

**Oracle® Communications**  
**Performance Intelligence Center**  
Incremental Upgrade Guide  
Release 10.2  
**E60678 Revision 2**

May 2016

Oracle Communications Performance Intelligence Center Incremental Upgrade, Release 10.2

Copyright ©2003, 2016 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

**CAUTION: Use only the guide downloaded from the Oracle Help Center (OHC) (<http://www.oracle.com/technetwork/indexes/documentation/oracle-comms-tekelec-2136003.html>). Before upgrading your system, access the My Oracle Support web portal (<https://support.oracle.com>) and review any Knowledge Alerts that may be related to the System Health Check or the Upgrade.**

Before beginning this procedure, contact My Oracle Support and inform them of your upgrade plans. Refer to Appendix "My Oracle Support (MOS)" for instructions on accessing My Oracle Support

# Contents

<b>CONTENTS .....</b>	<b>3</b>
<b>1 INTRODUCTION.....</b>	<b>5</b>
1.1 DOCUMENTATION ADMONISHMENTS .....	5
1.2 REFERENCE DOCUMENTS .....	5
1.3 RELATED PUBLICATIONS .....	5
1.4 SCOPE AND AUDIENCE .....	5
1.5 REQUIREMENTS AND PREREQUISITES.....	6
1.5.1 <i>Hardware Requirements</i> .....	6
1.5.2 <i>Software Requirements</i> .....	6
<b>2 INCREMENTAL UPGRADE OVERVIEW FLOWCHARTS .....</b>	<b>8</b>
2.1 FLOWCHART DESCRIPTION .....	8
2.2 OCPIC HIGH-LEVEL INCREMENTAL UPGRADE.....	9
2.3 MANAGEMENT INCREMENTAL UPGRADE .....	10
2.4 PROBES AND INTEGRATED ACQUISITION INCREMENTAL UPGRADE .....	11
2.5 MEDIATION INCREMENTAL UPGRADE .....	12
2.6 PROTOCOL UPGRADE.....	13
<b>3 INCREMENTAL BACK OUT OVERVIEW .....</b>	<b>14</b>
3.1 MANAGEMENT INCREMENTAL BACK OUT .....	14
3.2 ACQUISITION INCREMENTAL BACK OUT .....	14
3.3 MEDIATION INCREMENTAL BACK OUT.....	14
<b>4 OCPIC HEALTH CHECK .....</b>	<b>15</b>
4.1 MEDIATION SUBSYSTEM HEALTH CHECK.....	15
4.2 ACQUISITION HEALTH CHECK .....	16
4.3 MANAGEMENT PRE-UPGRADE HEALTH CHECK AND SETTINGS .....	19
4.3.1 <i>Pre-upgrade Health Check for Management One-box</i> .....	19
4.3.2 <i>Pre-upgrade health check for Standard Management Server</i> .....	21
4.4 CHECK MANAGEMENT BACKUP IS VALID.....	22
4.5 UPGRADE CONFIGURATIONS USING DEPRECATED FIELD(S).....	23
4.6 GLOBAL HEALTH CHECK .....	24
4.6.1 <i>iLO Access</i> .....	24
4.6.2 <i>System Cleanup</i> .....	24
4.6.3 <i>Engineering Document</i> .....	24
4.6.4 <i>Troubleshooting Session Status</i> .....	24
4.6.5 <i>Systems Alarms</i> .....	25
4.6.6 <i>Alarm Forwarding</i> .....	25
4.6.7 <i>KPI</i> .....	25
4.6.8 <i>Dashboard</i> .....	25
4.6.9 <i>Mediation Data Feed</i> .....	25
4.6.10 <i>Browser Export Scheduler</i> .....	25
4.6.11 <i>Capacity Management</i> .....	25
<b>5 MANAGEMENT INCREMENTAL UPGRADE .....</b>	<b>26</b>
5.1 MANAGEMENT PRE-UPGRADE CHECK ONE-BOX .....	26
5.2 UPGRADE MANAGEMENT SERVER.....	29
5.3 POST-UPGRADE SETTINGS .....	30
5.4 MANAGEMENT POST-UPGRADE CHECK .....	31

5.4.1 *Post Upgrade One-Box*..... 32

5.5 MANAGEMENT BACKUP.....32

5.6 UPLOAD MEDIATION PROTOCOL ISO TO MANAGEMENT.....33

**6 ACQUISITION INCREMENTAL UPGRADE .....34**

6.1 ACQUISITION UPGRADE ..... 34

6.2 SYNC MANAGEMENT WITH ACQUISITION .....34

**7 MEDIATION INCREMENTAL UPGRADE .....35**

7.1 MEDIATION SUBSYSTEM UPGRADE.....35

7.2 UPGRADE DTO PACKAGE.....36

7.3 CENTRALIZED MEDIATION PROTOCOL UPGRADE.....36

7.4 UNSET CONFIGURATION ON MANAGEMENT (ONEBOX) .....37

**APPENDIX A. MY ORACLE SUPPORT (MOS) .....38**




**APPENDIX B. LOCATE PRODUCT DOCUMENTATION ON THE ORACLE TECHNOLOGY NETWORK  
SITE 39**

# 1 Introduction

## 1.1 Documentation Admonishments

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

**Table 1:** Admonishments

	<b>DANGER:</b> (This icon and text indicate the possibility of <i>personal injury</i> .)
	<b>WARNING:</b> (This icon and text indicate the possibility of <i>equipment damage</i> .)
	<b>CAUTION:</b> (This icon and text indicate the possibility of <i>service interruption</i> .)

## 1.2 Reference Documents

- [1] [7.0 Platform Configuration Procedures References](#), E53486, December 2014
- [2] [PM&C Incremental Upgrade Procedures](#), E45387, November 2014
- [3] [PIC 10.2 Maintenance Guide](#), E60679, September 2015
- [4] [HP Solutions Firmware Upgrade Pack 2.2.9](#), E59723, March 2015
- [5] [Oracle Firmware Upgrade Pack](#), E54963, June 2014
- [6] [PIC 10.2 Installation Document](#), E60675, September 2015
- [7] Teklec Default Passwords ,TR006061
- [8] [PIC Hardware installation Guidelines](#), E66862
- [9] [MOS Information Center: Upgrade Oracle Communications Performance Intelligence Center 1984685.2](#)
- [10] [PIC 10.2 Upgrade document](#), E60676

## 1.3 Related Publications

Please refer to [MOS Information Center](#): Upgrade Oracle Communications Performance Intelligence Center 1984685.2

## 1.4 Scope and Audience

This document describes the incremental upgrade procedures for the OCPI system at Release 10. This document is intended for use by trained engineers in software installation on both SUN and HP hardware. A working-level understanding of Linux, Oracle and command line interface is expected to successfully use this document.

It is strongly recommended that prior to performing an installation of the operating system and applications software, the user read through this document.

**Note:** The procedures in this document are **not** necessarily in a sequential order. There are flow diagrams in the Incremental Upgrade Overview chapter that provide the sequence of the

procedures for each component of this OCPIC system. Each procedure describes a discrete action. It is expected that the individuals responsible for upgrading the OCPIC system should reference these flow diagrams during this upgrade process.

## 1.5 Requirements and Prerequisites

### 1.5.1 Hardware Requirements

Refer [PIC Hardware Guidelines](#) doc ID E66862

### 1.5.2 Software Requirements

The following software is required for the OCPIC 10.2 incremental upgrade.

Take in consideration you might need also the software from the installed release in case you would have to proceed a disaster recovery. Refer to [PIC 10.2 Maintenance Guide](#) doc ID E60679 for detailed instruction.

**Note:** For specific versions and part numbers, see the [MOS Information Center](#): Upgrade Oracle Communications Performance Intelligence Center 1984685.2.

The following software is required for the OCPIC 10.2 incremental upgrade.

Oracle Communication GBU deliverables:

- Management Server
- Mediation Server
- Mediation Protocol
- Acquisition Server
- TADAPT
- TPD
- TVOE (for blade only)
- PM&C (for blade only)

All the software must be downloaded from Oracle Software Delivery Cloud (OSDC).

<https://edelivery.oracle.com/>

Other required Oracle GA deliverables can be downloaded from Oracle web site:

- Oracle WebLogic Server 11gR1 (10.3.6) Generic and CoherenceWebLogic 10.3.6.0
  - wls1036\_generic.jar

[https://edelivery.oracle.com/EPD/Download/get\\_form?egroup\\_aru\\_number=11571971](https://edelivery.oracle.com/EPD/Download/get_form?egroup_aru_number=11571971)

- Download latest JDK7 available from [MOS Information Center](#)

Other required Oracle database patchset 13390677 deliverables can be downloaded from Oracle support [Error! Reference source not found. Error! Reference source not found.](#) site:

- Oracle Database 11.2.0.4 64bits product patchset
  - p13390677\_112040\_Linux-x86-64\_1of7.zip
  - p13390677\_112040\_Linux-x86-64\_2of7.zip
  - p13390677\_112040\_Linux-x86-64\_3of7.zip

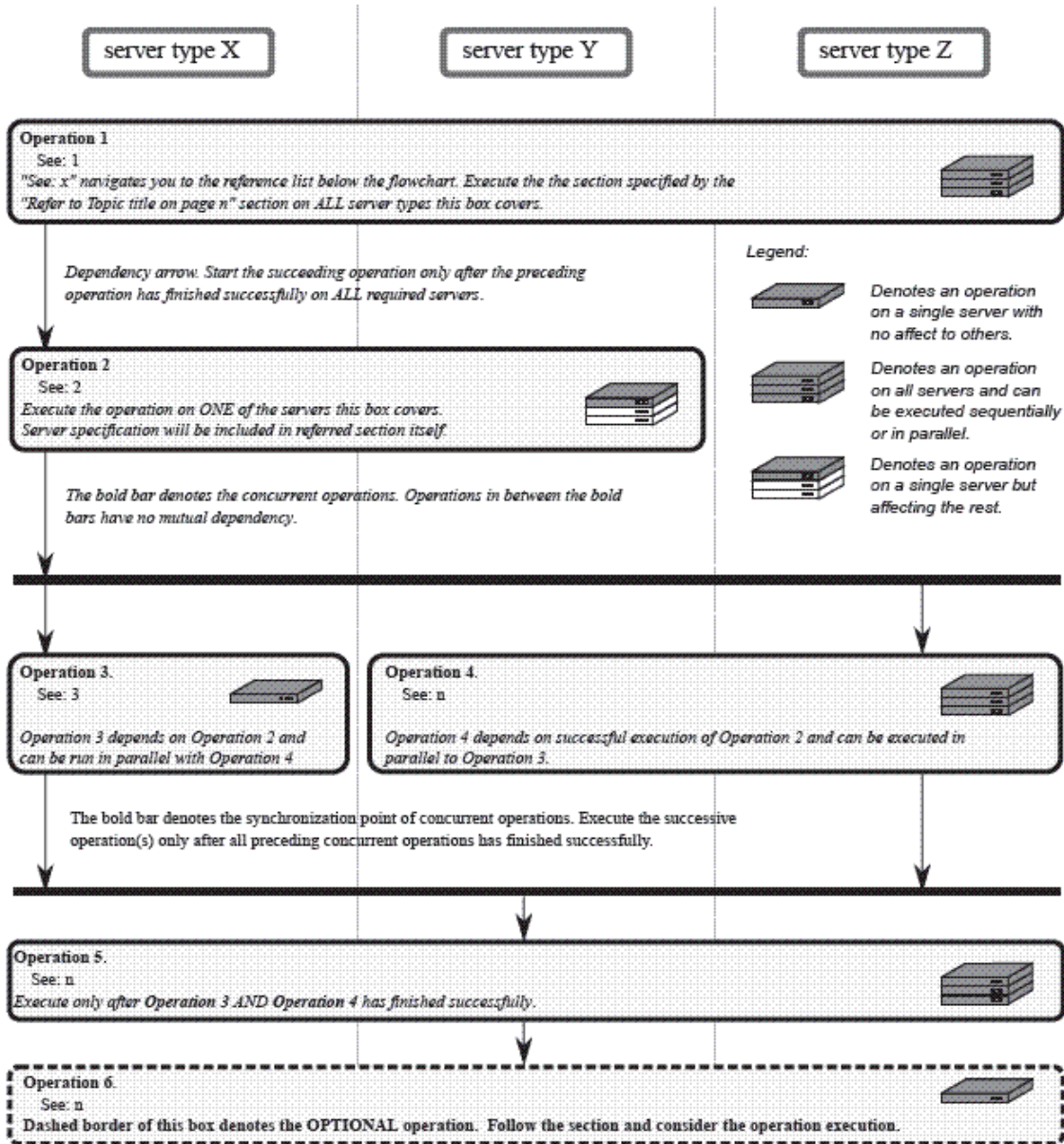
[https://updates.oracle.com/Orion/PatchDetails/process\\_form?patch\\_num=13390677&aru=16716375&release=80112040&plat\\_lang=226P&patch\\_num\\_id=1730815&](https://updates.oracle.com/Orion/PatchDetails/process_form?patch_num=13390677&aru=16716375&release=80112040&plat_lang=226P&patch_num_id=1730815&)

Note: The oracle patchset is same as in PIC 10.1.0

## 2 Incremental Upgrade Overview Flowcharts

### 2.1 Flowchart Description

The flowcharts within each section depict the sequence of procedures that need to be executed to install the specified subsystem.



Each flowchart contains the equipment associated with each subsystem, and the required tasks that need to be executed on each piece of equipment. Within each task, there is a reference to a specific procedure within this manual that contains the detailed information for that procedure.



## 2.2 OCPIC High-level Incremental Upgrade

This flowchart describes the OCPIC high-level incremental upgrade overview. Referring to the graphic below the applicable order of each component is depicted and for each component the applicable flowchart is identified by section of this document where it is located.

Described OCPIC incremental upgrade procedures are applicable to OCPIC systems installed in 10.2 releases.

It is recommended to upgrade the firmware needs to the latest Oracle supported levels for all hardware components, however this firmware upgrade is not mandatory. The system on the source release also need to have installed all necessary patches applicable to source release prior the incremental upgrade.

If running the OCPIC Incremental Upgrade on HP C-Class Blade platform the PM&C application must be upgraded first prior to OCPIC applications upgrade. Follow document [PM&C 6.5 Incremental Upgrade Procedure](#) doc ID E45387.

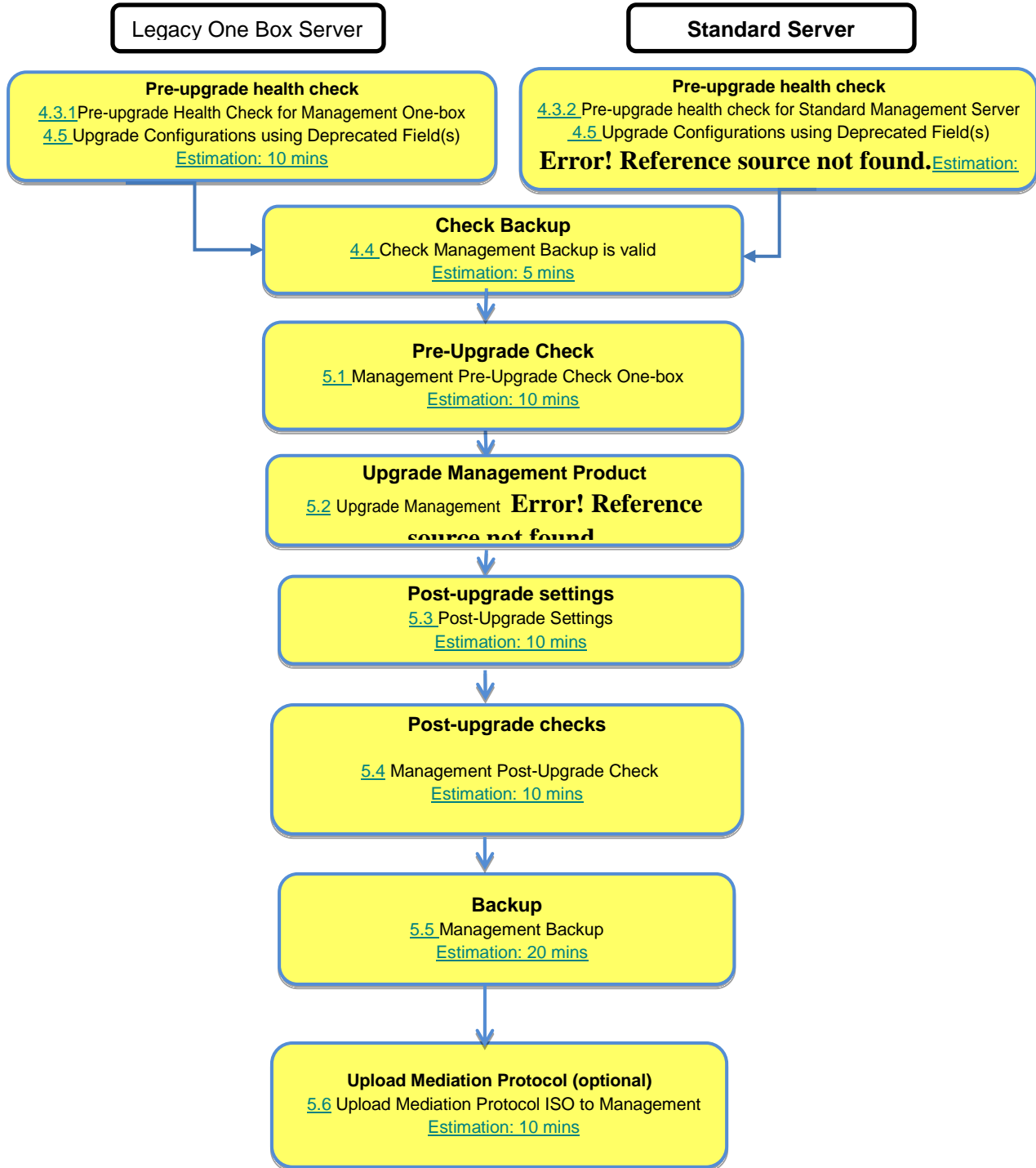
The general upgrade strategy is as follows:

1. Initial health check at least 2 weeks before the planned operation in order to have time to replace defective hardware
2. Firmware upgrade to the latest release available on the OSDC (optional)
3. PM&C Incremental upgrade and update the enclosure switches configuration
4. Management upgrade (one-box configuration)
5. Acquisition subsystems upgrade (Integration Acquisition servers and Probed Acquisition servers)
6. Mediation subsystems upgrade
7. Protocol Upgrade
8. Final Health check

**Note:** Firmware upgrade should be skipped for Data Record Storage server.

## 2.3 Management Incremental Upgrade

This flowchart depicts the sequence of procedures that must be executed to upgrade Management server setup. The same procedure shall be applicable for the incremental upgrade on standard server.

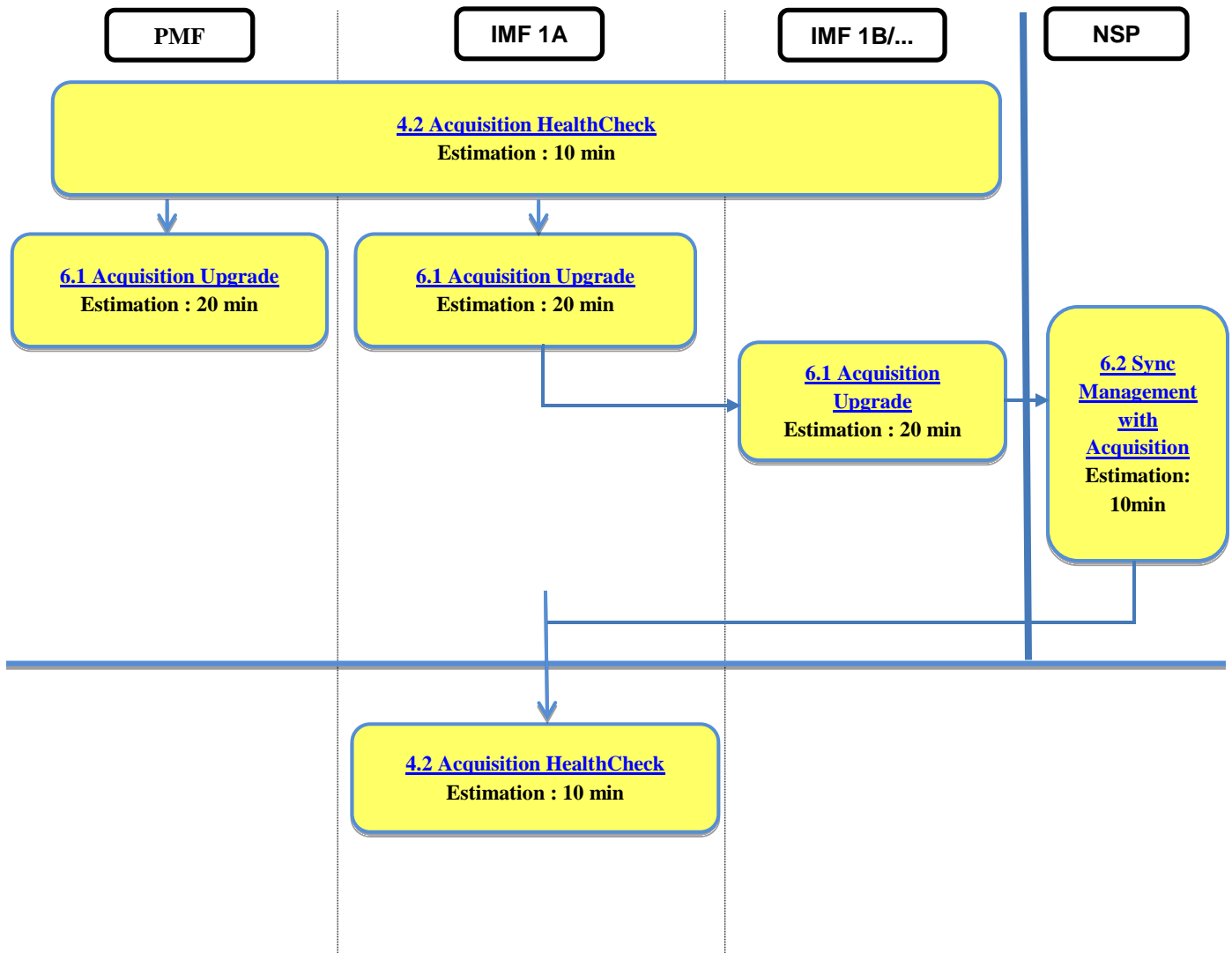


## 2.4 Probed and Integrated Acquisition Incremental Upgrade

This flowchart depicts the sequence of procedures that must be executed to upgrade standalone Probed/Integrated Acquisition Server.

For a Standalone Acquisition server, only PMF is to be updated (refer flowchart).

For Integrated Acquisition Sub-system, depending on the number of servers in a sub-system, the required procedures depicted in the flowchart will need to be repeated.



## 2.5 Mediation Incremental Upgrade

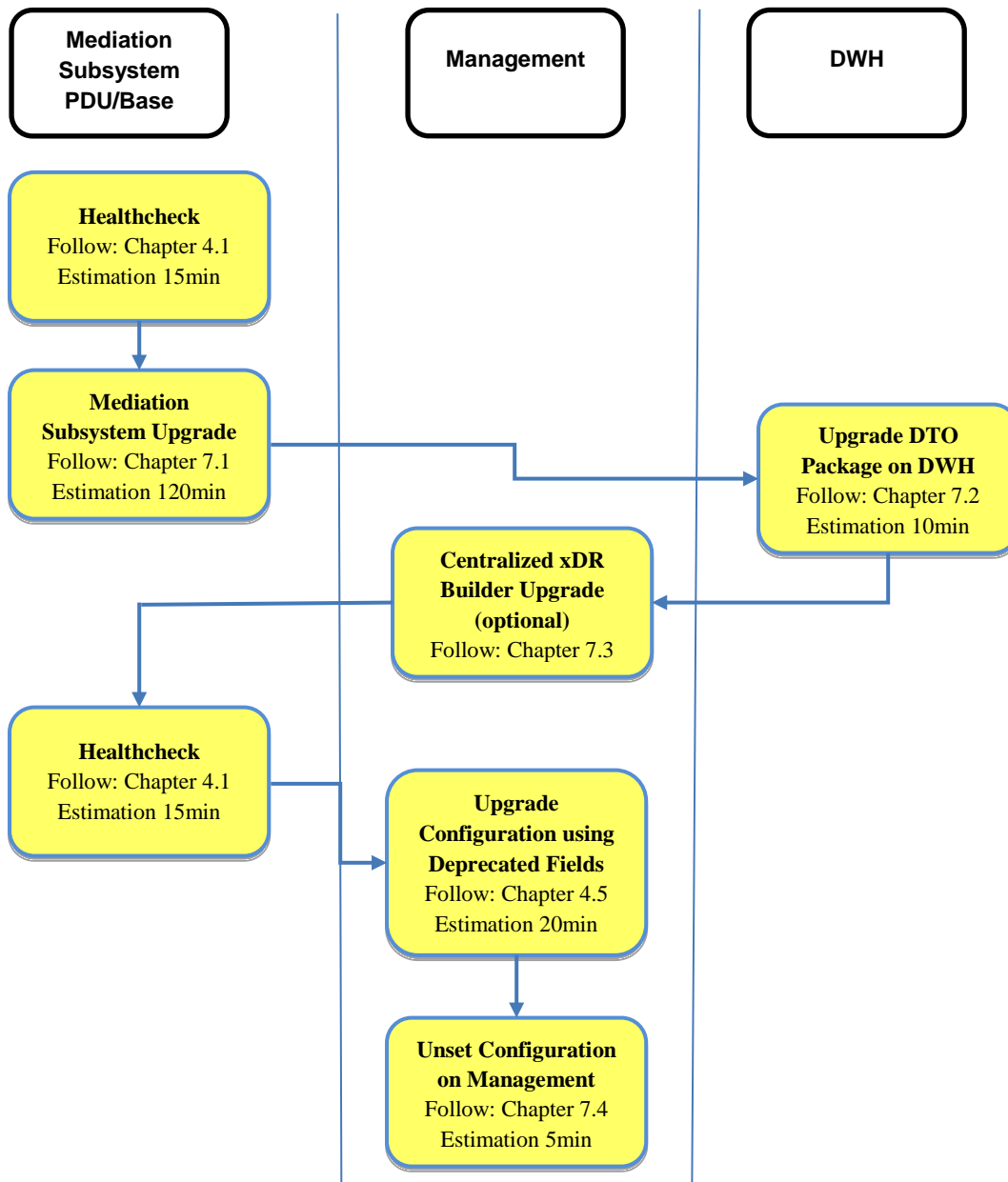
This flowchart depicts the sequence of procedures that must be executed to upgrade the Mediation subsystem and associated server functions.

The Mediation subsystem consists of the following types of servers:

- Mediation PDU storage server, which are part of sub-system and supports processing
- Mediation Base server

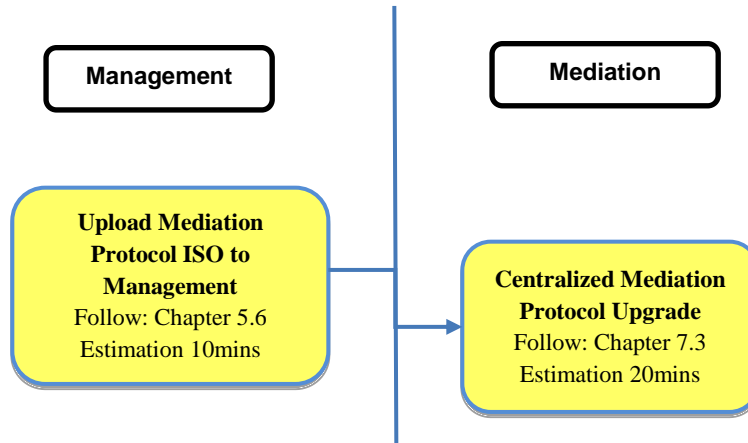
Mediation subsystem incremental upgrade procedure is triggered from one server in the subsystem and runs in parallel on all servers in the subsystem.

**Note:** Some of the xDR/KPI sessions are stored on different servers in the Data Record Storage pool. As Centralized Mediation Protocol upgrade is analyzing all session that are configured on particular Mediation subsystem, all Oracle servers where those sessions are stored must be accessible. Otherwise Centralized Mediation Protocol upgrade will fail.



## 2.6 Protocol Upgrade

This flowchart depicts the sequence of procedures that must be executed to upgrade the Protocols.



### 3 Incremental Back out Overview

The **back out** is design to come back to the previous release and is applicable **only in case of successful upgrade**. The back out sequence would be similar to the upgrade sequence starting with Management, then Acquisition, and Mediation.

#### 3.1 *Management Incremental Back out*

Management application incremental back out is implemented as a Disaster Recovery procedure. Follow the Management Disaster Recovery Procedure, described in the [PIC 10.2 Maintenance Guide](#) doc ID E60679.

#### 3.2 *Acquisition Incremental Back out*

Acquisition application incremental back out is implemented as a Disaster Recovery procedure. Follow the Acquisition Disaster Recovery Procedure, described in the [PIC 10.2 Maintenance Guide](#) doc ID E60679.

#### 3.3 *Mediation Incremental Back out*

Mediation application incremental back out is implemented as a Disaster Recovery procedure. Follow the Mediation Disaster Recovery Procedure, described in the [PIC 10.2 Maintenance Guide](#) doc ID E60679.

## 4 OCPIC Health check

### 4.1 Mediation Subsystem Health check

This procedure describes how to run the automatic health check of the Mediation subsystem.

1. Open a terminal window and log in on any Mediation server in the Mediation subsystem (but not a Data Record Storage server) you want to analyze.
2. As `cfguser`, run:

```
$ analyze_subsystem.sh
```

The script gathers the health check information from all the configured servers in the subsystem. A list of checks and associated results is generated. There might be steps that contain a suggested solution. Analyze the output of the script for any errors. Issues reported by this script must be resolved before any further use of this server.

The following examples show the structure of the output, with various checks, values, suggestions, and errors.

Example of overall output:

```
$ analyze_subsystem.sh
-----
ANALYSIS OF SERVER ixp2222-1a STARTED
-----
10:16:05: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
10:16:05: date: 05-20-11, hostname: ixp2222-1a
10:16:05: TPD VERSION: 4.2.3-70.86.0
10:16:05: IXP VERSION: [7.1.0-54.1.0]
10:16:05: XDR BUILDERS VERSION: [7.1.0-36.1.0]
10:16:05: -----
10:16:05: Analyzing server record in /etc/hosts
10:16:05:         Server ixp2222-1b properly reflected in /etc/hosts file
10:16:05: Analyzing IDB state
10:16:05:         IDB in START state
...
12:21:48: Analyzing disk usage
...
10:24:09: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp2222-1b

ixp2222-1a TPD:[ 4.2.3-70.86.0 ] IXP:[ 7.1.0-54.1.0 ] XB:[ 7.1.0-36.1.0 ] 0
test(s) failed
ixp2222-1b TPD:[ 4.2.3-70.86.0 ] IXP:[ 7.1.0-54.1.0 ] XB:[ 7.1.0-36.1.0 ] 0
test(s) failed
```

Example of a successful test:

```
10:24:08: Analyzing DaqServer table in IDB
10:24:08:         Server ixp2222-1b reflected in DaqServer table
```

Example of a failed test:

```
12:21:48: Analyzing IDB state
12:21:48: >>> Error: IDB is not in started state (current state X)
12:21:48: >>> Suggestion: Verify system stability and use 'prod.start' to start
the product
```

**Note:** if you get the error below you may use the WA of PR 222200 in order to increase the 80 threshold to 85 for the system having been installed originally with old TPD releases and the / partition is only 500M instead of the 1G allocated on the fresh installed system

```
# syscheck
Running modules in class net...
OK

Running modules in class hardware...
OK

Running modules in class disk...
* fs: FAILURE:: MINOR::5000000000000001 -- Server Disk Space Shortage Warning
* fs: FAILURE:: Space used in "/" exceeds the recommended limit 80%. 84 % used.

# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root
                          496M    398M   73M   85% /
```

Log on the server as root and get the current config:

```
# syscheckAdm --get disk fs
FS_MOUNT_LIST=/, -, -, 80, 5000000000000001, 90, 300000000001000, 80,
5000000000000001, 90, 300000000001000, /boot, -, -, 80, 5000000000000001,
90, 300000000001000, 80, 5000000000000001, 90, 300000000001000, /usr, -, -,
80, 5000000000000001, 90, 300000000001000, 80, 5000000000000001, 90,
300000000001000, /var, -, -, 80, 5000000000000001, 90, 300000000001000, 80,
5000000000000001, 90, 300000000001000, /var/TKLC, -, -, 80,
5000000000000001, 90, 300000000001000, 80, 5000000000000001, 90,
300000000001000, /tmp, -, -, 80, 5000000000000001, 90, 300000000001000, 80,
5000000000000001, 90, 300000000001000
```

Then set the new warning threshold value for "/" directory to 85, replace the first "80" in the value string following "/", -, -, " (note you have to copy all the variable value above and paste it between single quotes):

```
# syscheckAdm --set disk fs --var='FS_MOUNT_LIST' --val='/, -, -, 85,
5000000000000001, 90, 300000000001000, 80, 5000000000000001, 90,
300000000001000, /boot, -, -, 80, 5000000000000001, 90, 300000000001000,
80, 5000000000000001, 90, 300000000001000, /usr, -, -, 80, 5000000000000001,
90, 300000000001000, 80, 5000000000000001, 90, 300000000001000, /var, -, -,
80, 5000000000000001, 90, 300000000001000, 80, 5000000000000001, 90,
300000000001000, /var/TKLC, -, -, 80, 5000000000000001, 90,
300000000001000, 80, 5000000000000001, 90, 300000000001000, /tmp, -, -, 80,
5000000000000001, 90, 300000000001000, 80, 5000000000000001, 90,
300000000001000'
```

### 3. Remove back out file

- a) Login as root user on each server
- b) Execute the command to check if the back out file exists

```
# ls /var/TKLC/run/backout
```

- c) If the above command returns a result, run the below command to delete the file

```
# rm /var/TKLC/run/backout
```

## 4.2 Acquisition Health check

This procedure describes how to run the health check script on Acquisition servers.

The script gathers the health check information from each server in the Acquisition subsystem or from standalone server. The script should be **run from each of the server** of the Acquisition subsystem or on stand-alone. The output consists of a list of checks and results, and, if applicable, suggested solutions.

1. Run analyze\_server.sh script as cfguser:

```
$ analyze_server.sh -i
```

2. Analyze the output of the script for errors. Issues reported by this script must be resolved before any further usage of this server. Verify no errors are present.

If the error occurs, contact the Oracle Support, [Error! Reference source not found. Error!](#)



**Reference source not found.**

Example output for a healthy subsystem:

```

04:57:30: STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
04:57:31: date: 02-26-16, hostname: imf9040-1a
04:57:31: TPD VERSION: 7.0.3.0.0-86.40.0
04:57:31: XMF VERSION: [ 10.2.0.0.0-24.1.0 ]
04:57:32: -----
04:57:32: Checking disk free space
04:57:32:   No disk space issues found
04:57:32: Checking syscheck - this can take a while
04:57:43:   No errors in syscheck modules
04:57:44: Checking statefiles
04:57:44:   Statefiles do not exist
04:57:44: Checking runlevel
04:57:45:   Runlevel is OK (4)
04:57:45: Checking upgrade log
04:57:45:   Install logs are free of errors
04:57:45: Analyzing date
04:57:46:   NTP daemon is running
04:57:46:   IP of NTP server is set
04:57:46:   Server is synchronized with ntp server
04:57:47: Analyzing IDB state
04:57:47:   IDB in START state
04:57:47: Checking IDB database
04:57:48:   iaudit has not found any errors
04:57:48: Analyzing processes
04:57:49:   Processes analysis done
04:57:49: Analysing database synchronization
04:57:50:   Either Database synchronization in healthy state or errors found are non-blocking
04:57:50: Checking weblogic server entry
04:57:50:   Appserver is present
04:57:50: All tests passed. Good job!
04:57:51: ENDING HEALTHCHECK PROCEDURE WITH CODE 0

```

**Note:** if you get the error below you may use the WA of PR 222200 in order to increase the 80 threshold to 85 for the system having been installed originally with old TPD releases and the / partition is only 500M instead of the 1G allocated on the fresh installed system

```

# syscheck
Running modules in class net...
OK

Running modules in class hardware...
OK

Running modules in class disk...
* fs: FAILURE:: MINOR::5000000000000001 -- Server Disk Space Shortage Warning
* fs: FAILURE:: Space used in "/" exceeds the recommended limit 80%. 84 % used.

# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_root
                        496M  398M   73M  85% /

```

Log on the server as root and get the current config:

```
# syscheckAdm --get disk fs
FS_MOUNT_LIST=/, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000, /boot, -, -, 80, 5000000000000001,
90, 3000000000001000, 80, 5000000000000001, 90, 3000000000001000, /usr, -, -,
80, 5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000, /var, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000, /var/TKLC, -, -, 80,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000, /tmp, -, -, 80, 5000000000000001, 90, 3000000000001000, 80,
5000000000000001, 90, 3000000000001000
```

Then set the new warning threshold value for "/" directory to 85, replace the first "80" in the value string following "/", -, -, " (note you have to copy all the variable value above and paste it between single quotes):

```
# syscheckAdm --set disk fs --var='FS_MOUNT_LIST' --val='/, -, -, 85,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000, /boot, -, -, 80, 5000000000000001, 90, 3000000000001000,
80, 5000000000000001, 90, 3000000000001000, /usr, -, -, 80, 5000000000000001,
90, 3000000000001000, 80, 5000000000000001, 90, 3000000000001000, /var, -, -,
80, 5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000, /var/TKLC, -, -, 80, 5000000000000001, 90,
3000000000001000, 80, 5000000000000001, 90, 3000000000001000, /tmp, -, -, 80,
5000000000000001, 90, 3000000000001000, 80, 5000000000000001, 90,
3000000000001000'
```

## 4.3 Management Pre-Upgrade Health check and Settings

### 4.3.1 Pre-upgrade Health Check for Management One-box

**Note:** Before executing any steps, provide the root ssh access by executing following as root user on TPD based server.

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit
```

This procedure describes pre-upgrade sanity test for Management together with a few configuration settings.

1. **Execute step 12.5.2 Grant DBA privileges to NSP from [PIC 10.2 Maintenance Guide](#), doc ID E60679.**

2. **Mount PM&C repository**

**Note:** This step has to be followed only for c-class blades

Management ISO must be mounted on Management server Refer Section 8.3 from [PIC 10.2 Upgrade Guide](#) doc ID E60676.

2. **Log in and distribute the Management ISO file**

- a) Login as root user on the Management server (In case of One-box configuration). Copy the Management ISO on server.

3. **Mount the media**

As root, to mount the ISO file, run:

```
# mount -o loop iso_path /mnt/upgrade
```

where *iso\_path* is the absolute path of the ISO image, which includes the name of the image (for example, */var/TKLC/upgrade/iso\_file\_name.iso*).

4. **Pre-Upgrade Verification**

- a) Run health check:

```
# sh /mnt/upgrade/health_check/health_check_common.sh
```

- b) The logs are available at */var/log/nsp/install/nsp\_install.log*

**Note:** take care the logs keep the history from all previous installation, so make sure to start from the end of the file.

- c) Check the message on terminal console.

- d) If Connection for weblogic User is [ NOT OK ]. Please Change the weblogic User Password to Default Password.

#### Steps to change Weblogic Password

- I. Login as a root user on Primary Weblogic box

- II. Enter platcfg menu:

```
# su - platcfg
```

- III. Navigate to **NSP configuration** ⊙ **NSP Password Configuration** ⊙ **Weblogic Password Configuration**

**Note:** Under NSP Password Configuration menu there are two submenus

- NSP Password Configuration (for update/upgrade)
- Weblogic Password Configuration (for startup and deploy)

**Note:** To change the weblogic password during upgrade, second option must be used.

- IV. Change the weblogic password to the default value defined in TR006061 for "Weblogic console".

**Note:** The password must be set to the default value, otherwise upgrade will fail.

**Note:** This step can take a while to complete. Wait for Platcfg menu to return back and do not run any outside procedure in between.

- V. Exit platcfg menu.

#### Verification of successful password change

- I. Using browser open the URL <http://192.168.1.1/console>, where 192.168.1.1 is the IP address one-box server ( In case of One-box setup)
  - II. Enter the new Weblogic password to login to console.
  - III. If login is successful, weblogic password has been updated successfully.
  - IV. If login is unsuccessful, please contact Oracle Support [Error! Reference source not found. Error! Reference source not found.](#) and do not proceed with upgrade.
- e) If Connection for tekelec User is [ NOT OK ]. Please Change the tekelec User Password to Default Password.

**Steps to change tekelec user Password**

- I. Connect to Weblogic console.  
http://192.168.1.1:8001/console  
where **192.168.1.1** is the IP address of Management server
- II. Login with User name weblogic
- III. Click on **Security Realms** in left panel of console window
- IV. Click on **myrealm** in right Panel of console window.
- V. Click on **Users& Groups** Tab
- VI. Click on **users** Tab.
- VII. Select **tekelec** user.
- VIII. Select **Password** Tab
- IX. Change the password to Default Password

**Note:** If password of tekelec user is not set to default prior to upgrade then upgrade might fail

- f) If Connection for TklcSrv User is [ NOT OK ]. Please Change the TklcSrv User Password to Default Password.

**Steps to change TklcSrv user Password**

- I. Connect to Weblogic console.  
http://192.168.1.1:8001/console  
where **192.168.1.1** is the IP address of Management server
- II. Login with User name weblogic
- III. Click on **Security Realms** in left panel of console window
- IV. Click on **myrealm** in right Panel of console window.
- V. Click on **Users& Groups** Tab
- VI. Click on **users** Tab.
- VII. Select **TklcSrv** user.
- VIII. Select **Password** Tab
- IX. Change the password to Default Password

**Note:** If password of TklcSrv user is not set to default prior to upgrade then upgrade might fail

- g) **Verify State and Health** should be **RUNNING** and **OK** for all three servers.

- h) Verify the build number should be 10.x.x-X.Y.Z where X.Y.Z is the build number.

- i) Verify the RAM Size is [OK]

- j) Verify the space in /opt, /tmp, /var/TKLC is [OK]:

- If you have the message “space in /var/TKLC is [NOT OK]” make sure you have only one ISO file in /var/TKLC/upgrade. If not, remove all other files; they must be used one by one and not copied all at the same time because the partition is too small.
- If you still have space issue erase the content of the directory /var/TKLC/backout/pkg but not the directory itself.
- If the space is still [NOT OK] in any of the above partition, execute the following command to create some default space. Run:

```
# sh /mnt/upgrade/health_check/pre_upgrade_createspace.sh
type yes to continue.
```

Please follow step 3(a) again to verify if the space is [OK].

**Note:** Please do not proceed if space is shown [NOT OK] in any of the above partition. Contact Oracle Support [Error! Reference source not found. Error! Reference source not found.](#)

and ask for assistance.

- k) Verify the free space in /, /opt/oracle is [OK].  
If the space is [NOT OK] in any of the above partition contact Oracle Support **Error! Reference source not found. Error! Reference source not found.** and ask for assistance.
- l) Verify /tekelec symlink is present [ OK ].  
If /tekelec symlink is [NOT OK], please ignore as it will be automatically created on executing the script "pre\_upgrade\_config.sh" in section 5.1 2(c).
- m) As root, unmounts the ISO file:

```
# umount /mnt/upgrade
```

## 5. Verify the free space in vg-root-plat\_oracle partition

- a) Login to Management one box system as root user and execute the below command to know the size of vg-root-plat\_oracle partition

```
# df -kh
Filesystem                Size      Used Avail Use% Mounted on
/dev/mapper/vgroot-plat_oracle  7.9G    4.5G    3.1G  60% /usr/TKLC/oracle11
```

If the use% is 90% or above then perform below step to free some space.

- b) Move the logs from vg-root-plat\_oracle partition to vgroot-plat\_nsp partition as this partition has enough space by performing below steps.

```
# mkdir /usr/TKLC/nsp/alertlogs_backup
# mv /opt/oracle11/oracle/diag/rdbms/nsp_01/NSP/alert /log_*.xml
  /usr/TKLC/nsp/alertlogs_backup
```

If the enough space does not get free by doing above step contact Oracle Support **Error! Reference source not found. Error! Reference source not found.** and ask for assistance.

## 6. Check Weblogic console is not locked

Weblogic console must not be locked during upgrade. If console is locked upgrade will abort. If it is locked, please release lock from Weblogic console as follows:

- a) Connect to Weblogic console.  
<http://192.168.1.1:8001/console>  
where 192.168.1.1 is the IP address of Management server.
- b) On the left panel click on **Release configuration** button.

## 7. Remove backout file

- a) Login as root user on Management Server one-box configuration
- b) Execute the command to check if the backout file exists  

```
# ls /var/TKLC/run/backout
```
- c) If the above command returns a result, run the below command to delete the file  

```
# rm /var/TKLC/run/backout
```

## 8. Check the pkg directory exist

- a) Login as root user on Management Server one-box configuration.
- b) Execute the command to check if the backout file exists  

```
# ls /var/TKLC/backout/pkg
```
- c) If the above command does not returns a result, run the below command to create the directory  

```
# mkdir /var/TKLC/backout/pkg
```

## 4.3.2 Pre-upgrade health check for Standard Management Server

### 1. Pre-Upgrade Verification

- a) Please verify the system User Password is Default Password.
- b) Please Change the tekelec User Password to Default Password.

#### Steps to change tekelec user Password

- I. Connect to Weblogic console.

http://192.168.1.1:8001/console  
 where **192.168.1.1** is the IP address of Management server

- II. Login with User name weblogic
- III. Click on **Security Realms** in left panel of console window
- IV. Click on **myrealm** in right Panel of console window.
- V. Click on **Users& Groups** Tab
- VI. Click on **users** Tab.
- VII. Select **tekelec** user.
- VIII. Select **Password** Tab
- IX. Change the password to Default Password

**Note:** If password of tekelec user is not set to default prior to upgrade then upgrade might fail

- c) Please Change the TkIcSrv User Password to Default Password.

**Steps to change TkIcSrv user Password**

- I. Connect to Weblogic console.  
 http://192.168.1.1:8001/console  
 where **192.168.1.1** is the IP address of Management server
- II. Login with User name weblogic
- III. Click on **Security Realms** in left panel of console window
- IV. Click on **myrealm** in right Panel of console window.
- V. Click on **Users& Groups** Tab
- VI. Click on **users** Tab.
- VII. Select **TkIcSrv** user.
- VIII. Select **Password** Tab
- IX. Change the password to Default Password

**Note:** If password of TkIcSrv user is not set to default prior to upgrade then upgrade might fail

- d) Verify State and Health should be RUNNING and OK for all three servers
- e) Verify the build number should be 10.x.x-X.Y.Z where X.Y.Z is the build number

**2. Check Weblogic console is not locked**

**4.4 Check Management Backup is valid**

This procedure describes different steps to be followed for checking the backup of Management is valid. It is useful to have this backup in case of restoring the setup need arising from upgrade failure.

1. Login as a `root` user on Management Server.

2. Check the content of `/opt/oracle/backup`

There must be one directory for the last seven days and it is recommended to copy in a safe place the full content of at least the last of this directory:

```
# cd /opt/oracle/backup
# ls -lh
drwxrwxrwx 9 root root 4096 Jun 28 22:01 NSP_BACKUP_06_28_12_22_00_01
drwxrwxrwx 9 root root 4096 Jun 29 22:01 NSP_BACKUP_06_29_12_22_00_02
drwxrwxrwx 9 root root 4096 Jun 30 22:01 NSP_BACKUP_06_30_12_22_00_01
drwxrwxrwx 9 root root 4096 Jul 1 22:01 NSP_BACKUP_07_01_12_22_00_01
drwxrwxrwx 9 root root 4096 Jul 2 22:01 NSP_BACKUP_07_02_12_22_00_01
drwxrwxrwx 9 root root 4096 Jul 3 22:01 NSP_BACKUP_07_03_12_22_00_01
drwxrwxrwx 9 root root 4096 Jul 4 22:01 NSP_BACKUP_07_04_12_22_00_01
```

3. Check the content of the last backup directory

- a) On Management Server:

```

-rw-r--r-- 1 root root 391K Mar 24 22:01 apache-conf.tgz
-rw-r--r-- 1 root root 169 Mar 24 22:01 backup.log
-rw-r--r-- 1 root root 186 Mar 24 22:00 boot.properties
-rw-r--r-- 1 root root 116 Mar 24 22:01 bulkconfig
drwxr-xr-x 10 root root 4.0K Mar 24 22:00 config
-rw-r--r-- 1 root root 6.9K Mar 24 22:01 customer_icon.jpg
-rw-r--r-- 1 oracle oinstall 3.0M Mar 24 22:01 ExpNSP.dmp.gz
-rw-r--r-- 1 oracle oinstall 52K Mar 24 22:01 ExpNSP.log
drwxr-xr-x 2 root root 4.0K Mar 24 22:00 exportrealm
-rw-r--r-- 1 root root 230k Mar 24 22:01 failedconnection.txt
-rw-r--r-- 1 root root 2.5K Mar 24 22:01 global_versions.properties
-rw-r--r-- 1 root root 235 Mar 24 22:01 hosts
-rw-r--r-- 1 root root 1585 Mar 24 22:01 hosts.csv
-rw-r--r-- 1 root root 163 Mar 24 22:01 ifcfg-eth01
-rw-r--r-- 1 root root 23 Mar 24 22:01 ifcfg-eth02
-rw-r--r-- 1 root root 47K Mar 24 22:01 install.log
drwxrwxrwx 2 root root 4096 Mar 24 22:01 IXP
-rw-r--r-- 1 root root 59M Mar 24 22:01 jmxagentproperties.tgz
drwxr-xr-x 7 root root 4.0K Mar 24 22:00 ldap
-rw-r--r-- 1 root root 85 Mar 24 22:01 network
-rw-r--r-- 1 root root 600 Mar 24 22:01 nsp_setenv.sh
-rw-r--r-- 1 root root 1.6K Mar 24 22:01 ntp.conf
-rw-r--r-- 1 root root 298 Mar 24 22:01 optional_modules_list
-rw-r--r-- 1 root root 320 Mar 24 22:00 preBackupTests.log
-rw-r--r-- 1 root root 148 Mar 25 05:44 restore_10.248.19.35.log
-rw-r--r-- 1 root root 64 Mar 24 22:00 SerializedSystemIni.dat
-rw-r--r-- 1 root root 0 Mar 24 22:01 snmpd.conf
drwxrwxrwx 2 root root 4096 Mar 24 22:01 XMF Make sure the file
ExpNSP.dmp.gz exist and have a size coherent with the amount of data of your
customer. Check the content of ExpNSP.log.

```

Check the contents of IXP folder. It will be similar to the one below.

```

-rw-r--r-- 1 root root 610 Mar 24 22:01 IXP_ixp1000-1a.tgz
-rw-r--r-- 1 root root 645 Mar 24 22:01 IXP_ixp1000-1b.tgz
-rw-r--r-- 1 root root 560 Mar 24 22:01 IXP_ixp1000-1z.tgz

```

Check the contents of XMF folder. It will be similar to the one below

```

-rw-r--r-- 1 root root 296 Mar 24 22:01 PMF_pmf-9010.tgz

```

**Note:** the backup is automatically executed each night at 22H00 and depending on the time you start Management upgrade you may execute a manual backup just before to start the upgrade.

### 4.5 Upgrade Configurations using Deprecated Field(s)

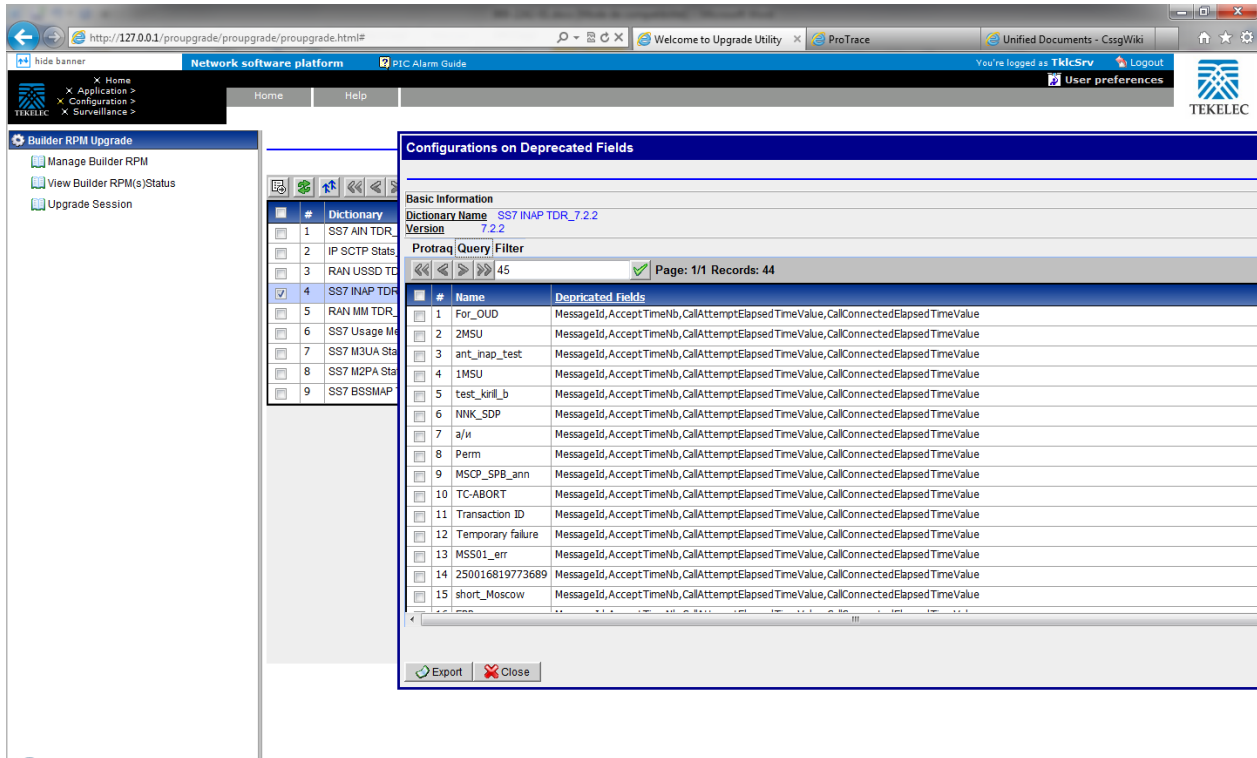
This step is to be performed to upgrade configurations which are using Deprecated field(s) so as to make sure none of the configuration will use Deprecated field which may get removed in later releases.

1. Login to Management application interface as TklcSrv user.
2. Click **Upgrade Utility**
3. Click **Dictionaries with Deprecated Field(s)** link on home page, this will a list of dictionaries having deprecated field(s).
4. Select any one of the dictionaries and choose **View Dependent Configurations** icon from tool bar. This will display list of KPIs, Queries and Filters using deprecated fields. You can also export this list by clicking on **Export** button given on that popup. If there are no dependent configurations then this list will be empty.

Take care to check each Tab and not Only the default one KPI.

The Screen shot bellow shows an example where the job has not been done at

the end of the previous upgrade.



## 4.6 Global Health check

### 4.6.1 iLO Access

Make sure you can access the iLO interface of all servers and you can open the remote console for each server.

### 4.6.2 System Cleanup

Discuss with the customer to clean up the system as much as possible in order to reduce the risk and avoid any issue due to some objects that would no more be used.

### 4.6.3 Engineering Document

Make sure you get the latest available engineering document and it is up to date.

The latest version should be documented on the Customer Info Portal, as well as the current password for the admin users

### 4.6.4 Troubleshooting Session Status

Navigate from the home screen to Troubleshooting

**NOTE:** Look for any sessions that are lagging behind the current time.

1. View All records
2. Filter by end date
3. Screen capture the information

Verify which sessions are lagging. Statistics sessions must also be considered but take in consideration records are periodically generated.

Try to access the session it-self and check the session content and especially make sure the PDU are properly recorded.



### **4.6.5 Systems Alarms**

Access the system alarm and fix all alarms on the system. In case some alarms can't be fixed due to overloaded system for example, the remaining alarms before the upgrade must be captured in order to compare with the alarms we would get at the end of the upgrade.

### **4.6.6 Alarm Forwarding**

Connect on Management Primary and Navigate in platcfg menu to check the SNMP and SMTP configuration. Make sure the SNMP and SMTP configuration are up to date in the Engineering Document.

### **4.6.7 KPI**

Access to KPI configuration and check which configuration are NOT-SYNC

### **4.6.8 Dashboard**

Access to Dashboard Application and check each dashboard is working fine

### **4.6.9 Mediation Data Feed**

Access to the Mediation Data Feed configuration and capture the Feed Status  
Make sure each Feed configuration is Documented in the Engineering Document

### **4.6.10 Browser Export Scheduler**

Access to the Browser Export Scheduler and check the scheduled tasks configured are working as expected.  
Make sure each task is documented in the Engineering Document.

### **4.6.11 Capacity Management**

Access Troubleshooting and open CapacityManagement PIC\_UsageStats session to verify if normal activity is monitored hourly for probed acquisition, integrated acquisition, mediation and mediation protocol.

## 5 Management Incremental Upgrade

### 5.1 Management Pre-Upgrade Check One-box

**Note:** Please proceed on this procedure for **Management Standard Server from 2 f) onwards**.

1. **Make sure you executed the sections:**

- a) Management Pre-Upgrade Health check and settings
- b) Upgrade configuration using deprecated fields
- c) Check Management Backup is Valid

2. **Pause JMS and Purge terminated alarm**

This procedure does the following tasks:

- a. Pauses JMS consumption
  - b. Purges Alarm
  - c. Corrects /tekelec symlink path
  - d. Reconfigures Enterprise manager if it is not correctly configured
- a) Login as root user on Management Server In case of One-box configuration)
  - b) Execute the following command to mount Management ISO:

```
# mount -o loop iso_path /mnt/upgrade
```

where *iso\_path* is the absolute path of the ISO image, which includes the name of the image (for example, */var/TKLC/upgrade/iso\_file\_name.iso*).

c) Run pre-upgrade config:

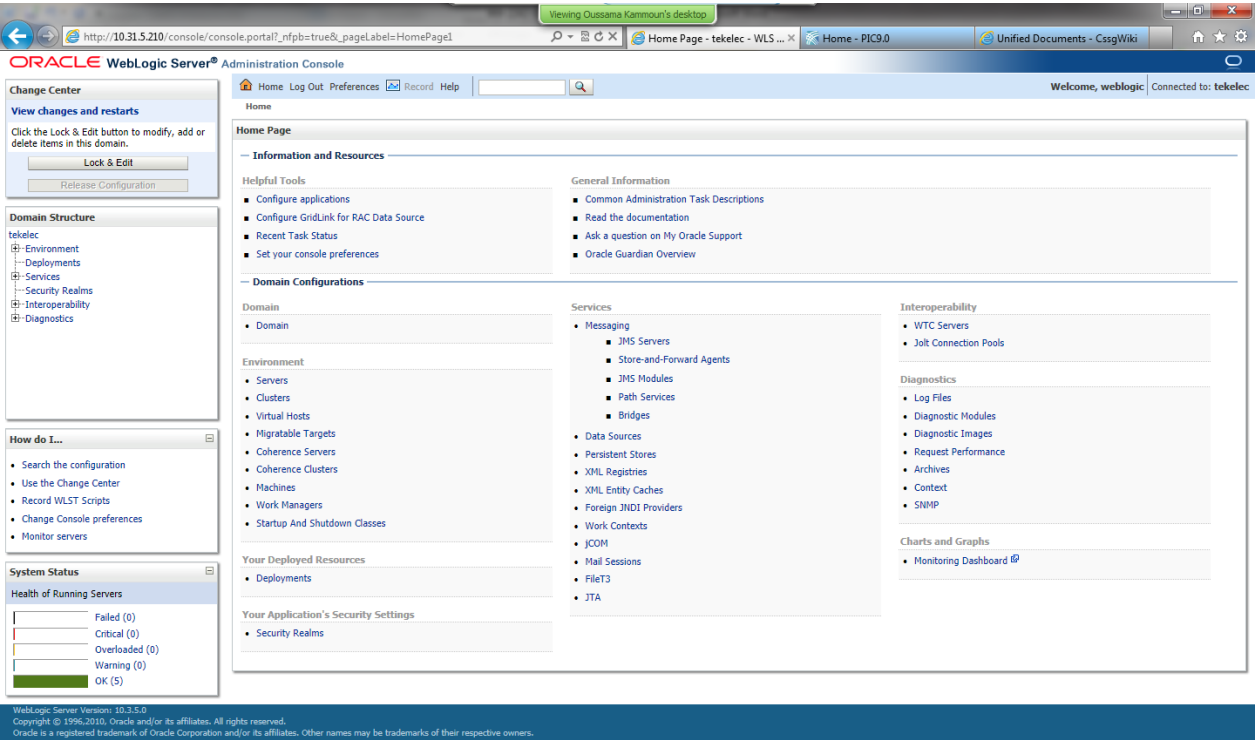
```
# sh /mnt/upgrade/health_check/pre_upgrade_config.sh
```

**Note:** If you get the message below just answer “y” in order to unlock weblogic console

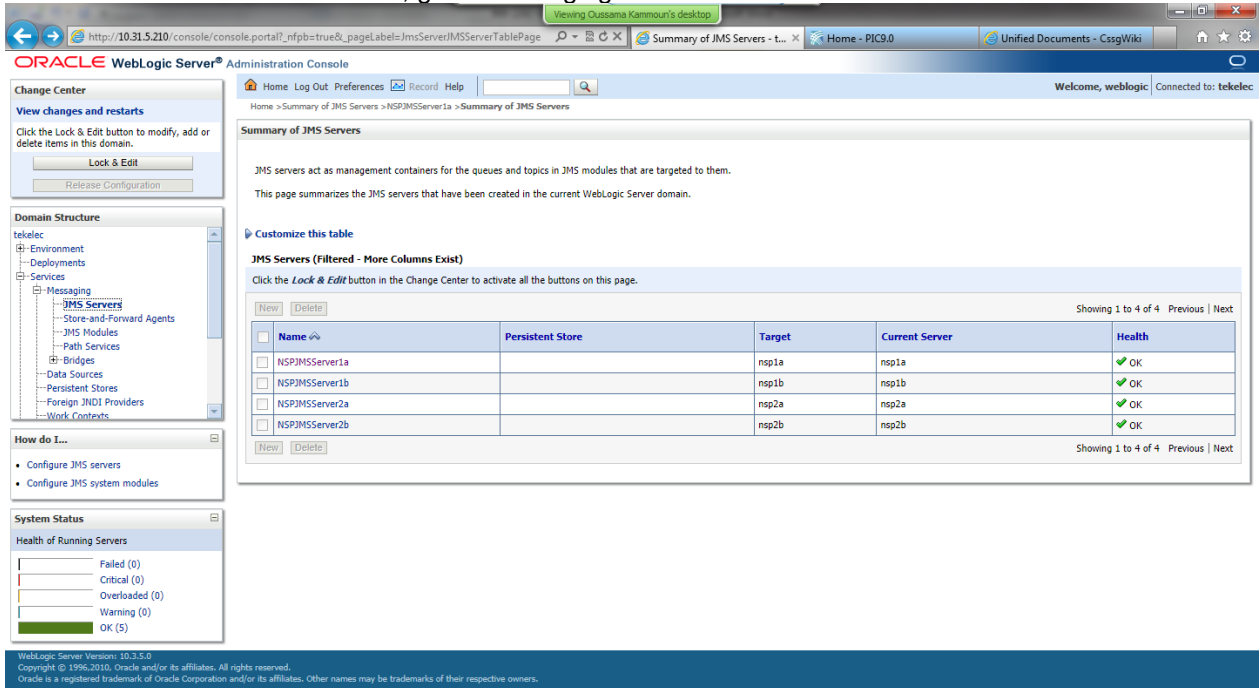
```
***** Purge Terminated Alarms *****
Purging Terminated Alarms
Number of Terminated Alarms: 92456
Number of All Alarms: 92639
Do you want to purge Alarms prior to backing up oracle db [y/n]?
```

- d) Type “y” to continue for purging of terminated alarms.  
To purge terminated Alarms enter 1 or to purge All Alarms enter 2
  - e) Unmount Management Server ISO
- ```
# umount /mnt/upgrade
```
- f) Connect to Weblogic console in order to check JMS consumption is really stopped.

# Incremental Upgrade Guide

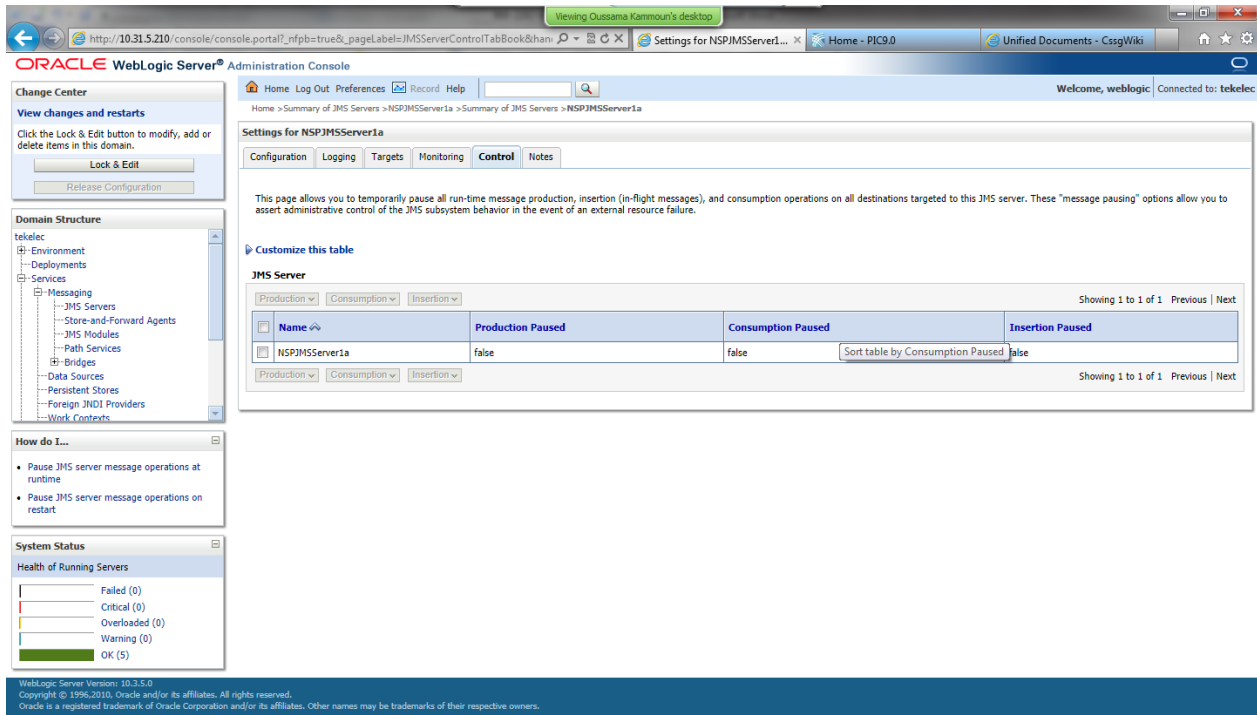


In the Services section, go to messaging and then JMS Servers menu:

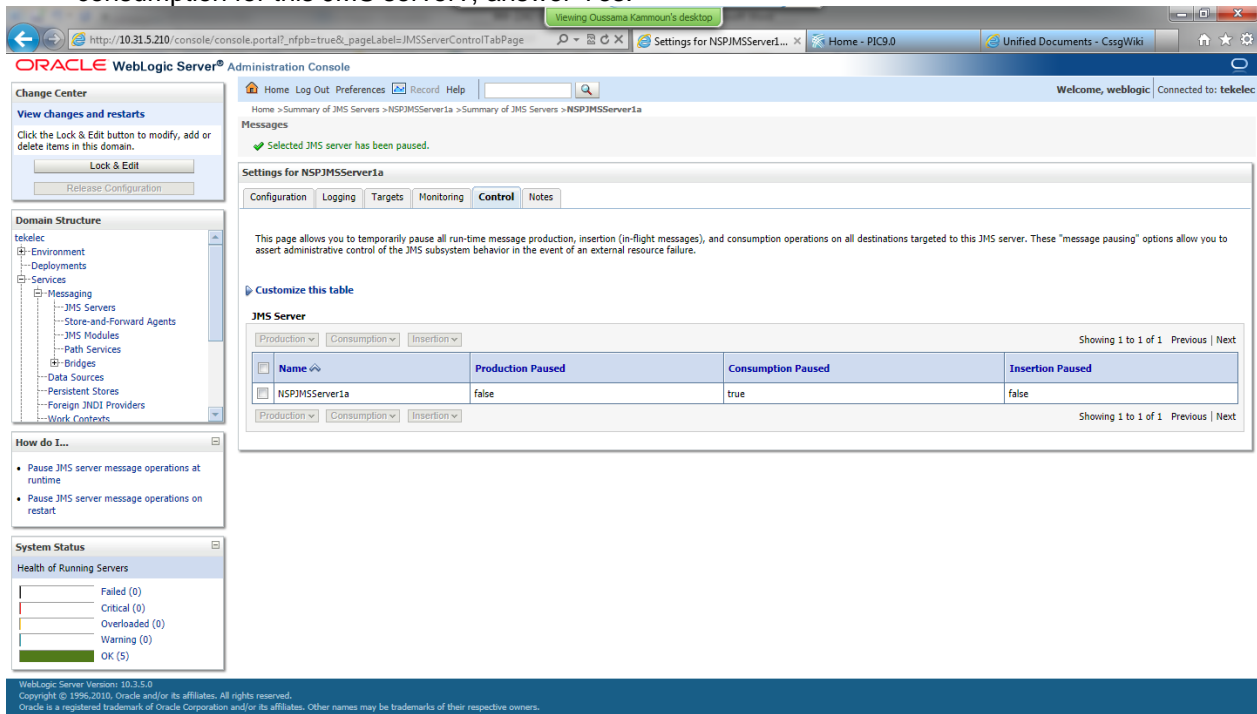


For Each JMS servers, click on the name of the server and then to the menu Control:

# Incremental Upgrade Guide



If the value in consumption paused is true, this server is paused and you can return to previous step in order to check the status of the next JMS server.  
 If the value is false like of the screenshot, select the checkbox in order to activate the menu consumption, and then select pause. When asked to confirm if you Are sure you want to pause consumption for this JMS server?, answer Yes.



The value in consumption paused is true now as expected, so you can return to the JMS server list in order to check the status of the next one, or continue next step if this was the last one.

3. Check minimum free disk space in /opt/oracle/backup

a) As root run:

```
# df -kh /opt/oracle/backup
```

Example output:

| Filesystem        | Size | Used | Avail | Use% | Mounted on         |
|-------------------|------|------|-------|------|--------------------|
| /dev/cciss/c0d2p1 | 67G  | 11G  | 57G   | 16%  | /opt/oracle/backup |

b) Check the space available under Avail column of this table. This should be at least 15-20 GB approx. e.g. in above table shown total space available is 57GB.

**Note:** If total available space is less than 2 GB, then do not continue with upgrade. Contact Oracle Support [Error! Reference source not found.](#) and ask for assistance.

4. Generate the “Bulk Export Configurations” and “Create Configuration Report”

Go to the Centralized Configuration home page and click on the link to generate this files. Keep it in a safe place on your laptop in the worst case where even a disaster recovery would not work with would help you to get in information, in order to re-create the configuration.

5. Synchronize the Integrated Acquisition

Go to the Centralized Configuration and synchronize the Integrated Acquisition in the acquisition part before to start any operation in order to avoid discovering new links while the upgrade.

Take care if the Custom Name Override feature is enable on the link set, the names would be replaced by the one used on the Eagle.

The function is available on the Linksets list page tool bar.

The screenshot shows a web interface with a table of linksets. A modal dialog titled "Set Link Custom Name Override" is open over the table. The dialog contains the following text:

Setting the Linkset Name Override to 'Enabled' will replace the Linkset Custom Name with the Eagle Name for each IMF monitored Linkset. In addition, whenever discovery occurs, the Linkset Custom Name will be set to the discovered Eagle Name.

If the Linkset Name Override is set to 'Disabled', the Linkset Custom Name will not be set to the Eagle Name during discovery.

The 1 selected Linksets with valid Eagle Name values will be modified on the subsystem(s).

Buttons:  Enable  Disable

| # | Linkset Custom Name    | Custom Name Override             | Eagle Name           | Description | RID Group Id | Linkset Type | Near End  |
|---|------------------------|----------------------------------|----------------------|-------------|--------------|--------------|-----------|
| 1 | stp9070901-Iss110111   | <input type="radio"/>            | stp9070901-Iss110111 |             |              | A            | eagle_100 |
| 2 | stp9070901-Iss120611   | <input checked="" type="radio"/> | stp9070901-Iss120611 |             |              | A            | eagle_100 |
| 3 | stp9070901-Iss110311n  | <input type="radio"/>            |                      |             |              |              | eagle_100 |
| 4 | stp9070901-Iss110411   | <input type="radio"/>            |                      |             |              |              | eagle_100 |
| 5 | stp9070901-Iss120811   | <input type="radio"/>            |                      |             |              |              | eagle_100 |
| 6 | stp9070901-Iss1207atms | <input type="radio"/>            |                      |             |              |              | eagle_12- |
| 7 | stp9070901-Iss1313n7   | <input type="radio"/>            |                      |             |              |              | eagle_14€ |
| 8 | stp9070901-Iss1313n6   | <input type="radio"/>            |                      |             |              |              | eagle_14€ |
| 9 | stp9070901-Issr153602  | <input type="radio"/>            |                      |             |              |              | eagle_14€ |

| # | Link Custom Name       | Eagle Name             | Description | SLC | Interface Name | Protocol Name | Error Correction | Remo |
|---|------------------------|------------------------|-------------|-----|----------------|---------------|------------------|------|
| 1 | stp9070901-Iss110111-0 | stp9070901-Iss110111-0 |             | 0   | FASTCOPY_M2PA  | M2PA_SCTP_N   | NONE             |      |

## 5.2 Upgrade Management Server

1. Mount PM&C repository

**Note:** This step has to be followed only for c-class blades Management ISO must be mounted on Management server Refer 8.3 from [PIC 10.2 Upgrade Guide](#) doc ID E60676

2. Upgrade Management Server

- a) Login as root user on terminal console of Management server.
- b) Copy the Management ISO on server.

c) Mount the ISO file

```
# mount -o loop iso_path /mnt/upgrade
```

where iso\_path is the absolute path of the Management ISO image, which includes the name of the image (for example, /var/TKLC/upgrade/iso\_file\_name.iso).

d) As root, run:

**Note:** Run this procedure via iLO or through any disconnectable console only.

```
# /mnt/upgrade/upgrade_nsp.sh
```

**Note:** /mnt/upgrade is the mount point where Management ISO is mounted

e) Wait for Management upgrade to get complete. Remove this file to save disk space.

As root, run:

```
# rm -f /var/TKLC/upgrade/iso_file
```

where iso\_file is the absolute path of the ISO image, which includes the name of the image.

After the installation the server will restarts automatically. Log back in and review the Management installation log ( /var/log/nsp/install/nsp\_install.log) and TPD upgrade log ( /var/TKLC/log/upgrade/upgrade.log) for errors. If Management did not install successfully, contact [Error! Reference source not found. Error! Reference source not found.](#)

**Note:** When user will login back to machine then a message will appear asking to accept or reject upgrade. Ignore this message for now. It will be automatically accepted when user will execute post\_upgrade\_sanity\_check.sh script.

### 5.3 Post-Upgrade Settings

#### 1. Resume JMS Consumption

**Note:** On Management Standard Server the JMS consumption must be resumed from weblogic console.

**Execute below script for TPD based platform**

- a) Open a terminal console and Login as a root user on Management server
- b) Execute the command below to resume JMS consumption

```
# sh /opt/nsp/scripts/procs/post_upgrade_config.sh
```

#### 2. Configure Apache HTTPS Certificate (Optional)

**Note:** This step should be skipped for Management Standard Server.

- a) Copy the files server.crt and server.key that are provided by the customer to /root, if the certificate key files are not present then self signed certificate can be used.

**Note:** The certificates if already present before upgrade must be restored manually from the backup (/opt/oracle/backup/NSP\_BACKUP\_XX\_XX\_XX\_XX\_XX\_XX) used in the upgrade, after the management server has been upgraded. This should prevent warning about the SSL certificate error in case of https access.

- b) From platcfg root menu navigate to **NSPConfiguration**  **Configure Apache HTTPS Certificate**

This would install certificate provided by customer

#### 3. Restrict access of Management frontend to HTTPS (Mandatory) Disable access to HTTP

**Note:** This step should be skipped for Management Standard Server.

- a) Open a terminal console and Login as a root user on Management server
- b) Enter the platcfg menu

```
# su - platcfg
```

- c) Navigate to **NSP Configuration**  **Enable HTTP Port**  **Edit**

- d) Select **NO** and press **Ok** to disable access to HTTP

#### 4. Configure host file for Mail Server (Optional)

**Note:** On Management Standard Server please refer section 7.5 and 7.6 in [PIC 10.2 Maintenance Guide](#) doc ID E60679

**Note:** This configuration is optional and required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined and no server address override defined by app).

- a) Open a terminal window and log in as `root` user on Management server.
- b) Enter the `platcfg` menu. As `root` run:  

```
# su - platcfg
```
- c) Navigate to Network **Configuration**  $\odot$  **Modify host file**  $\odot$  **Edit** and press enter
- d) Select **Add Alias** menu and press enter
- e) Select line with machine `<ip>` and press enter
- f) Enter new alias as `mail.server` in the text field press **OK**
- g) Repetitive exit to exit `platcfg` menu

#### 5. Transfer Ownership of TklcSrv object

**Note:** Follow the steps only if some object belonging to TklcSrv were created in previous version.

- a) Open a web browser and log in to the Management application interface TklcSrv user.
- b) Navigate to **security application**  $\odot$  **Transfer ownership value**
- c) Transfer all the TklcSrv object to and other user (tekelec for example)

## 5.4 Management Post-Upgrade Check

**Box:** must be done from a browser (IE/Mozilla).

This procedure describes the steps for the Sanity Tests of Management.

#### 1. WebLogic Console

From Internet Explorer, connect to the WebLogic console using the following URL:

<http://192.168.1.1:8001/console>

where **192.168.1.1** is the IP address of the Management Server (In case of One-box configuration)

#### 2. Login

You should be prompted to “Log in to work with the WebLogic Server domain “.

Connect with User **weblogic**

#### 3. Console Display

Under the **Environment** heading, click on the “**Servers**”.

#### 4. Health Check

- a) On clicking the “Servers” link in the last step, the console would display the **Summary of Servers**, with a list of the three servers, `nsp1a`, `nsp1b` and `nspadmin` (In case of One-box configuration)
- b) Entries in the columns **State** and **Health** should be **RUNNING** and **OK** for all three servers (In case of One-box configuration)

#### 5. Management GUI

From Internet Explorer, connect to the Management Application GUI using the following URL:

<http://192.168.1.1/>

where **192.168.1.1** is the IP address of the Management Server (in case of One-box configuration)

#### 6. Login

Login to the Application with User name **tekelec**

#### 7. Portal

- a) In the top frame, on mouse-over on the link **Portal**, click on the **About** link that will be displayed.
- b) A pop-up window with the build information will be displayed.

**8. Build Verification**

The build version should display “Portal 10.2.0-X.Y.Z”. Where 10.2.0-X.Y.Z should be the new build number.

**9. Check Oracle Enterprise manger connection**

- a) From Internet Explorer, connect to the following URL:  
<https://192.168.1.1:1158/em/>  
where 192.168.1.1 is the IP of the Management server (in case of One-box configuration)
- b) You should be prompted to log in to work with the Enterprise manager.  
Connect with User **nsp**.

Refer section 5.4.1 for Management Server on TPD.

**5.4.1 Post Upgrade One-Box**

1. Open a terminal window and log in as root on the Management One-box.

2. As root, run:

```
# /opt/nsp/scripts/procs/post_upgrade_sanity_check.sh
```

**Note:** When user will execute this script it will automatically accept the upgrade.

3. Review the Management installation logs ( /var/log/nsp/install/nsp\_install.log).

Verify the following:

- Port 80 connectivity is OK
- Oracle server health is OK
- WebLogic health for ports 5556, 7001, 8001 is OK
- Oracle em console connectivity is OK
- The disk partition includes the following lines, depending on whether rackmount or blades setup:
- If rackmount, the output contains the following lines:

```
/dev/sdc1          275G  4.2G  271G   2% /usr/TKLC/oracle/ctrl1
/dev/sdb1          825G  8.6G  817G   2% /usr/TKLC/oracle/oradata
/dev/sdd1          275G  192M  275G   1% /usr/TKLC/oracle/backup
```

**Note:** The lines must begin with the /dev/cciss/c1d\*p1 designations; the remaining portion of the lines may differ.

- If blades, output contains following lines:

```
/dev/mapper/nsp_redo_vol 69G 4.2G 61G 7% /usr/TKLC/oracle/ctrl1
/dev/mapper/nsp_data_vol 413G 76G 316G 20% /usr/TKLC/oracle/oradata
/dev/mapper/nsp_backup_vol 138G 9.2G 121G 8% /usr/TKLC/oracle/backup
```

**5.5 Management Backup**

Refer section 5.4 Management Server Backup from [PIC 10.2 Upgrade Guide](#), doc ID E60676.

**Note:** For incremental upgrade, please ignore the step to disable crontab entry for launch\_pic\_global\_backup.sh.

Revoke the root ssh access by executing following as root user on TPD based server.



```
# /usr/TKLC/plat/sbin/rootSshLogin --revoke
```

Execute step 12.5.1 to revoke DBA privileges to Management from [PIC 10.2 Maintenance Guide](#), doc ID E60679

## **5.6 Upload Mediation Protocol ISO to Management**

Refer section 5.5 Upload xDR Builder ISO to Management Server from [PIC 10.2 Upgrade Guide](#), doc ID E60676.

## 6 Acquisition Incremental Upgrade

### 6.1 Acquisition Upgrade

**Note:** 1. Please perform step2 using ILO or any non-disconnectable media.

2. In case of TPD 5.5, the early checks may fail if the upgrade is not attempted from the non disconnectable media, so before attempting the next upgrade remove the “UNKNOWN” entry from “/usr/TKLC/plat/etc/platform\_revision” file.

#### 1. Copy ISO image to the server

Copy ISO image to the /var/TKLC/upgrade directory of the server.

#### 2. Upgrade the server

- a) As root on the Acquisition server
- b) Enter platcfg configuration menu
- c) Navigate to Maintenance > Upgrade
- d) Select Initiate Upgrade
- e) Select the desired upgrade media

```
# su - platcfg
```

#### 3. Upgrade completed

The server will reboot and after the reboot, login prompt will be displayed.

#### 4. Check the log

- a) In platcfg navigate to Diagnostics > View Upgrade Logs > Upgrade Log
- b) Check on the bottom of the file the upgrade is complete

### 6.2 Sync Management with Acquisition

#### 1. Apply Changes Acquisition

- a) To Apply Changes for each subsystem go to **Acquisition** **⊙ Sites** **⊙ XMF**.
- b) Right click on subsystem and click on **Apply Changes** option on menu.

#### 2. Test the VIP function.

- a) After sync from Management, the VIP will be available to access the active master server in the site. In order to verify the VIP setup please login to any server in the subsystem and execute the `iFoStat` command. As `cfguser` run:

```
$ iFoStat
```

Example of correct output:

```
query 10.236.2.79 for failover status
```

```
+-----+-----+-----+-----+-----+-----+-----+
| name   | state | loc  | role      | mGroup  | assg  | HbTime                |
+-----+-----+-----+-----+-----+-----+-----+
IMF-1a	IS	1A	ActMaster	sde_m2pa	8	2009-06-19 23:14:08
IMF-1b	IS	1B	StbMaster	sde_stc	6	2009-06-19 23:14:06
IMF-1c	IS	1C	Slave		0	2009-06-19 23:14:06
+-----+-----+-----+-----+-----+-----+-----+
```

- b) The state should be 'IS' for all servers and the HbTime time should be updated every few seconds.

## 7 Mediation Incremental Upgrade

### 7.1 Mediation Subsystem Upgrade

This procedure describes the Mediation application incremental upgrade procedure. Be aware of each step. The Mediation incremental upgrade is executed on each server in the subsystem in parallel. The parallel Mediation subsystem incremental upgrade is triggered from one server in the subsystem; it cannot be triggered more than once per subsystem. The upgrade must be triggered from any connectable medium or using ILO.

#### 1. Permit root ssh login

**On each Mediation server permit root ssh login.**

a) As `root` run:

```
# /usr/TKLC/plat/sbin/rootSshLogin --permit
```

#### 2. Distribute the Mediation ISO

**Note:** Choose one of the servers in the subsystem. From this server you will trigger the parallel Mediation subsystem incremental upgrade.

a) Distribute the Mediation ISO file to `/var/TKLC/upgrade` directory.

a. On the rack mount server copy the Mediation ISO into the `/var/TKLC/upgrade` using the `scp` command.

b. On the c-class blade server download the Mediation ISO from the PM&C ISO repository. ISOs are available on the PM&C server under the `/var/TKLC/smac/image` directory. Store the ISO file to `/var/TKLC/upgrade` directory. If the Mediation ISO is not present in the PM&C ISO repository add the ISO file using the Section 8.4 from [PIC 10.2 Upgrade Guide](#) doc ID E60676.

#### 3. Run parallel Mediation subsystem upgrade

**Note:** Run this step on where server where you distributed the Mediation ISO. This step will trigger the parallel incremental upgrade on all servers in the subsystem.

b) As `root` run:

```
# misc_upgrade_subsystem.sh -i iso_filename
```

where `iso_filename` is the name of the Mediation ISO file that has been previously distributed on this server.

c) You will be prompted to confirm the upgrade; then, you will be asked to enter the root password. The incremental upgrade is triggered on all the servers of the subsystem.

#### 4. Monitor parallel Mediation incremental upgrade

**Note:** The whole subsystem is upgrading now. Keep logged on the server where you have triggered the parallel upgrade, as you will see the progression. The server will reboot after successful upgrade.

a) Once the server where you have triggered the parallel upgrade is accessible again, start monitoring script: it will apply some subsystem post-upgrade settings, after all the servers have successfully upgraded (and rebooted). As `root` run:

```
# misc_upgrade_subsystem.sh --postsync
```

b) You will see the regular monitoring of the upgrade progress. Keep this script running and look for successfully upgraded servers. **Do not interrupt** the script. Wait until the results of upgrade are shown and synchronization is restored. Monitor the script output for any errors. The logs for the upgrade must be verified at `/var/TKLC/log/upgrade/upgrade.log` on the server from where the upgrade is triggered. If any error appears contact Oracle Support [Error! Reference source not found. Error! Reference source not found.](#) The script will only finish once all servers in the subsystem have finished the upgrade.

#### 5. Discover Mediation application in Centralized Configuration

This procedure describes how to discover Mediation application in the Management

Centralized Configuration application.

Discover all Mediation servers in Centralized Configuration application.

- a) Open a web browser and go to the Management application interface main page.
- b) Click Centralized Configuration.
- c) Navigate to **Equipment registry** view.
- d) Open **Sites**, open the site, open **IXP** and then click on the particular Mediation subsystem.
- e) The list of all Mediation servers in the Mediation subsystem will appear. Check the check box of the first server and click the **Discover Applications** button. Wait until the Mediation application will be discovered. Then repeat this step for all servers in the subsystem.
- f) Navigate to Mediation and Apply the changes on the Mediation subsystem.

## 6. Revoke root ssh login

On each Mediation server revoke root ssh login.

- a) As root run:

```
# /usr/TKLC/plat/sbin/rootSshLogin --revoke
```

## 7.2 Upgrade DTO Package

Refer section 7.8 Upgrade DTO Package from [PIC 10.2 Upgrade Guide](#), doc ID E60676.

## 7.3 Centralized Mediation Protocol Upgrade

This procedure describes how to trigger the Mediation Protocol installation on the Mediation subsystem from the Centralized Configuration. Login in the Centralized Configuration as TklcSrv user and go to the upgrade utility. It is **recommended to proceed with this step after each Mediation subsystem upgrade**, and not to wait all subsystem are upgraded to install all at the same time.

**Note:** In order to avoid installation issues login on each Mediation server as cfguser and execute the command:

```
$ iaudit -cvf
```

### 1. Associate Mediation Protocol RPM with the Mediation subsystem

- a) Click on **View Builder RPM Status** link on the left tree. This will display a list of all Mediation subsystems.
- b) Before initiating the Mediation Protocol association, make sure the supported platform of the Mediation Protocol RPM is in accordance with the platform architecture of the Mediation subsystem you want to associate it with.
- c) Choose one or more Mediation subsystems and click on **Associate RPM Package** icon in the tool bar. This will show a popup containing the list of Mediation Protocol RPMs that are uploaded in Management.
- d) Select required Mediation Protocol RPM and click on the **Associate** button.
- e) After the successful association the list of the subsystems will be updated. The **RPM Name** column will contain the new RPM package name and **Association Status** will be marked as OK.

### 2. Apply the configuration to the Mediation subsystem

- a) Go to the Management application interface main page.
- b) Click **Centralized Configuration**.
- c) Navigate to the **Mediation** view.
- d) Open **Sites**, open the site, and open **Mediation**.
- e) Right-click on the subsystem and click on **Apply changes...** from popup menu.
- f) Click **Next** button
- g) Click **Apply Changes** button.
- h) Wait until changes are applied and check there's no error.

Check there's no error in the result window.

### 3. Install Mediation Protocol RPM on Mediation

- a) Login to **the Management application** interface as the TkIcSrv user.
- b) Click **Upgrade Utility**.
- c) Click on **View Builder RPM** Status from the left tree.
- d) This will display all the available Mediation subsystem with their respective RPM **Associate Status** and **Install Status**.
- e) Before initiating the Mediation Protocol installation make sure the Mediation Protocol RPM that you want to install on the Mediation subsystem is associated with the Mediation subsystem as indicated by **RPM Name** column and **Association Status** should be OK and **Install Status** should be either - or **Not Started**.
- f) Select one or more Mediation subsystem and choose **Install RPM Package** from the tool bar.
- g) After the successful installation the **Install status** will change to OK.

### 4. Session Upgrade

- a) Go back to Management application interface main page.
- b) Click **Upgrade Utility**.
- c) Click **Upgrade Session** link on left tree, this display all the sessions to be upgraded due to upgrade of associated dictionary.
- d) Select one or more session(s) (use ctrl key for selecting multiple sessions) with **Session Upgrade Status** as either **Need Upgrade** or **Error** and choose **Upgrade** icon from tool bar. You may use available quick filter options on this list page to filter out sessions which you want to upgrade in one go.  
Caution: Do not choose more than 5 sessions to be upgraded in one go.  
Once upgrade is initiated for a session, its **Upgrade Status** will become **Upgrade Initiated**.
- e) Once session is upgraded its **Upgrade Status** will become **Upgraded Successfully**.

### 5. Exceptions


After successful completion of Mediation Protocol Upgrade procedure:

- a) Datafeed should be verified to check if they are using either Deprecated or Removed Field and should be upgraded separately.
- b) KPI based reports should be verified to check if they are using either Deprecated or Removed Field and should be upgraded separately.
- c) Static enrichment if any configured should be verified to check if they are using either Deprecated or Removed Field and should be upgraded separately.
- d) Update the Mediation license if needed and recreate the Mediation session for the obsolete Mediation Protocol

## 7.4 Unset Configuration on Management (onebox)

Unset configuration application access restriction automatically set during Management upgrade by performing the below steps.

**Note:** Configuration application are automatically restricted to TkIcSrv and tekelec user during Management upgrade. After required reconfiguration, Management shall return to normal.

1. **Open a web browser and log in to the NSP application interface as TkIcSrv user.**
2. **Navigate to security application  Filter access**
3. **Select None for Restricted configuration setting.**
4. **Apply modification.**

## Appendix A. 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 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

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

## Appendix B. Locate Product Documentation on the Oracle Technology Network 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 [www.adobe.com](http://www.adobe.com).

1. Access the **Oracle Help Center** site at <http://docs.oracle.com>.
2. Click **Industries** icon.
3. Under the **Oracle Communications** heading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Go to the **Network Visibility and Resource Management** section.
4. Click on **Performance Intelligence Center** and then the release number. A list of the entire documentation set for the selected release appears.
5. To download a file to your location, right-click the **PDF** link and select Save Target As (or similar command based on your browser), and save to a local folder.

**Note:** As long as the documentation site has not been significantly refactored, you can use this link as a shortcut to step 4: <http://docs.oracle.com/en/industries/communications/performance-intelligence-center/index.html>