Oracle® Communications
Oracle Firmware Upgrade Pack

Upgrade Guide

Release 3.1.8

E87832 Revision 01

February 2018

ORACLE®

Oracle Communications Oracle Firmware Upgrade Pack, Upgrade Guide, Release 3.1.8

CAUTION: Use only the Upgrade procedure included in the Upgrade Pack.

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

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.

Table of Contents

1 Introduction

Topics:

1.1 Purpose and Scope

This document details the procedures used to perform firmware upgrades on Oracle Rack Mount Server environments. Included in the scope are Oracle Rack Mount Servers running Telecom Platform Distribution (TPD) software releases 6.7.1 and 7.0.1 or greater.. The intended audience for this document consists of the following: Software Development, Product Verification, Documentation, and Customer-Service.

1.2 References

1. *Oracle X5 Series Servers Administration Guide*

   http://docs.oracle.com/cd/E23161_01/pdf/E52424.pdf
2. *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.X*

   http://docs.oracle.com/cd/E37444_01/pdf/E37446.pdf
3. *Oracle Communications© Oracle Firmware Upgrade Pack 3.1.8, Release Notes, E87833*

1.3 Software Release Numbering

Oracle server environments contain several firmware components, all of which are versioned differently. Please refer to the *Release Notes* for the specific versions contained.

1.4 Acronyms

Table 1 Acronyms

BIOS	Basic Input Output System
GUI	Graphical User Interface
ILOM	Integrated Lights Out Manager
RMS	Rack Mount Server
ISO	ISO 9660 file system optical disk image
OSA	Oracle System Assistant
USB	Universal Serial Bus
PM&C	Platform Management and Configuration
TFTP	Trivial File Transfer Protocol
IOS	Internetwork Operating System

1.5 Terminology

This section describes some of the terminology used in this document.

Table 2 - Terminology

Firmware	Program code and data stored directly into an area of persistent memory for the purpose of controlling the operation of a server or one of its devices
Upgrade	The process of updating the firmware of a server to a newer release.
System Health Check	Procedure used to determine the health and status of a server
Upgrade-Ready	A state that allows for a successful upgrade to be performed.
Oracle System Assistant	A management application stored on an embedded USB drive in the server. This is the application used to store firmware images and to upgrade the server's firmware.
Oracle System Assistant Updater	An ISO image used to update or recover the OSA associated with a particular server.
Integrated Lights Out Manager	The service processor and associated firmware used to provide management services for the server.

1.6 Documentation Conventions

- GUI menu items, action links, and buttons to be clicked on are in bold font
- GUI fields and values to take note of during a step are in bold font
- Each command that the user must enter is formatted in a code block as show below:

```
$ ls -al
```

- Command output is formatted in a code block as shown below

```
$ ls -al
Total 32
drwx------. 3 admusr admgrp 4096 Dec 2  10:13 .
drwxr-xr-x. 6 root   root   4096 Nov 27 16:01 ..
```

- Variable, user entered command line input is surrounded by angled brackets and formatted in a code block.

2 Upgrade Overview

Topics:

This section presents a list of materials that will be required to perform these procedures, as well as the steps to take when planning to perform an upgrade.

2.1 Required Materials

- *Oracle Firmware Upgrade Pack 3.1.8, Release Notes, E87833*
- A local workstation running MS Windows 7 or Windows 10, WinZip or 7Zip, Java, and one of the following supported browsers:
    - Internet Explorer 11+
    - Firefox 3.6.x +
- User logins, passwords, IP addresses and other administrative data. Refer to the Data Collection Worksheets in Appendices A and B.

VPN access to the customer's network is required if that is the only method to login to the target servers. The connection into the customer's network must support both *ssh* and *https* as both may be required to perform firmware upgrades. Firmware upgrades should not be attempted in environments where virtual media would be used over slow and/or unreliable connections.

2.2 Firmware Upgrade Planning

The following steps should be done when planning for an execution of the upgrade procedures contained in this document.

1. Identify the systems that are to be upgraded. The upgrade process per rack mount server could take up to 40 minutes. This should be taken into account when determining how much time will be required to perform all upgrades.
2. Collect logins, passwords, and ILOM IP addresses for the servers being upgraded. *Appendix A - Data Collection Worksheet for Oracle RMS* can be used to collect this data.
3. Verify that the workstation that will be used to perform the upgrades has access to the ILOM IP addresses from step 2.
4. Collect PM&C IP address and login/password. Verify connectivity to the PM&C
5. If there are any Cisco 4848 E-F switches purchased through Oracle, collect the switch login information for each. Record this data in *Appendix B - Data Collection Worksheet for Cisco 4948E-F* and *Appendix C - Data Collection Worksheet for Cisco 9372TX-E*.

3 Upgrade Preparation

This section provides the prerequisites and procedures required to prepare for a firmware upgrade. **They should be executed outside of a maintenance window**.

3.1 Important Instructions and Warnings

Before upgrading, users must perform the system health check in the *Perform System Health Check* section. This check ensures that the servers requiring upgrade are in an upgrade-ready state.

******WARNING******

If the server being upgraded is not in an upgrade ready state, as determined by the System Health Check, the server should be brought to this state before an upgrade is attempted.

Before an upgrade is attempted, any applications should be gracefully brought down as per the appropriate application documentation. In addition, it should be verified that any server being upgraded is actually in a position where it can be taken down.

Please read the following notes on upgrade procedures:

Command response outputs are shown accurately as possible. EXCEPTIONS are as follows:

- Session banner information such as time and date
- System-specific configuration information such as hardware locations, IP addresses, and hostnames
- ANY information marked with "XXXX" or "YYYY"
- Aesthetic differences that are unrelated to functionality: i.e. browser attributes, window size, colors, toolbars, and button layouts

After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade must initial each step. The space on either side of the step can be used.

Capturing data is required for future support reference if Oracle Technical Services is not present during the upgrade.

3.2 Prerequisites

Before attempting upgrades, verify that the following prerequisite steps, needed to perform an upgrade, have been completed.

1. Verify all required materials are present.

   Materials are listed in the *Required Materials* section.

2. Review the *Release Notes*.

   Review the Oracle Firmware Upgrade Pack Release Notes for the target release. Take note of any special instructions that may be included.

3. Verify all administrative data needed during upgrade.

   Double check that all the information in the required worksheets has been filled-in and is accurate.

4. Contact Oracle Support.

   Contact the Oracle Support and inform them of your plans to perform upgrades. Refer to *Appendix E – Contacting Oracle Support* for contact information

3.3 Perform System Health Check

These procedures are part of the firmware upgrade preparation process and are used to determine the health and status of Oracle rack mount servers being upgraded. The health checks must be performed once for each server being upgraded within the time frame of 24-36 hours prior to the start of a maintenance window.

3.3.1 System Health Check for Oracle Servers

Repeat this procedure for each Oracle Rack Mount Server to be upgraded.

1. Access the command prompt and login to the server as "admusr". If the server being upgraded is a TVOE host, be sure to login to the host and not to one of the guests.

   ```
   login as: admusr
   password: <admusr_password>
   ```

2. Verify integrity of system health by running alarmMgr command

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

   - Examine the output of the alarmMgr command to determine if there are any alarms that are currently set
   - If there are any alarms reported by alarmMgr contact Oracle Customer Care for further instructions as to how to proceed.

3. If there are no alarms reported by alarmMgr, continue with the upgrade process.

3.4 Determine Firmware Upgrade Procedure for Rack Mount Servers

Depending on what server components are in need of upgrade, there are different procedures that can be followed. If the ILOM/BIOS are the only components that need to be upgraded, then the Firmware Pack can used to perform the upgrade via the ILOM web interface. This procedure will be referred to as the ILOM/BIOS Only Procedure and can only be used to upgrade that single component (ILOM/BIOS are packaged together and treated as a single component). Refer to Table 2.3.3 in the Release Notes. If any other components need to be updated, the Oracle System Assistant upgrade procedure should be used for X5-2 and Netra X5-2. This procedure will upgrade the Oracle System Assistant so that it contains all of the latest firmware. The OSA can then be used to upgrade every component, including the ILOM/BIOS. Refer to Table 2.3.1 in the Release Notes. For the X6-2 and X7-2, if there are components that need to be upgraded in addition to the ILOM/BIOS use the Live ISO Media Upgrade procedure. For each server to be upgraded, only one of the three procedures will be required.

Repeat this procedure for each Oracle Rack Mount procedure.

1. From TPD/TVOE command line execute the firmwareInfo command to find ILOM, BIOS, and RAID controller firmware versions. Note that the ILOM is identified in the below command as IPMI (Intelligent Platform Management Interface).

```
[admusr@hostname9aa81f1611e6 ~]$ sudo firmwareInfo -i -b -r
BIOS
      Version: 38040100
      Release date: 06/06/2016
IPMI
      Version: v3.2.6.46 r110665
RAID controller # 0
      Type: LSI Logic
      Firmware version: 4.230.40-3739
      Drives
            c0d0: A990
            c0d1: A990
```

   Record the version in *Appendix A - Data Collection Worksheet for Oracle RMS*.

2. Execute the following procedure to determine NIC firmware versions.

   i) Determine present Ethernet Devices

```
[admusr@hostname9aa81f1611e6 ~]$ ip link | grep "eth..:"
2: eth32: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 90:e2:ba:af:33:80 brd ff:ff:ff:ff:ff:ff
3: eth31: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 90:e2:ba:af:33:81 brd ff:ff:ff:ff:ff:ff
4: eth01: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen
1000
    link/ether 00:10:e0:95:de:22 brd ff:ff:ff:ff:ff:ff
5: eth02: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:10:e0:95:de:23 brd ff:ff:ff:ff:ff:ff
6: eth03: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:10:e0:95:de:24 brd ff:ff:ff:ff:ff:ff
7: eth04: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:10:e0:95:de:25 brd ff:ff:ff:ff:ff:ff
```

ii) For each eth (ethxx) device determine the firmware version and the PCI bus position. Use the following command. Substitute the numbers give from the ip link command above for the ethxx. Record the firmware-version and the bus-info field.

`[admusr@hostname9aa81f1611e6 ~]$ ethtool -i eth01`
example:

```
[admusr@hostname9aa81f1611e6 ~]$ ethtool -i eth01
driver: ixgbe
version: 4.0.1-k
firmware-version: 0x800005dd
bus-info: 0000:3a:00.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: no
```

iii) Identify the NIC type

The bus-info field contains the PCI bus position of a NIC in the form domain:bus:slot.function.Each NIC can be identified by the address domain:bus:slot. The function portion of the bus-info field identifies individual ports on the same card. For the below command it is only necessary to use the first port for each card, for example, 0000:3a:00.0, since each port on the same card will return the same firmware version.

```
[admusr@hostname9aa81f1611e6 ~]$ lspci -vmmns 0000:3a:00.0
Slot:  3a:00.0
Class: 0200
Vendor:       8086
Device:       1528
SVendor:      108e
SDevice:      4852
Rev:   01
```

The needed information is underlined and italicized. The "Slot" number seen above corresponds to a "Bus Number" for each NIC as recorded in the worksheet in the previous step.

From the output above you need to record the following information in the given order for each NIC.

Vendor-Device-SVendor-SDevice

iv) Determine the NIC model from the Device ID

Use *Appendix D – NIC Device ID and Model Tables* to determine the NIC “Model” by matching the Device ID recorded in the last step with the corresponding Device ID and NIC Model in the table.

Record the Model value in the *Appendix A - Data Collection Worksheet for Oracle RMS*.

3. Execute the following command to determine the firmware for the disk drives.

```
$sudo raidconfig list disk --verbose | egrep 'Disk|Model|Version'
Disk c0d0
 Model: H101212SESUN1.2T
 F/W Version: A720
 Disk c0d1
 Model: H101212SESUN1.2T
 F/W Version: A720
 Disk c0d2
 Model: H101212SESUN1.2T
 F/W Version: A720
 Disk c0d3
 Model: H101212SESUN1.2T
 F/W Version: A720
 Disk c0d4
 Model: HSCAC2DA4SUN400G
 F/W Version: A122
 Disk c0d5
 Model: HSCAC2DA4SUN400G
 F/W Version: A122
 Disk c0d6
 Model: HSCAC2DA4SUN400G
 F/W Version: A122
 Disk c0d7
 Model: HSCAC2DA4SUN400G
 F/W Version: A122
```

For echo Disk record the Disk ID (ex. c0d0), the Model and the Firmware Version in the *Appendix A - Data Collection Worksheet for Oracle RMS*.

Compare the recorded firmware versions for each component to the *Server Firmware Components* section in the *Release Notes*. Sample output is provided below. Please note that this output may be different for any given server. If the ILOM and/or BIOS versions are the only components that need to be upgraded then the ILOM/BIOS only procedure can be used. Otherwise, the Oracle System Assistant Upgrade procedure should by followed for X5-2 or Netra X5-2. For Oracle X6-2 and X7-2 servers that require additional components to be upgraded use the Live Update Media procedure. Record the upgrade method in the *Appendix A - Data Collection Worksheet for Oracle RMS*.

3.5 Acquiring Firmware

Refer to the *Release Notes* for procedures on how to download the firmware for Oracle rack mount servers. The file obtained and the procedure to be used are dependent on the findings from the *Determining Firmware Upgrade Procedure for Rack Mount Servers* section. In order to obtain firmware for third party switches, contact Oracle Support.

If the determined procedure is the Oracle System Assistant based upgrade, then the Oracle System Assistant Updater must be used. Refer to section 2.3.1 of the *Release Notes*.

If the determined procedure is the ILOM/BIOS only upgrade, then the Firmware Pack can be used. Refer to section 2.3.3 of the *Release Notes*.

If the Live ISO Media Upgrade procedure for the X6-2 or X7-2 is to be used, refer to section 2.3.4 in the Release Notes

3.6 Preparing Firmware Upgrade Media

3.6.1 Oracle System Assistant Upgrade

Use whatever means are available to place the software patch zip file on the local workstation that is being used to perform the upgrades. Use the following procedure to extract the Oracle System Assistant Updater from the zip file. Refer to the *Release Notes* to determine which Software Release is required for the model of server being upgraded, as well as procedures on how to obtain the patch from My Oracle Support.

1. **Local WorkStation**

   Locate the software patch zip file on the local workstation. Right-click on the zip file and move the cursor over the **Open With** menu option. If this option shows WinZip or 7-zip File Manager, select one of those options. If neither shows up, select '**Choose Program...**'. In the window that opens there will be an **Other Programs** list. If WinZip or 7-Zip File Manager is there, then select one of them. If they are not there then click the ***Browse*** button and locate the 7zFM.exe or WinZip.exe file.

2. **Extract the Oracle System Assistant Updater**

   On the local workstation open the folder you are going to copy the OSA updater to. In the extraction utility window find the Oracle System Assistant Updater ISO file. Drag and drop the file or use any other means that are provided by the extraction utility to extract the file to the open folder.

3. **Make note of where the file is**

   Record the location of where the extracted file is on the local workstation. In subsequent parts of this document this location will be referred to as: **<local_OSAU_image_path**>.

3.6.2 ILOM/BIOS Only Upgrade

Refer to the *Release Notes* to determine which file to download and for procedures on how to do so. Note that the ILOM/BIOS only upgrade procedure uses the Firmware Only Upgrade Patch. Note the patch number provided for the type of server being upgraded in the appropriate table for these procedures.

Use whatever means are available to place the software patch zip file on the local workstation that is being used to perform the upgrades.

1. **Local Workstation**

   Locate the software patch zip file on the local workstation. Right-click on the zip file and move the cursor over the **Open With** menu option. If this option shows WinZip or 7-zip File Manager, select one of those options. If neither shows up, select '**Choose Program...**'. In the window that opens there will be an **Other Programs** list. If WinZip or 7-Zip File Manager are there select one of them. If they are not there then click the ***Browse*** button and locate the 7zFM.exe or WinZip.exe file.

2. **Extract the ILOM/BIOS package file**.

   Navigate to the service_processor folder in the firmware directory. Extract the .pkg file located there.

4 Firmware Upgrade Procedures

• *Firmware Upgrade Execution* • *Cisco 4948E-F* • *Cisco 9372TX-E* • *Oracle Rack Mount Servers*	This section provides procedures for upgrading the firmware on approved hardware

4.1 Firmware Upgrade Execution

These procedures are meant to be executed inside a maintenance window. It is assumed that each server to be upgraded has already been properly installed and configured. For new installations please refer to the application specific documentation. It is also assumed that the appropriate upgrade media has been delivered to the local workstation that will be used to perform the upgrades.

4.2 Cisco 4948E-F

CBBU Platform only supports one version of the Cisco 4948 E-F IOS firmware. If the IOS firmware is older or newer, then the upgrade procedure should be used. This procedure will be referred to as an upgrade even if the firmware itself is being downgraded.

4.2.1 Determine Current Cisco 4948E-F IOS Firmware Versions

The following procedure is used to identify the current PROM and IOS firmware versions installed on Cisco 4948E-F switches. If any of the firmware is at a lower level than that provided with the target Firmware Upgrade Pack, additional procedures are provided to perform the upgrades.

Important: If any unexpected errors are seen contact My Oracle Support (MOS).

1. **Access the Management Server :**

   Access the command prompt of the PM&C at **<virt_pmac_server_IP>**.

   The system connected to will be referred to as the "**Management Server:**" at the beginning of many of the steps below.

2. **Login as the "admusr" user.**

```
login as: admusr
password: <admusr_password>
```

3. **Management Server:**

   List the devices.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
Devices:

Device: switch1A
    Vendor:   Cisco
    Model:    4948E-F
    Access:   Network: 10.240.8.2
    Access:   OOB:
                  Service: console_service
                  Console: switch1A_console
    Init Protocol Configured
    Live Protocol Configured
```

   Record the device names of the 4948E-F switches as <switch1A_device_name> and <switch1B_device_name> in *Appendix B - Data Collection Worksheet for Cisco 4948E-F*.

4. **Management Server:**

Determine the current "IOS" revision.

The use of **switch1A** in the command below is an example and should be replaced by the correct device name of the switch as noted in step 3.

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

Firmware Version: (cat4500e-ENTSERVICESK9-M), Version 12.2(54)WO
```

Record the IOS version as the <current_IOS_version> in *Appendix B - Data Collection Worksheet for Cisco 4948E-F*. In the example above, the version would be 12.2(54)WO.

5. **Management Server:**.

   Repeat step 4 for the second switch.

   The device names **switch1A** or **switch1B** are examples and the actual device name should have been noted on step 3. If necessary, repeat step 3 to recheck the device name of the second switch.

6. **Determine if an IOS upgrade is required.**

   For each switch, compare the current IOS version recorded in steps 4 and 5 to the supported FW version listed in the Release Notes. If a switch requires upgrading mark the "Needs Upgrade?" check box in *Appendix B - Data Collection Worksheet for Cisco 4948E-F*.

4.2.2 Upgrade 4948E-F IOS Firmware

Prerequisites and Materials Needed:

- Complete the Determine Current Cisco 4948E-F IOS Firmware Version procedure.
- Switch Firmware IOS File. In order to obtain third-party switch firmware contact Oracle Support

Use this procedure to upgrade 4948E-F switches IOS firmware, if necessary. Refer to the Release Notes document for known issues and workarounds.

1. **Workstation:**

   Use any available means to transfer the switch firmware to the PM&C. Place the file in the directory /home/admusr.

2. **Login to the Management Server:**

   Access the command prompt of the PM&C at **<virt_pmac_server_IP>**.

   The system connected to will be referred to as the "**Management Server:**" at the beginning of many of the steps below.

3. **Login as the "admusr" user:**

   ```
   login as: admusr
   password: <admusr_password
   ```

4. **Management Server:**

Get the name of the tftp service.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listServices | grep -C2 tftp

Service Name:    tftp_service
            Type:    tftp
            Host:    10.240.4.5
            Options:
```

The tftp service name will be used in the next step. In this example the service name is tftp_service

5. **Management Server:**

   Locate the directory for tftp use.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=<tftp_service_name>
    Service Name:    tftp_service
            Type:    tftp
            Host:    10.240.8.4
            Options:
               dir: /var/TKLC/smac/image/
```

   Record the directory as <tftp_directory> in the *Data Collection Worksheet for Cisco 4948E-F*. In the example above the tftp directory is /var/TKLC/smac/image.

6. **Management Server:**

   Copy the switch firmware to the tftp service directory.

```
$ sudo /bin/cp /home/admusr/<IOS_image_file> <tftp_directory>/
```

7. **Management Server:**

   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. **Management Server:**

   Install the new IOS firmware.

   Note: If upgrading Switch1B, replace **<switch1A_device_name>** with **<switch1B_device_name>** for the following command.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch1A_device_name>
upgradeFirmware service=<tftp_service_name> filename=<IOS_image_file> --debug

>>> DEVICE COMMAND:
copy tftp://10.240.123.131/cat4500e-entservicesk9-mz.122-54.WO.bin
bootflash:cat4500e-entservicesk9-mz.122-54.WO.bin
<<< DEVICE RESPONSE:
copy tftp://10.240.123.131/cat4500e-entservicesk9-mz.122-54.WO.bin
bootflash:cat4500e-entservicesk9-mz.122-54.WO.bin
Destination filename [cat4500e-entservicesk9-mz.122-54.WO.bin]
```

```
=======OUTPUT REMOVED TO CONSERVE SPACE========

System configuration has been modified. Save? [yes/no]: YES
Building configuration...
Compressed configuration from 5268 bytes to 2174 bytes[OK]
Proceed with reload? [confirm]Connection to 10.240.123.129 closed by remote
host.
Connection to 10.240.123.129 closed.

>>> DEVICE RESPONSE.
Upgrade complete. Monitoring reload status...
```

Note: Once you see "**`Upgrade complete. Monitoring reload status`**…" the switch is being rebooted. This will take about 6 minutes. Then you will see the following output.

```
Show version | include Cisco IOS Software
Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-
M), Version 12.2(54)WO, RELEASE SOFTWARE (fc1)
switch1A#
>>> DEVICE RESPONSE.
```

9. **Management Server:**

   Check that the switch is now running the correct IOS version.

   Note: If upgrading Switch1B, replace **`<switch1A_device_name>`** with **`<switch1B_device_name>`** for the following command.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch1A_device_name> getVersion
Firmware Version: (cat4500e-ENTSERVICESK9-M), Version 12.2(54)WO
```

   Review the output and look for the IOS version. Verify that the version is the desired new version. If the switch does not boot properly or has the wrong IOS version, contact My Oracle Support (MOS).

10. **Management Server:**

    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

4.3 Cisco 9372TX-E

CBBU Platform only supports one version of the Cisco 9372TX-E NXOS firmware. If the NXOS firmware is older or newer, then the upgrade procedure should be used. This procedure will be referred to as an upgrade even if the firmware itself is being downgraded.

4.3.1 Determine Current Cisco 9372TX-E NXOS Firmware Versions

The following procedure is used to identify the current NXOS firmware versions installed on Cisco 9372TX-E switches. If any of the firmware is at a lower level than that provided with the target Firmware Upgrade Pack, additional procedures are provided to perform the upgrades.

Important: If any unexpected errors are seen contact My Oracle Support (MOS).

1. **Access the Management Server :**

   Access the command prompt of the Virtual PM&C at **<virt_pmac_server_IP>**.

   The system connected to will be referred to as the "**Management Server:**" at the beginning of many of the steps below.

2. **Login as the "admusr" user.**

   ```
   login as: admusr
   password: <admusr_password>
   ```

3. **Management Server:**

   List the devices.

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
   Devices:

   Device: P6-Switch1
       Vendor:   Cisco
       Model:    9372TX-E
       Access:   Network: 10.196.6.2
       Access:   OOB:
                     Service: oobm_F1-A
                     Console:
       Init Protocol Configured
       Live Protocol Configured

   Device: P6-Switch2
       Vendor:   Cisco
       Model:    9372TX-E
       Access:   Network: 10.196.6.2
       Access:   OOB:
                     Service: oobm_F1-B
                     Console:
       Init Protocol Configured
       Live Protocol Configured
   ```

   Record the device names of the 9372TX-E switches, such as **P6-Switch1** and **P6-Switch2** in this example, as **<switchA_device_name> and <switchB_device_name>** in *Appendix C - Data Collection Worksheet for Cisco 9372TX-E*.

   Note: The order in which the switches are displayed may differ and the system may report different switch names.

4. **Management Server:**

   Determine the current "NXOS" revision.

   The use of **P6-Switch1** in the command below is an example and should be replaced by the correct device name of the switch as noted in step 3.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=P6-Switch1 getFirmware

Version: 7.0.3.I3.1

Flash: nxos.7.0.3.I3.1.bin
```

   Note the NXOS version. For instance '**7.0.3.I3.1**' is the version in the example above. Record this version information in *Appendix C - Data Collection Worksheet for Cisco 9372TX-E* under **Current NXOS Version** for the appropriate switch. This information will be evaluated later.

5. **Management Server:**

   Use the switch's OOB Service name from step 3 command output to determine the ssh service name for the switch.

   For this example switch **P6-Switch1** from step 3 shows that its OOB Service name is oobm_F1-A. Use the following command to match that OOB Service name with the correct SSH Service name.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listServices
Services:

    Service Name:    ssh_service
            Type:    ssh
            Host:    192.168.1.1
            Options:
               password: 390F1FAE4A420C1F2ABB05C372E30FA9
               user: admusr

    Service Name:    oobm_F1-A
            Type:    oobm
            Host:    192.168.1.2
            Options:
               dir: /home/admusr
               password: 418BABB26885193883AAE71298AFD714
               user: plat
               vlan: 1
```

   Use the the first three octets from the oobm service to find the correct SSH service name. Here we can see that the switch's oobm service (oobm_F1-A) has an IP address starting with "192.168.1" which matches the SSH service name "ssh_service". So this switch's SSH Service name would be recorded as **<switchA_ssh_service_name>** with the value **ssh_service** in *Appendix C - Data Collection Worksheet for Cisco 9372TX-E*.

6. **Management Server:**

   Repeat for the second 9372TX-E switch.

   Repeat steps 4 and 5 replacing **<switchA_device_name>** with **<switchB_device_name>** in the command.

7. **Determine if a NXOS upgrade is required:**

   For each switch, compare the current IOS version recorded in steps 4 and 5 to the supported FW version listed in the Release Notes. If a switch requires upgrading, in *Appendix C - Data*

Collection Worksheet for Cisco 9372TX-E circle YES on the "Needs Upgrade?" line for each switch that needs upgrading.

4.3.2 Upgrade 9372TX-E NXOS Firmware

Prerequisites and Materials Needed:

- Complete the Determine Current Cisco 9372TX-E NXOS Firmware Version procedure.
- Switch Firmware NXOS File. In order to obtain third-party switch firmware contact Oracle Support

Use this procedure to upgrade 9372TX-E switches NXOS firmware, if necessary. Refer to the Release Notes document for known issues and workarounds.

1. **Workstation:**

   Use any available means to transfer the switch firmware to the PM&C. Place the file in the directory /var/TKLC/upgrade/.

2. **Access the Management Server:**

   Access the command prompt of the Virtual PM&C at **<virt_pmac_server_IP>**.

   The system connected to will be referred to as the "**Management Server:**" at the beginning of many of the steps below.

3. **Login as the "admusr" user:**

   ```
   login as: admusr
   password: <admusr_password>
   ```

4. **Management Server:**

   Change to the admusr home directory and create a symbolic link to the firmware file:

   ```
   $ cd /home/admusr

   $ ln -s /var/TKLC/upgrade/<switch_firmware_file>
   ```

5. **Management Server:**

   Note: If upgrading switchB replace **<switchA_device_name>** with **<switchB_device_name>**.

   Upgrade the switch's firmware:

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switchA_device_name>
   upgradeFirmware service=ssh_service filename=<switch_firmware_file> --debug
   ```

   Output similar to the following should be seen.

   ```
   =======OUTPUT REMOVED TO CONSERVE SPACE========
   >>> DEVICE COMMAND:
   copy scp://admusr@192.168.1.1/home/admusr/nxos.7.0.3.I4.2.bin
   bootflash:nxos.7.0.3.I4.2.bin
   <<< DEVICE RESPONSE:
    copy scp://admusr@192.168.1.1/home/admusr/nxos.7.0.3.I4.2.bin
   bootflash:nxos.7.0.3.I3.1.bin
   Enter vrf (If no input, current vrf 'default' is considered): management
   admusr@192.168.1.1's password:
   nxos.7.0.3.I4.2.bin
   ```

```
nxos.7.0.3.I4.2.bin

nxos.7.0.3.I4.2.bin

=======OUTPUT REMOVED TO CONSERVE SPACE========
nxos.7.0.3.I4.2.bin

                 100%  665MB  16.6MB/s   00:40
Copy complete, now saving to disk (please wait)...
P6-Switch1(config)#
>>> DEVICE RESPONSE.
>>> DEVICE COMMAND:
boot nxos bootflash:nxos.7.0.3.I4.2.bin
<<< DEVICE RESPONSE:
 boot nxos bootflash:nxos.7.0.3.I4.2.bin
Performing image verification and compatibility check, please wait....
P6-Switch1(config)#
>>> DEVICE RESPONSE.
>>> DEVICE COMMAND:
exit
<<< DEVICE RESPONSE:
 exit
P6-Switch1
>>> DEVICE RESPONSE.
>>> DEVICE COMMAND:
copy running-config startup-config
<<< DEVICE RESPONSE:
# copy running-config startup-config
[########################################] 100%
Copy complete.
P6-Switch1
>>> DEVICE RESPONSE.
>>> DEVICE COMMAND:
reload
<<< DEVICE RESPONSE:
# reload
This command will reboot the system. (y/n)?  [n] y

>>> DEVICE RESPONSE.
Upgrade complete. Monitoring reload status...
```

Several minutes will pass at this point.

```
=======OUTPUT REMOVED TO CONSERVE SPACE========
P6-Switch1#
>>> DEVICE RESPONSE.
>>> DEVICE COMMAND:
exit
<<< DEVICE RESPONSE:
 exit
Connection to 10.196.6.2 closed
```

6. **Management Server:**

   Note: If upgrading switchB replace **<switchA_device_name>** with **<switchB_device_name>**.

   Reboot the switch to ensure the System firmware matches the NXOS firmware. This command has no output and will take about a minute to complete.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=<switchA_device_name> reboot
```

7. **Management Server:**

   Note: If upgrading switchB replace **<switchA_device_name>** with **<switchB_device_name>**.

   Verifiy the switch is using the expected firmware file. After the reboot from the last step the switch will take serveral minutes to become available again. Wait a few minutes and retry the command below until it succeeds.

   ```
   $ sudo /usr/TKLC/plat/bin/netConfig --device=<switchA_device_name>
   getFirmware

   Version: 7.0.3.I4.2

   Flash: nxos.7.0.3.I4.2.bin
   ```

   Check that the **<switch_firmware_file>** that was applied matches current running "Flash" file indicated above in bold.

8. **Management Server:**

   Repeat steps 8 and 9 for any other switches that need to be upgraded. Once all applicable switches have been upgraded cleanup the management server disk.

   ```
   $ rm /home/admusr/<switch_firmware_file>

   $ rm /var/TKLC/upgrade/<switch_firmware_file>
   ```

4.4 Oracle Rack Mount Servers

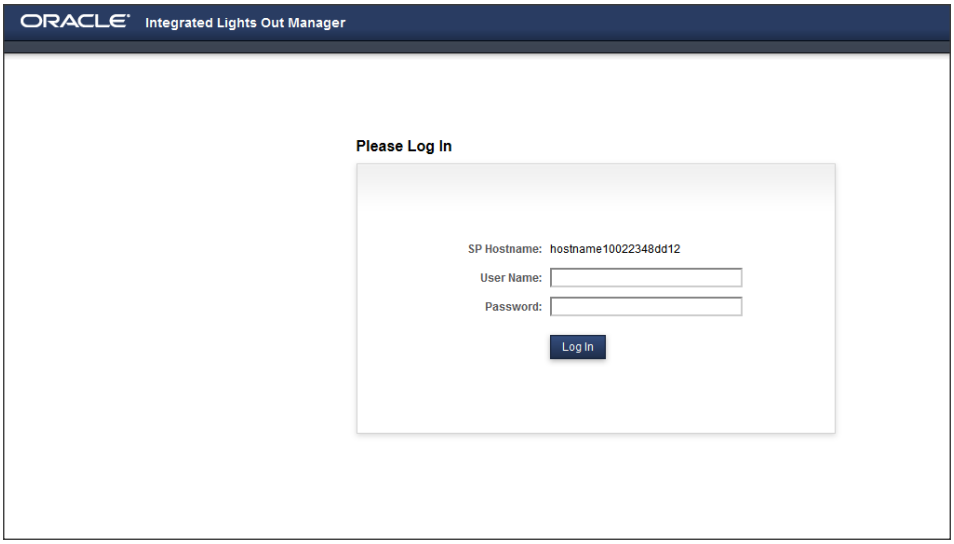
4.4.1 Oracle System Assistant Upgrade for Rack Mount Servers

1. **Local Workstation**

   Using one of the supported browsers listed in the *Required Materials* section, navigate to the ILOM Web GUI by typing its address into the browser's address bar: **(https://<ILOM_IP>)**.

2. **ILOM Web GUI:**

   Login to the ILOM as an "administrator" user.

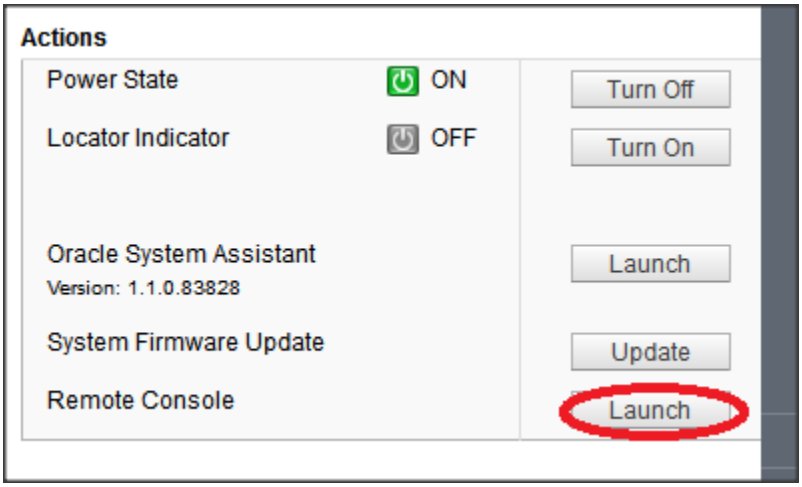


User name = **<ILOM_admin_user>**

Password **=<ILOM_admin_password>**

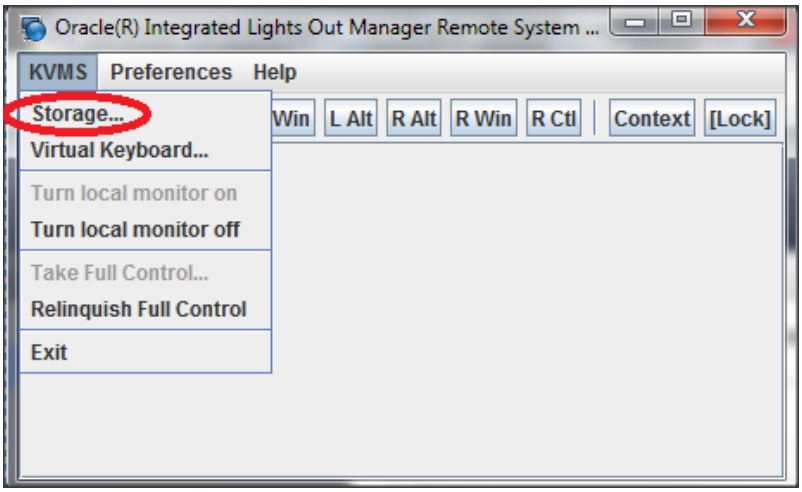
3. **ILOM Web GUI:**

   On the System Summary page click on the Remote Console **Launch** button in the Actions Pane.



4. **ILOM Remote Console:**

   In the KVMS menu, select the *Storage*….option.

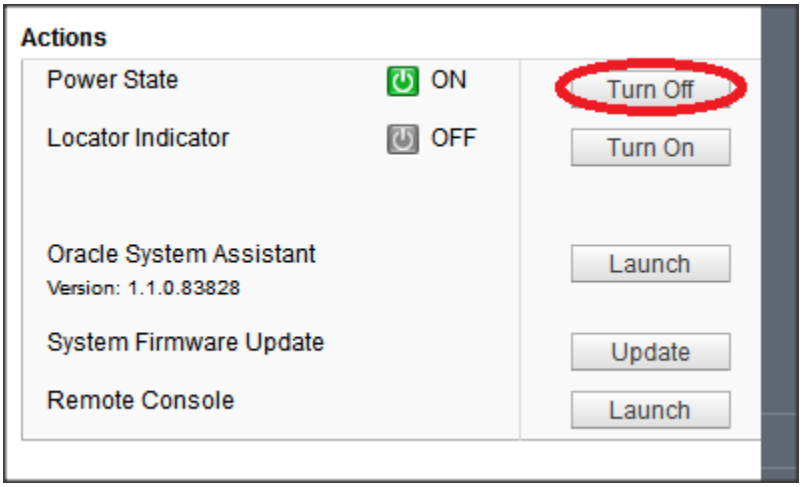


5. A window entitled Storage Devices will open up. Click the **Add..** button and navigate to the location of the ISO on the local workstation. Select the ISO and then click the **Select** button

6. The ISO file will now be included in the list of available storage devices. Select it in the Storage Devices window and then click the **Connect** button.

7. **ILOM Web GUI:**

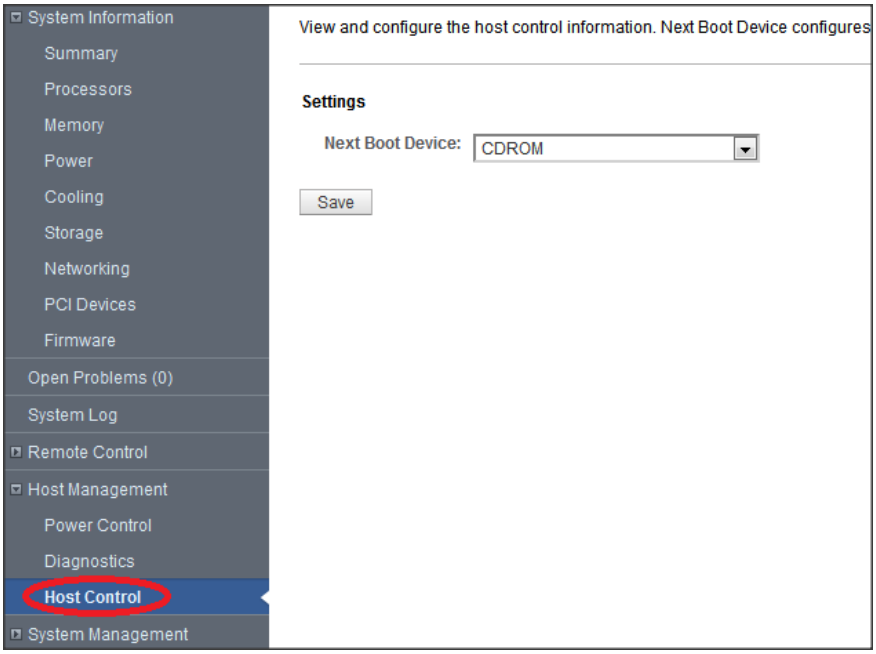
   On the System Summary page click on the Power State **Turn Off** button in the Actions Pane. Click **OK** at the confirmation prompt. This will perform a graceful shutdown of the operating system prior to powering off the host server. Wait for the indicator to signify that the server is powered down before proceeding to the next step.



****Note: If at any point the internet connection on the local workstation is lost or the browser being used is closed and the OSA has not yet been updated, the Oracle System Assistant Updater ISO must be remounted using the previous steps.**

8. **ILOM Web GUI**

   Under the Host Management tab select the Host Control option. From the drop-down menu for Next Boot Device, select the CDROM option and then click the **Save** button.



9. **ILOM Web GUI:**

On the System Summary page click on the Power State **Turn On** button in the Actions Pane to boot into the Oracle System Assistant Updater ISO. Click OK at the confirmation prompt.

10. **ILOM Remote Console:**

    Go back to the window that contains the Remote Console. If the window was closed, re-launch the console in the Actions Pane. Wait for the Oracle System Assistant Updater ISO to boot up and reply **'yes'** to the prompt.

    ```
    Would you like to proceed? [yes or no] yes
    ```

11. **ILOM Remote Console:**

    Wait for the Oracle System Assistant to finish updating. Reply 'yes' to the verification prompt.

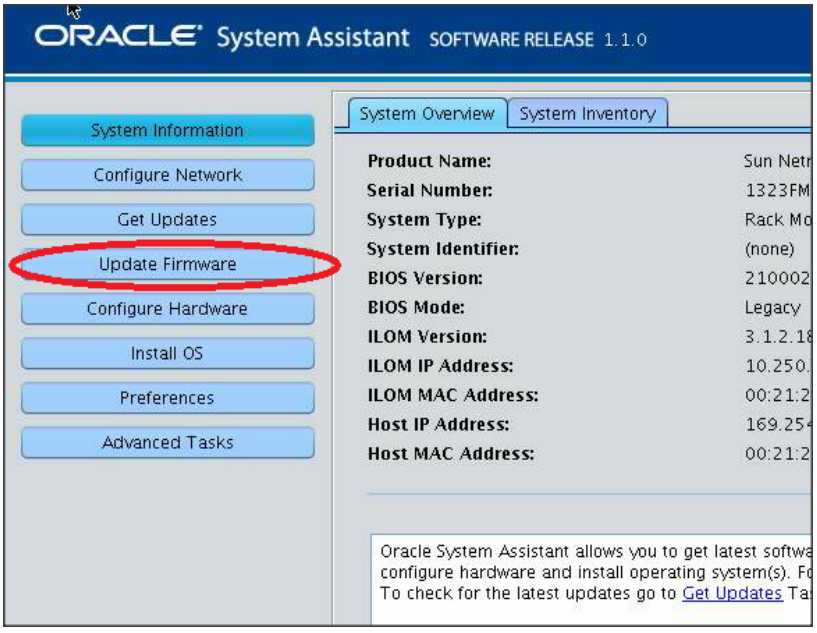
    ```
    Would you like to verify the device? [yes or no] yes
    ```

12. **ILOM Remote Console:**

    When verification is complete, the system will reboot and launch the Oracle System Assistant. After the Oracle System Assistant has launched, press the **Accept** button in the License Agreement Window and then close the Oracle System Assistant Help widow.

13. **OSA GUI:**

    Click the **Update Firmware** button on the left-hand side of the OSA GUI and then click **Check for Firmware Updates**.



14. **OSA GUI:**

    After the OSA has finished determining what needs to be updated, click the **Install All Updates** button to proceed with the upgrade.

15. Depending on whether the ILOM is being upgraded, a prompt may be displayed to enter credentials for activation of the internal LAN over USB interconnect between the host server and the ILOM service processor. Supplying a valid ILOM user account with Administrator privileges will result in the interconnect being activated for faster upgrade of the ILOM. If there is no prompt ignore this step and move on to the next step. Also, depending on the version of the OSA, the supplied credentials may not be accepted. Refer to the *Known Issues* section of the *Release Notes* to determine if the version you are using is an affected release. If so, click Cancel to continue with the upgrade.

****Note: If the server requires a reboot as part of the upgrade process it will reboot automatically.**

****Note: If ILOM is being upgraded there will be a temporary loss of connection with it while it resets. Wait a few minutes and then log back into the ILOM Web GUI and re-launch the Remote Console.**

16. **OSA GUI:**

Wait for the firmware upgrade process to complete. One or more reboots may be part of this process and, as noted, will take place automatically. When the upgrade is complete the following output will be shown in the OSA GUI.

17. **OSA GUI:**

    Click on the **OK** button. The OSA will then run another Firmware Update Check. Review the output to ensure that the installed versions are correct as per the *Release Notes* and then click on the **Cancel** button.

18. **OSA GUI:**

    Click on the **Exit** button in the bottom right corner of the OSA GUI and then press the **reboot** option to reboot the server.

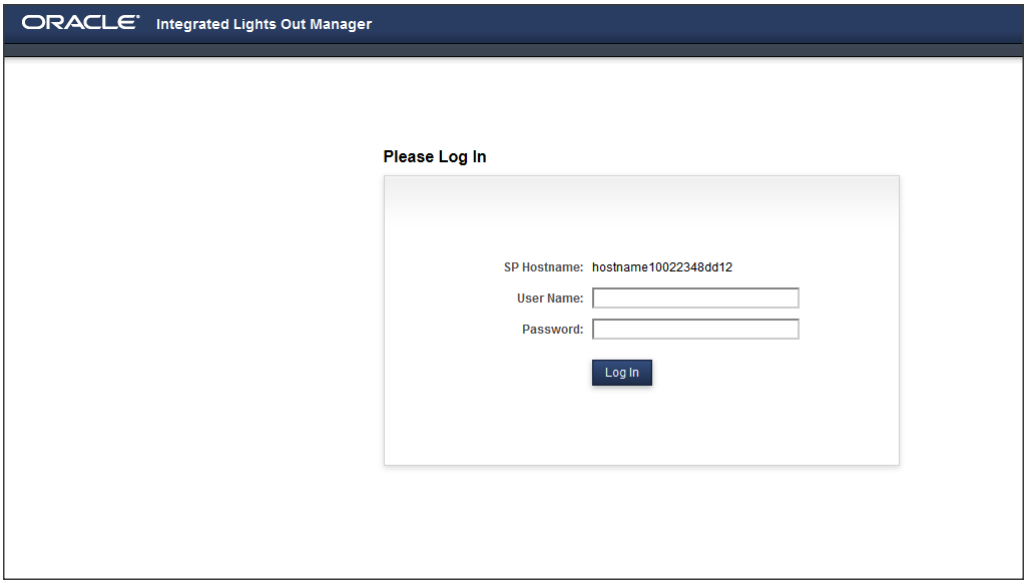
4.4.2 ILOM/BIOS Only Upgrade

1. **Local Workstation**

   Using one of the supported browsers listed in *2.1 Required Materials*, navigate to the ILOM Web GUI by typing its address into the browser's address bar: **(https://<ILOM_IP>)**.

2. **ILOM Web GUI:**

   Login to the ILOM as an "administrator" user.

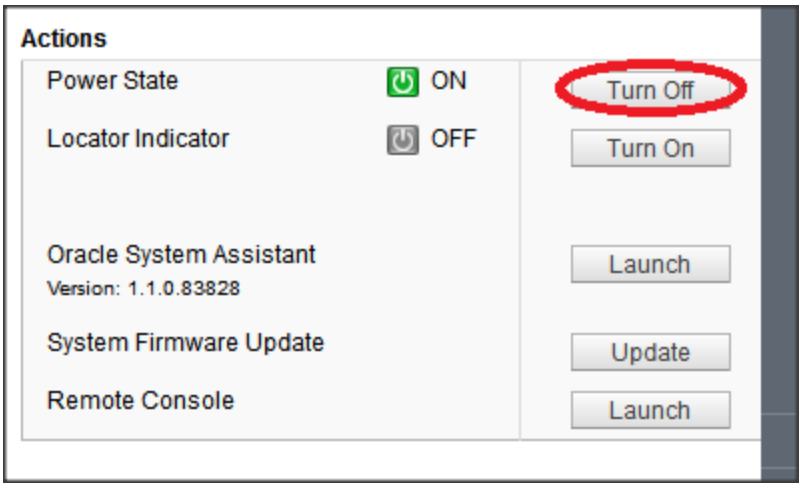


   User name = <ILOM_admin_user>

   Password =<ILOM_admin_password>

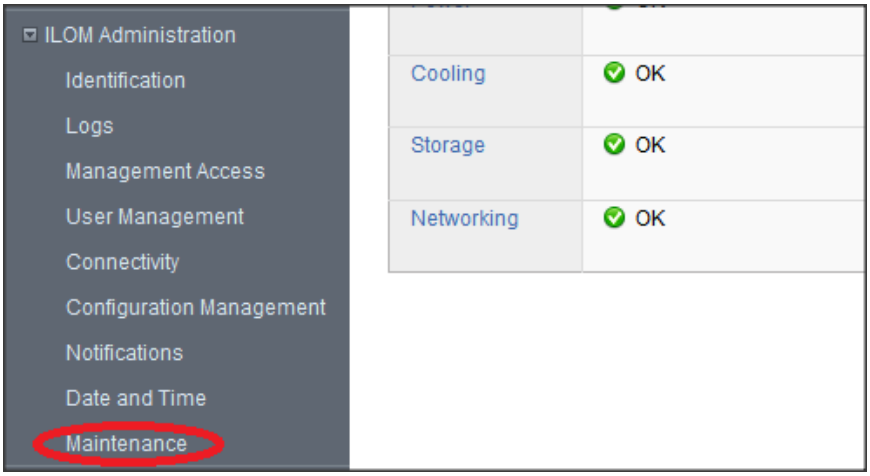
3. **ILOM Web GUI:**

   On the **System Summary** page click on the Power State **Turn Off** button in the **Actions Pane**. Click **OK** at the confirmation prompt. This will perform a graceful shutdown of the operating system prior to powering off the host server. Wait for the indicator to signify that the server is powered down before proceeding to the next step.



4. **ILOM Web GUI:**

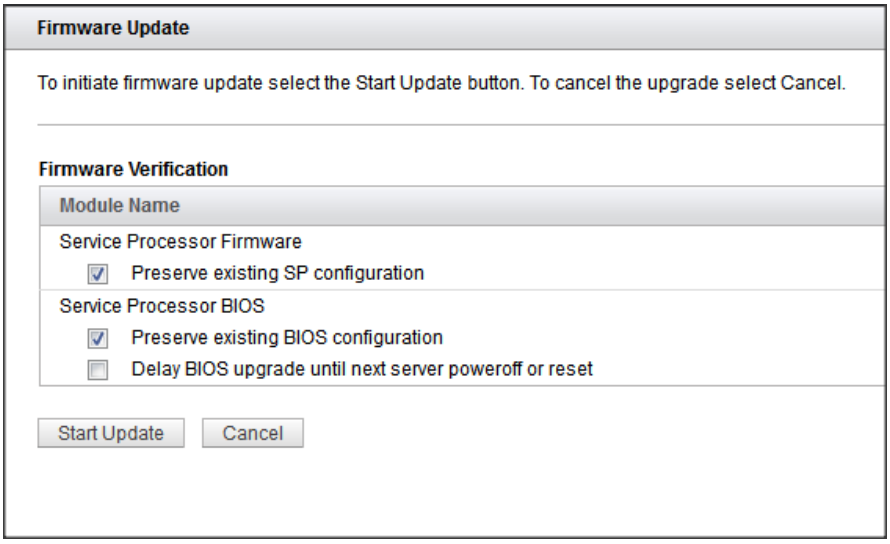
   From the ILOM Administration drop-down list, select the **Maintenance** link.



5. Click on the **Enter Update Mode** button.
6. Click on the **Browse …** button to locate the firmware package file on the local workstation and click **Open**.
7. Click on the **Upload** button. This step may take a few minutes while the file is being transferred.

8. In the Firmware Verification Table make sure that the following options are checked.

    - Preserve existing SP configuration
    - Preserver existing BIOS configuration



9. Click the **Start Upgrade** button. Once the upgrade is started, it is important that the process not be interrupted. After the ILOM has been upgraded, it will reset. This will cause the current connection to the ILOM to be lost.
10. Clear the browser's cache before attempting to reconnect to the ILOM.

4.4.3 X6-2 Live ISO Media Upgrade

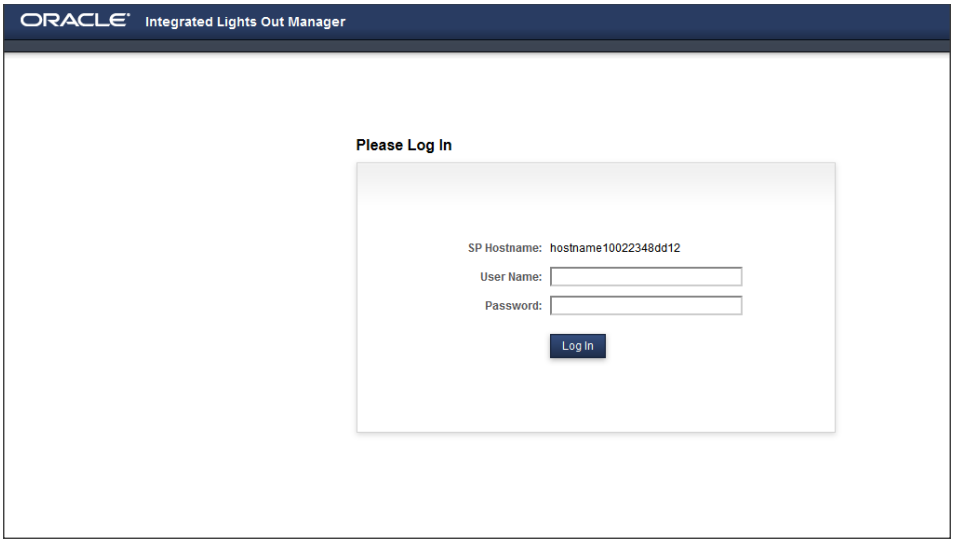
The following procedure is used to upgrade the firmware on X6-2 servers when there are multiple components requiring upgrade. For previous generations of servers the Oracle System Assitant (OSA) was used for this purpose. The OSA is no longer supported as of the X6-2 generation. This procedure uses a bootable ISO that can be used to upgrade all of the firmware components in an offline environment.

1. **Local Workstation**

   Using one of the supported browsers listed in the *Required Materials* section, navigate to the ILOM Web GUI by typing its address into the browser's address bar: **(https://<ILOM_IP>)**.

2. **ILOM Web GUI:**

   Login to the ILOM as an "administrator" user.

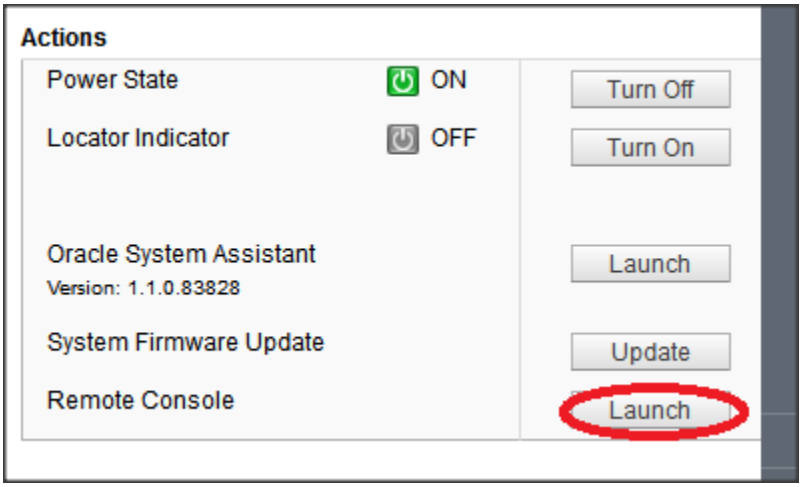


   User name = **<ILOM_admin_user>**

   Password **=<ILOM_admin_password>**

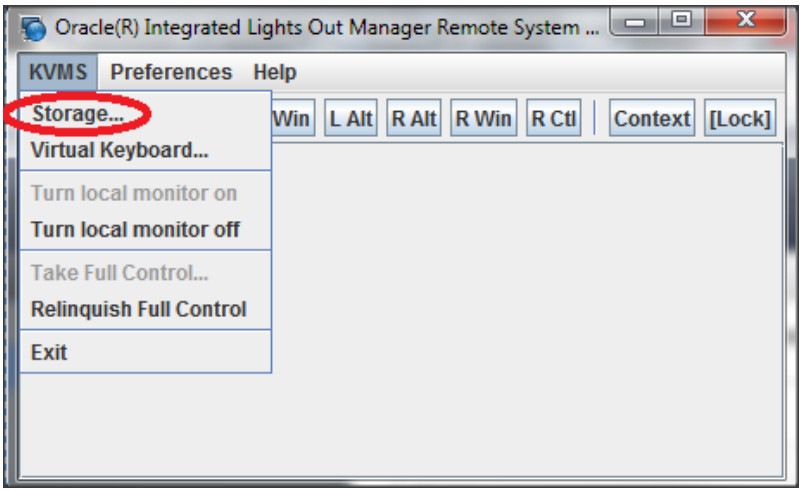
3. **ILOM Web GUI:**

   On the System Summary page click on the Remote Console **Launch** button in the Actions Pane.



4. **ILOM Remote Console:**

   In the KVMS menu, select the *Storage*….option.

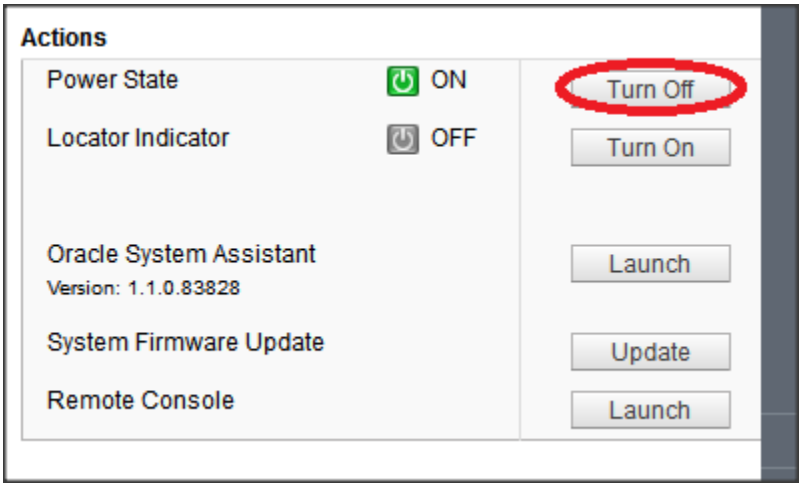


5. A window entitled Storage Devices will open up. Click the **Add..** button and navigate to the location of the Live Update Media ISO on the local workstation. Select the ISO and then click the **Select** button

6. The ISO file will now be included in the list of available storage devices. Select it in the Storage Devices window and then click the **Connect** button.

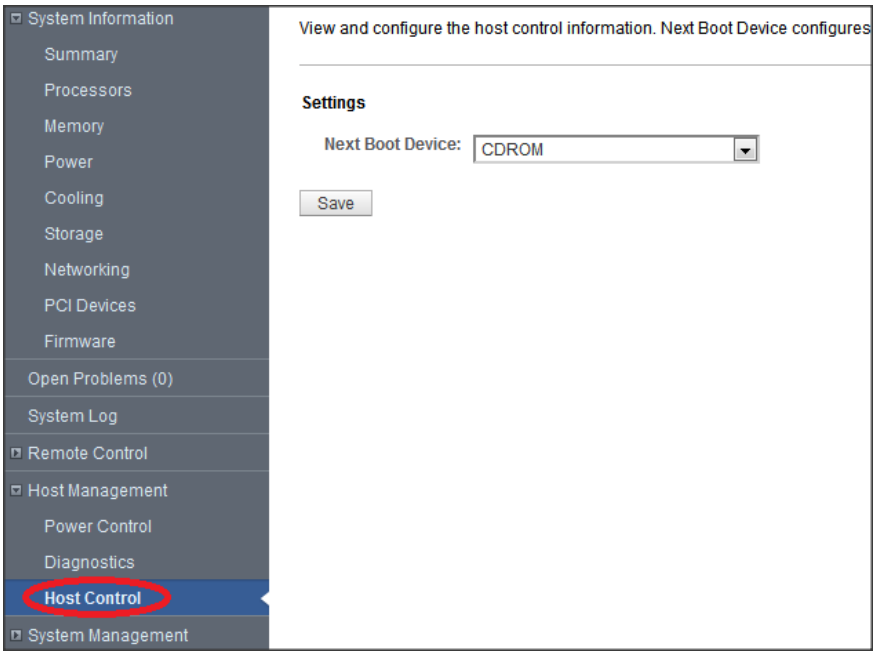
7. **ILOM Web GUI:**

   On the System Summary page click on the Power State **Turn Off** button in the Actions Pane. Click **OK** at the confirmation prompt. This will perform a graceful shutdown of the operating system prior to powering off the host server. Wait for the indicator to signify that the server is powered down before proceeding to the next step.



8. **ILOM Web GUI**

   Under the Host Management tab select the Host Control option. From the drop-down menu for Next Boot Device, select the CDROM option and then click the **Save** button.



9. **ILOM Web GUI:**

   On the System Summary page click on the Power State **Turn On** button in the Actions Pane to boot into the live update media ISO. Click OK at the confirmation prompt.

10. **ILOM Remote Console**

    After the ISO has booted log into the command line with root credentials <live_root_user_pass> when prompted.

4.4.3.1 Upgrade H101812SFSUN1.2T SAS HD

1. From the command line enter the following command. Answer 'y' when prompted.

```
[root@localhost ~]# fwupdate update disk -x /Oracle/Oracle_Server_X6-2-
1.1.1.85777-FIRMWARE_PACK/Firmware/H101812SFSUN1.2T/metadata.xml

The following components will be upgraded as shown:
=========================================================
ID        Priority Action     Status      Old Firmware Ver.   Proposed Ver.
New Firmware Ver.   System Reboot
-------------------------------------------------------------------------------
----------------------------------------
c0d0      1        Check FW   Success     A770                A990
N/A                 N/A
c0d1      1        Check FW   Success     A770                A990
N/A                 N/A
Do you wish to process all of the above component upgrades? [y/n]? y
Updating c0d0:  Success
Updating c0d1:  Success

Verifying all priority 1 updates

Execution Summary
=========================================================
ID        Priority Action     Status      Old Firmware Ver.   Proposed Ver.
New Firmware Ver.   System Reboot
-------------------------------------------------------------------------------
----------------------------------------
c0d0      1        Validate   Success     A770                A990
A990                N/A
c0d1      1        Validate   Success     A770                A990
A990                N/A
```

4.4.3.2 Upgrade Onboard Twinville 10-Gigabit Ethernet Adapters

1. From the command line enter the following command. Answer 'y' when prompted

```
[root@localhost ~]# fwupdate update controller -x /Oracle/Oracle_Server_X6-2-
1.1.1.85777-FIRMWARE_PACK/Firmware/X540-LOM/metadata.xml

The following components will be upgraded as shown:
=========================================================
ID        Priority Action     Status      Old Firmware Ver.   Proposed Ver.
New Firmware Ver.   System Reboot
-------------------------------------------------------------------------------
----------------------------------------
c2        1        Check FW   Success     8000047B            800005DD
N/A                 System Power Cycle
c3        1        Check FW   Success     8000047C            800005DE
N/A                 System Power Cycle
Do you wish to process all of the above component upgrades? [y/n]? y
```

2. If there are other firmware components requiring upgrade, answer ‘n’ when prompted to reboot. Otherwise answer ‘y’.

```
Updating c2:  Success
Sleeping for 30 seconds for component to recover
Updating c3:  Success
Sleeping for 30 seconds for component to recover

Verifying all priority 1 updates

Execution Summary
=========================================================
ID        Priority Action     Status      Old Firmware Ver.   Proposed Ver.
New Firmware Ver.   System Reboot
-------------------------------------------------------------------------------
----------------------------------------
c2        1        Post Power Pending     8000047B            800005DD
N/A                 System Power Cycle
c3        1        Post Power Pending     8000047C            800005DE
N/A                 System Power Cycle
System Reboot required for some applied firmware
Do you wish to automatically reboot now? [y/n]? n
Automatic system power action cancelled.
Terminating fwupdate.  Please reset system manually and then proceed.
```

4.4.3.3 Upgrade ILOM and System ROM

1. Determine the ILOM Interconnect IP address. This value is given as “SP Interconnect IP address” in the command output below. Replace any instances of <ILOM_Interconnect_IP> with this value.

```
[root@localhost ~]# ilomconfig list interconnect
Interconnect
============
State: enabled
Type: USB Ethernet
SP Interconnect IP Address: 169.254.182.76
Host Interconnect IP Address: 169.254.182.77
Interconnect Netmask: 255.255.255.0
SP Interconnect MAC Address: 02:21:28:57:47:16
Host Interconnect MAC Address: 02:21:28:57:47:17
```

2. Use the fwupdate command to upgrade the ILOM and the System ROM. Use an ILOM administrative account for the <ILOM_USER> below. Provide the password for this account when prompted.

   ***Note**: After the ILOM is finished updating, it will undergo a reset. This will cause the Remote Console to drop the current connection. Wait a few minutes and then log back into the ILOM and re-launch the Remote Console.

```
[root@localhost ~]# fwupdate update sp_bios -x /Oracle/Oracle_Server_X6-2-
1.1.1.85777-FIRMWARE_PACK/Firmware/service-processor/metadata.xml -U root -H
169.254.182.76
Enter password (8 to 16 characters):
********

The following components will be upgraded as shown:
=============================================================
ID        Priority Action     Status      Old Firmware Ver.   Proposed Ver.
New Firmware Ver.   System Reboot
-------------------------------------------------------------------------------
----------------------------------------
sp_bios   1        Check FW   Success     3.2.6.24            3.2.6.46
N/A                 System Power Cycle
REMOTE HOST WILL SHUT DOWN DURING SP FIRMWARE UPDATE!
Do you wish to process all of the above component upgrades? [y/n]? y
Updating sp_bios:  Success
Sleeping for 180 seconds for component to recover
```

3. Re-launch Remote Console and continue with upgrade. If there are other components to be upgraded, answer 'n' when prompted to reboot. Otherwise, answer 'yes'.

```
Execution Summary
=============================================================
ID        Priority Action     Status      Old Firmware Ver.   Proposed Ver.
New Firmware Ver.   System Reboot
-------------------------------------------------------------------------------
----------------------------------------
sp_bios   1        Post Power Pending     3.2.6.24            3.2.6.46
N/A                 System Power Cycle
System Reboot required for some applied firmware
Do you wish to automatically reboot now? [y/n]?
```

4.4.4 X7-2 Live ISO Media Upgrade

Note: For this initial release of X7-2 firmware the BIOS and iLOM are the only components with an upgrade procedure because all other components either do not have any newer versions released to test the upgrade process with or cannot currently be upgraded.

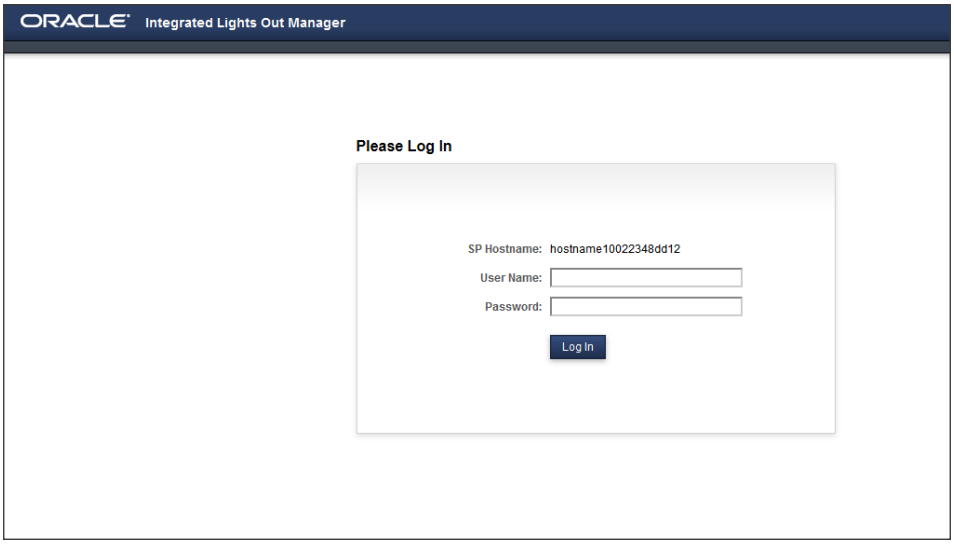
The following procedure is used to upgrade the firmware on X7-2 servers when there are multiple components requiring upgrade. This procedure uses a bootable ISO that can be used to upgrade all of the firmware components in an offline environment.

1. **Local Workstation**

   Using one of the supported browsers listed in the *Required Materials* section, navigate to the ILOM Web GUI by typing its address into the browser's address bar: **(https://<ILOM_IP>)**.

2. **ILOM Web GUI:**

   Login to the ILOM as an "administrator" user.

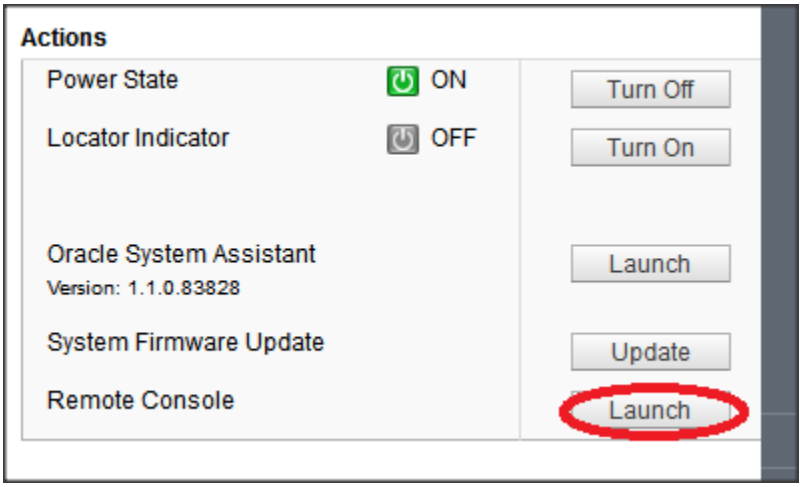


User name = **<ILOM_admin_user>**

Password **=<ILOM_admin_password>**

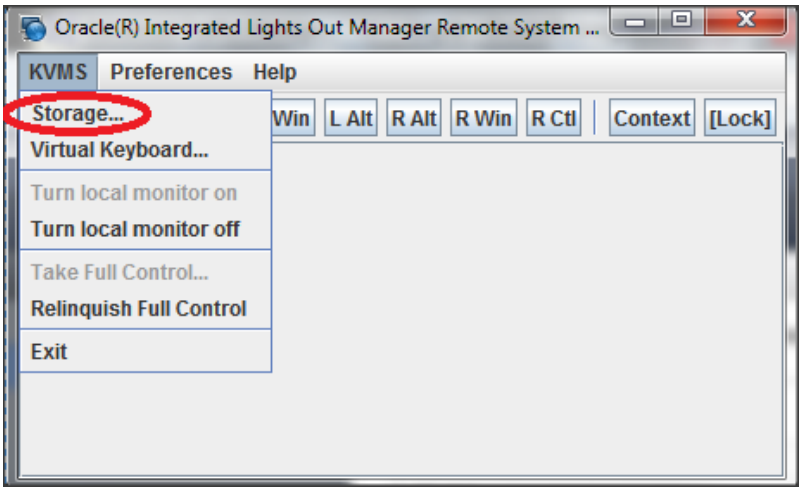
3. **ILOM Web GUI:**

   On the System Summary page click on the Remote Console **Launch** button in the Actions Pane.



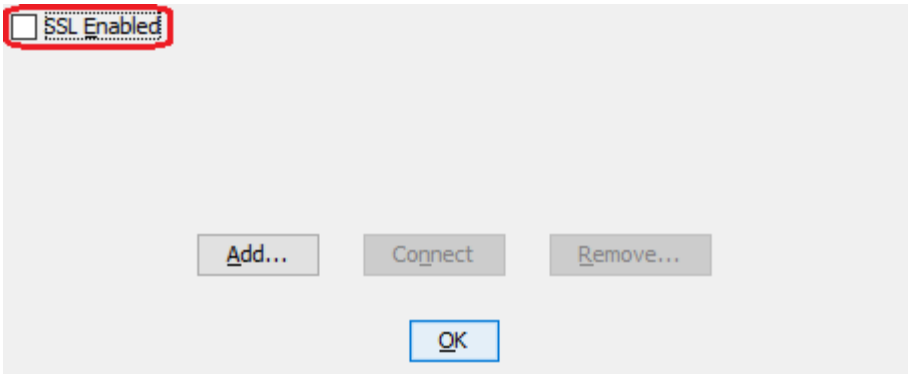
4. **ILOM Remote Console:**

   In the KVMS menu, select the *Storage*….option.



5. A window entitled Storage Devices will open up.

   Uncheck the box next to "Enable SSL":

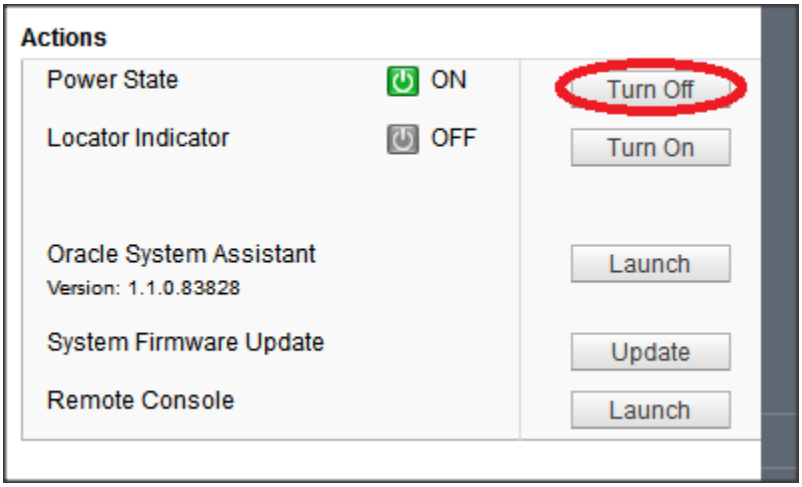


6. Click the **Add..** button and navigate to the location of the Live Update Media ISO on the local workstation. Select the ISO and then click the **Select** button

7. The ISO file will now be included in the list of available storage devices. Select it in the Storage Devices window and then click the **Connect** button.

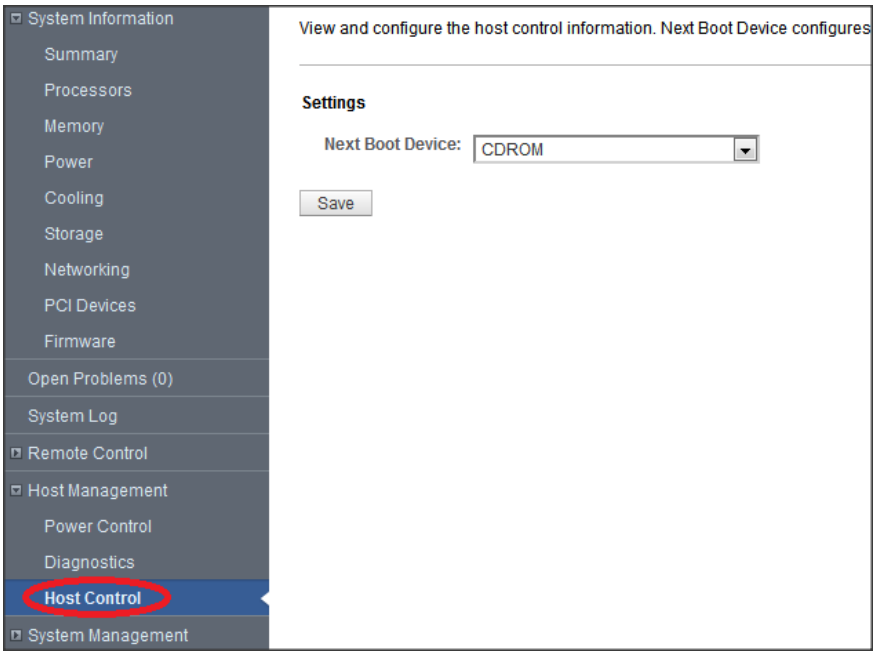
8. **ILOM Web GUI:**

   On the System Summary page click on the Power State **Turn Off** button in the Actions Pane. Click **OK** at the confirmation prompt. This will perform a graceful shutdown of the operating system prior to powering off the host server. Wait for the indicator to signify that the server is powered down before proceeding to the next step.



9. **ILOM Web GUI**

   Under the Host Management tab select the Host Control option. From the drop-down menu for Next Boot Device, select the CDROM option and then click the **Save** button.



10. **ILOM Web GUI:**

    On the System Summary page click on the Power State **Turn On** button in the Actions Pane to boot into the live update media ISO. Click OK at the confirmation prompt.

11. ILOM Remote Console

After the ISO has booted log into the command line with root credentials <live_root_user_pass> when prompted.

4.4.4.1 Upgrade ILOM and System ROM

1. Determine the ILOM Interconnect IP address. This value is given as “SP Interconnect IP address” in the command output below. Replace any instances of <ILOM_Interconnect_IP> with this value.

```
[root@localhost ~]# ilomconfig list interconnect
Interconnect
============
State: enabled
Type: USB Ethernet
SP Interconnect IP Address: 169.254.182.76
Host Interconnect IP Address: 169.254.182.77
Interconnect Netmask: 255.255.255.0
SP Interconnect MAC Address: 02:21:28:57:47:16
Host Interconnect MAC Address: 02:21:28:57:47:17
```

2. Use the fwupdate command to upgrade the ILOM and the System ROM. Use an ILOM administrative account for the <ILOM_USER> below. Provide the password for this account when prompted.

   Note: After the ILOM is finished updating, it will undergo a reset. This will cause the Remote Console to drop the current connection. Wait a few minutes and then log back into the ILOM and re-launch the Remote Console.

```
[root@localhost ~]# fwupdate update sp_bios -x /Oracle/ Oracle_Server_X7-2-
1.0.0.87485-FIRMWARE_PACK/Firmware/service-processor/metadata.xml -U root -H
169.254.182.76
Enter password (8 to 16 characters):
********

The following components will be upgraded as shown:
=============================================================
ID        Priority Action     Status      Old Firmware Ver.   Proposed Ver.
New Firmware Ver.   System Reboot
-------------------------------------------------------------------------------
----------------------------------------
sp_bios   1        Check FW   Success     x.x.x.x             4.0.0.22
N/A                 System Power Cycle
REMOTE HOST WILL SHUT DOWN DURING SP FIRMWARE UPDATE!
Do you wish to process all of the above component upgrades? [y/n]? y
Updating sp_bios:  Success
Sleeping for 180 seconds for component to recover
```

3. Re-launch Remote Console and continue with upgrade. If there are other components to be upgraded, answer ‘n’ when prompted to reboot. Otherwise, answer ‘yes’.

```
Execution Summary
=============================================================
ID        Priority Action     Status      Old Firmware Ver.   Proposed Ver.
New Firmware Ver.   System Reboot
-------------------------------------------------------------------------------
----------------------------------------
sp_bios   1        Post Power Pending     x.x.x.x             4.0.0.22
N/A                 System Power Cycle
System Reboot required for some applied firmware
Do you wish to automatically reboot now? [y/n]?
```

5 Appendices

Appendix A - Data Collection Worksheet for Oracle RMS

For convenience, this worksheet provides space to record information for up to 12 target servers. If more are to be upgraded, you should print another copy.

Oracle RMS Server Common Information

ILOM Administrator User

<ILOM_admin_user>_____

ILOM Administrator Password

<ILOM_admin_password>_____

Live ISO "root" user credentials for X6-2 and X7-2 Live ISO upgrades (Contact Customer Service)

<live_root_user_pass>_____

Oracle RMS Sever ILOM IP Addresses

Server 1

<ILOM_IP>_____

<Upgrade Procedure> _____

ILOM Firmware Version _____

BIOS Firmware Version _____

RAID Controller Firmware Version _____

Network Interface Card
- Device ID_____
- Model_____
- Interface Name <interface_name>_____
- Firmware Version_____

Network Interface Card
- Device ID_____
- Model_____
- Interface Name <interface_name>_____
- Firmware Version_____

Network Interface Card
- Device ID_____
- Model_____
- Interface Name <interface_name>_____

Firmware Version_____

Network Interface Card
Device ID_____
Model_____
Interface Name <interface_name>_____
Firmware Version_____

Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____

Server 2

<ILOM_IP>_____

<Upgrade Procedure> _____

Network Interface Card
Device ID_____
Model_____
Interface Name <interface_name>_____
Firmware Version_____

Network Interface Card
Device ID_____
Model_____
Interface Name <interface_name>_____
Firmware Version_____

Network Interface Card
Device ID_____
Model_____
Interface Name <interface_name>_____
Firmware Version_____

Network Interface Card
Device ID_____
Model_____
Interface Name <interface_name>_____
Firmware Version_____

Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____
Disk Drive
Disk ID _____
Model _____
Firmware Version _____

Disk Drive

Disk ID _____

Model _____

Firmware Version _____

Disk Drive

Disk ID _____

Model _____

Firmware Version _____

Appendix B - Data Collection Worksheet for Cisco 4948E-F

NetConfig Management Server

PM&C IP address (ssh)
<virt_pmac_server_IP>_____

Common Switch Information

Console Password
<switch_console_password>_____

Enable Password
<switch_enable_password>_____

TFTP Directory
<tftp_directory>_____

IOS File Name
<IOS_image_file> _____

General Information - Switch1A

Switch1A Device Name
<switch1A_device_name>_____

Current IOS Version
<current_IOS_version>_____

Target 4948E-F IOS Needs Upgrade (Circle One)?___YES___NO

General Information - Switch1B

Switch1B Device Name
<switch1B_device_name>_____

Current IOS Version
<current_IOS_version>_____

Target 4948E-F IOS Needs Upgrade (Circle One)?___YES___NO

Appendix C - Data Collection Worksheet for Cisco 9372TX-E

Common Switch Information

Console Password
<switch_console_password>_____

Enable Password
<switch_enable_password>_____

Target Firmware File Name
<switch_firmware_file>_____

Target 9372TX-E SwitchA

This is the "A" 9372TX-E switch in the redundant pair. This switch MUST have a direct oobm connection with the Management Server being used.

General Information - SwitchA

Current NXOS Version
<current_NXOS_version>_____

Target 9372TX-E NXOS Needs Upgrade (Circle One)?___YES___NO

NetConfig Information - SwitchA

SwitchA Device Name
<switchA_device_name>_____

SwitchA SSH Service Name
<switchA_ssh_service_name>_____

Target 9372TX-E SwitchB

This is the "1B" 9372TX-E switch in the redundant pair. This switch MUST have a direct oobm connection with the Management Server being used.

General Information - SwitchB

Current NXOS Version
<current_NXOS_version>_____

Target 9372TX-E NXOS Needs Upgrade (Circle One)?___YES___NO

NetConfig Information - SwitchB

SwitchB Device Name
<switchB_device_name>_____

SwitchB SSH Service Name
<switchB_ssh_service_name>_____

Appendix D – NIC Device ID and Model Tables

X6-2 NIC Device ID and Model Table

Model	Device ID
On-Board Twinville 10-Gigabit Ethernet Adapter (Net0-Net1)	8086-1528-108e-4852 (Slot 3a:00.0)
On-Board Twinville 10-Gigabit Ethernet Adapter (Net2-Net3)	8086-1528-108e-4852 (Slot 82:00.0)
Twinville 10Gb Ethernet Adapter PCIe Add-in Card	8086-1528-108e-7b15
Niantic 10-Gb Ethernet SFP+ Adapter	8086-10fb-108e-7b11
On-board Fortville 10 Gb Ethernet Adapter	8086-1586-108e-4857

X7-2 NIC Device ID and Model Table

Model	Device ID
Oracle-BASE-T-25Gb-lom Embedded NIC	14e4-16d9-108e-4866
Fortville Oracle Quad 10 Gb and 40 Gb PCIe Add-in NIC	8086-1583-108e-7b1b
Fortpond Oracle Quad Port 10GBase-T PCIe Add-in NIC	8086-1589-108e-7b1c

Appendix E – Contacting Oracle Support

My Oracle Support (MOS)

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

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

1. Select **2** for New Service Request

2. Select **3** for Hardware, Networking and Solaris Operating System Support

3. Select one of the following options:

• For Technical issues such as creating a new Service Request (SR), Select **1**

• For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

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

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

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

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

Locate Product Documentation on the Oracle Help Center Site

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

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

2. Click **Industries**.

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

The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then the Release Number.

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

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