ESC>** 2 times to return to the main menu

D.3 OS IPM Install

The IPM installation media must now be inserted into the system. Installation will then begin by resetting (or power cycling) the system so that the BIOS can find and boot from the installation media. Setting the clock and other BIOS parameters from the BIOS setup screen does not require an OS to be installed.

Note: On the HP G6 and newer rack mount servers, this procedure can be accomplished by using a directly connected computer and by configuring an IP address on the iLO and accessing the console using the iLO, or by using a VGA monitor and keyboard. The remote media function of the iLO can also be used to provide access to the installation media.

D.3.1 HP Rack Mount Servers - Boot from CD/DVD/USB

1. Insert the OS IPM media (CD or DVD) into the CD/DVD tray of the Application Server and close the CD/DVD tray, or insert the OS IPM USB media into the of the Application Server.

   Note: Refer to Appendix K to create a bootable USB drive.

2. Power cycle the server:
   For HP Rack Mount servers, hold the power button in until the button turns amber, then release. Wait 5 seconds, then press the power button and release it again to power on the system.
3. Proceed to steps in the next section.

D.4 IPM Command line procedures

1. *Figure 3: Example Boot from Media Screen, TPD 6.5* is a sample output screen indicating the initial boot from the install media was successful. The information in this screen output is representative of TPD 6.5.

   Note: Note that based on the deployment type, either TPD or TVOE can be installed.

2. Optional Step: If media has not been previously verified, perform a media check now; refer to *D.6 Media Check*.
3. The command to start the installation is dependent upon several factors, including the type of system, knowledge of whether an application has previously been installed or a prior IPM install failed, and what application will be installed.

   Note: Text case is important, and the command must be typed exactly.

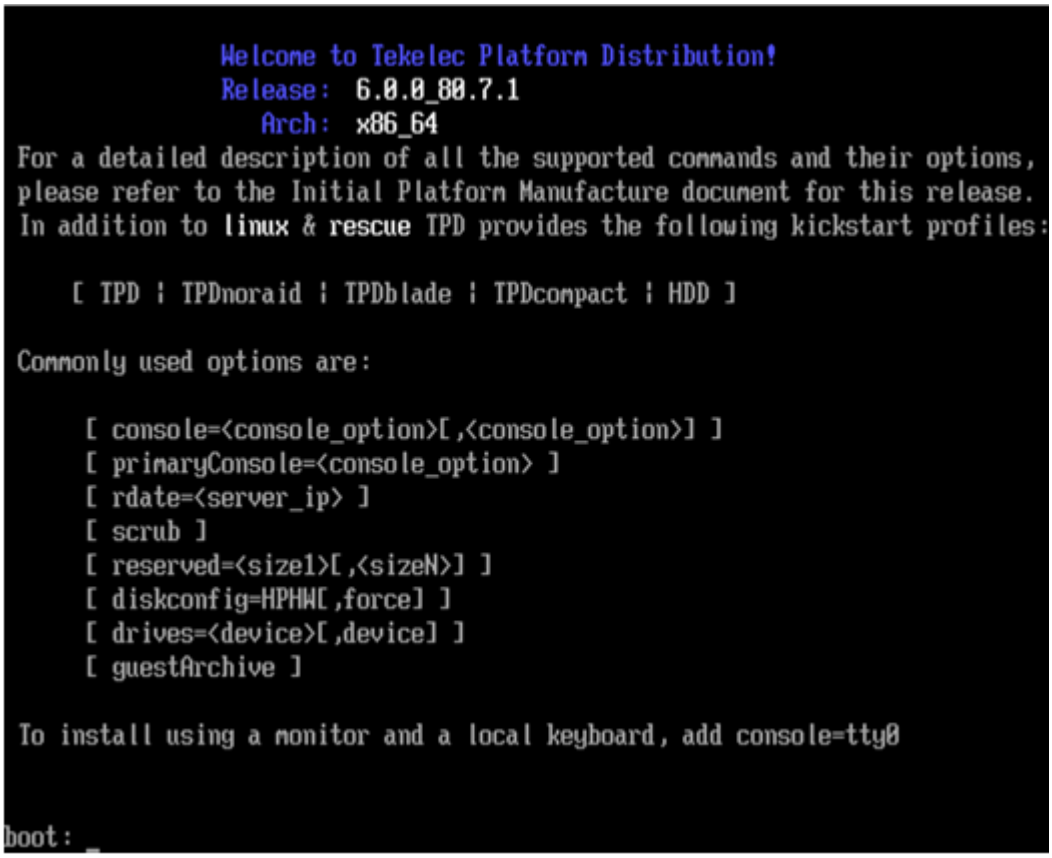


Figure 3: Example Boot from Media Screen, TPD 6.5

IPM the server by entering the TPD command at the boot prompt:

```
TPDnoraid diskconfig=HPHW,force console=tty0
```

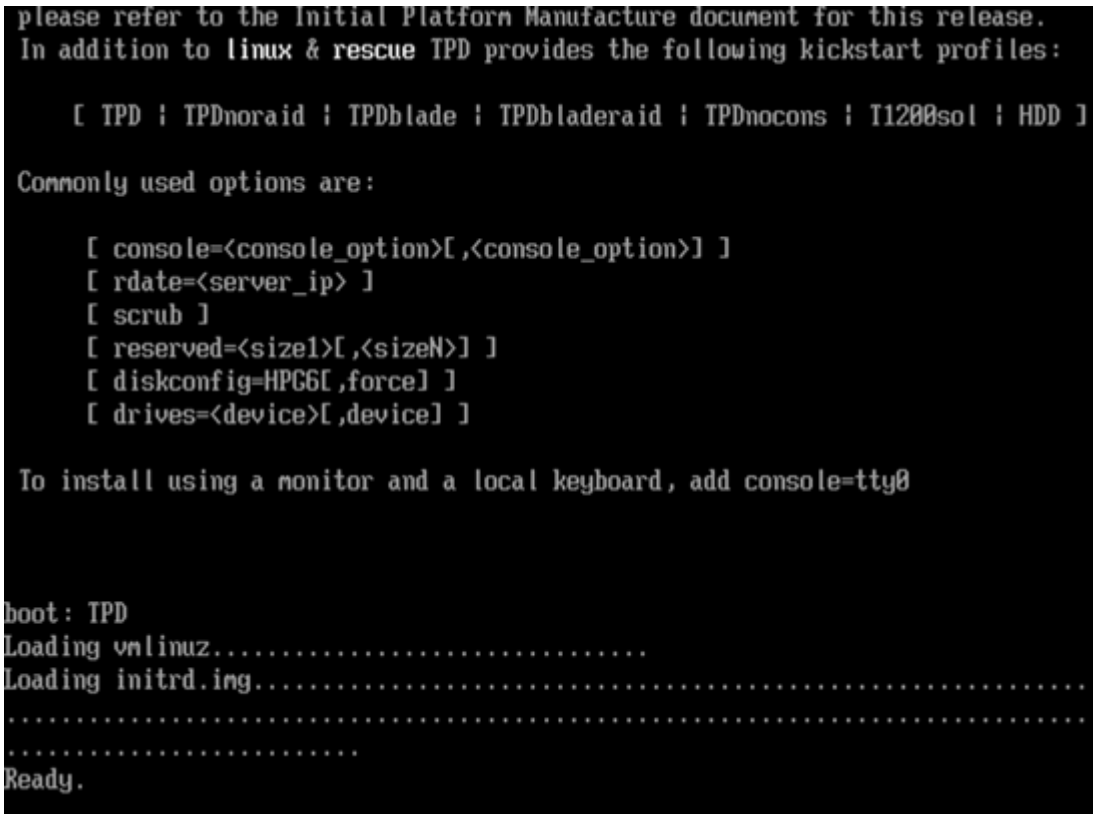


Figure 4: Example Kernel Loading Output

4. After a few seconds, additional messages will begin scrolling by on the screen as the Linux kernel boots, and then the drive formatting and file system creation steps will begin:

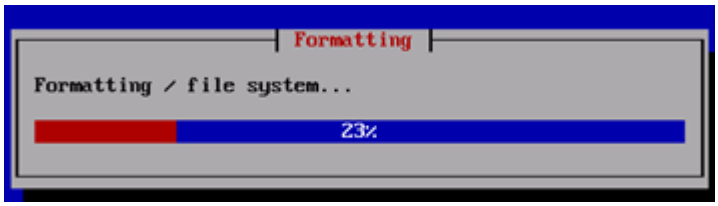


Figure 5: Example File System Creation Screen

5. Once the drive formatting and file system creation steps are complete, the following screen will appear indicating that the package installation step is about to begin.

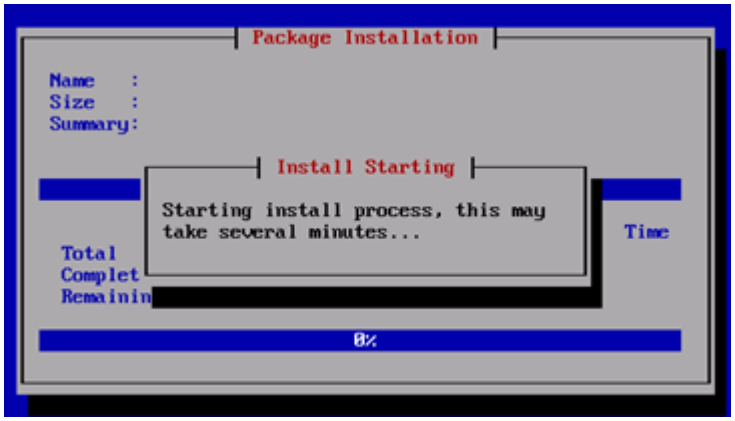


Figure 6: Example Package Installation Screen

6. Once the screen shown in Figure : Example package installation screen appears, it may take several minutes before anything change. However, after a few minutes, you will see a screen similar to that below, showing the status of the package installation step. For each package, there will be a status bar at the top indicating how much of the package has been installed, with a cumulative status bar at the bottom indicating how many packages remain. In the middle, you will see text statistics indicating the total number of packages, the number of packages installed, the number remaining, and current and projected time estimates:

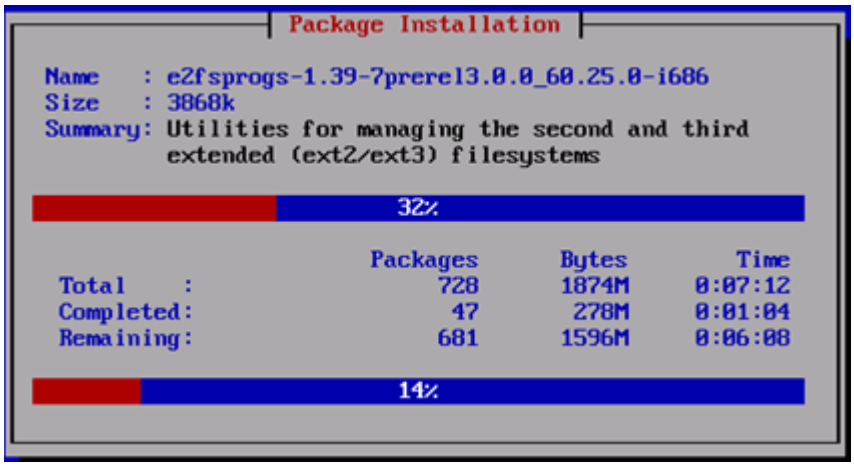


Figure 7: Example Installation Statistics Screen

7. Once all the packages have been successfully installed, the following screen will appear, letting you know the installation process is complete. **Remove the installation media** (DVD or USB key) and then press <ENTER> to reboot the system.

   Note: It is possible that the system will reboot several times during the IPM process. No user input is required if this occurs.

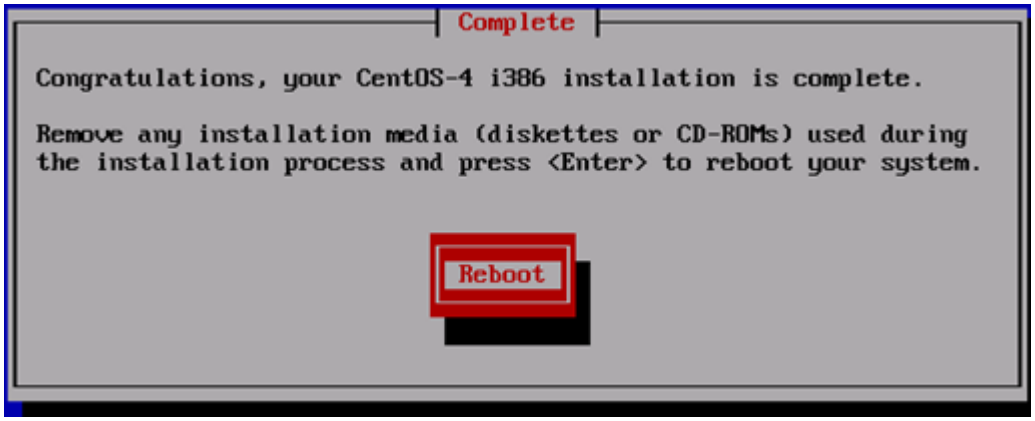


Figure 8: Example Installation Complete Screen

8. After a few minutes, the BIOS screen will appear again, followed by several messages about each of the Ethernet ports in the system, and finally followed by the following message printed by the boot loader, indicating that it is booting the new IPM load.

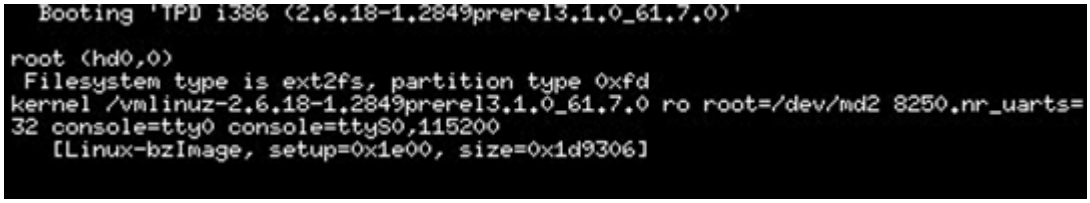


Figure 9: Example Boot Loader Output

9. 10. A successful IPM platform installation process will result in a user login prompt.

D.5 Post Install Processing

Login as user syscheck, and the system health check will run automatically. This will check the health of the server, and print out an **OK** if the tests passed, or a descriptive error of the problem if anything failed. The screenshot below shows a successful run of syscheck, where all tests pass, indicating the server is healthy.

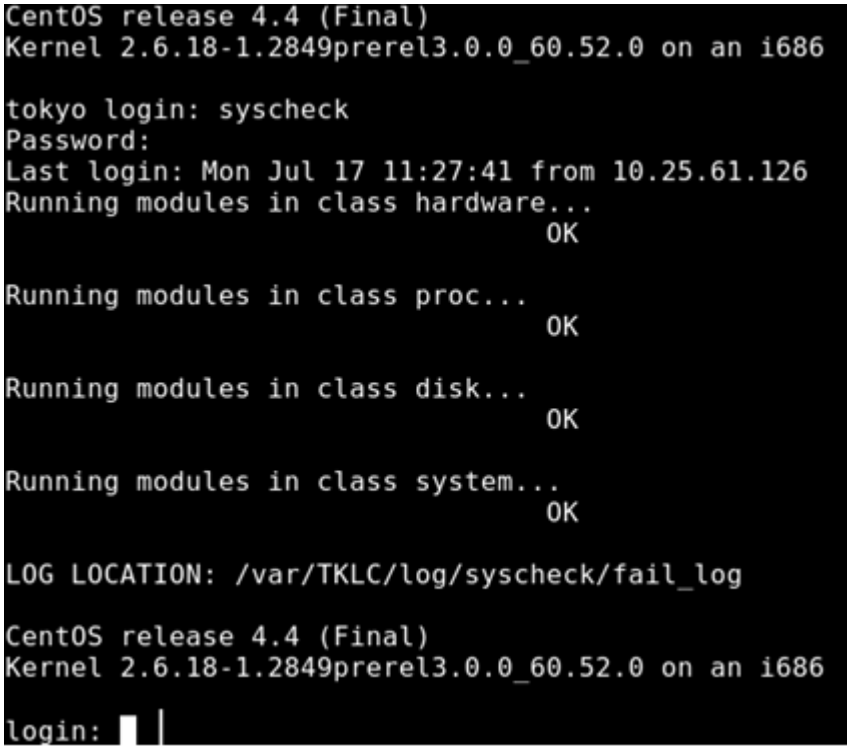


Figure 10: Example Successful Syscheck Output

Since an NTP server will not normally be configured at this point, syscheck may fail due to the NTP test as shown in *Figure 11: Example Syscheck Output with NTP Error*. The syscheck NTP test will not give this failure during the first 20 minutes after the server is booted up. The error shown in Figure : Example syscheck output with NTP error is acceptable and can be ignored.

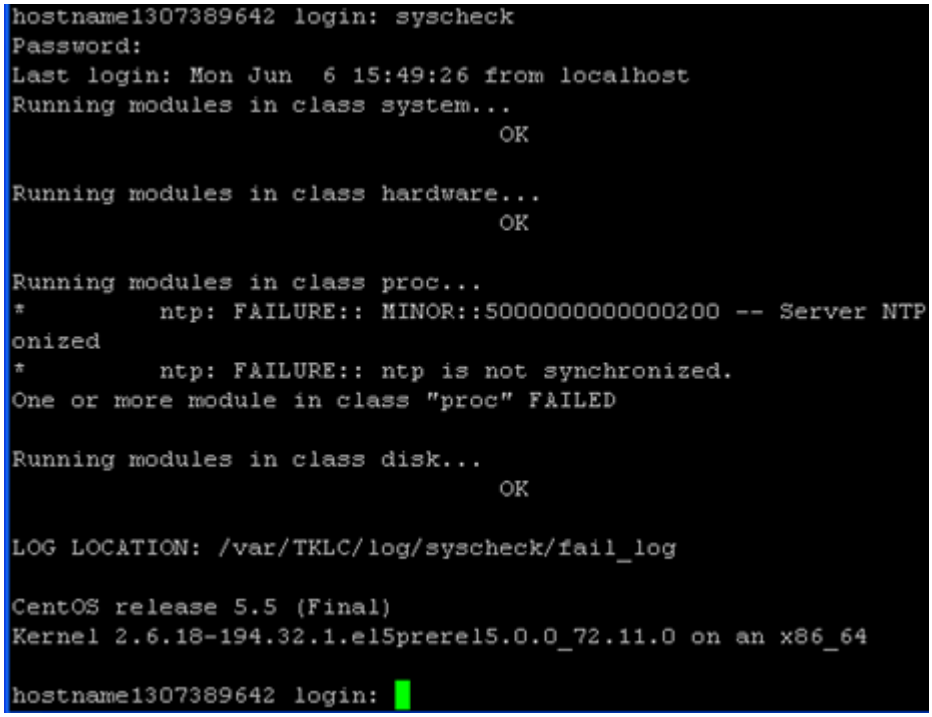


Figure 11: Example Syscheck Output with NTP Error

Figure 12: Example Syscheck Disk Failure Output indicates a disk failure in one of the syscheck tests. If the server is using software disk mirroring (RAID1), the syscheck disk test will fail until the disks have synchronized. The amount of time required to synchronize the disks will vary with disk speed and capacity. Continue executing system check every 5 minutes (by logging in as syscheck to run syscheck again) until the health check executes successfully as shown in *Figure 10: Example Successful Syscheck Output*. If the disk failure persists for more than two (2) hours, or if system check returns any other error message besides a disk failure or the NTP error shown in Figure : Example syscheck output with NTP error, do not continue, contact the Customer Care Center and report the error condition.

Figure 12: Example Syscheck Disk Failure Output

1. 1. Verify that the IPM completed successfully by logging in as admusr and running verifyIPM. Contact Customer Service if any output is printed by the verifyIPM command.

```
$ sudo /usr/TKLC/plat/bin/verifyIPM
```

2. If successful, the following message is displayed:

```
Congratulations!
Application Server IPM Process is complete and Post-install checks have passed...
You have successfully completed this procedure.
Refer to sales order to load appropriate application.
```

D.6 Media Check

1. Refer to *D.3.1 HP Rack Mount Servers - Boot from CD/DVD/USB* to automatically boot from the DVD or USB IPM media.
2. The screen output shown below indicates the initial boot from DVD is successful. Enter the command "**linux mediacheck**" and press **Enter**.

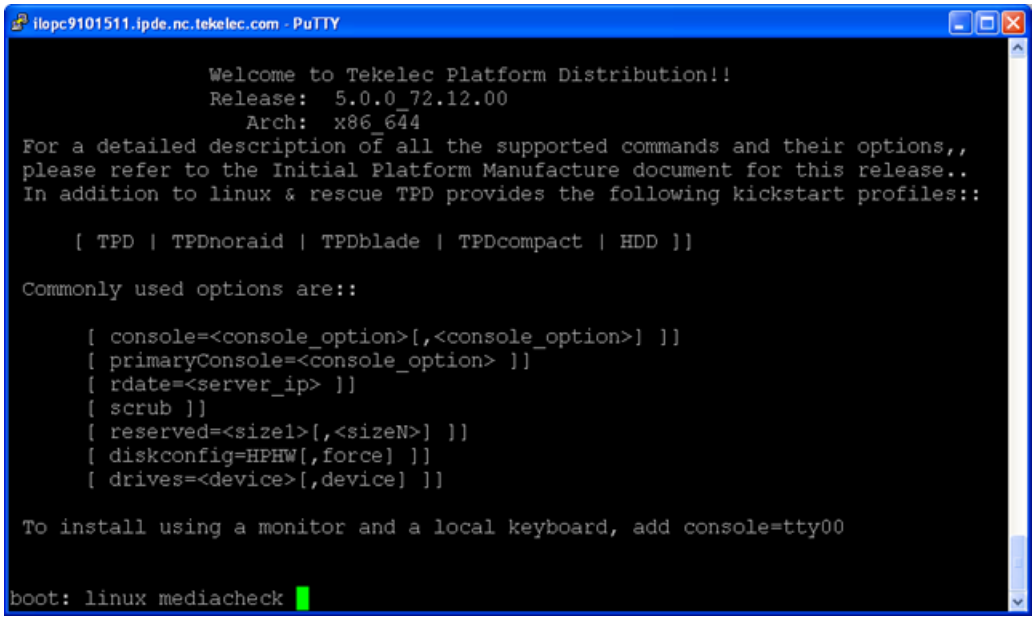


Figure 13: Example Media Check Command

3. When the following screen appears, press **Tab** until "**OK**" is highlighted and then press **Enter**.

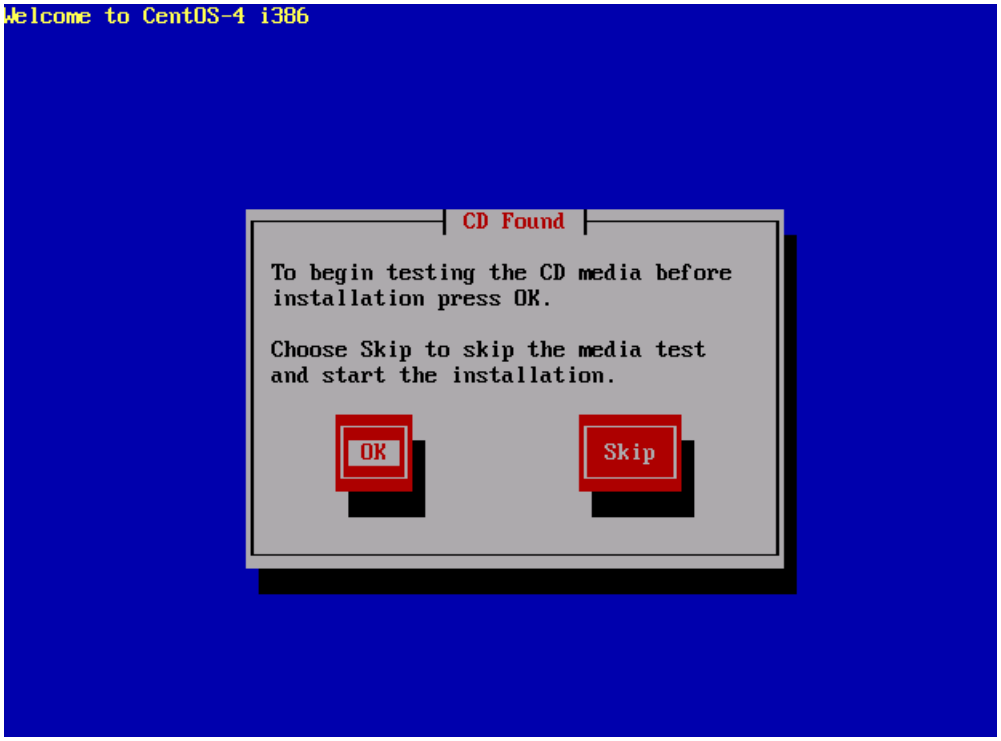


Figure 14: Example Media Test Dialog

4. Next, press **Tab** until "**Test**" is highlighted, and press **Enter** to begin testing the currently installed media.

Figure 15: Example Dialog with Test Highlighted

5. The media check will begin, with a status bar indicating the progress, as shown in the screen shot below:

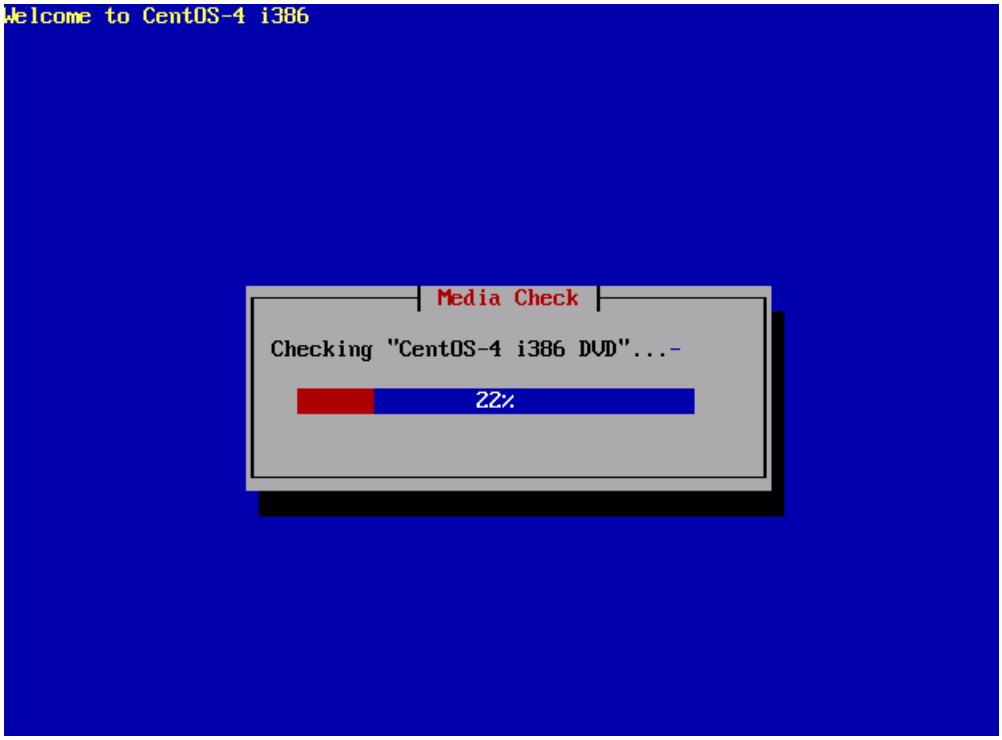


Figure 16: Example Media Check Progress Screen

6. If the media check is successful, the following screen will be displayed. Press **Enter** to continue.

Figure 17: Example Media Check Result

7. To test additional media, remove original media, insert new media, press **Tab** until "**Test**" is highlighted and press **Enter**. If no additional media is available, and the media check passed, remove the current media, insert the original media (first disk or USB pen), press **Tab** until "**Continue**" is highlighted and press **Enter** to continue the installation again.

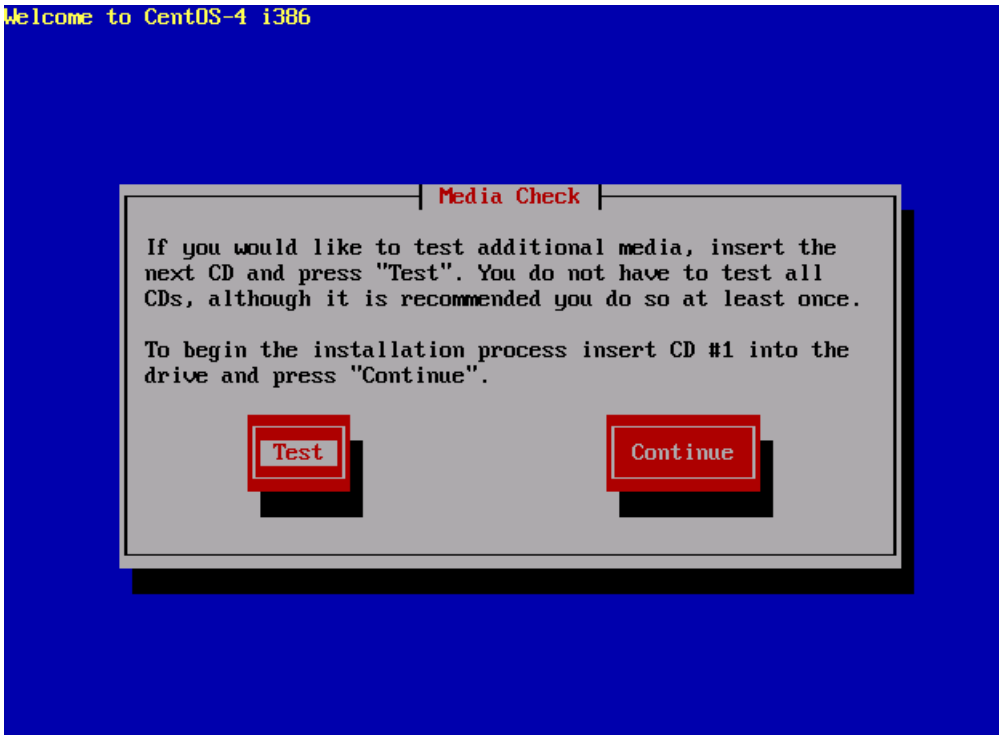


Figure 18: Example Media Check Continuation Dialog

D.7Initial Product Manufacture Arguments

1. reserved

The reserved option provides the capability to create one or more extra partitions that are not made part of the vgroot LVM volume group. The sizes of the partition(s) are indicated after "reserved=" and are separated by commas without any whitespace if there are more than one. The sizes use a suffix to indicate whether the value is in units of megabytes ('M') or gigabytes ('G'). In this context, a megabyte is 10242 and a gigabyte is 10243.

In the case of a software RAID-1 configuration, such as TPD (but not TPDnoraid), a single value will actually cause the creation of a partition on 2 drives and a metadevice (md) that incorporates the two partitions.

Examples:

1. TPD reserved=2G - On a T1200, this will create reserved partitions on sda and sdb of 2 GB, and a RAID-1 metadevice using those reserved partitions.

2. TPDnoraid reserved=512M – On an HP server, this will create a reserved partition on sda of 0.5 GB.
3. TPDnoraid reserved=4G,128M – On an HP server, this will create two reserved partitions on cciss/c0d0 of 4 GB and of 128 MB.

The partition(s) or metadevice(s) can be used by storageMgr to create a DRBD device or LVM physical volume. However, to do so, one will need to know the partition number or metadevice number.

Numbering of partitions is performed by anaconda and is controlled by anaconda. Therefore, to get the partition number, a developer would need to examine the partition table after an IPM to determine the number. Also, this number may change due to changes in anaconda in future releases of TPD.

2. scrub

This option is typically used as part of the IPM process on machines that have had TPD loaded in the past. The usage of the "scrub" option is used to ensure that the disk and logical volume partitioning that occurs during the early phase of IPM operates correctly. Note that this option should not be used during hardware USB media based IPM since doing so will erase the TPD installation media.

It is extremely important to understand that the "scrub" option will remove all data from ALL attached disk devices to the machine being IPM'ed.

Note: this includes disk drives that are not mentioned in the "drives" parameter as well as USB install media. Therefore, whenever the "scrub" option is used, any and all disk drives attached to the machine being IPM'ed, including those not mentioned in the "drives" parameter, will lose all of their data. Technically, this is accomplished by writing zeroes to the entire disk of each attached disk drive.

3. diskconfig

This option is intended to direct the IPM process to configure the disks in different ways. At this time diskconfig supports the following options:

- HPHW – specify that the server is an HP server that should be configured to use hardware RAID1 (mirroring). This option only applies to HP servers G6 and above. The expected configuration is that the first two physical drives on the array controller in slot 0 of the server will be configured as one logical disk. This is the default if no diskconfig or drives option is passed.
- HPSW – specify that the server is an HP server that should be configured to use software RAID1 (mirroring). This option only applies to HP servers G6 and above. This mode is intended for use during development and testing and is not supported on fielded systems.
- force – specify that if the current disk configuration does not match the desired configuration, that the desired configuration should forcibly installed. Loss of data on any disk on the same RAID disk controller may result.

Appendix E

Using WinSCP

Topics:

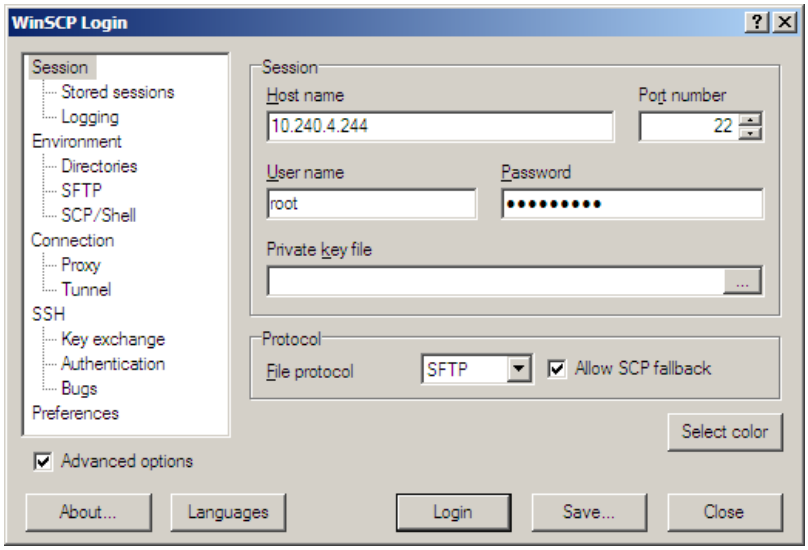
E.1 Using WinSCP

The following is an example of how to copy a file from the management server to your PC desktop

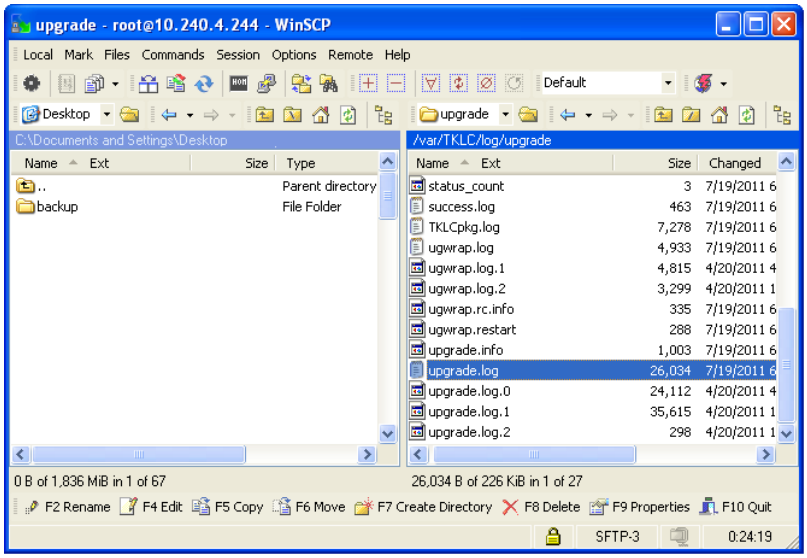
1. **Download the WinSCP Application**
   Downlaod the WinSCP application:

```
http://winscp.net/eng/download.php
```

2. **Connect to the management server**
   After starting this application, navigate to Session and enter: **<management_server_IP>** into the `Host name`, field, **root** into the `User name` field, and **<root_password>** into the `Password` field. Click **Login**.



3. **Copy the target file from the management server**
   On the left side is your own desktop filesystem. Navigate within it to Desktop directory. On the right side is the management server file system. Within it, navigate into the location of the file you would like to copy to your desktop. Highlight the file in the management server file system by pressing the insert key and press **F5** to copy the file.



4. **Close the WinSCP application**
   Then close application by pressing **F10** and confirm to terminate session by pressing **OK**.

Appendix F

Backup Procedures

Topics:

F.1 Backup HP (6120XG, 6125G) Enclosure Switch

This procedure should be executed after every change to the switch configuration after completing *4.8.2.1 Configure HP 6120XG switch (netConfig)*and/or .

Prerequisites:

- *4.1.1.1 IPM DL360 or DL380 Server* must be completed
- *4.1.1 Installing TVOE on the Management Server* must be completed
- *4.1.4 TVOE Network Configuration* must be completed
- *4.2.1 Deploy PM&C Guest* must be completed
- *4.8.2.1 Configure HP 6120XG switch (netConfig)*
-

Procedure Reference Tables:

Variable	Value
<switch_name>	hostname of the switch

1. Ensure the directory where the backups will be stored exists.

```
$ /bin/ls -i -l /usr/TKLC/smac/etc/switch/backup
```

   If you receive an error such as the following:

```
-bash: ls: /usr/TKLC/smac/etc/switch/backup: No such file or directory
```

   Then the directory must be created by issuing the following command:

```
$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/backup
```

2. Execute the backup command

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration
service=ssh_service filename=<switch_name>-backup
```

3. Copy the files to the backup directory.

```
$ sudo /bin/mv -i ~admusr/<switch>-backup* /usr/TKLC/smac/etc/switch/backup
```

4. Verify switch configuration was backed up by cat <switch_name> and inspecting its contents to ensure it reflects the latest known good switch configurations.

```
$ /bin/ls -i /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup*
$
$ /bin/cat /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup
$
```

5. Repeat *Step 2* - *Step 4* for each HP switch to be backed up.

F.2 Backup Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)

Tekelec Provided Aggregation Switch Prerequisites for RMS system:

- *4.1.1.1 IPM DL360 or DL380 Server* must be completed.
- *4.3.2 Configure Cisco 4948/4948E/4948E-F aggregation switches (PM&C installed)(netConfig)*)
- Application username and password for creating switch backups must be configured on the management server prior to executing this procedure.

Tekelec Provided Aggregation Switch Prerequisites for c-Class system:

- *4.1.1.1 IPM DL360 or DL380 Server* must be completed
- *4.1.1 Installing TVOE on the Management Server* must be completed
- *4.1.4 TVOE Network Configuration* must be completed
- *4.2.1 Deploy PM&C Guest* must be completed
- *4.3.2 Configure Cisco 4948/4948E/4948E-F aggregation switches (PM&C installed)(netConfig)*)

Prerequisites for Cisco 3020 Enclosure switches:

- *4.1.1.1 IPM DL360 or DL380 Server* must be completed
- *4.1.1 Installing TVOE on the Management Server* must be completed
- *4.1.4 TVOE Network Configuration* must be completed
- *4.2.1 Deploy PM&C Guest* must be completed
- *4.8.1.1 Configure Cisco 3020 switch (netConfig)*

Procedure Reference Tables:

Variable	Value
<switch_backup_user> (also needed in switch configuration procedure)	admusr
<switch_backup_user_password> (also needed in switch configuration procedure)	Check application documentation
<switch_name>	hostname of the switch
<switch_backup_directory>	**Non-PM&C System:** /usr/TKLC/plat/etc/switch/backup
	PM&C System: /usr/TKLC/smac/etc/switch/backup

1. Verify switch is at least initialized correctly and connectivity to the switch by verifying hostname

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> getHostname
Hostname: switch1A
$
```

Note: The value beside "Hostname:" should be the same as the <switch_name> variable.

2. Run command "netConfig --repo showService name=ssh_service" and look for ssh service.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service
    Service Name:    ssh_service
            Type:    ssh
            Host:    10.250.62.85
            Options:
               password: C20F7D639AE7E7
               user: admusr
$
```

   In the ssh_service parameters, the value for 'user:' will be the value for the variable <switch_backup_user>.

3. Verify existence of the backup directory.

```
$ /bin/ls -i <switch_backup_directory>
```

   If the output contains

```
ls: cannot access <switch_backup_directory>: No such file or directory
```

   create the directory with:

```
$ sudo /bin/mkdir -p <switch_backup_directory>
```

4. Execute the backup command

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration
service=ssh_service filename=<switch_name>-backup
```

5. Verify switch configuration was backed up by cat <switch_name>-backup and inspect its contents to ensure it reflects the latest known good switch configurations. Then, copy the files over to the backup directory.

```
$ /bin/ls -i ~<switch_backup_user>/<switch_name>-backup*
$
$ /bin/cat ~<switch_backup_user>/<switch_name>-backup*
$
$ sudo /bin/mv -i  ~admusr/<switch name>-backup* <switch_backup_directory>/
```

   Note: The cat command may leave garbled text on the next terminal prompt. Disregard this text.

   Example:

```
[admusr@pmac ~]$
PuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTY
```

6. Repeat steps 1, 4-6 for each switch to be backed up.

Appendix G

How to Access a Server Console using the iLO

Topics:

G.1 How to Access a Server Console using the iLO

For each server, fill in the iLO IPs in the following table:

Server ID	Hostname	iLO IP

The following two tables show a list of default IP Addresses assigned by Manufacturing to the RMS and OA ILOs.

Management VLAN 2	
Network	192.168.100.0
Netmask	255.255.255.0
VLAN 2-VIP (Gateway)	192.168.100.1
Switch1A	192.168.100.2
Switch1B	192.168.100.3
PMAC Server	192.168.100.4 bond0.2
PMAC iLO	192.168.100.5

First HP c7000 Enclosure		Second HP c7000 Enclosure	
HP c7000 OA 1	192.168.100.6	HP c7000 OA 1	192.168.100.28
HP c7000 OA 2	192.168.100.7	HP c7000 OA 2	192.168.100.29
HP Enclosure 1 Blade 1 iLO	192.168.100.10	HP Enclosure 2 Blade 1 iLO	192.168.100.30
HP Enclosure 1 Blade 2 iLO	192.168.100.11	HP Enclosure 2 Blade 2 iLO	192.168.100.31
HP Enclosure 1 Blade 3 iLO	192.168.100.12	HP Enclosure 2 Blade 3 iLO	192.168.100.32
HP Enclosure 1 Blade 4 iLO	192.168.100.13	HP Enclosure 2 Blade 4 iLO	192.168.100.33
HP Enclosure 1 Blade 5 iLO	192.168.100.14	HP Enclosure 2 Blade 5 iLO	192.168.100.34
HP Enclosure 1 Blade 6 iLO	192.168.100.15	HP Enclosure 2 Blade 6 iLO	192.168.100.35
HP Enclosure 1 Blade 7 iLO	192.168.100.16	HP Enclosure 2 Blade 7 iLO	192.168.100.36

First HP c7000 Enclosure		Second HP c7000 Enclosure	
HP Enclosure 1 Blade 8 iLO	192.168.100.17	HP Enclosure 2 Blade 8 iLO	192.168.100.37
HP Enclosure 1 Blade 9 iLO	192.168.100.18	HP Enclosure 2 Blade 9 iLO	192.168.100.38
HP Enclosure 1 Blade 10 iLO	192.168.100.19	HP Enclosure 2 Blade 10 iLO	192.168.100.39
HP Enclosure 1 Blade 11 iLO	192.168.100.20	HP Enclosure 2 Blade 11 iLO	192.168.100.40
HP Enclosure 1 Blade 12 iLO	192.168.100.21	HP Enclosure 2 Blade 12 iLO	192.168.100.41
HP Enclosure 1 Blade 13 iLO	192.168.100.22	HP Enclosure 2 Blade 13 iLO	192.168.100.42
HP Enclosure 1 Blade 14 iLO	192.168.100.23	HP Enclosure 2 Blade 14 iLO	192.168.100.43
HP Enclosure 1 Blade 15 iLO	192.168.100.24	HP Enclosure 2 Blade 15 iLO	192.168.100.44
HP Enclosure 1 Blade 16 iLO	192.168.100.25	HP Enclosure 2 Blade 16 iLO	192.168.100.45
Cisco 3020 switch Bay 1	192.168.100.26	Cisco 3020 switch Bay 1	192.168.100.46
Cisco 3020 switch Bay 2	192.168.100.27	Cisco 3020 switch Bay 2	192.168.100.47

1. **Access the iLO GUI**

   Using a laptop or desktop computer connected to the customer network, navigate with Internet Explorer to the IP address of the iLO of the Management Server. Log in to the iLO as the user "Administrator".

2. **If the iLO is an iLO 2, configure Hot Keys**

   The iLO GUI will indicate the iLO version as iLO 2 ("Integrated Lights-Out 2"), iLO 3, iLO 4, etc. If this is an iLO 2, perform the following Hot Key configuration:

   a) Click the **Remote Console** tab
   b) Click the **Settings** menu item and then the **Hot Keys** sub-tab
   c) In the row starting with **Ctrl-T** change the first dropdown to **L_CTRL** and the second dropdown to **]** (right bracket). The rest of the dropdowns in the row should be **NONE**.
   d) Click **Save Hot Keys**

   As a result, pressing **Ctrl-T** rather than **Ctrl-]** will now exit the console of a TVOE guest and return to the console of the TVOE host.

3. **Launch the Remote Console Window**

   Navigate to **Remote Console** > **Remote Console** to launch the remote console in a new window.

4. **Log in to the Console**

In the Remote Console window, log in to the console as user "admusr":

```
login as: admusr
Password:
Last login: Wed Jun  5 17:52:28 2013
[admusr@tvoe ~]$
```

5. **Return to the referencing procedure**

   Return to the procedure which referenced this appendix.

Appendix H

How to Exit a Guest Console Session on an iLO

Topics:

H.1 How to Exit a Guest Console Session on an iLO

1. **Enter the appropriate control sequence for the iLO version**

   If the main iLO GUI window indicates that this is an iLO 2 ("Integrated Lights-Out 2"), press **Ctrl-T**. Otherwise, press **Ctrl-]**.

   This corresponds to the configuration of iLO 2 Hot Keys performed in *Appendix G: How to Access a Server Console using the iLO*.

2. **Return**
   Return to the procedure which referenced this appendix.

Appendix I

Changing SNMP Configuration Settings for iLO

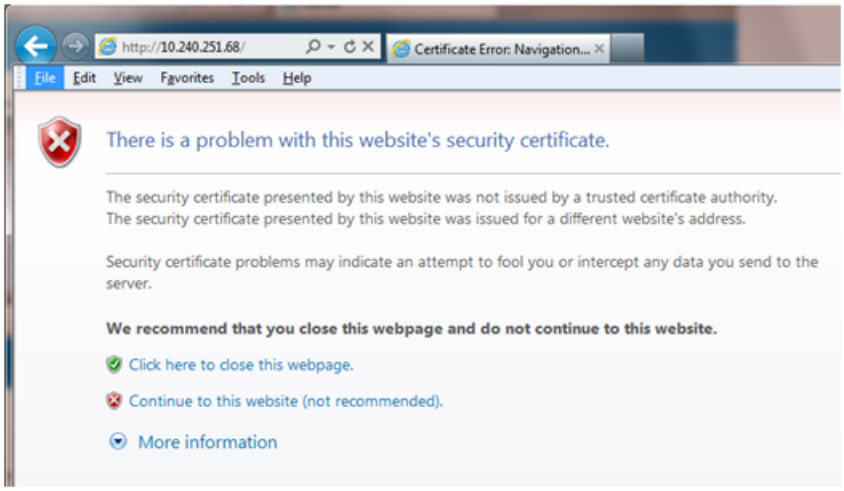
Topics:

I.1 Changing SNMP Configuration settings for iLO2

This procedure provides instructions to change the default SNMP settings for the HP ProLiant iLO 2 devices.

Perform this procedure for every iLO 2 device on the network. For instance, for every HP ProLiant G1/G5/G6 Blade and Rack Mount server.

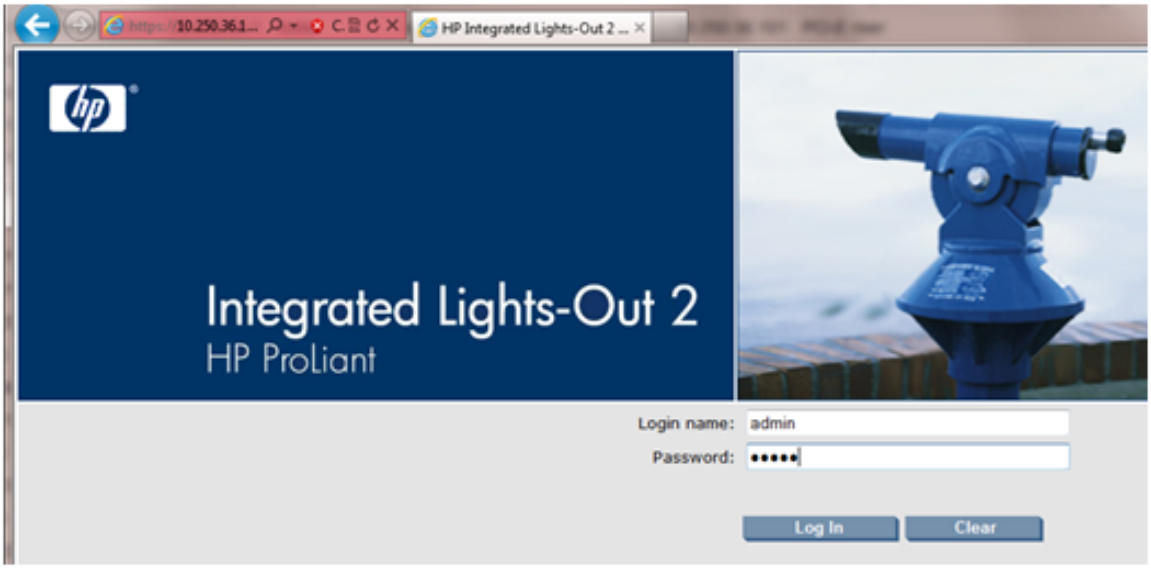
1. **From Workstation:** Launch Internet Explorer 7.x or higher and connect to the iLO2 device using "https://"



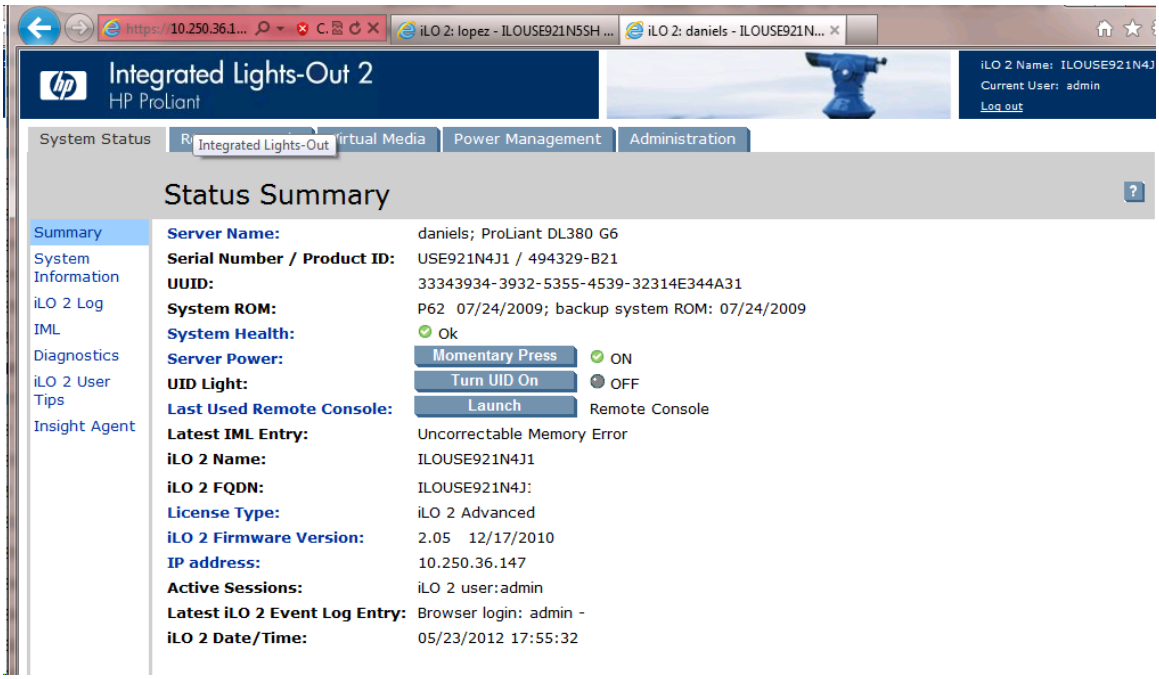
2. **iLO2 Web UI:**

   The user should be presented the login screen shown below.

   Login to the GUI using an Administrator account name and password.



3. **iLO2 Web UI:** The user should be presented the iLO2 System Status page as shown on the right



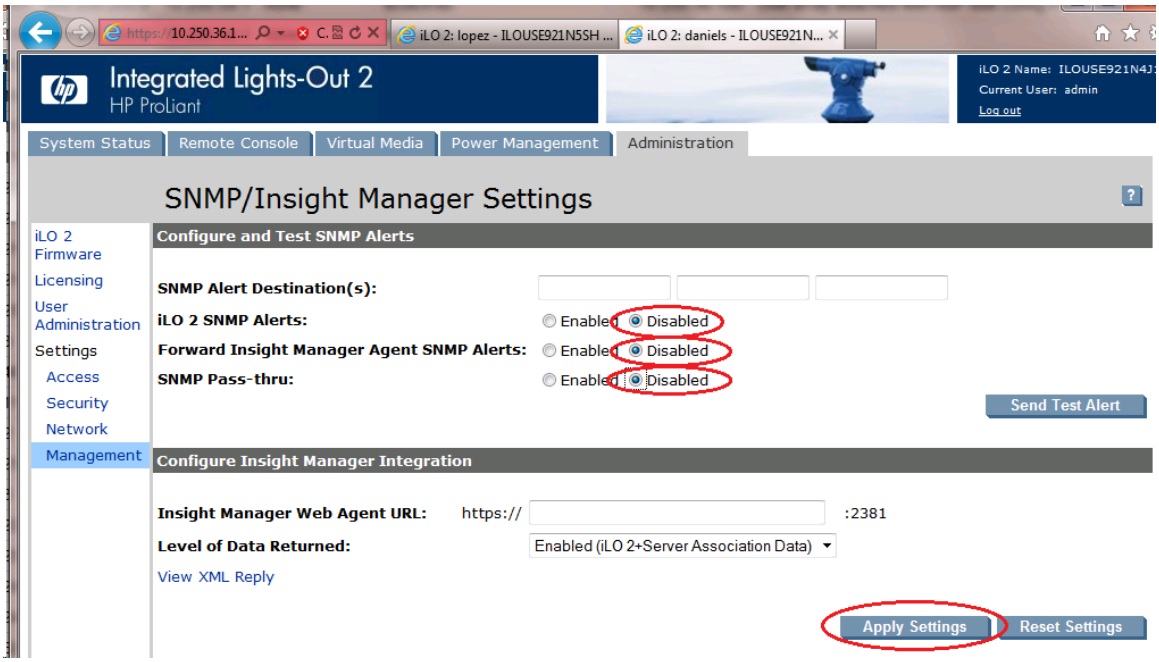
4. **iLO 2 Web UI:**
   1. Select the [Administration] tab on the top navigation bar.
   2. Select the [Management] menu item on the left navigation bar to display the SNMP Settings page.

5. **iLO2 Web UI:**

   The user should be presented the SNMP/Insight Manager Settings page.

   1. Select option [Disabled] for each of the 3 SNMP settings as shown to the right
   2. Click [Apply Settings] to save the change.

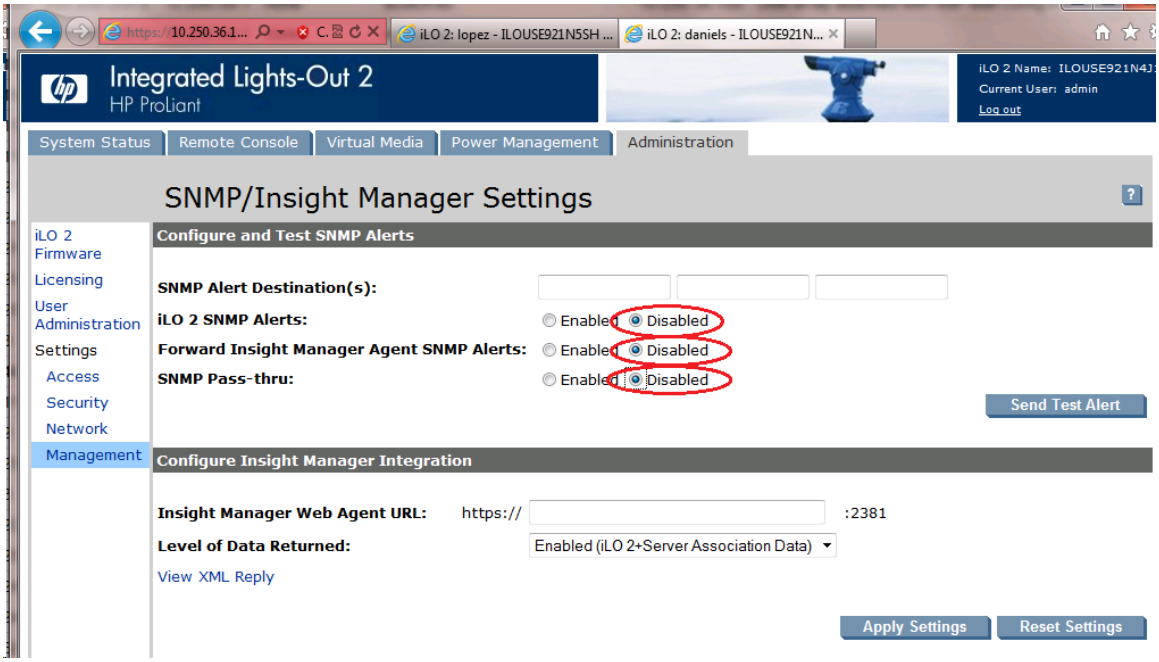
   The web page will refresh but no specific indication will be given that settings have been saved.



6. **iLO 2 Web UI:**

   To verify the setting change navigate away from the SNMP/Insight Manager Settings page and then go back to it to verify the SNMP settings as shown on the right.

   1. Click [Log out] link in upper right corner of page to log out of the iLO Web UI.



7. Complete for remaining iLO2 devices

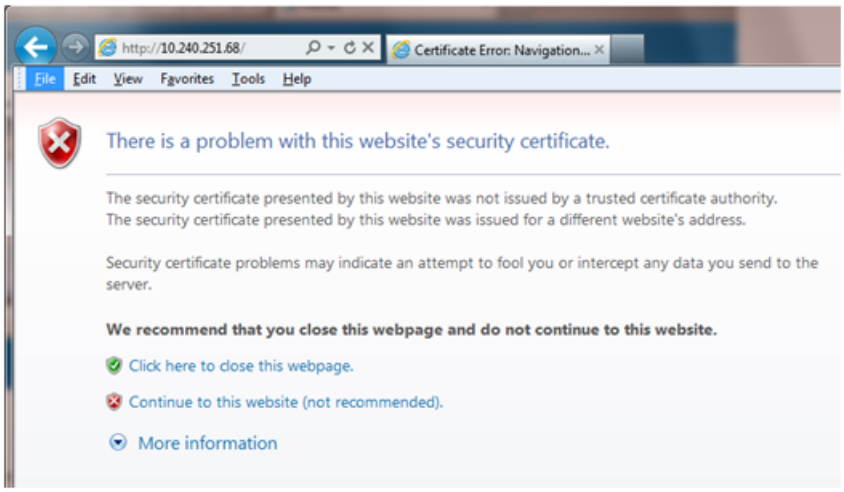
   Repeat this procedure all remaining iLO 2 devices on network.

I.2 Changing SNMP Configuration Settings for iLO 3 and iLO4

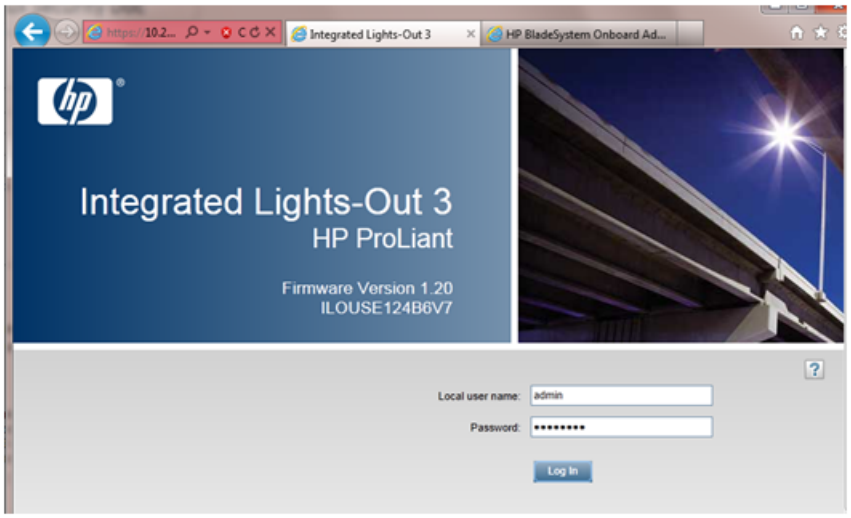
This procedure provides instructions to change the default SNMP settings for the HP ProLiant iLO 3 devices.

Perform this procedure for every iLO 3 device on the network. For instance, for every HP ProLiant G7 Blade and Rack Mount server.

1. **From Workstation:** Launch Internet Explorer 7.x or higher and connect to the iLO 3/iLO 4 device using "https://"

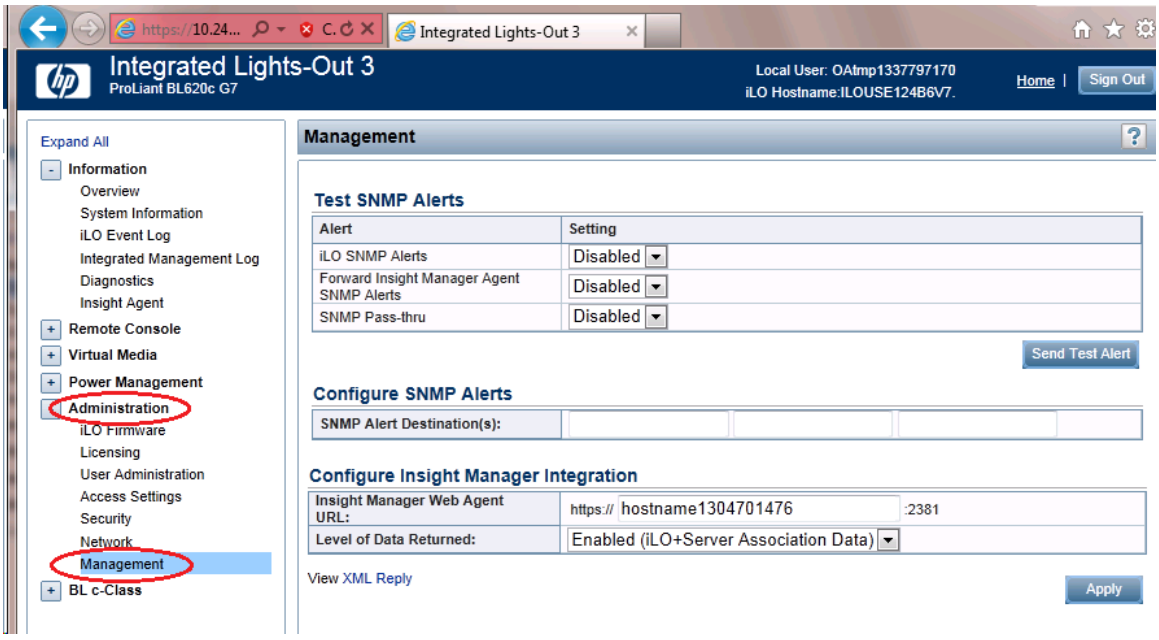


2. **iLO 3/iLO 4 Web UI:**
   The user should be presented the login screen shown below.
   Login to the GUI using an Administrator account name and password.



3. **iLO 3/iLO 4 Web UI:**
   The user should be presented the iLO 3/iLO 4 Overview page as shown below.

4. **iLO 3/iLO 4 Web UI:**
   1. Expand the [Administration] menu item in the left hand navigation pane.
   2. Select the [Management] sub-menu item to display the Management configuration page.

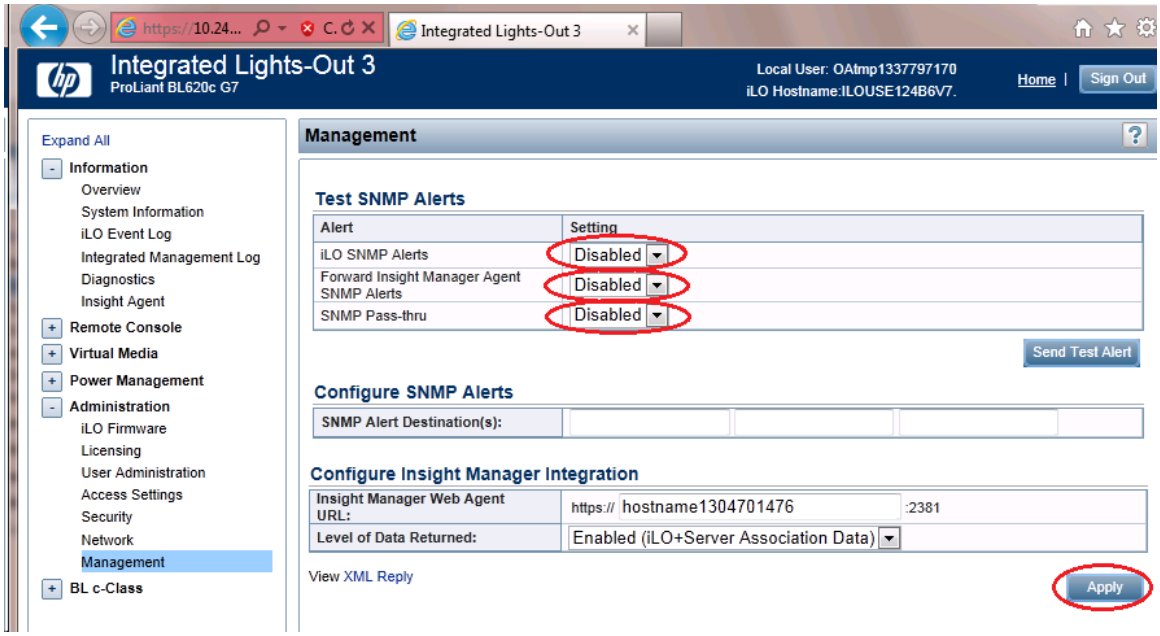


5. **iLO 3/iLO 4 Web UI:**

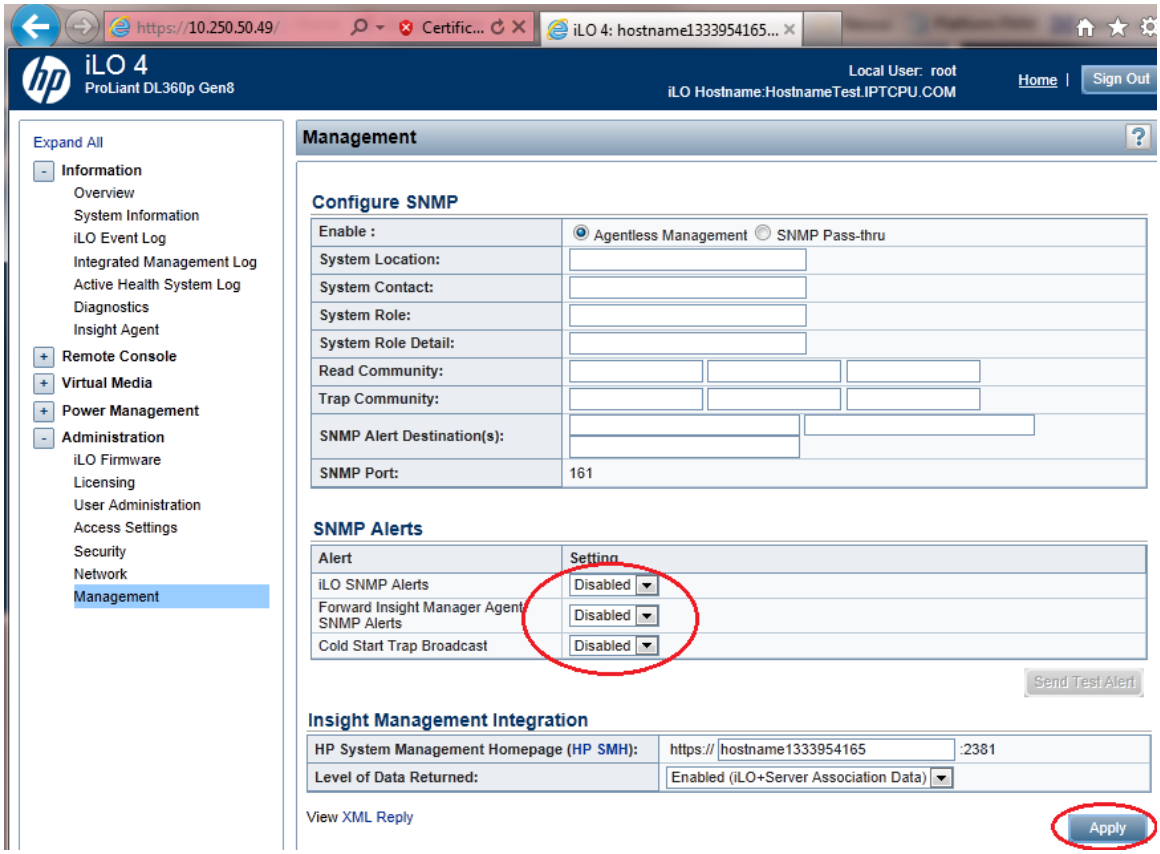
   The user should be presented the Management configuration page as shown on the right.
   1. Select setting [Disabled] for each of the 3 SNMP Alerts options as shown to the right.
   2. Click [Apply] to save the change.

On the iLO 3 the web page will refresh but no specific indication will be given that settings have been saved.

iLO3 Web UI:



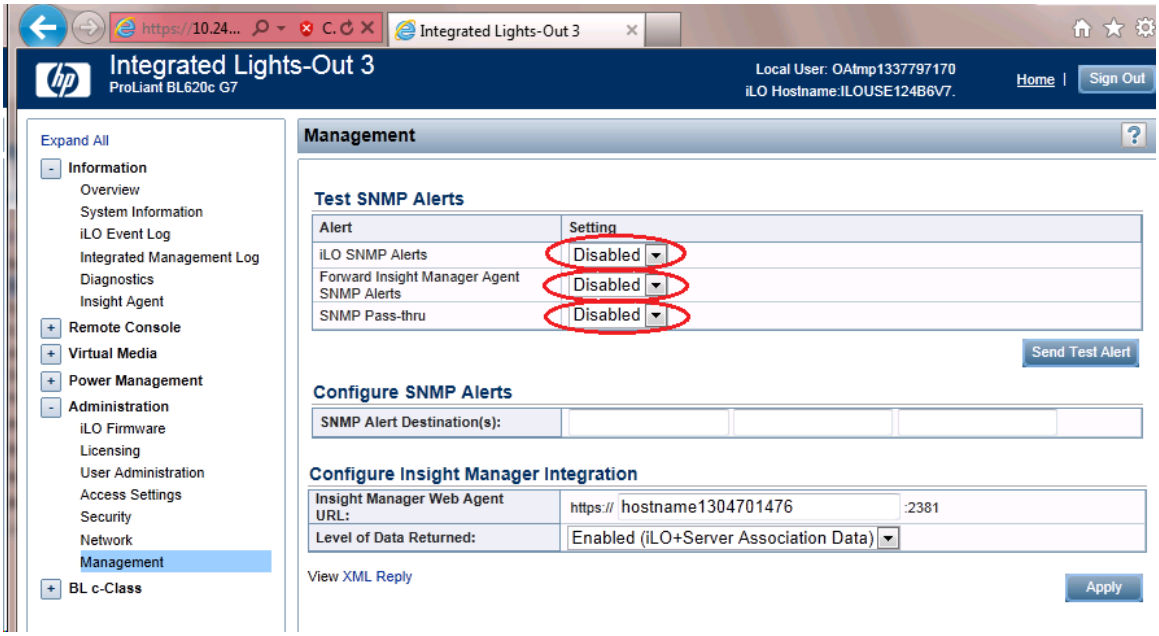
iLO4 Web UI:



6. **iLO 3/iLO 4 Web UI:**

   To verify the setting changes navigate away from the Management configuration page and then go page back to it to verify the SNMP settings as shown on the right.

   1. Click [Sign Out] link in upper right corner of page to log out of the iLO Web UI.



7. Complete for remaining iLO3/iLO 4 devices
   Repeat this procedure all remaining iLO 3/iLO 4 devices on network.

Appendix J

Creating a Bootable USB Drive

Topics:

J.1 Creating a Bootable USB Drive on Windows

Note: This procedure will create a Bootable USB drive from a .usb file.

1. **Insert USB Media:** Insert the USB Media into the USB Port.
2. **Install Media Builder:** Download the Tekelec Media Builder tool from the Tekelec shared drive (m:\mbuilder) and follow the instructions on how to install it.
3. **Copy the .USB file to your local machine:** Using sftp, copy the .usb image file to your local machine.
4. **Use Media Builder to create a bootable USB** Use the Media Builder tool to create a bootable USB drive from the .usb image file copied in Step 3.

J.2 Creating a Bootable USB Drive on Linux

Note: This procedure will create a Bootable USB drive from a .usb file on a Linux machine.

1. **Insert USB Media:** Insert the USB Media into the USB Port. It should automatically be mounted under /media.
   a) Obtain the path of the USB drive by running:

```
# ls /media
```

   The output should be similar to the following:

```
sdb1
```

   b) Note down the path without the partition number (in this case, it would be /dev/sdb).
2. **Linux machine:** Obtain the <product> **.usb** file and copy it onto the local Linux machine (e.g., under /tmp).
3. **Copy the .USB file onto the USB drive:** Use the `dd` command to copy the .usb file onto the USB drive.

   Note: Make sure you **do not** use the partition number when copying the file

```
# dd if=<path_to_usb_image> of=/dev/sdb oflag=direct
```

4. **Remove USB from Port:** Once the `dd` command is done, remove the USB drive from the USB port and delete the .usb file.

Appendix K

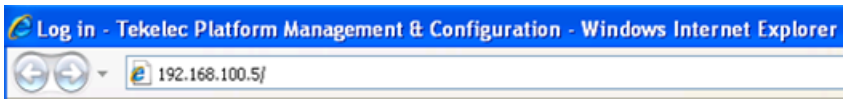
TVOE iLO GUI Access

Topics:

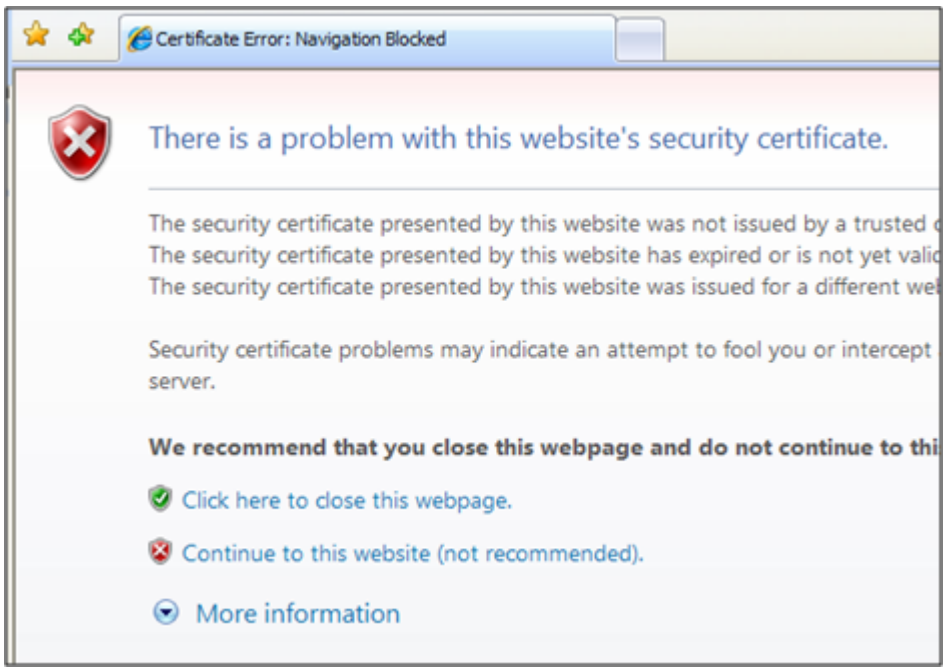
K.1 Accessing the TVOE iLO GUI

This procedure contains the steps to access the TVOE iLO GUI.

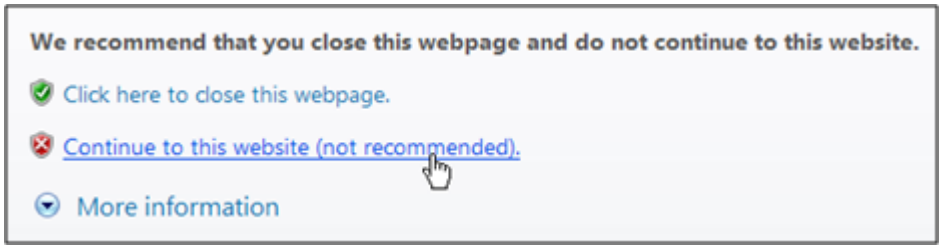
1. Launch Internet Explorer and "Go To" 192.168.100.5 (manufacturing default) or customer IP set during installation.



2. Internet Explorer may display a warning message regarding the Security Certificate.



3. Select the option to "Continue to the website (not recommended)."



4. Log in as user "**root**".

5. The TVOE iLO Home page is displayed.

6. Click on Launch to start the pmac iLO CLI.

Appendix L

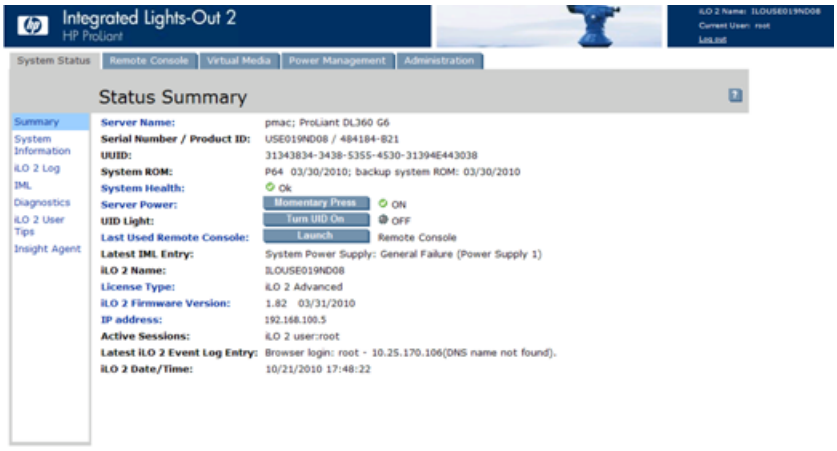
Changing TVOE iLO Address

Topics:

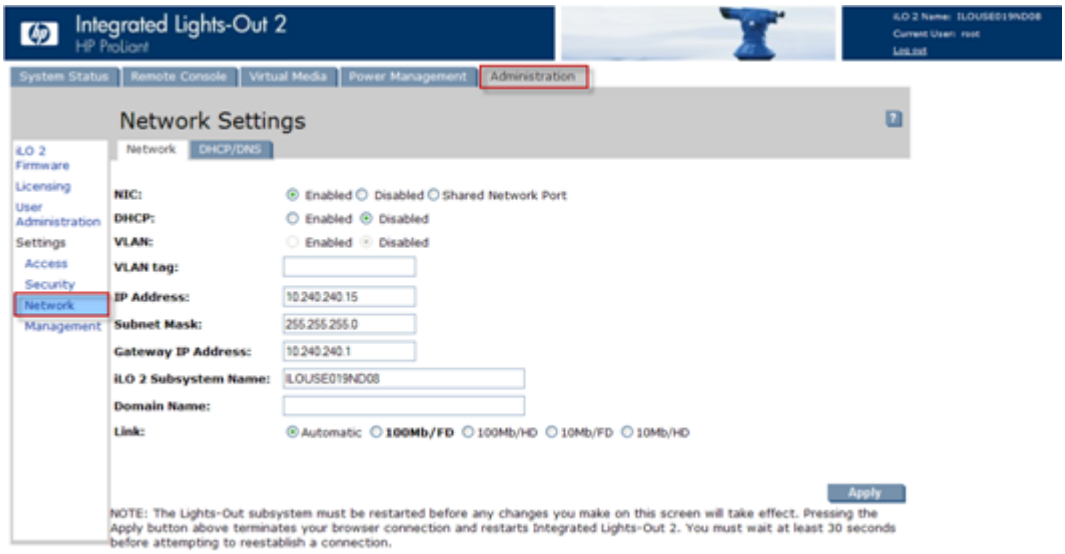
L.1 Changing the TVOE iLO Address

This procedure contains the steps to access the TVOE iLO GUI.

1. Connect to the TVOE iLO GUI using the instructions in *TVOE iLO GUI Access*



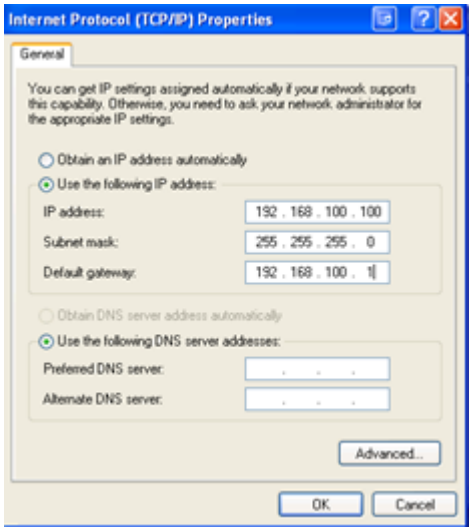
2. Click the "**Administration**" tab. Under "**Settings**"in the left column click on "**Network**".



3. Change the **IP Address**, **Subnet Mask** and **Gateway IP Address** to the values supplied in the IP Site Survey for the TVOE iLO. Click **Apply**.

   Note: You will lose access after you hit the **Apply** button.

4. Using the instructions found in Appendix B *NetBackup Procedures (Optional)*, reset the PC's network connection, replacing the **Subnet Mask** and **Gateway** with those just used for the TVOE iLO. Use an appropriate **IP address** for this subnet. Contact Customer Support if needed.



5. Connect to the TVOE iLO GUI using the instructions in *TVOE iLO GUI Access*.

   Note: Use the IP address entered in Step 3 and not 192.168.100.5.


Integrated Lights-Out 2
HP ProLiant
iLO 2 Name: ILOUSE019ND08
Current User: root
Log out
System Status
Remote Console
Virtual Media
Power Management
Administration
Status Summary
Summary
System Information
iLO 2 Log
IML
Diagnostics
iLO 2 User Tips
Insight Agent
Server Name: pmac; ProLiant DL360 G6
Serial Number / Product ID: USE019ND08 / 484184-B21
UUID: 31343834-3438-5355-4530-31394E443038
System ROM: P64 03/30/2010; backup system ROM: 03/30/2010
System Health: Ok
Server Power: Momentary Press ON
UID Light: Turn UID On OFF
Last Used Remote Console: Launch Remote Console
Latest IML Entry: System Power Supply: General Failure (Power Supply 1)
iLO 2 Name: ILOUSE019ND08
License Type: iLO 2 Advanced
iLO 2 Firmware Version: 1.82 03/31/2010
IP address: 192.168.100.5
Active Sessions: iLO 2 user:root
Latest iLO 2 Event Log Entry: Browser login: root - 10.25.170.106(DNS name not found).
iLO 2 Date/Time: 10/21/2010 17:48:22