Oracle® Communications
Diameter Signaling Router

DSR Cloud Software Upgrade Guide

Release 7.3

E76625 , Revision 01

September 2016

ORACLE

Oracle® Communications Diameter Signaling Router, DSR Cloud Software Upgrade Guide, Release 7.3

CAUTION: Use only the upgrade procedure included in the Upgrade Kit.
Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

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. Refer to Appendix J for instructions on accessing this site.

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

LIST OF FIGURES

List of Tables

List of Procedures

This page intentionally left blank.

1 INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform the following upgrades:

- Major upgrade from DSR 7.0.1, 7.1.x, or 7.2 to 7.3
- Incremental upgrade from an earlier DSR 7.3 release to a later 7.3 release

The upgrade of cloud deployments is covered by this document. The audience for this document includes Oracle customers as well as following internal groups: Software Development, Quality Assurance, Information Development, and Consulting Services including NPx. This document provides step-by-step instructions to execute any incremental or major cloud software upgrade.

The execution of this procedure assumes that the target DSR software load (ISO file, CD-ROM or other form of media) has already been delivered to the customer's premises. This includes delivery of the software load to the local workstation being used to perform this upgrade.

1.1.1 What is Not Covered by this Document

The following items are beyond the scope of this document. Refer to the specified reference for additional information.

- Distribution of DSR 7.3 software loads. It is recommended to contact MOS for the software loads as described in Appendix J
- Initial installation of DSR software. Refer to [1]
- SDS upgrade. Refer to [2]

1.2 References

[1] *DSR 7.2/7.3 Cloud Installation Guide, E64814, Oracle*
[2] *SDS 7.3 Upgrade document. E76623, Oracle*
[3] *Maintenance Window Analysis Tool CGBU_010314, Oracle*
[4] *IPFE Feature Activation and Configuration, CGBU_694, Oracle*
[5] *DSR 6.0 to 7.0 Migration – IPFE Aspects, CGBU_770, Oracle*
[6] *Fast Deployment and Configuration Tool Technical Reference, CGBU_ENG_24_2353, Oracle*
[7] *Cloud DSR 7.3 Disaster Recovery Guide, E64815, Oracle*

1.3 Acronyms

Table 1: Acronyms

CD-ROM	Compact Disc Read-only Media
CPA	Charging Proxy Agent
CSV	Comma-separated Values
cSBR	Charging Session Binding Repository
DA	Diameter Agent
DA MP	Diameter Agent Message Processor
DB	Database
DP	Data Processor
DR	Disaster Recovery
DSR	Diameter Signaling Router
FABR	Full Address Based Resolution
FOA	First Office Application
GA	General Availability
GPS	Global Product Solutions

Table 1: Acronyms

GUI	Graphical User Interface
HA	High Availability
IDIH	Integrated Diameter Intelligence Hub
IMI	Internal Management Interface
IP	Internet Protocol
IPM	Initial Product Manufacture
IPFE	IP Front End
ISO	ISO 9660 file system (when used in the context of this document)
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
MW	Maintenance Window
NE	Network Element
NOAM	Network OAM
OAM	Operations, Administration and Maintenance
OFCS	Offline Charging Solution
PCA	Policy and Charging Agent (formerly known as PDRA)
PDRA	Policy Diameter Routing Agent
SBR	Session Binding Repository
SDS	Subscriber Database Server
SOAM	System OAM
TPD	Tekelec Platform Distribution
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
XMI	External Management Interface
XSI	External Signaling Interface

1.4 Terminology

This section describes terminology as it is used within this document.

Table 2: Terminology

Upgrade	The process of converting an application from its current release on a system to a newer release.
Major Upgrade	An upgrade from one DSR release to another DSR release. E.g. DSR 7.1.x to DSR 7.3.
Incremental Upgrade	An upgrade within a given DSR release e.g. 7.3.x to 7.3.y.
Release	Release is any particular distribution of software that is different from any other distribution.
Single Server Upgrade	The process of converting a DSR 7.0.1 server from its current release to a newer release.
Backout	The process of converting a single DSR 7.3 server to a prior version. This could be performed due to failure in Single Server Upgrade or the upgrade cannot be accepted for some other reason. Backout is a user initiated process.
Rollback	Automatic recovery procedure that puts a server into its pre-upgrade status. This procedure occurs automatically during upgrade if there is a failure.
Source release	Software release to upgrade from.
Primary NOAM Network Element	The network element that contains the Active and Standby NOAM servers in a DSR. In a 2-tier DSR, there is only a single network element, and it contains the NOAMs and all MPs. So this single network element is both the primary NOAM network element and the signaling network element. In a 3-tier DSR, there are more possible combinations.
Signaling Network Element	Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. In a 2-tier DSR, the signaling network element and the "site" are one and the same. In a 3-tier DSR, each SOAM pair and its associated C-level servers are considered a single signaling network element. And if a signaling network element includes a server that hosts the NOAMs, that signaling network element is also considered to be the primary NOAM network element.
Site	Physical location where one or more network elements reside. For a 2-tier DSR, the site is defined by the NOAM. For a 3-tier DSR, the site is defined by the SOAM.
Target release	Software release to upgrade to.
Health Check	Procedure used to determine the health and status of the DSR's internal network. This includes status displayed from the DSR GUI. This can be observed pre-server upgrade, in-progress server upgrade, and post-server upgrade.
Upgrade Ready	State that allows for graceful upgrade of a server without degradation of service. It is a state that a server is required to be in before upgrading a server. The state is defined by the following attributes: • Server is Forced Standby • Server is Application Disabled (signaling servers will not process any traffic)
UI	User interface. Platcfg UI refers specifically to the Platform Configuration Utility User Interface which is a text-based user interface.
1+1	Setup with one Active and one Standby server.
N+0	Setup with N active DA-MP(s) but no standby DA-MP.
NOAM	Network OAM for DSR.
SOAM	System OAM for DSR.
Migration	Changing policy and resources after upgrade (if required). For example, changing from 1+1 (Active/Standby) policy to N+ 0 (Multiple Active) policies.

Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware, and is not responsible for hardware installation, configuration, or maintenance.
Enablement	The business practice of providing support services (hardware, software, documentation, etc) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.

1.5 How to Use this Document

When executing the procedures in this document, there are a few key points which help to ensure that the user understands procedure convention. These points are:

1) Before beginning a procedure, completely read the instructional text (it will appear immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.

2) Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.

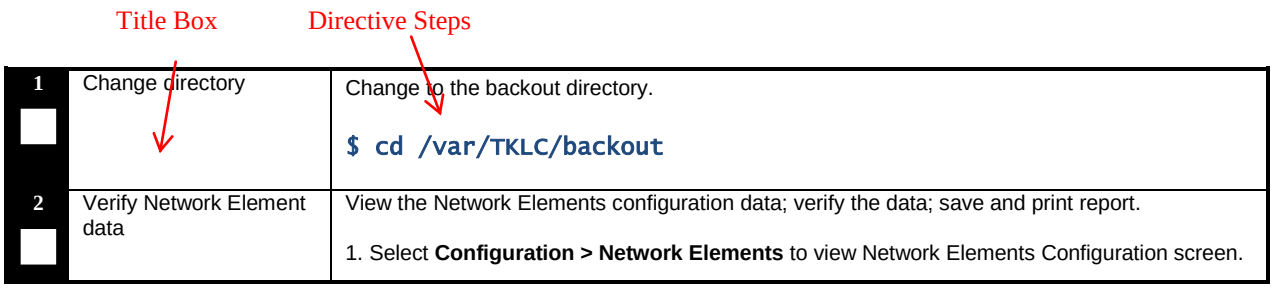
3) If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP. It is recommended to contact MOS for assistance, as described in Appendix J, before attempting to continue.

1.5.1 Executing Procedures

Figure 1 below shows an example of a procedural step used in this document.

- Each step has a checkbox that the user should check-off to keep track of the progress of the procedure.
- Any sub-steps within a step are referred to as Step X.Y. The example in Figure 1 shows Step 1 and Step 2.1 to Step 2.6.
- The title box describes the operations to be performed during that step
- GUI menu items, action links and buttons to be clicked on are in **bold Arial** font.
- GUI fields and values to take note of during a step are in **bold Arial** font.
- Each command that the user enters, as well as any response output, is formatted in `10-point bold Courier` font.

Figure 1. Example Procedure steps used in this document



1.6 Recommendations

This section provides some recommendations to consider when preparing to execute the procedures in this document.

1.6.1 Frequency of Health Checks

The user may execute the **Perform Health Check** or **View Logs** steps repetitively between procedures during the upgrade process. It is not recommended to do this between steps in a procedure, unless there is a failure to troubleshoot.

1.6.2 Large Installation Support

For large systems containing multiple Signaling Network Elements, it is impossible to upgrade multi-site systems in a single maintenance window.

1.6.3 Logging of Upgrade Activities

It is a best practice to use a terminal session with logging enabled to capture user command activities and output during the upgrade procedures. These can be used for analysis in the event of issues encountered during the activity. These logs should be saved off line at the completion of the activity.

1.7 Warnings, Cautions, and Notes

This section presents notices of warnings and cautions that directly relate to the success of the upgrade. It is imperative that each of these notices be read and understood before continuing with the upgrade. If there are any conflicts, issues, or questions related to these notices, it is recommended to contact MOS as directed in Appendix J before starting the upgrade.

1.7.1 PCA/PDRA Application – PCRF Pooling Migration Precheck

If the PCA application or the PDRA application has been activated in the source release, PCRF Pooling **MUST** be enabled, and the PCRF Pooling Migration **MUST** be completed prior to the start of a major upgrade to DSR 7.3.

!! WARNING!! **THE UPGRADE TO RELEASE 7.3 WILL FAIL IF PCRF POOLING MIGRATION IS NOT COMPLETED WHEN THE PCA/PDRA APPLICATION IS ENABLED**

The PCRF Pooling Migration Tool is provided to determine the status of the PCRF Pooling Migration. The tool has options to determine if the migration is complete, to indicate if upgrade is allowed or not allowed, and to estimate the time required to complete the Pooling migration.

The upgrade to DSR 7.3 CANNOT be scheduled until the PCRF Pooling Migration Tool is run to determine the status of the migration. Pooling migration can take days or weeks to complete, depending on the PCA/PDRA configuration and when PCRF Pooling was enabled.

When the tool determines that pooling migration is completed, a flag is set internally, which will allow the upgrade to proceed.

Refer to Appendix C: PCRF Pooling Migration Check for instructions on how to execute the PCRF Pooling Migration check.

The PCRF Pooling Migration Check is not required in the following scenarios:

1. The PCA/PDRA application has not been activated
2. When upgrading from release 7.1.x or 7.2 to 7.3 (in this case, pooling migration has already completed)
3. DSR 7.3 incremental upgrade.

1.7.2 Review Release Notes

Before starting the upgrade, it is recommended to review the Release Notes for the target release to understand the functional differences and possible traffic impacts of the upgrade.

2 GENERAL DESCRIPTION

This document defines the step-by-step actions performed to execute an upgrade of an in-service DSR from the source release to the target release. A major upgrade advances the DSR from source release 7.0.1, 7.1.x, or 7.2 to target release 7.3. An incremental upgrade advances the DSR from an earlier DSR 7.3 source release to a more recent 7.3 target release.

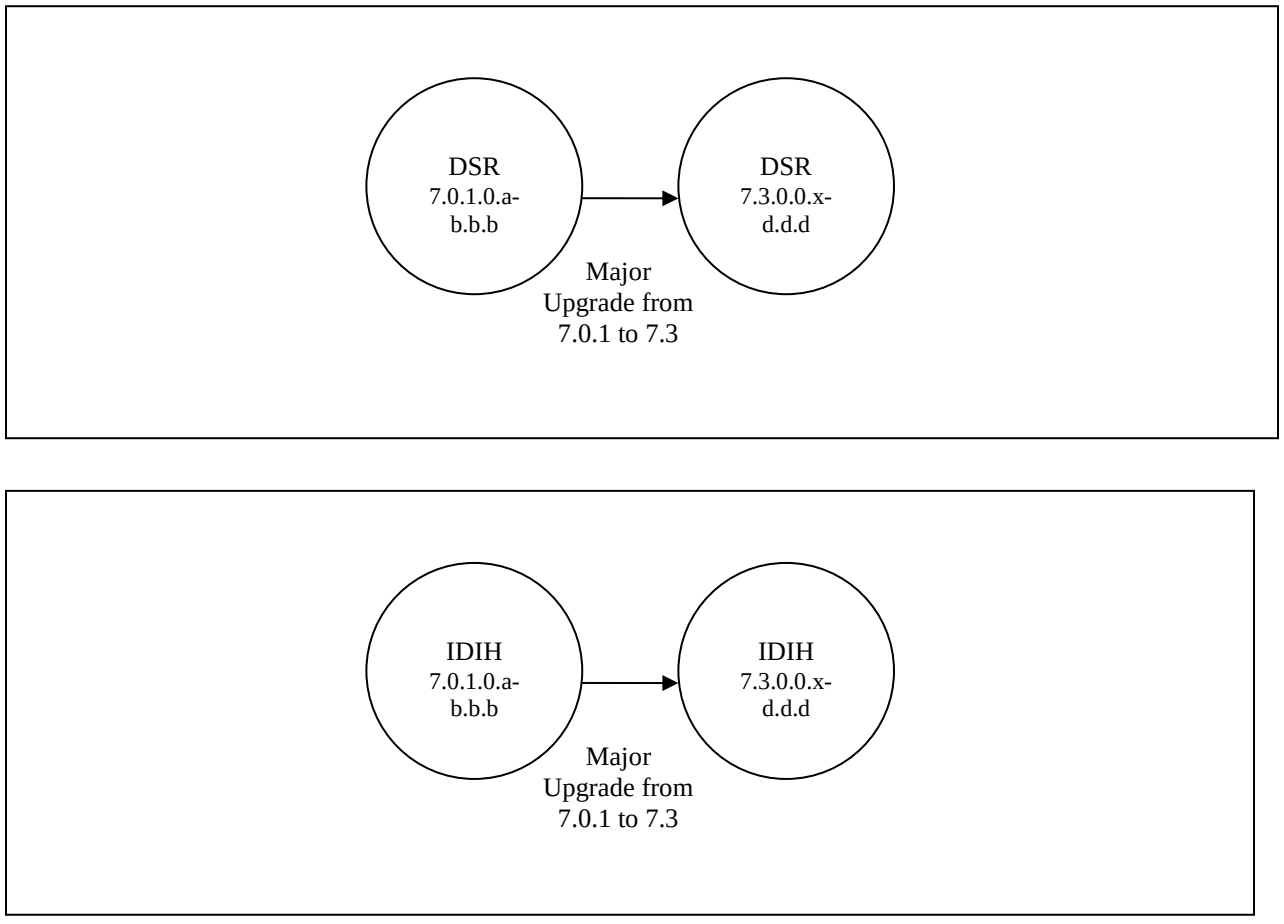
Note that for any incremental upgrade, the source and target releases must have the same value of "x". For example, advancing a DSR from 7.3.0.0.0-73.5.0 to 7.3.0.0.0-73.6.0 is an incremental upgrade. But advancing a DSR running a 7.0.1 release to a 7.3 target release constitutes a major upgrade.

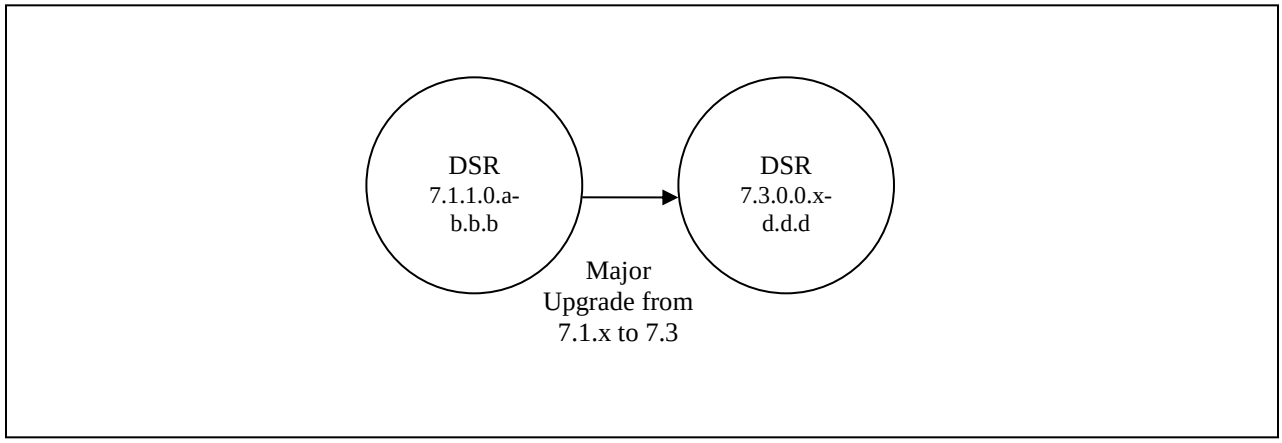
2.1 Supported Upgrade Paths to Release 7.3

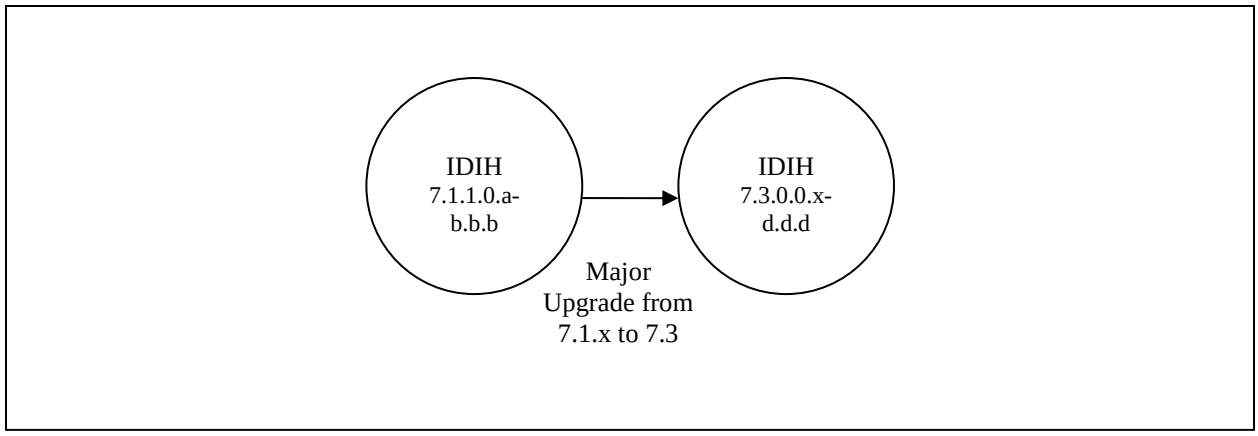
The supported paths to upgrade to a DSR 7.3 target release are shown in Figure 2 below.

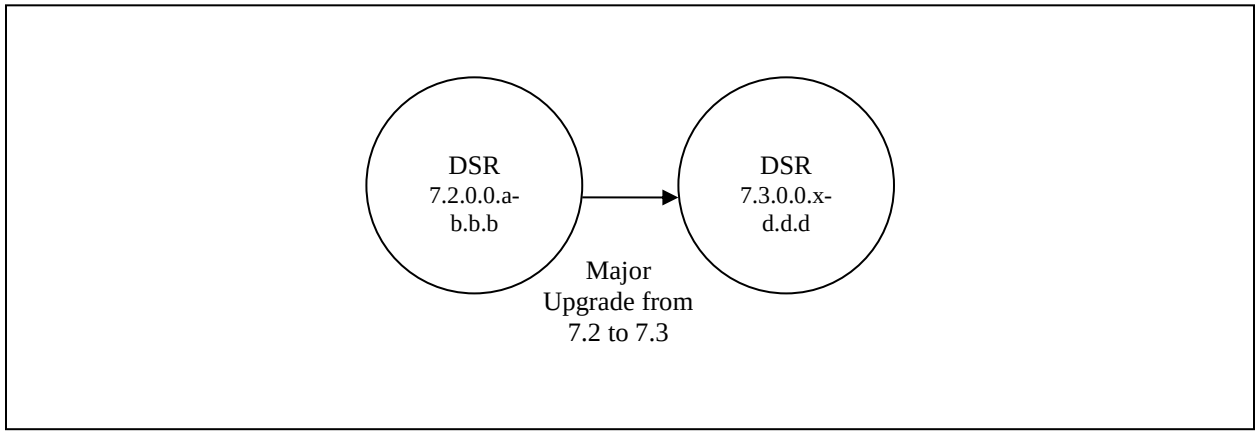
NOTE: DSR upgrade procedures assume the source and target releases are the GA or LA builds in the upgrade path.

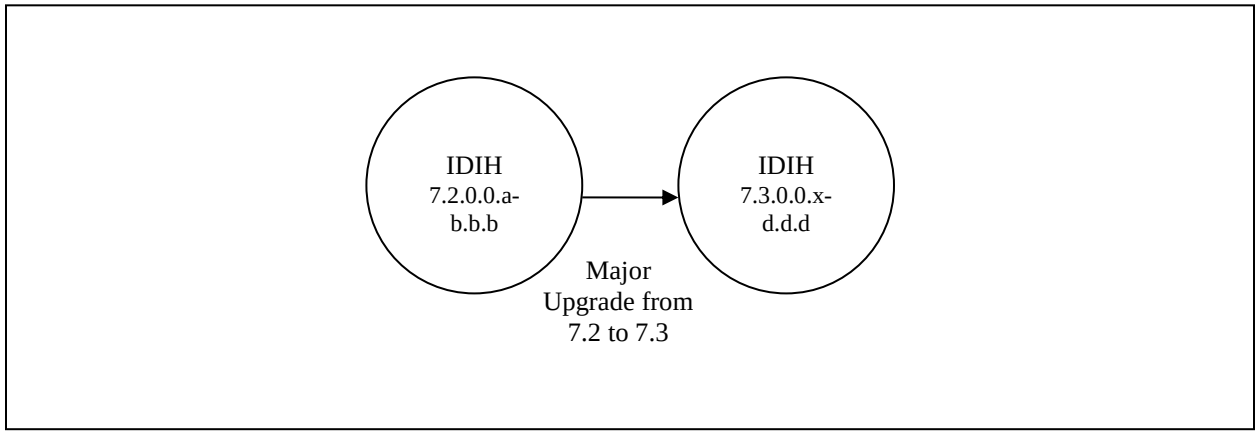
Figure 2. DSR 7.3 Supported Upgrade Paths

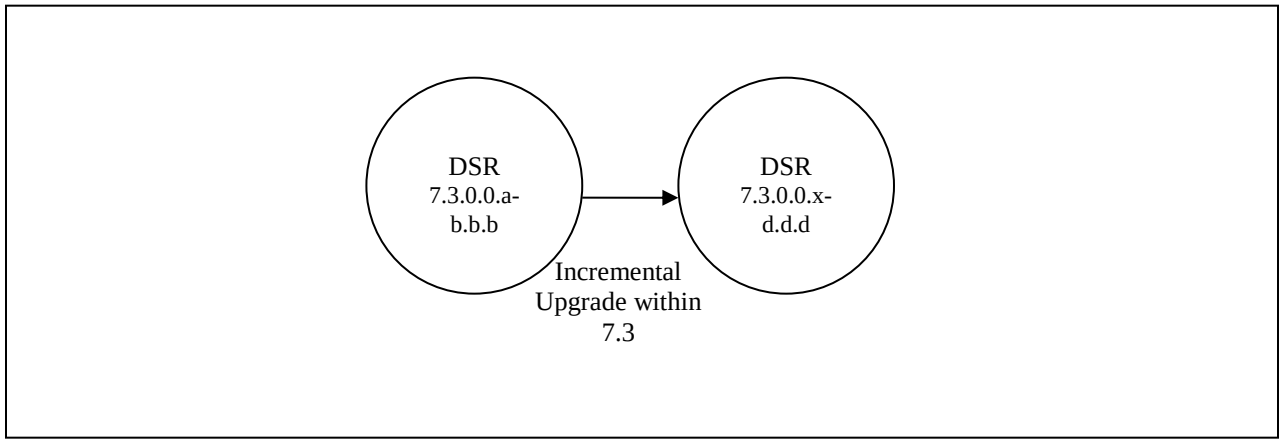



DSR
7.1.1.0.a-
b.b.b
DSR
7.3.0.0.x-
d.d.d
Major
Upgrade from
7.1.x to 7.3


IDIH
7.1.1.0.a-
b.b.b
IDIH
7.3.0.0.x-
d.d.d
Major
Upgrade from
7.1.x to 7.3


DSR
7.2.0.0.a-
b.b.b
DSR
7.3.0.0.x-
d.d.d
Major
Upgrade from
7.2 to 7.3





2.2 Geo-diverse Site (Active/Standby/Spare PCA configuration)

With a Geo-Diverse site, the upgrade of the SOAM Active/Standby servers must also include an upgrade of the Spare SOAM at the geo-redundant site, in the same maintenance window.

2.3 SDS Upgrade

It is recommended to upgrade the SDS topology (NOAMs, SOAMs, DPs) before the DSR topology. If this is not possible, then comAgent backward compatibility between the target and the source releases must be verified. comAgent is the process used to facilitate communication (Client/Server) between the SDS DP and the DA-MP on the DSR.

2.4 Traffic Management during Upgrade

Upgrade of NOAM and SOAM servers is not expected to affect traffic handling at the DA-MPs and other traffic-handling servers.

For the upgrade of the DA-MPs, traffic connections are disabled only for the servers being upgraded. The remaining servers continue to service traffic.

2.5 Automated Server Group Upgrade

The Automated Server Group (ASG) upgrade feature allows the user to automatically upgrade all of the servers in a server group simply by specifying a set of controlling parameters.

The purpose of ASG is to simplify and automate segments of the DSR upgrade. The DSR has long supported the ability to select multiple servers for upgrade. In doing so however, it was incumbent on the user to determine ahead of time which servers could be upgraded in parallel, considering traffic impact. If the servers were not carefully chosen, the upgrade could adversely impact system operations.

When a server group is selected for upgrade, ASG will upgrade each of the servers serially, or in parallel, or a combination of both, while enforcing a minimum service availability. The number of servers in the server group that are upgraded in parallel is user selectable. The procedures in this document provide the detailed steps for when to use ASG, as well as the appropriate parameters that should be selected for each server group type.

ASG is the default upgrade method for most server group types associated with the DSR. However, there are some instances in which the manual upgrade method is utilized. In all cases where ASG is used, procedures for a manual upgrade are also provided. **Note that in order to use ASG on a server group, no servers in that server group can be already upgraded – either by ASG or manually**.

DSR continues to support the parallel upgrade of server groups, including any combination of automated and manual upgrade methods.

2.5.1 Pausing, Restarting, and Canceling Automated Server Group Upgrade

When a server group is upgraded using ASG, each server within that server group is automatically prepared for upgrade, upgraded to the target release, and returned to service on the target release. Once an ASG upgrade is initiated, the task responsible for controlling the sequencing of servers entering upgrade can be paused, restarted, and even canceled from the **Status & Manage > Active Tasks** screen (Figure 3).

For example, in Figure 3, task ID #1 is an ASG task, while task ID #2 is the corresponding individual server upgrade task. When the ASG task is selected (highlighted in green), the Cancel and Pause buttons are enabled. When the ASG task is paused, the Restart and Cancel buttons are enabled. Pausing or canceling the ASG task affects only the ASG task. It has no effect on the individual server upgrade tasks that were started by the ASG task (i.e., task ID #2 in Figure 3).

When the ASG task is paused, it can be restarted by selecting the task and clicking the **Restart** button. When restarted, the ASG task will resume the process of initiating upgrade on the server group using the parameters that were initially selected.

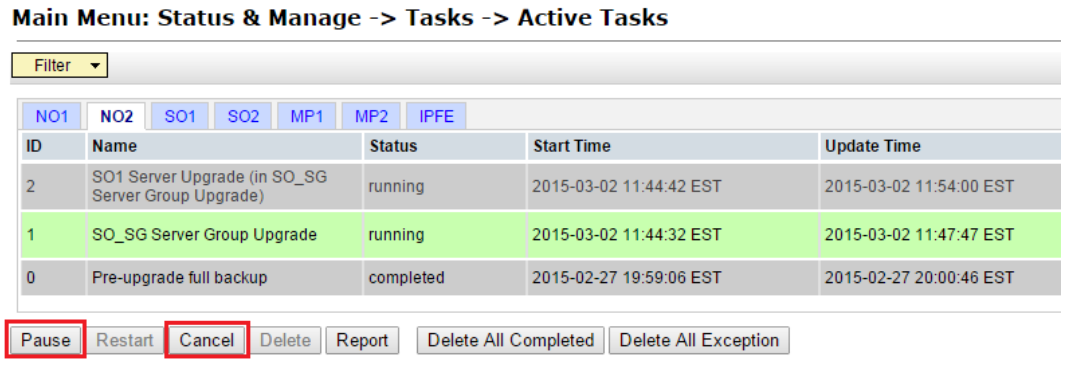


Figure 3. Active Tasks Screen

In the event that a server fails upgrade, that server will automatically roll back to the previous release in preparation for backout_restore and fault isolation. Any other servers in that server group that are in the process of upgrading will continue to upgrade to completion. However, the ASG task itself will pause and no other servers in that server

group will be upgraded. Pausing the ASG task provides an opportunity for troubleshooting to correct the problem. Once the problem is corrected, the server group upgrade can resume by restarting the paused ASG task. Note that the failed server will NOT be selected for upgrade upon resuming the ASG task.

If the user chooses to cancel the ASG task, the task will stop running and cannot be restarted. This means that the automated upgrade option will no longer be available for that server group. Any remaining servers in the affected server group must be upgraded manually.

3 UPGRADE PLANNING AND PRE-UPGRADE PROCEDURES

This section contains all information necessary to prepare for and execute an upgrade. The materials required to perform an upgrade are described, as are pre-upgrade procedures that should be run to ensure the system is fully ready for upgrade. Then, the actual procedures for each supported upgrade path are given.

There are overview tables throughout this section that help plan the upgrade and estimate how long it will take to perform various actions. The stated time durations for each step or group of steps are estimates only. Do not use the overview tables to execute any actions on the system. Only the procedures should be used when performing upgrade actions, beginning with Procedure 1. .

3.1 Required Materials and Information

The following materials and information are needed to execute an upgrade:

- Target-release application ISO image file or target-release application media.
- The capability to log into the DSR 7.x Network OAM servers with Administrator privileges**.**

  NOTE: All logins into the DSR NOAM servers are made via the External Management VIP unless otherwise stated.
- User logins, passwords, IP addresses and other administration information. See [Table 3**]**.
- VPN access to the customer's network is required if that is the only method to log into the OAM servers.

3.1.1 Application ISO Image File / Media

Obtain a copy of the target release ISO image file or media. This file is necessary to perform the upgrade.

The DSR ISO image file name will be in the following format (version will change from release to release):

DSR-7.1.1.0.0_71.28.0-x86_64.iso

NOTE: Prior to the execution of this upgrade procedure it is assumed that the DSR ISO image file has already been delivered to the customer's premises. The ISO image file must reside on the local workstation used to perform the upgrade, and any user performing the upgrade must have access to the ISO image file. If the user performing the upgrade is at a remote location, it is assumed the ISO file is already available before starting the upgrade procedure.

The ISO will be deployed as part of the pre-upgrade activities in Section 3.3.

3.1.2 Logins, Passwords and Server IP Addresses

Table 3 identifies the information that will be called out in the upgrade procedures, such as server IP addresses and login credentials. For convenience, space is provided in Table 3 for recording the values, or the information can be obtained by other means. This step ensures that the necessary administration information is available prior to an upgrade.

Consider the sensitivity of the information recorded in this table. While all of the information in the table is required to complete the upgrade, there may be security policies in place that prevent the actual recording of this information in hard-copy form.

Table 3: Logins, Passwords and Server IP Addresses

Item	Description	Recorded Value
Target Release	Target DSR upgrade release	
Credentials	GUI Admin Username[1] GUI Admin Password	
	DSR admusr Password[2]	
VPN Access Details	Customer VPN information (if needed)	
NOAM	XMI VIP address[2]	
	NOAM 1 XMI IP Address	
	NOAM 2 XMI IP Address	
SOAM	XMI VIP address	
	SOAM 1 XMI IP Address (Site 1)	
	SOAM 2 XMI IP Address (Site 1)	
	PCA (DSR) Spare System OAM&P server – Site 1 Spare in Site 2, XMI IP Address	
	SOAM 1 XMI IP Address (Site 2)	
	SOAM 2 XMI IP Address (Site 2)	
	PCA (DSR) Spare System OAM&P server – Site 2 Spare in Site 1, XMI IP Address	
Binding SBR Server Groups	Binding SBR SR1 Server Group Servers (Site 1)	
	Binding SBR SR2 Server Group Servers (Site 1)	
	Binding SBR SR3 Server Group Servers (Site 1)	
	Binding SBR SR4 Server Group Servers (Site 1)	
PCA MP Server Group	PCA MP Server Group Servers (Site 1)	
	PCA MP Server Group Servers (Site 1)	
IPFE Server Groups(For PDRA)	PCA IPFE A1 Server Group Server (Site 1)	
	PCA IPFE A 2 Server Group Server (Site 1)	
	PCA IPFE B 1 Server Group Server (Site 1)	
	PCA IPFE B 2 Server Group Server (Site 1)	
Binding SBR Server Groups	Binding SBR SR1 Server Group Servers (Site 2)	
	Binding SBR SR2 Server Group Servers (Site 2)	
	Binding SBR SR3 Server Group Servers (Site 2)	
	Binding SBR SR4 Server Group Servers (Site 2)	

[1] NOTE: The user must have administrator privileges. This means the user belongs to the **admin** group in Group Administration.
[2] NOTE: All logins into the NOAM servers are made via the External Management VIP unless otherwise stated.

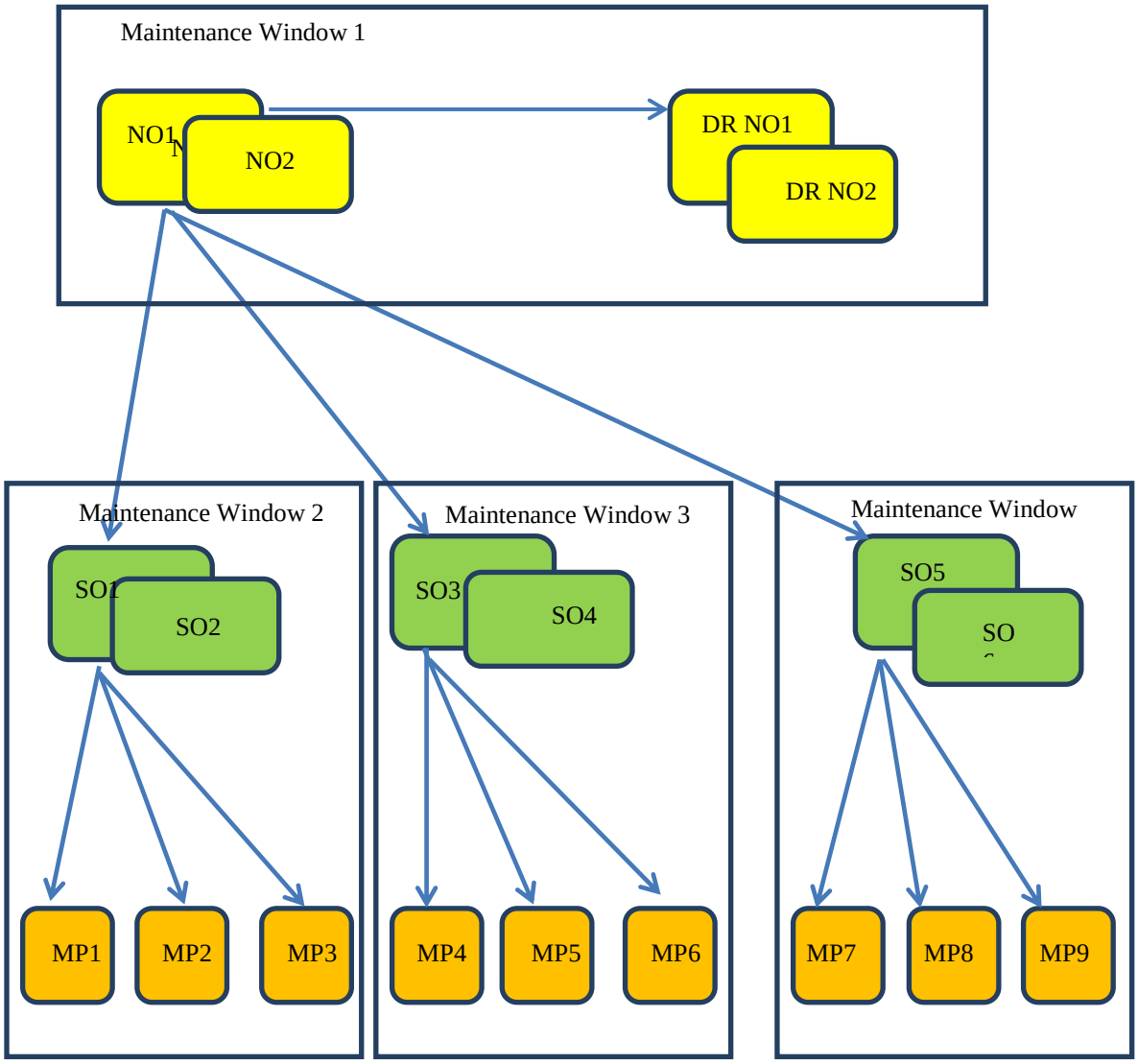
PCA MP Server Group	PCA MP Server Group Servers (Site 2)	
IPFE Server Groups (For PCA)	PCA IPFE A1 Server Group Server (Site 2)	
	PCA IPFE A 2 Server Group Server (Site 2)	
	PCA IPFE B 1 Server Group Server (Site 2)	
	PCA IPFE B 2 Server Group Server (Site 2)	
SS7-IWF Server Groups	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
	SS7-IWF Server Group Server	
Software	Target Release Number	
	ISO Image (.iso) file name	
Misc.[3]	Miscellaneous additional data	

[3] As instructed by Oracle CGBU Customer Service.

3.2 Plan Upgrade Maintenance Windows

This section provides a high-level checklist to aid in tracking individual server upgrades. The servers are grouped by maintenance window, and it is expected that all servers in a group can be successfully upgraded in a single maintenance window. Use this high-level checklist together with the detailed procedures that appear later in this document.

Figure 4. Upgrade Maintenance Windows for 3-Tier Upgrade



!! WARNING!! **MATED SOAM SITES MUST BE UPGRADED IN SEPARATE MAINTENANCE WINDOWS**

3.2.1 Calculating Maintenance Windows Required

The number of maintenance windows required for DSR setup and upgrade can be calculated by using the Maintenance Window Analysis Tool (see ref [3]).

This Excel spreadsheet takes setup details as input from the user and accordingly calculates the number of maintenance windows required for upgrade. The spreadsheet also specifies, in detail, which servers need to be upgraded in which maintenance window. Complete DSR upgrade maintenance window details and timings can be found in Reference [3]. Please see the instructions tab of the spreadsheet for more information and details.

3.2.2 Maintenance Window 1 (NOAM Site Upgrades)

During the first maintenance window, the NOAM servers are upgraded.

Maintenance Window 1 ***(NOAM Sites)*** **Date: _____** **NOTE 1:** *The* ***NE Name*** *may be viewed from the DSR NOAM GUI under* **[Main Menu → Configuration → Network Elements].**	1. Record the Site **NE Name** of the DSR NOAM to be upgraded during Maintenance Window 1 in the space provided below: 2. **"Check off"** the associated **Check Box** as upgrade is completed for each server. ☐ Primary Standby NOAM *(Guest)*: _____ ☐ Primary Active NOAM *(Guest)*: _____

3.2.3 Maintenance Window 2 and beyond (SOAM Site Upgrades)

During Maintenance Window 2, all servers associated with the first SOAM Site are upgraded. All servers associated with the second SOAM Site are upgraded during Maintenance Window 3.
For DSRs configured with multiple mated-pair Sites, or DSRs having multiple, distinct Sites (e.g. geo-redundant PCA installations), the following form should be copied and used for the subsequent SOAM Site upgrades.

It is strongly recommended that Mated pair SOAM Sites are NOT upgraded in the same Maintenance Window.

Maintenance Window ***(SOAM Sites)*** **Date: _____**	1. Record the Site **NE Name** of the DSR SOAM and the MP(s) to be upgraded during Maintenance Window 2 in the space provided. 2. **"Check off"** the associated **Check Box** as upgrade is completed for each server. SOAM Site: _____ ☐ Spare SOAM1 *(Guest)*: _____ *(If equipped)* ☐ Spare SOAM2 *(Guest)*: _____ *(If equipped)* ☐ Standby SOAM *(Guest)*: _____ ☐ Active SOAM *(Guest)*: _____
	☐ DA-MP1: _____ ☐ DA-MP2: _____ ☐ DA-MP3: _____ ☐ DA-MP4: _____ ☐ DA-MP5: _____ ☐ DA-MP6: _____ ☐ DA-MP7: _____ ☐ DA-MP8: _____ ☐ DA-MP9: _____ ☐ DA-MP10: _____ ☐ DA-MP11: _____ ☐ DA-MP12: _____ ☐ DA-MP13: _____ ☐ DA-MP14: _____ ☐ DA-MP15: _____ ☐ DA-MP16: _____

	☐ IPFE1: _____ ☐ IPFE2: _____ ☐ IPFE3: _____ ☐ IPFE4: _____
	☐ SS7-MP1: _____ ☐ SS7-MP2: _____ ☐ SS7-MP3: _____ ☐ SS7-MP4: _____ ☐ SS7-MP5: _____ ☐ SS7-MP6: _____ ☐ SS7-MP7: _____ ☐ SS7-MP8: _____

	Binding Server Group 1 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Binding Server Group 2 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Binding Server Group 3 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Binding Server Group 4 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Binding Server Group 5 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Binding Server Group 6 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Binding Server Group 7 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Binding Server Group 8 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)*

	Session Server Group 1 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Session Server Group 2 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Session Server Group 3 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Session Server Group 4 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Session Server Group 5 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Session Server Group 6 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Session Server Group 7 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)* Session Server Group 8 ☐ Standby SBR: _____ ☐ Active SBR: _____ ☐ Spare SBR1 *(Mate)*: _____ ☐ Spare SBR2 *(Mate)*: _____ *(If equipped)*

3.3 Prerequisite Procedures

The pre-upgrade procedures shown in the following table are executed outside a maintenance window, if desired. These steps have no effect on the live system and can save upon maintenance window time, if executed before the start of the Maintenance Window.

Table 4: Prerequisite Procedures Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cum.		
Procedure 1	0:10-0:30	0:10-0:30	Required Materials Check	None
Procedure 2	0:20-0:30	0:30-1:00	Verification of Configuration Data	None
Procedure 3 or Procedure 4 or Procedure 5	0:45-2:00 0:45-1:00 0:15-0:20	1:15-3:00 1:15-2:00 0:45-1:20	Data Collection for Source Release 7.0.1 Data Collection for Source Release 7.1.x Data Collection for Source Release 7.2 and later	None None None
Procedure 6	0:15-3:00	1:00-6:00	DSR ISO Administration	None
Procedure 7 or Procedure 8	0:10-2:00	1:10-8:00	Full Backup of DB Rbun Environment for Release 7.0.1 or Full Backup of DB Run Environment for Release 7.1.x and later	None None
Procedure 9	0:03-2:30	1:13-10:30	Network Interface Workaround	None

* ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. These factors may significantly affect total time needed, and may require the scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed prior to, and outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

3.3.1 Required Materials Check

This procedure verifies that all required materials needed to perform an upgrade have been collected and recorded.

Procedure 1. Required Materials Check

S T E P #	This procedure verifies that all required materials are present. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Verify all required materials are present	Materials are listed in Section 3.1: Required Materials. Verify required materials are present.
2 ☐	Verify all administration data needed during upgrade	Double-check that all information in Section 3.2 is filled-in and accurate.
3 ☐	Contact MOS	It is recommended to contact MOS and inform them of plans to upgrade this system. See Appendix J for these instructions. Note that obtaining a new online support account can take up to 48 hours.
THIS PROCEDURE HAS BEEN COMPLETED.		

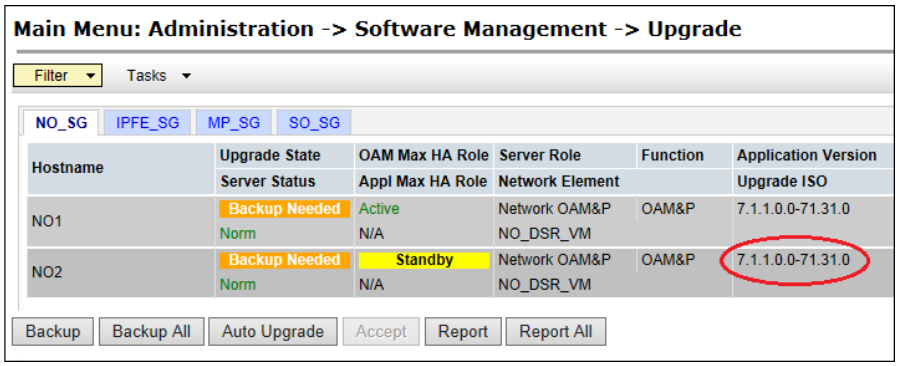
3.3.2 Data Collection - Verification of Global and Site Configuration Data

The procedures in this section are part of Software Upgrade Preparation and are used to collect data required for network analysis, Disaster Recovery, and upgrade verification. Data is collected from both the Active NOAM and various other servers at each site.

3.3.2.1 Verification of Configuration Data

This procedure checks the configuration data of the system and servers to ensure a successful upgrade.

Procedure 2: Verification of Configuration Data

S T E P #	This procedure checks the configuration data and server status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**Active NOAM VIP:**	1. Select **Administration > Software Management > Upgrade**. 2. Verify that the Upgrade path to the target release is supported as documented in **Section 2.1** *(Supported Upgrade Paths).* 3. Select the NOAM Server Group and verify the Application Version 
2 ☐	**Server CLI:** Check if the setup has customer supplied Apache certificate installed and protected with a passphrase.	1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active NOAM `ssh admusr@<NOAM_VIP>` (Answer 'yes' if you are prompted to confirm the identity of the server.) 2. cd to `/etc/httpd/conf.d` and open the file named `ssl.conf`. 3. Locate the line beginning with the phrase "`SSLCertificateFile`" 4. The path that follows "SSLCertificateFile" is the location of the Apache certificate. If the path is `/usr/TKLC/appworks/etc/ssl/server.crt`, then the certificate is supplied by Oracle and no further action is required. Continue with the next procedure. 5. If the path is anything other than `/usr/TKLC/appworks/etc/ssl/server.crt`, then a customer-supplied Apache certificate is likely installed. Rename the certificate to "server.crt-orig", but note the original certificate pathname. During the upgrade, the file "server.crt" will be overwritten, and will need to be restored in Section 5.6
	THIS PROCEDURE HAS BEEN COMPLETED.	

3.3.2.2 Data Collection for Source Release 7.0.1

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.0.1.

Procedure 3: Data Collection for Source Release 7.0.1

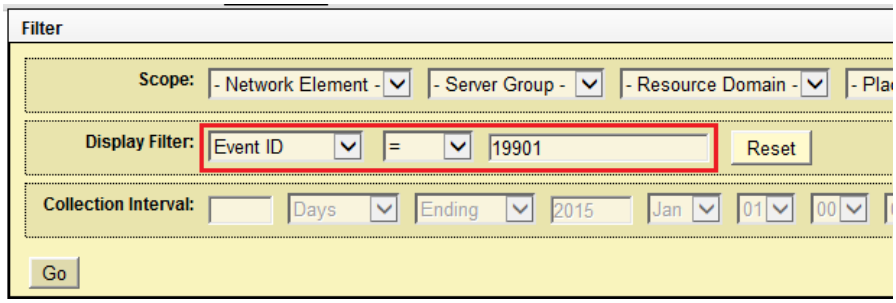
S T E P #	This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

1 ☐	**Active SOAM CLI**
	
	Database consistency check
		1. Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the Active SOAM:
		
		`ssh admusr@<SOAM_VIP>`
		
		Check the transport connections tables.
		
		2. Enter the following commands to count the number of entries in the ConnectionAdmin and TransportConnection tables.
		
		`iqt -zhp ConnectionAdmin | wc -l`
		`iqt -zhp TransportConnection | wc -l`
		
		Sample output:
		
		`[admusr@EVO-SO-1 ~]$ iqt -zhp ConnectionAdmin | wc -l`
		`7196`
		`[admusr@EVO-SO-1 ~]$ iqt -zhp TransportConnection | wc -l`
		`7196`
		
		3. If the entry counts match, **proceed to the next step**.
		
		If the ConnectionAdmin table entry count does not match the TransportConnection table entry count, DO NOT PROCEED WITH THE UPGRADE. It is recommended to consult with MOS before continuing.

2 ☐	**Server CLI:**
	
	Verify uptime for each server in the topology.
		1. Use the SSH command (on UNIX systems - or putty if running on windows) to login to each physical server in the topology using the server XMI IP Address.
		
		`ssh admusr@<target_server_XMI_IP>`
		
		(Answer 'yes' if you are prompted to confirm the identity of the server.)
		
		2. Execute the "uptime" command:
		
		`[admusr@ipfe-freeport-a1 ~]$ uptime`
		`02:02:49 up 27 days,6:48, 1 user,load average:0.87,0.99,0.83`
		`[admusr@ipfe-freeport-a1 ~]$`
		
		3. Record the hostname of any server with an "uptime" value > 200 days.
		
		4. Inform the customer that a "**Cold Reboot**" will be required for all servers with an "uptime" value > 200 days prior to beginning any upgrade activity.
		
		NOTE: ***This is required response due to Red Hat Bug 765720. It is recommended to contact MOS if instruction is needed on how to gracefully perform a "Cold Reboot".***

3 ☐	Repeat Port Check	Repeat steps 1 and 2 for each SOAM site in the topology.

Procedure 3: Data Collection for Source Release 7.0.1

4 ☐	**Active NOAM VIP:** Alarm Check	Check for the presence of alarm 19901 – CFG-DB Validation Error. From the Active NOAM GUI: 1. Navigate to **Alarms & Events > View Active**. 2. Click **Filter** to open the filter selection box. 3. Enter the following values and click **Go**.  4. If the filter returns no results, the database is consistent; proceed to the next step. **Otherwise, do not continue with the upgrade until the alarm is cleared.** It is recommended to consult with MOS for guidance if the alarm does not clear within 60 minutes.
5 ☐	**Active NOAM VIP:** Verify IPFE Server Groups	Verify the IPFE Server Groups are properly configured. 1. Login to the NOAM GUI using the VIP. 2. Navigate to **Configuration > Server Groups**. 3. Examine each IPFE Server Group. Verify that each IPFE Server Group is configured with one, **and only one**, IPFE server. 4. If any IPFE Server Group contains more than one IPFE server, refer to the Server Group Configuration procedure of [4] to correct the configuration.
6 ☐	**Active NOAM VIP:** Verify and collect Network Element Configuration data	1. Select **Configuration > Network Elements** to view Network Elements Configuration screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
7 ☐	**Active NOAM VIP:** Verify and collect Server Group Configuration data	1. Select **Configuration > Server Groups** to view the Server Group screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
8 ☐	**Active NOAM VIP:** Verify and collect Server Configuration data	1. Select **Configuration > Servers** to view the Server screen 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.
9 ☐	**Active NOAM VIP:** Verify and collect Services Configuration data	1. Select **Configuration > Services** to view Services screen. 2. Click **Report** at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference.

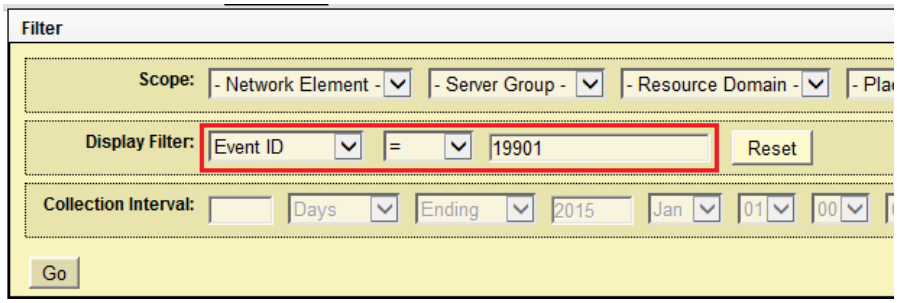
Procedure 3: Data Collection for Source Release 7.0.1

10 ☐	**Active NOAM VIP:** Verify and collect Signaling Network Configuration data for DSR	1. Select **Configuration > Network** to view the Signaling Networks. 2. Click "**Report**" at the bottom of the table to generate a report for all entries. 3. Verify the configuration data is correct for the network. 4. Save the report and/or print the report. Keep these copies for future reference. 5. Select **Configuration > Network > Devices**. 6. Click "**Report All**" at the bottom of the table to generate a report for all entries. 7. Save the report and/or print the report. Keep these copies for future reference. 8. Select **Configuration > Network > Routes**. 9. Click "**Report All**" at the bottom of the table to generate a report for all entries. Save the report and/or print the report. Keep these copies for future reference.
11 ☐	**Active NOAM VIP:** Verify Server Status is Normal - NOAM	1. Select **Status & Manage > Server.** The Server Status screen is displayed. 2. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). 3. Do not proceed with the upgrade if any server status displayed is not **Norm**. 4. Do not proceed if there are any Major or Critical alarms.
12 ☐	**Active NOAM VIP:** Log all current alarms at NOAM.	1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and/or print the report. Keep these copies for future reference. NOTE: It is not recommended to continue with the upgrade if any server status has unexpected values. An upgrade should only be executed on a server with unexpected alarms if the upgrade is specifically intended to clear those alarm(s). This would mean that the target release software contains a fix to clear the "stuck" alarm(s) and upgrading is the ONLY method to clear the alarm(s). Do not continue otherwise.
13 ☐	**Active NOAM VIP:** View Communication Agent status for all connections.	1. Select **Communication Agent > Maintenance > Connection Status;** The Communication Agent > Connection Status screen is displayed. 2. Verify the Connection Status of each connection is InService.
14 ☐	**Active NOAM VIP:** View SBR status (if equipped)	View SBR status if PDRA/PCA is enabled. **If the Active NOAM is on release 7.0.1, 7.1.x:** 1. Select **Policy and Charging > Maintenance > SBR Status** The SBR Status screen is displayed. 2. Select the **Binding** tab. 3. Expand each Server Group. 4. Verify Congestion Level is 'Normal' for all servers. 5. Repeat sub-steps 3 and 4 for the **PDRA Mated Triplet** tab. **If the Active NOAM is on release 7.2 and later:** 1. Select **SBR > Maintenance > SBR Status** The SBR Status screen is displayed. 2. Select the **Binding** tab. 3. Expand each Server Group. 4. Verify Congestion Level is '**Normal**' for all servers. 5. Repeat sub-steps 3 and 4 for the **PCA Mated Triple**t tab
15 ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP/IPFE/SBR/PCA which will be out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Steps 1 through 16. 2. It is recommended to plan for any MP upgrades by consulting MOS to assess the impact of out-of-service MP servers 3. Determine the exact sequence in which MP servers will be upgraded for each site.

3.3.2.3 Data Collection for Source Release 7.1.x

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.1.x.

Procedure 4: Data Collection for Source Release 7.1.x

S T E P #	This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**Active NOAM VIP:** Verify IPFE Server Groups	Verify the IPFE Server Groups are properly configured. **From the Active NOAM GUI:** 1. Login to the NOAM GUI using the VIP. 2. Navigate to **Configuration > Server Groups**. 3. Examine each IPFE Server Group. Verify that each IPFE Server Group is configured with one, **and only one**, IPFE server. If any IPFE Server Group contains more than one IPFE server, DO NOT PROCEED WITH THE UPGRADE. It is recommended to consult with MOS before continuing.
2 ☐	**Active NOAM VIP:** Alarm Check	Check for the presence of alarm 19901 – CFG-DB Validation Error. **From the Active NOAM GUI:** 1. Navigate to **Alarms & Events > View Active**. 2. Click **Filter** to open the filter selection box. 3. Enter the following values and click **Go**.  4. If the filter returns no results, the database is consistent; proceed to the next step. Otherwise, **do not proceed with the upgrade until the alarm is cleared**. It is recommended to consult with MOS for guidance if the alarm does not clear within 60 minutes.

Procedure 4: Data Collection for Source Release 7.1.x

3 ☐	**Active NOAM CLI:**
	
	Verify NOAM pre-Upgrade Status
		Execute the following commands on the Active DSR NOAM and Active DR NOAM servers.
		
		From the Active NOAM CLI:
		1. Use an SSH client to connect to the Active NOAM:
		
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: The static XMI IP address for each server should be available in Table 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck preUpgradeHealthCheck`
		
		This command creates files in `/var/TKLC/db/filemgmt/ UpgradeHealthCheck/` with the filename format:
		
		`<NOserver_name>_ServerStatusReport_<date-time>.xml`
		`<NOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		
		If there are alarms on the system:
		`<NOserver_name>_AlarmStatusReport_<date-time>.xml`
		
		If the system is PDRA:
		`<NOserver_name>_SBRStatusReport_<date-time>.xml`
		
		Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.
		
		3. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message. If the following message appears in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended to contact MOS for guidance.
		
		4. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

4 ☐	**Server CLI:**
	
	Verify uptime for each server in the topology
		1. Use the SSH command (on UNIX systems - or putty if running on windows) to login to each physical server in the topology using the server XMI IP Address.
		
		NOTE: ***The user is only required to login to the TVOE host for any OAM server (A / B level) but must log into all C level servers directly (MP, IPFE, etc.).***
		
		`ssh admusr@<target_server_XMI_IP>`
		
		(Answer 'yes' if you are prompted to confirm the identity of the server.)
		
		2. Execute the "uptime" command:
		
		`[admusr@ipfe-freeport-a1 ~]$ uptime`
		` 02:02:49 up 27 days,6:48, 1 user,load average:0.87,0.99,0.83`
		`[admusr@ipfe-freeport-a1 ~]$`
		
		3. Record the hostname of any server with an "uptime" value ≥ 200 days.
		
		4. Inform the customer that a **"Cold Reboot"** will be required for all servers with an "uptime" value ≥ 200 days prior to beginning any upgrade activity.
		
		NOTE: ***This is required response due to Red Hat Bug 765720. It is recommended to contact MOS if instruction is needed on how to gracefully perform a "Cold Reboot".***

Procedure 4: Data Collection for Source Release 7.1.x

5 ☐	**Active SOAM CLI:**
	Database consistency check
		Check the transport connections tables.
		
		From the Active SOAM CLI:
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active SOAM
		
		`ssh admusr@<SOAM_VIP>`
		
		(Answer 'yes' if you are prompted to confirm the identity of the server.)
		
		2. Enter the following commands to count the number of entries in the ConnectionAdmin and TransportConnection tables.
		
		`iqt -zhp ConnectionAdmin | wc -l`
		`iqt -zhp TransportConnection | wc -l`
		
		Sample output:
		
		`[admusr@EVO-SO-1 ~]$ iqt -zhp ConnectionAdmin | wc -l`
		`7196`
		`[admusr@EVO-SO-1 ~]$ iqt -zhp TransportConnection | wc -l`
		`7196`
		
		3. If the entry counts match, **proceed to step 6**.
		
		If the ConnectionAdmin table entry count does not match the TransportConnection table entry count, DO NOT PROCEED WITH THE UPGRADE. It is recommended to consult with MOS before continuing.

6 ☐	**Active SOAM CLI:**
	Log SOAM Alarm Status
		From the Active SOAM CLI:
		1. Use an SSH client to connect to the Active SOAM:
		
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: The static XMI IP address for each server should be available in Table 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck preUpgradeHealthCheckOnSoam`
		
		This command creates files in `/var/TKLC/db/filemgmt/ UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		
		If there are alarms on the system:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		
		Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. If the following message appears in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		
		3. Verify all Peer MPs are available
		4. Note the number of Total Connections Established _____
		
		5. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

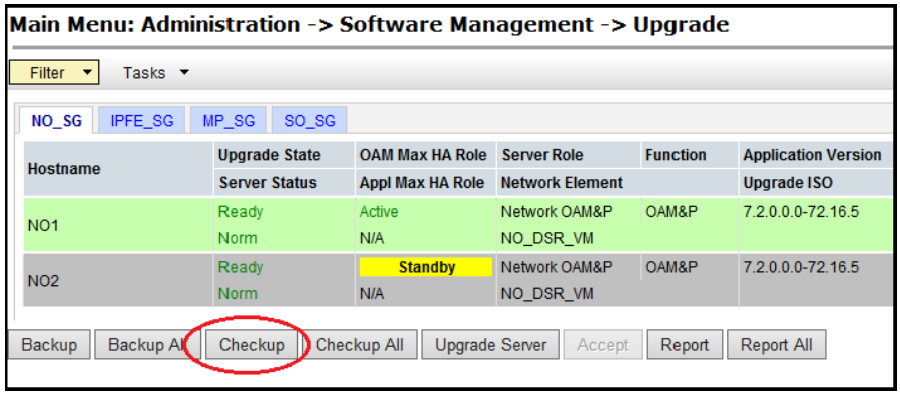
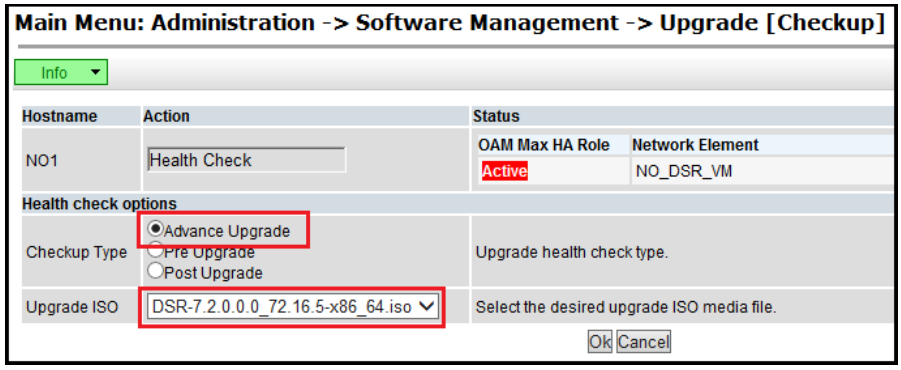
Procedure 4: Data Collection for Source Release 7.1.x

7 ☐	**Active SOAM CLI:** Verify PCA status (if equipped)	**From the Active SOAM CLI:** 1. Enter the command: `$ upgradeHealthCheck pcaStatus` This command outputs status to the screen for review. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify Operational Status is '**Available**' for all applications
8 ☐	Repeat for each Network Element	Repeat **Steps 5 - 7** for each SOAM site in the topology.
9 ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP/IPFE/SBR/PCA which will be out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Section 3.3.1 and steps 1 through 10 of this procedure. 2. It is recommended to plan for MP upgrades by consulting MOS to assess the impact of out-of-service MP servers 3. Determine the exact sequence in which MP servers will be upgraded for each site.
		THIS PROCEDURE HAS BEEN COMPLETED.

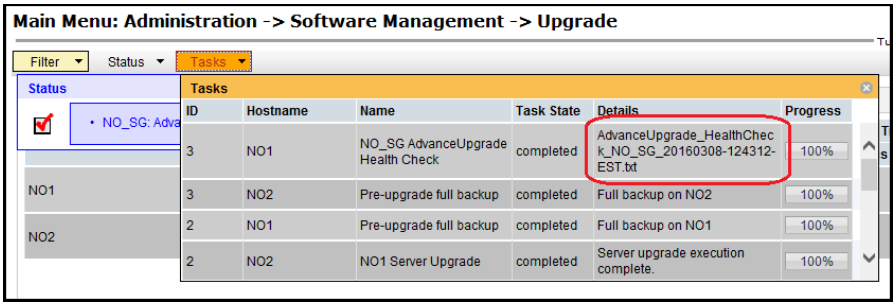
3.3.2.4 Data Collection for Source Release 7.2 and later

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 7.2 or later.

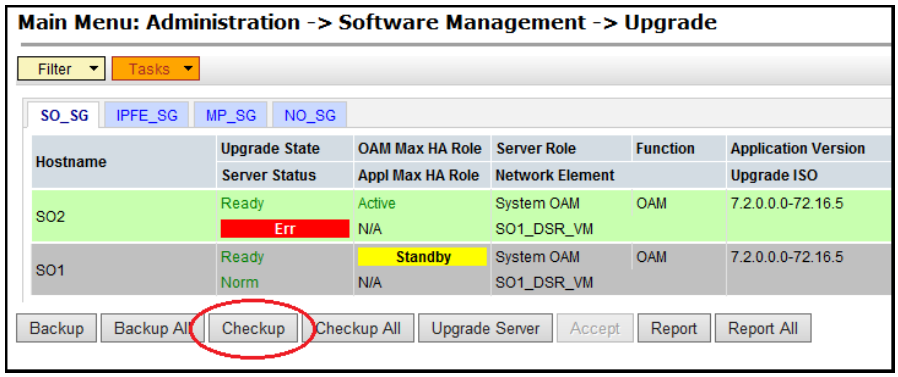
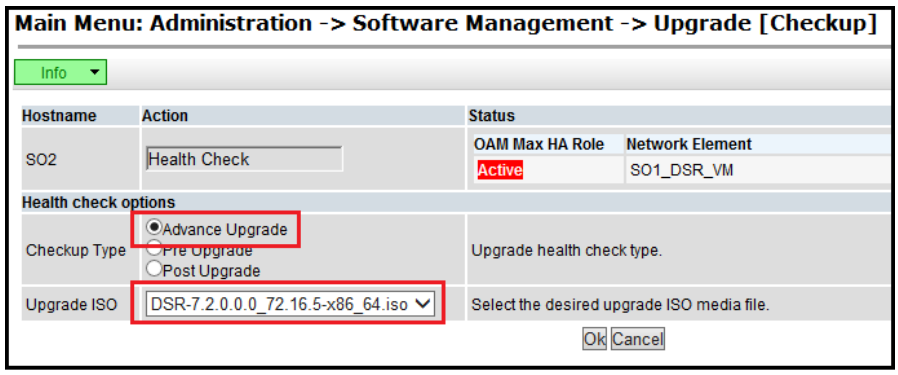
Procedure 5: Data Collection for Source Release 7.2 and later

S T E P #	This procedure retrieves and retains system status data for analysis and future use. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**Active NOAM VIP:** Initate NOAM health check	This procedure will run the automated Health Checks on the Active NOAM. 1. Select **Administration > Software Management > Upgrade**. The Upgrade screen is displayed. 2. Select the Active NOAM.  3. Click the **Checkup** button. The Upgrade [Checkup] screen is displayed. 4. In the 'Health check options' section, select the **Advance Upgrade** option. 5. If the ISO Administration procedure has already been performed for the target ISO, use the Upgrade ISO pulldown to select the target release ISO. Otherwise, do not select an ISO. 6. Click **Ok**. Control returns to the Upgrade screen. 

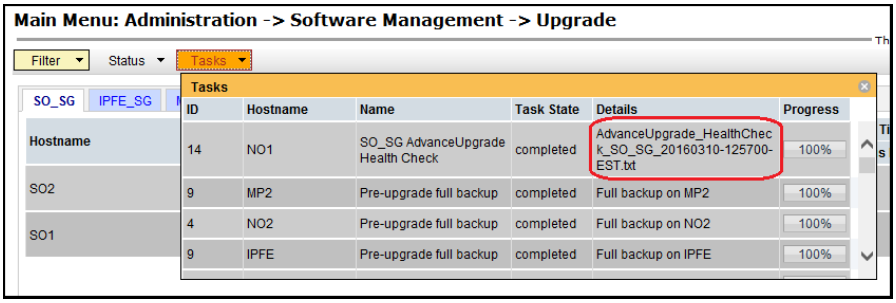
Procedure 5: Data Collection for Source Release 7.2 and later

2 ☐	**Active NOAM VIP:** Monitor health check progress	Monitor for the completion of the Health Check. 1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as <NOServerGroup> **AdvanceUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column will display a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. Open the report and review the results. 
3 ☐	**Active NOAM VIP:** Analyze any Health Check failure	If the Health Check report status is anything other than “Pass”, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the file named “UpgradeHealthCheck.log” and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix J.

Procedure 5: Data Collection for Source Release 7.2 and later

4 ☐	**Active NOAM VIP:** Initate SOAM health check	This procedure will run the automated Health Checks on the Active SOAM. 1. Select **Administration > Software Management > Upgrade**. The Upgrade screen is displayed. 2. Select the SOAM server group tab. 3. Select the Active SOAM.  4. Click the **Checkup** button. The Upgrade [Checkup] screen is displayed. 5. In the 'Health check options' section, select the **Advance Upgrade** option. 6. For a major upgrade, use the Upgrade ISO pulldown to select the target release ISO. Do not select an ISO for an incremental upgrade. 7. Click **Ok**. Control returns to the Upgrade screen. 

Procedure 5: Data Collection for Source Release 7.2 and later

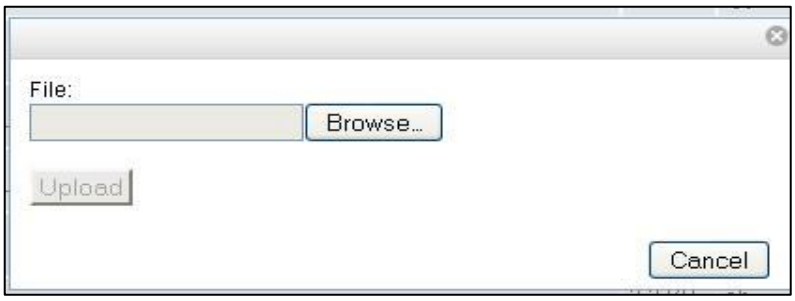
5 ☐	**Active NOAM VIP:** Monitor health check progress	Monitor for the completion of the Health Check. 1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as <SOServerGroup> **AdvanceUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column will display a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. Open the report and review the results. 
6 ☐	**Active NOAM VIP:** Analyze Health Check failure	If the Health Check report status is anything other than “Pass”, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the Active SOAM tab. 3. Select the file named “UpgradeHealthCheck.log” and click **View**. 4. Locate the log entries for the most recent health check. 5. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix J. If the health check log contains the message “Unable to execute Health Check on <Active NOAM hostname>”, perform health checks in accordance with Procedure 3 or Procedure 4, depending on the source release.
7 ☐	Analyze and plan MP upgrade sequence	From the collected data, analyze system topology and plan for any DA-MP / IPFE / SBR / PCA which will be out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Section 3.3.2.1 and steps 1 through 6 of this procedure. The Health Check reports from steps 3 and 6 can be found in **Status & Manage > Files** on the Active NOAM. 2. It is recommended to plan for MP upgrades by consulting MOS to assess the impact of out-of-service MP servers 3. Determine the manner in which the MP servers will be upgraded: Manually or Automated Server Group Upgrade. If the MPs will be upgraded manually, determine the exact sequence in which MP servers will be upgraded for each site.
		THIS PROCEDURE HAS BEEN COMPLETED.

3.3.3 DSR ISO Administration

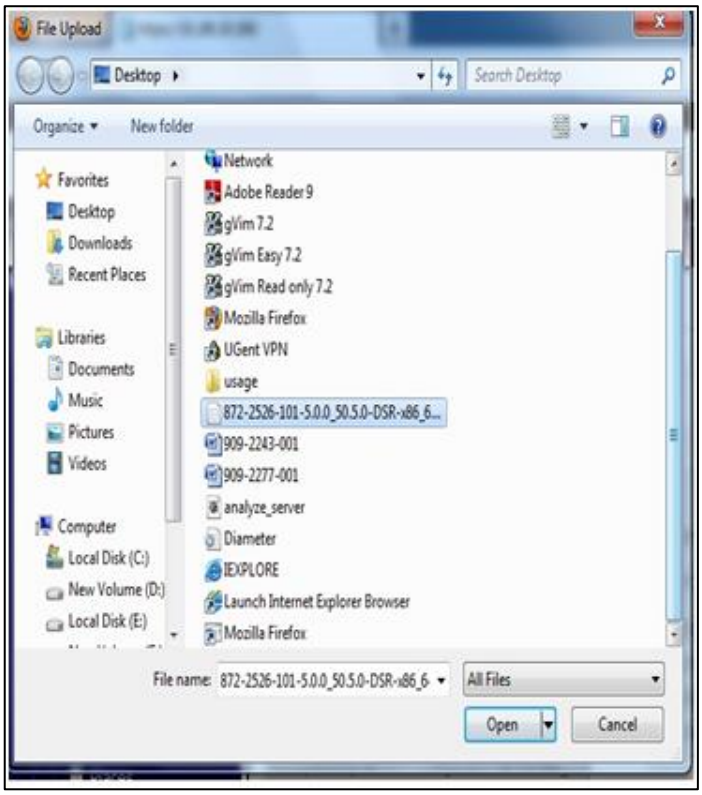
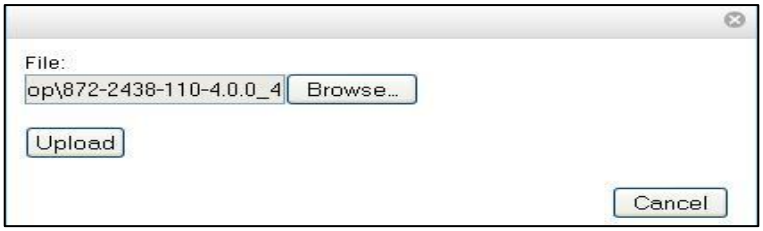
This section provides the steps to upload the new DSR ISO to the NOAMs and then transfer the ISO to all servers to be upgraded.

NOTE: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. These factors may significantly affect total time needed and require the scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed prior to, and outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

Procedure 6: DSR ISO Administration

S T E P #	This procedure verifies that ISO Administration steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**Active NOAM VIP:** Transfer via NOAM GUI	Use the NOAM GUI Upload function for ISO file transfer over the network Upload the target release ISO image file to the File Management Area of the Active NOAM server: 1. Log into the Active NOAM GUI. 2. Select **Status & Manage > Files** The Files menu is displayed 3. Click the Active NOAM server in the network. All files stored in the file management storage area of this server display on the screen. 4. Ensure that this is actually the Active NOAM server in the network by comparing the hostname in the screen title vs. the hostname in the session banner in the GUI. Verify that they are the same and the status is **ACTIVE** in the session banner. 5. Click the **Upload** button. The Browse window will open: 

Procedure 6: DSR ISO Administration

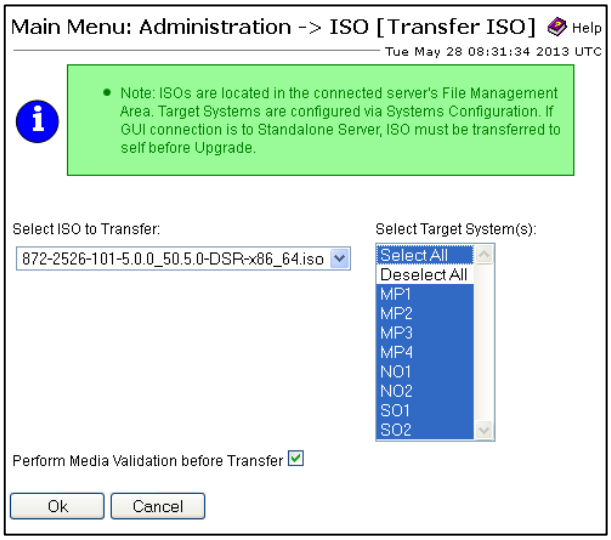
2 ☐	**Active NOAM VIP:**	1. **Browse** to select the file to upload. 2. The Choose File window displays, allowing selection of the file to upload.  3. Select the target release ISO image file and click **Open**. 4. The selected file and its path display on the screen.  5. Click **Upload.** The ISO file begins uploading to the file management storage area. 6. Wait for the screen to refresh and display the uploaded ISO filename in the files list. This will usually take between 2 to 10 minutes, but more if the network upload speed is slow.

Procedure 6: DSR ISO Administration

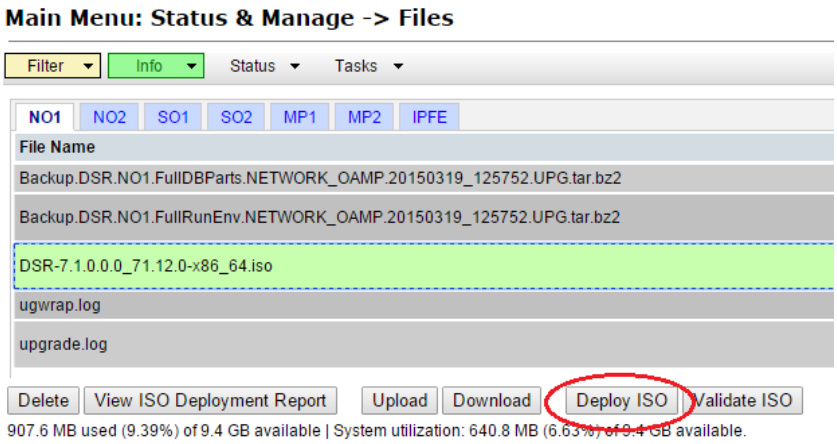
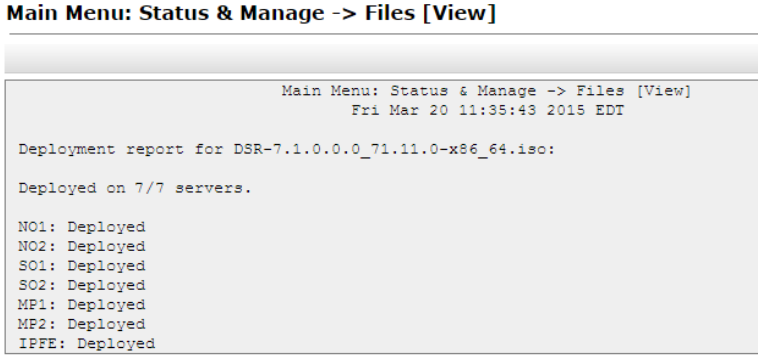
3 ☐	**Active NOAM VIP:**
	Copy ISO to the Standby NOAM
	
	For an Active NOAM on release 7.0.1
		If the Active NOAM is on release 7.0.1, perform this step; otherwise, proceed to step 6.
		
		Copy the ISO file to the Standby NOAM.
		
		1. Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the Active NOAM:
		
		`ssh admusr@<NOAM_VIP>`
		`login as: admusr`
		`password: <enter password>`
		
		2. Copy the ISO file to the Standby NOAM
		
		`scp -p /var/TKLC/db/filemgmt/<DSR_ISO_Filename>`
		`admusr@<Standby_NOAM_IP>:/var/TKLC/db/filemgmt`

4 ☐	**Active NOAM VIP:** Using NOAM GUI, transfer ISO to all servers to be upgraded. **For Active NOAM on release 7.0.1**	**If the Active NOAM is on release 7.0.1:** Transfer the target release ISO image file from the Active NOAM to all other DSR servers. 1. Navigate to **Administration >Software Management > ISO Deployment** 2. Click "**Transfer ISO**" 

Procedure 6: DSR ISO Administration

5 ☐	**Active NOAM VIP:** ISO transfer continued **For Active NOAM on release 7.0.1**	**If the Active NOAM is on release 7.0.1:** 1. Under the "**Select ISO to Transfer:**" drop down menu select the target release ISO. Under the "**Select Target System(s):**" select "**Select All**". 2. Select the checkbox next to "**Perform Media Validation before Transfer**".  3. Click **Ok** 4. Control will return to the ISO screen. Monitor the progress until all file transfers have completed. Click **Refresh** to update the status of the transfer. If a file transfer fails, it must be retried. NOTE: In the unlikely event that an ISO file transfer fails, repeat the transfer selecting only the specific system to which the transfer failed. If file transfers fail repeatedly, it is recommended to contact MOS for assistance.
		THIS PROCEDURE HAS BEEN COMPLETED.

Procedure 6: DSR ISO Administration

6 ☐	**Active NOAM VIP:** Using NOAM GUI, deploy ISO to all servers to be upgraded. **For Active NOAM on release 7.1.1 or later**	Deploy ISO to all servers. 1. Select **Status & Manage > Files** The Files menu is displayed 2. Click the Active NOAM server tab. All files stored in the file management storage area of this server display on the screen. 3. Select the target release ISO, and click the **View ISO Deployment Report** button. 4. In the resulting report, determine if the ISO has been deployed to all servers in the system. 5. If the ISO has been deployed to all servers, this procedure is complete. Proceed to the next procedure per Table 4 6. If the ISO has not been deployed, select the target release ISO in the file list, and click the **Validate ISO** button. Click **Ok** on the resulting confirmation dialog box. 7. Verify the ISO status is valid. If the ISO is not valid, repeat this procedure beginning with step 1.If the ISO fails validation more than once, it is recommended to contact MOS. 8. If the ISO is valid, select the ISO, and click the **Deploy ISO** button. Click **Ok** on the resulting confirmation dialog box. 
7 ☐	**Active NOAM VIP:** Monitor ISO deployment **For Active NOAM on release 7.1.1 or later**	The deployment progress can be monitored by viewing the tasks dropdown list on the **Status & Manage > Files** screen. 1. Select the target release ISO, and click the **View ISO Deployment Report** button. Monitor deployment progress until the ISO has been deployed to all servers in the system. 

THIS PROCEDURE HAS BEEN COMPLETED.

3.3.4 Full Backup of DB Run Environment at Each Server

The procedures in this section are part of software upgrade preparation and are used to conduct a full backup of the run environment on each server, to be used in the event of a backout of the new software release. The backup procedure to be executed is dependent on the software release that is running on the Active NOAM.

NOTE: Do not perform this procedure until the ISO Deployment is completed to all servers in the topology. Failure to complete the ISO may disrupt ISO deployment/undeployment in the event of a partial backout (e.g. backout of one site).

!! WARNING!! **IF BACKOUT IS NEEDED, ANY CONFIGURATION CHANGES MADE AFTER THE DB IS BACKED UP AT EACH SERVER WILL BE LOST**

3.3.4.1 Full Backup of DB Run Environment for Release 7.0.1

This procedure is used to backup the DB run environment when the Active NOAM is on release 7.0.1.

Procedure 7: Full Backup of DB Rbun Environment for Release 7.0.1

S T E P #	This procedure (executed from the Active NOAM server) conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**Active NOAM CLI:** Log into the Active NOAM	Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the Active NOAM: `ssh admusr@<NOAM_VIP>`
2 ☐	**Active NOAM CLI:** Start a screen session.	Enter the following commands: `$ screen` (The screen tool will create a no-hang-up shell session, so that the command will continue to execute if the user session is lost.)

Procedure 7: Full Backup of DB Rbun Environment for Release 7.0.1

S T E P #	This procedure (executed from the Active NOAM server) conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

3 ☐	**Active NOAM CLI:**
	Execute Full Backup for all servers (managed from this NOAM)
		Execute the backupAllHosts utility on the Active NOAM. This utility will remotely access each server managed by the NOAM, and run the backup command for that server.
		`$ /usr/TKLC/dpi/bin/backupAllHosts`
		`Do you want to remove the old backup files (if exists ) from all the servers (y/[n])?y`
		It may take from 10 to 30 minutes for this command to complete, depending upon the number of servers and the data in the database.
		Do not proceed until the backup on each server is completed.
		Output similar to the following will indicate successful completion:
		`Script Completed. Status:`
		`HOSTNAME | STATUS`
		`----------`
		`HPC3blade02 | PASS`
		`HPC3blade01 | PASS`
		`HPC3blade03 | PASS`
		`HPC3blade04 | PASS`
		(Errors will also report back to the command line.)
		NOTE: There is no progress indication for this command; only the final report when it completes.

4 ☐	**Active NOAM CLI:**
	Exit the screen session.
		`$ exit`
		`[screen is terminating]`
		NOTE: "screen -ls" is used to show active screen sessions on a server, and "screen -dr" is used to re-enter a disconnected screen session.

5 ☐	ALTERNATIVE METHOD (Optional)
	Server CLI:
	If needed, the alternative backup method can be executed on each individual server instead of using the "backupAllHosts" script.
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the script above. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		Output similar to the following will indicate successful completion:
		`Success: Full backup of COMCOL run env has completed.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullDBParts.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`

Procedure 7: Full Backup of DB Rbun Environment for Release 7.0.1

S T E P #	This procedure (executed from the Active NOAM server) conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

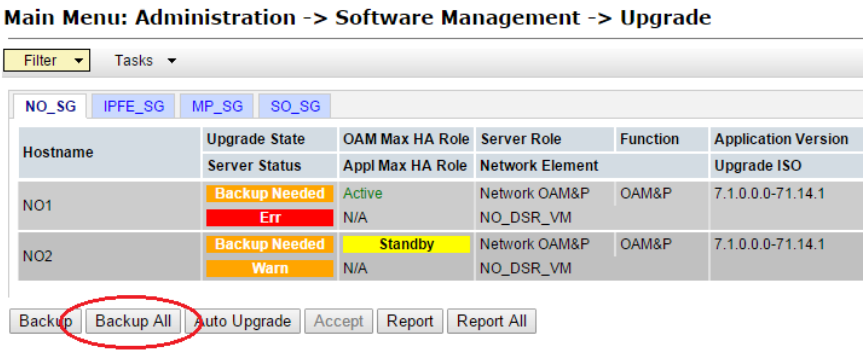
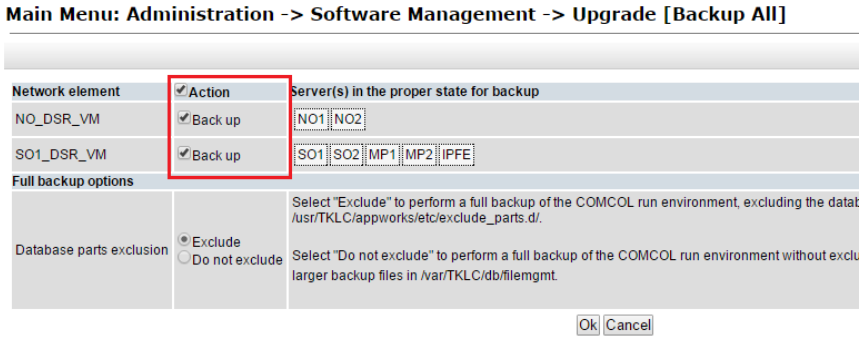
6 ☐	**Active NOAM VIP:**
	Verify that backup files are present on each server.
		1. Log into the Active NOAM.
		2. Select **Status & Manage > Files**
		The Files menu is displayed
		3. Click on each server tab, in turn
		4. For each server, verify that the following (2) files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`

THIS PROCEDURE HAS BEEN COMPLETED.		

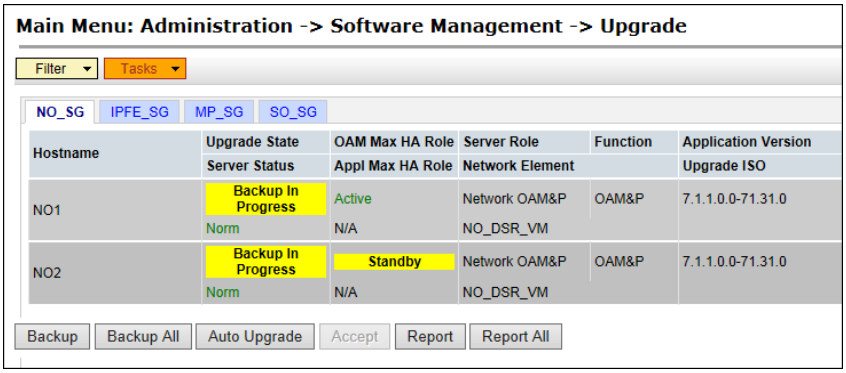
3.3.4.2 Full Backup of DB Run Environment for Release 7.1.x and later

This procedure is used to backup the DB run environment when the Active NOAM is on release 7.1.x and later.

Procedure 8: Full Backup of DB Run Environment for Release 7.1.x and later

S T E P #	This procedure (executed from the Active NOAM server) conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**Active NOAM VIP:** Start backup of all servers	1. Login to the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade.** 3. Click the **Backup All** button. 
2 ☐	**Active NOAM VIP:** Select network elements to backup	The **Upgrade [Backup All]** screen is displayed. This screen displays the various Network Elements, and identifies which servers are ready for backup. 1. In the **Action** column, select the **Back up** checkbox for each Network Element. 2. Ensure the 'Exclude' radio button is selected. 3. Click the **Ok** button. This initiates a full backup on each eligible server. 

Procedure 8: Full Backup of DB Run Environment for Release 7.1.x and later

S T E P #	This procedure (executed from the Active NOAM server) conducts a full backup of the run environment on each server, so that each server has the required data to perform a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
3 ☐	**Active NOAM VIP:** Monitor backup progress	Monitor the upgrade progress. 1. Select each server group tab and verify that each server transitions from 'Backup in Progress' to 'Ready'. Refresh the page as each tab is selected to ensure the latest status is displayed. 

4 ☐	ALTERNATIVE METHOD (Optional)
	Server CLI:
	If needed, the Alternative backup method can be executed on each individual server instead of using the **"backupAllHosts"** script.
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the GUI method above. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		Output similar to the following will indicate successful completion:
		`Success: Full backup of COMCOL run env has completed.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.01.FullDBParts.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.01.FullRunEnv.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`

5 ☐	**Active NOAM VIP:**
	Verify that backup files are present on each server.
		1. Log into the Active NOAM.
		2. Select **Status & Manage > Files**
		The **Files** menu is displayed
		3. Click on each Server tab, in turn
		4. For each Server, verify that the following (2) files have been created:
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`

THIS PROCEDURE HAS BEEN COMPLETED.		

3.3.5 Network Interface Workaround

In some Cloud environments, the network interface names are not persistent across a server boot or upgrade. Interface renaming can result in the loss of IP access to the server. To prevent this from occurring, this procedure creates a network persistence rules file on each server. This procedure is required prior to upgrading to DSR Release 7.3.

!! WARNING!! **THIS PROCEDURE MUST BE COMPLETED PRIOR TO UPGRADING TO DSR RELEASE 7.3**

Procedure 9: Network Interface Workaround

S T E P #	This procedure creates a network persistence rules file. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

1 ☐	**Server CLI**
	
	Create network rules file
		Execute the following commands on the server.
		
		1. Use an SSH client to connect to the Active NOAM:
		
		`ssh admusr@<server_ip>`
		`password: <enter password>`
		
		2. Enter the following command to create the rules file:
		
		`$ sudo udevadm trigger --subsystem-match=net`
		
		Verify the rules file "`70-persistent-net.rules`" is created:
		
		`$ ls /etc/udev/rules.d`
		`/etc/udev/rules.d/70-persistent-net.rules`

2 ☐	Repeat for all servers	Repeat step 1 for each server in the Cloud deployment.

3.3.6 IDIH Pre-Upgrade

If IDIH is a component of a Network Element, it may be upgraded either before or after the DSR. The order of upgrade will not impact the functionality of either component. However, it should be noted that certain compatibility limitations may exist while the two components are not on the same release.

The IDIH upgrade procedures are provided in Appendix F and may be performed at any time after Section 3.3.6.1 has been completed.

Table 5: IDIH Upgrade Preparation Overview.

Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 10	0:15-0:30	0:15-0:30	IDIH Upgrade Preparation	None

3.3.6.1 IDIH Upgrade Preparation

This procedure prepares the Mediation and Application guests for upgrade.

Procedure 10: IDIH Upgrade Preparation

S T E P #	This procedure prepares the Mediation and Application guests for upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	Place the Mediation and Application OVAs in the Cloud repository.	1. Follow the hypervisor's instructions to add the Mediation and Application OVAs to the cloud software repository.

3.4 Software Upgrade Execution Overview

It is recommended to contact MOS as described in Appendix J *prior* to executing this upgrade to ensure that the proper media are available for use.

Before upgrade, users must have performed the data collection and system health check instructions in section 3.3. This check ensures that the system to be upgraded is in an upgrade-ready state. Performing the system health check determines which alarms are present in the system and if upgrade can proceed with alarms.

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

If there are servers in the system which are not in a Normal state, these servers should be brought to the Normal or Application Disabled state before the upgrade process is started. The sequence of upgrade is such that servers providing support services to other servers will be upgraded first.

If alarms are present on the server, it is recommended to contact MOS to diagnose those alarms and determine whether they need to be addressed, or if it is safe to proceed with the upgrade.

Please read the following notes on upgrade procedures:

- All procedure completion times shown in this document are estimates. Times may vary due to differences in database size, user experience, and user preparation.
- The shaded area within response steps must be verified in order to successfully complete that step.
- Where possible, command response outputs are shown as 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***." Where appropriate, instructions are provided to determine what output should be expected in place of "***XXXX***" or "***YYYY***"
  - Aesthetic differences unrelated to functionality such as ***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. A check box is provided. For procedures which are executed multiple times, the check box can be skipped, but the technician must initial each iteration the step is executed. The space on either side of the step number can be used (margin on left side or column on right side).
- Captured data is required for future support reference if an MOS representative is not present during the upgrade.
- Answer these questions, and record:

  What is the DSR Application version to be upgraded? _____

  What is the DSR Application new version to be applied? _____

  Is this a Major or Incremental Upgrade? _____

  Are there IPFE servers to upgrade? _____

  Is SDS also deployed (co-located) at the DSR site? _____

  Note: SDS does not need to be upgraded at the same time.

  Is IDIH also deployed (co-located) at the DSR site? _____

3.4.1 Accepting the Upgrade

After the upgrade of **ALL** Servers in the topology has been completed, and following an appropriate soak time, the Post-Upgrade procedures in **Section 5.6** are performed in a separate Maintenance Window to finalize the upgrade. Procedure 42 "Accepts" the upgrade and performs a final Health Check of the system to monitor alarms and server status. Accepting the upgrade is the last step in the upgrade. Once the upgrade is accepted, the upgrade is final and cannot be backed out.

4 NOAM UPGRADE EXECUTION

NOAM UPGRADE

The NOAM upgrade section is common to all topologies. This section must be completed before executing the site upgrade procedures.

Procedures for the NOAM upgrade include steps for the upgrade of the Disaster Recovery NOAM (DR NOAM) servers also. If no DR NOAM is present in the customer deployment, then the DR NOAM-related steps can be safely ignored.

Global Provisioning will be disabled before upgrading the NOAM servers. Provisioning activities at the NOAM and SOAM servers will have certain limitations during the period where the NOAMs are upgraded and the sites are not yet upgraded.

The Elapsed Time mentioned in table below specifies the time to upgrade the DSR application without the upgrade of the corresponding TVOE. If the TVOE Host upgrades are performed with the application, an additional 60 minutes should be added to the estimated time. All times are estimates.

Table 6: NOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 11 or Procedure 12	0:30-0:45 0:20-0:30	0:30-0:45 0:20-0:30	NOAM Health Check for Source Release 7.0.1, 7.1.x NOAM Health Check for Source Release 7.2 and later	None None
Procedure 13	0:05-0:10	0:25-0:55	NOAM Pre-Upgrade Backup	None
Procedure 14	0:01-0:05	0:26-1:00	Disable Global Provisioning	Global Provisioning Disabled
Procedure 15	0:40-1:20	1:06-2:20	NOAM Upgrade	No Traffic Impact
Procedure 16	0:01-0:05	1:07-2:25	PCA (formerly PDRA) Topology Hiding Configuration	No Traffic Impact
Procedure 17	0:05-0:15	1:12-2:40	Verify NOAM Post Upgrade Status	None
Procedure 18	0:05-0:10	1:17-2:50	Allow Provisioning (post NOAM Upgrade)	Global Provisioning Enabled

4.1 NOAM Pre-Upgrade Checks and Backup

The procedures in this section perform health checks and backups to prepare the NOAM NE for upgrade. These procedures must be executed on the Active NOAM.

Note: These procedures may be executed outside of the maintenance window, but should be executed within 6 to 8 hours prior to Procedure 15.

4.1.1 NOAM Health Check for Source Release 7.0.1, 7.1.x

This procedure is used to determine the health and status of the network and servers when the NOAM is on source release 7.0.1 or 7.1.x. This procedure must be executed on the Active NOAM.

Procedure 11: NOAM Health Check for Source Release 7.0.1, 7.1.x

S T E P #	This procedure performs a Health Check of the system prior to upgrading the NOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Verify ISO for Upgrade has been deployed For Active NOAM on release 7.0.1.only	**This step is for an Active NOAM on release 7.0.1. If the Active NOAM is on release 7.1.x, proceed to step 2.** Verify the DSR ISO file has been transferred to all servers. 1. Navigate to **Administration > Software Management > ISO Deployment** 2. Verify the "**Transfer Status**" is "**Complete**" for each server in the topology. 3. If any server shows "**Not Complete**", perform Section 3.3.3 - DSR ISO Administration Example: **Main Menu: Administration -> ISO** Help Wed Sep 25 17:39:13 2013 UTC Display Filter: - None - = Go (LIKE wildcard: "*") • Transfer ISO Complete. ISO: 872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso 7 of 7 Transfers Successful. 0 of 7 Transfers Failed. Table description: List of Systems for ISO transfer. Displaying Records 1-7 of 7 total | First | Prev | Next | Last | [Transfer ISO] **Proceed to step 3 to complete this procedure.**

System Name / Hostname	ISO	Transfer Status
MP1	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
MP2	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
MP3	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
T2-NO-228-A	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
T2-NO-228-B	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
ipfe1	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete
ipfe2	872-2526-101-5.0.0_50.12.0-DSR-x86_64.iso	Complete

Procedure 11: NOAM Health Check for Source Release 7.0.1, 7.1.x

2. ☐	**Active NOAM VIP:**
	
	Verify ISO for Upgrade has been deployed
	
	For Active NOAM on release 7.1.x only
		Verify the DSR ISO file has been transferred to all servers.
		
		1. Navigate to **Status & Manage > Files**
		2. Select the target release DSR ISO and click "**View ISO Deployment Report**".
		3. Review the report to ensure the ISO is deployed to all servers in the topology
		
		Sample report:
		
		`Deployment report for DSR-7.1.1.0.0_71.27.0-x86_64.iso:`
		
		`Deployed on 7/7 servers.`
		
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

3. ☐	**Active NOAM CLI:**
	
	Verify NOAM pre-Upgrade Status
		Execute the following commands on the Active DSR NOAM and Active DR NOAM servers.
		
		1. Use an SSH client to connect to the Active NOAM:
		
		`ssh <NOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: The static XMI IP address for each server should be available in Table 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck preUpgradeHealthCheck`
		
		This command creates two files in `/var/TKLC/db/filemgmt/UpgradeHealthCheck/` with the filename format:
		
		`<NOserver_name>_ServerStatusReport_<date-time>.xml`
		`<NOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		
		If any alarms are present in the system:
		`<NOserver_name>_AlarmStatusReport_<date-time>.xml`
		
		If the system is PDRA, one additional file is generated:
		`<NOserver_name>_SBRStatusReport_<date-time>.xml`
		
		Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.
		
		3. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message. If the following message appears in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended to contact MOS for guidance.
		
		4. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

Procedure 11: NOAM Health Check for Source Release 7.0.1, 7.1.x

4. ☐	**Active NOAM VIP:** Export and archive the Diameter configuration data	Export Diameter configuration data. 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the Diameter data by choosing the drop down entry labeled "**ALL**". 3. Verify the data export is complete using the tasks button at the top of the screen. 4. Browse to **Main Menu > Status & Manage > Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the Active NOAM to the client machine.

5. ☐	**Active SOAM CLI:**
	Pre-upgrade health checks
		Execute SOAM pre-upgrade alarm status health checks.
		
		1. Use an SSH client to connect to the Active SOAM:
		
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: The static XMI IP address for each server should be available in Table 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck alarmStatusOnSoam`
		
		If any alarms are present in the system, this command creates a file in `/var/TKLC/db/filemgmt/ UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		
		Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.
		
		3. Keep this report for future reference. This report will be compared to alarm and status reports after the upgrade is complete.

6. ☐	**Active SOAM CLI:** Pre-upgrade health checks	Execute SOAM pre-upgrade DA-MP status health checks. 1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established _____
7. ☐	**Active SOAM CLI:** Verify PCA status (if equipped)	Execute SOAM pre-upgrade PCA status health checks, if equipped. 1. Enter the command: `$ upgradeHealthCheck pcaStatus` This command outputs status to the screen for review. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify Operational Status is '**Available**' for all applications
8. ☐	Repeat for each Network Element	Repeat **Steps 5 - 7** for each SOAM site in the topology.

Procedure 11: NOAM Health Check for Source Release 7.0.1, 7.1.x

9. ☐	**Active NOAM VIP:**
	Verify that backups are created for all servers
		Verify that a recent COMCOL Environment backup has been performed.
		
		1. Select **Status and Manage > Files.**
		2. Select each server tab, in turn.
		3. Verify the following two files have been created and have a current timestamp:
		
		`Backup.DSR.<hostname>.FullRunEnv.NETWORK_OAMP.<timestamp>.UPG.tar.bz2`
		
		`Backup.DSR.<hostname>.FullDBParts.NETWORK_OAMP.<timestamp>.UPG.tar.bz2`
		
		4. Repeat this procedure for each site.
		
		See **Section 3.3.4** to perform (or repeat) a full Backup, if needed.

THIS PROCEDURE HAS BEEN COMPLETED.		

4.1.2 NOAM Health Check for Source Release 7.2 and later

This procedure is used to determine the health and status of the network and servers when the NOAM is on release 7.2 and later. This procedure must be executed on the Active NOAM.

Note: This procedure may be executed outside of the maintenance window, but should be executed within 6 to 8 hours prior to Procedure 15.

Procedure 12: NOAM Health Check for Source Release 7.2 and later

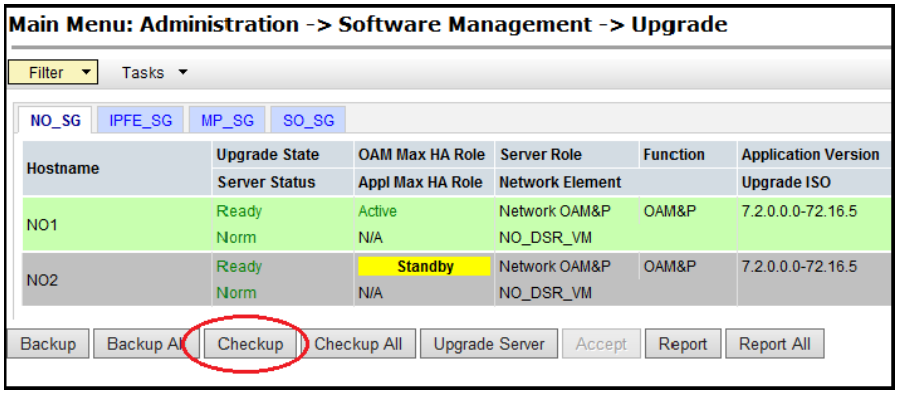
S T E P #	This procedure performs a Health Check on the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**Active NOAM VIP:**
	Verify Upgrade ISO has been deployed
		Verify the DSR ISO file has been transferred to all servers.
		
		1. Navigate to **Status & Manage > Files**
		2. Select the target release DSR ISO and click "**View ISO Deployment Report**".
		3. Review the report to ensure the ISO is deployed to all servers in the topology
		
		Sample report:
		
		`Deployment report for DSR-7.2.0.0.0_72.27.0-x86_64.iso:`
		
		`Deployed on 7/7 servers.`
		
		`NO1: Deployed`
		`NO2: Deployed`
		`SO1: Deployed`
		`SO2: Deployed`
		`MP1: Deployed`
		`MP2: Deployed`
		`IPFE: Deployed`

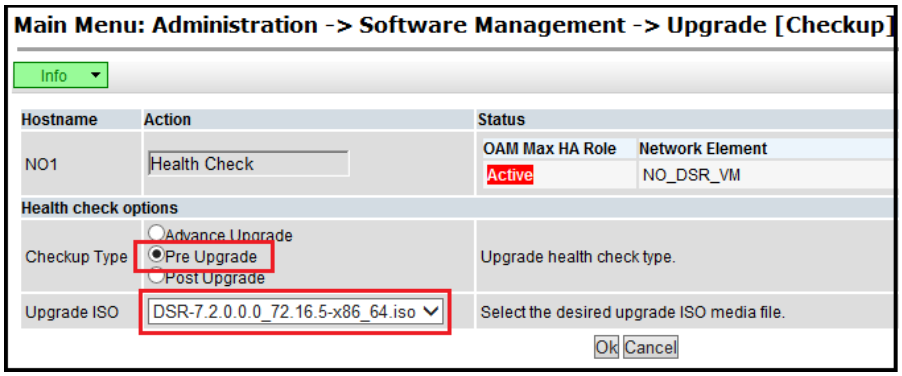
2 ☐	**Active NOAM VIP:** Export and archive the Diameter configuration data	Export Diameter configuration data. 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the Diameter data by choosing the drop down entry labeled "**ALL**". 3. Verify the data export is complete using the tasks button at the top of the screen. 4. Browse to **Main Menu > Status & Manage > Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the Active NOAM to the client machine.

Procedure 12: NOAM Health Check for Source Release 7.2 and later

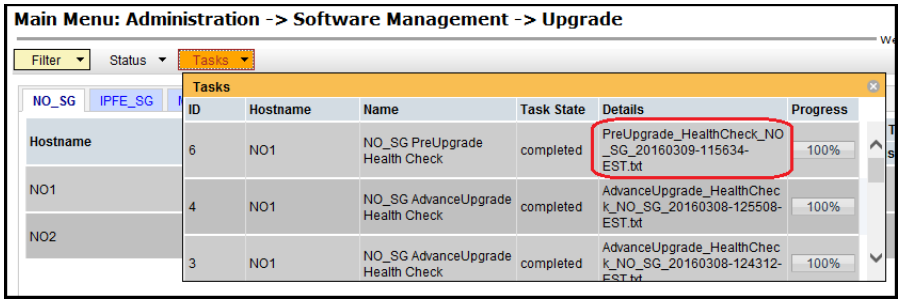
3	**Active NOAM VIP:** Initiate NOAM health checks	This procedure runs the automated pre-upgrade Health Checks. 1. Select **Administration > Software Management > Upgrade**. The Upgrade screen is displayed. 2. Select the Active NOAM.



3. Click the **Checkup** button.
   The Upgrade [Checkup] screen is displayed.
4. Under Health check options, select the **Pre Upgrade** option.
5. Use the **Upgrade ISO** pulldown to select the target release ISO.
6. Click **Ok**. Control returns to the Upgrade screen.



Procedure 12: NOAM Health Check for Source Release 7.2 and later

4 ☐	**Active NOAM VIP:** Monitor health check progress	Monitor for the completion of the Health Check. 1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as **<NOServerGroup> PreUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The **Details** column will display a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. Open the report and review the results. 
5 ☐	**Active NOAM VIP:** Analyze health check results	Analyze Health Check report for failures. If the Health Check report status is anything other than “Pass”, the Health Check logs must be analyzed to determine if the upgrade can proceed. 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the file named “UpgradeHealthCheck.log” and click **View**. 3. Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix J. If the health check log contains the message “Unable to execute Health Check on <Active NOAM hostname>”, perform health checks in accordance with Procedure 11.
		THIS PROCEDURE HAS BEEN COMPLETED.

4.1.3 NOAM Pre-Upgrade Backup

This procedure takes a backup of the NOAM servers just prior to the upgrade.

Procedure 13: NOAM Pre-Upgrade Backup

S T E P #	This procedure takes a backup of the NOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	**Active NOAM VIP:** Backup all global configuration databases for NOAM **IMPORTANT: Required for Disaster Recovery**	Backup NOAM database. 1. Select **Status & Manage > Database** to return to the Database Status screen. 2. Click to highlight the **Active NOAM** server; click **Backup. NOTE: the Backup button will only be enabled when the Active server is selected.** The Database [Backup] screen is displayed. 3. Select the **Configuration** checkbox**.** 4. Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. 5. Enter **Comments** (optional) 6. Click **OK**. **NOTE:** On the **Status & Manage >Database** screen, the Active NOAM server will display the word **"Active"** in the **"OAM Max HA Role"** column.
2 ☐	**Active NOAM VIP:** Save database backups for NOAM **IMPORTANT: Required for Disaster Recovery**	Download database files from the NOAM. 1. Select **Status & Manage > Files** The **Files** menu is displayed. 2. Click on the Active NOAM server tab**.** 3. Select the configuration database backup file and click the **Download** button. 4. If a confirmation window is displayed, click **Save**. 5. If the **Choose File** window is displayed, select a destination folder on the local workstation to store the backup file. Click **Save**. 6. If a **Download Complete** confirmation is displayed, click **Close**.
THIS PROCEDURE HAS BEEN COMPLETED.		

4.2 Disable Global Provisioning

The following procedure disables provisioning on the NOAM. This step ensures that no changes are made to the database while the NOAMs are upgraded. Provisioning will be re-enabled once the NOAM upgrade is complete.

Procedure 14: Disable Global Provisioning

S T E P #	This procedure disables provisioning for the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Disable global provisioning and configuration.	Disable global provisioning and configuration updates on the entire network: 1. Log into the Active NOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Disable Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 002] - Global provisioning has been manually disabled**. The Active NOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
THIS PROCEDURE HAS BEEN COMPLETED.		

4.3 NOAM Upgrade

This procedure is used to upgrade the NOAM and DR NOAM servers.

Procedure 15: NOAM Upgrade

S T E P #	This procedure upgrades the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	Upgrade Standby DSR NOAM servers or standalone NOAM server.	1. Upgrade the Standby DSR NOAM server using Upgrade Single Server procedure: **Execute Appendix D** -- Single Server Upgrade Procedure **Note:** If the DSR deployment does not have a Standby NOAM then perform Appendix G.1 for the standalone NOAM. **Execute Appendix G.1** – Server Upgrade Using platcfg 2. After successfully completing the procedure in Appendix D or **Appendix G.1**, return to this point and continue with the next step. The Active NOAM server may have some or all of the following expected alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31106 (DB Merge to Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31225 (HA Service Start Failure)** Alarm ID = **31226 (HA Availability Status Degraded)** Alarm ID = **31233 (HA Path Down)** Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** **If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action.** **If the Active NOAM is on release 7.1.1 or later, proceed to step 3.**
2. ☐	**Active NOAM VIP:** Prepare the Active NOAM for upgrade **For NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** Prepare the Active NOAM for Upgrade. 1. Select **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 2. Select the NOAM Server Group: 3. Select the Active NOAM. 4. On the upgrade form, make the Active NOAM 'Upgrade Ready', by selecting the **Prepare** button. 5. On the Upgrade [Prepare] form, select '**Prepare**' in the **Action** dropdown list. Click the **Ok** button. This starts the Prepare action on the Active NOAM and forces an HA failover. 6. Log out of the GUI, **clear the browser cache**, and log back into the Active NOAM via the VIP before continuing. Clear the 'Prepared' state for the now-standby NOAM. This is required due to the transition from release 7.0.1 to release 7.3. 7. Select **Status & Manage > HA.** The HA status screen is displayed. 8. Click the **Edit** button. 9. For the NOAM to be upgraded (now the Standby), set the **Max Allowed HA Role** to Active, and click **Ok**. 10. Select **Status & Manage > Server**. The server status screen is displayed. 11. Select the Standby NOAM and click the **Restart** button. 12. Click Ok and verify the **Appl State** changes to **Enabled**.

Procedure 15: NOAM Upgrade

3. ☐	Upgrade Active NOAM servers	Upgrade the second NOAM server using the Upgrade Single Server procedure: **Execute Appendix D** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix D, continue to the next procedure per Table 6. **If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action.**
4. ☐	Upgrade Standby DR NOAM	Upgrade the Standby DR NOAM server using the Upgrade Single Server procedure: **Execute Appendix D** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
5. ☐	Upgrade Active DR NOAM	Upgrade the second DR NOAM server using the Upgrade Single Server procedure: **Execute Appendix D** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix D, return to this point and continue with the next procedure per Table 6.
		THIS PROCEDURE HAS BEEN COMPLETED.

4.3.1 PCA (formerly PDRA) Topology Hiding Configuration

In DSR 7.0, the Policy and Charging Topology Hiding configuration moved from being site-specific at the SOAM, to being network-wide specific at the NOAM. Because each site could be independently configured, manual intervention is required to determine the appropriate setting for the network-wide configuration. The network-wide settings will apply to ALL sites once the site is upgraded.

This procedure is applicable only to systems with the Policy and Charging feature enabled.
This procedure is applicable only to major upgrades from 7.0.1 to DSR 7.3.

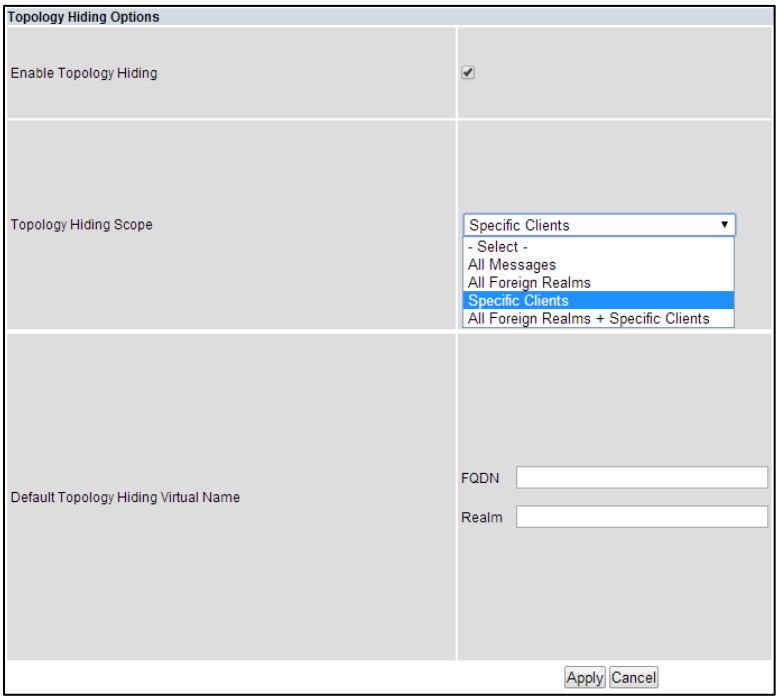
NOTE: The network-wide Topology Hiding settings at the NOAM will apply to each site as it is upgraded. Please note that this may result in a behavior change if the pre-upgrade site settings differ from the network-wide settings.

NOTE: This procedure can be skipped if Topology Hiding is not in use for this system.

Procedure 16: PCA (formerly PDRA) Topology Hiding Configuration

S T E P #	This procedure sets the network-wide Topology Hiding configuration. This procedure applies only to systems with the Policy and Charging feature enabled. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Enable Global Provisioning	Before the Topology Hiding configuration can be modified, Global Provisioning must be enabled temporarily. 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed. 3. Click the **Enable Provisioning** button. 4. Verify the button text changes to **Disable Provisioning**.

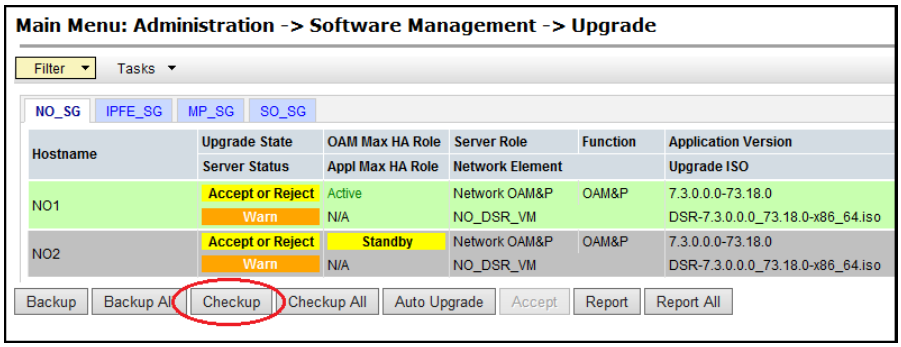
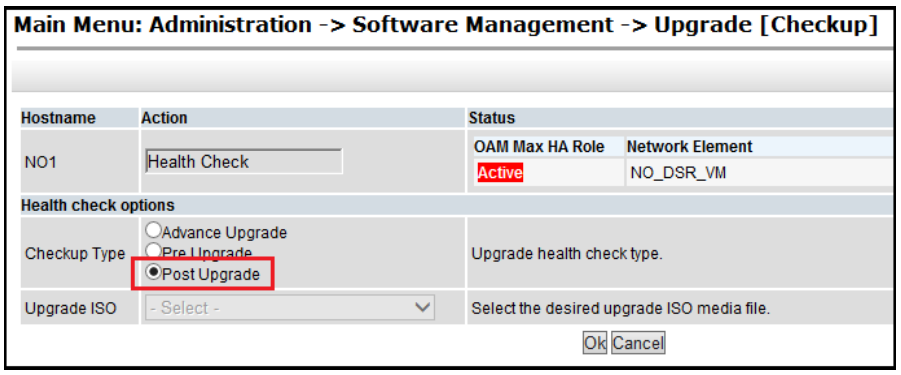
Procedure 16: PCA (formerly PDRA) Topology Hiding Configuration

2. ☐	**Active NOAM VIP:** Configure Topology Hiding settings	Configure the topology hiding settings. 1. Navigate to **Policy and Charging > Configuration > Policy DRA > Network-Wide Options**. 2. In the Topology Hiding Options section, select the **Enable Topology Hiding** checkmark. 3. Select the appropriate Topology Hiding Scope setting. 4. Enter a Default Topology Hiding Virtual Name – FQDN and Realm. These default values will be used if specific values have not been set at a site. 5. Select **Apply**. 
3. ☐	**Active NOAM VIP:** Disable global provisioning and configuration.	Disable global provisioning. 1. Select **Status & Manage > Database.** The Database Status screen is displayed 2. Click the **Disable Provisioning** button. 3. Confirm the operation by clicking **Ok** in the popup dialog box. 4. Verify the button text changes to **Enable Provisioning**. A yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 002] - Global provisioning has been manually disabled**. The Active NOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
		THIS PROCEDURE HAS BEEN COMPLETED.

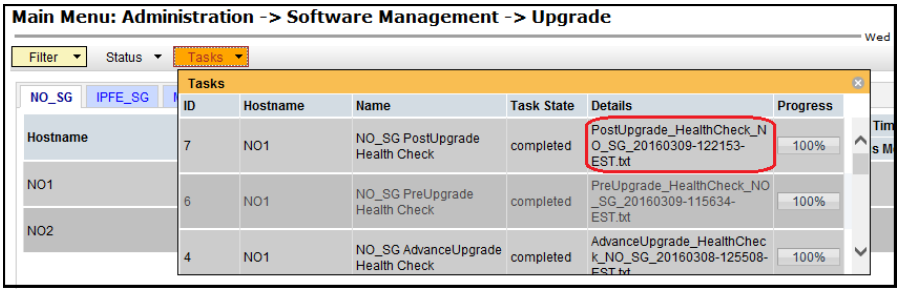
4.4 Verify NOAM Post Upgrade Status

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers.

Procedure 17: Verify NOAM Post Upgrade Status

S T E P #	This procedure verifies Post Upgrade Status for NOAM upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	**Active NOAM VIP:** Post-upgrade health checks	This procedure will run the automated post-upgrade Health Checks. **From the Active NOAM GUI:** 1. Select **Administration > Software Management > Upgrade**. The Upgrade screen is displayed. 2. Select the Active NOAM.  3. Click the **Checkup** button. The Upgrade [Checkup] screen is displayed. 4. Under Health check options, select the **Post Upgrade** option. 5. Click **Ok**. Control returns to the Upgrade screen.  	

Procedure 17: Verify NOAM Post Upgrade Status

2 ☐	**Active NOAM VIP:** Monitor health check progress	Monitor for the completion of the Health Check. **From the Active NOAM GUI:** 1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as <NOServerGroup> **PostUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column will display a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. Open the report and review the results. 
3 ☐	**Active NOAM VIP:** Analyze health check results	Analyze Health Check failure. If the Health Check report status is anything other than “Pass”, the Health Check logs must be analyzed to determine if the upgrade can proceed. **From the Active NOAM GUI:** 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the file named “UpgradeHealthCheck.log” and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix J.
		THIS PROCEDURE HAS BEEN COMPLETED.

4.5 Allow Provisioning (post NOAM Upgrade)

The following procedure enables Global Provisioning after the NOAM upgrade.

CAUTION

ANY NETWORK-WIDE PROVISIONING CHANGES MADE AT THE NOAM SITE BEFORE THE UPGRADE IS ACCEPTED WILL BE LOST IF THE UPGRADE IS BACKED OUT

Procedure 18: Allow Provisioning (post NOAM Upgrade)

S T E P #		
	This procedure enables provisioning for the NOAM and DR NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Enable global provisioning and configuration.	Enable global provisioning and configuration updates on the entire network: 1. Log into the Active NOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Enable Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Disable Provisioning.**
	Note: After enabling provisioning at the NOAM, it is possible that the SOAM GUI(s) will display a banner indicating that global provisioning is disabled. This message can be ignored – global provisioning is enabled. This is a display issue only and will be corrected when the SOAMs are upgraded.	
2. ☐	**Active NOAM VIP:** Add new Network Element (if required).	**Perform this step only if the addition of a new Network Element is required at this time** If a new Network Element is to be added, this procedure can be started now. Addition of the new Network Element will require a separate maintenance window. The servers in the new Network Element must be installed with the same DSR release as that of the upgraded NOAM(s). Follow the DSR 7.3 Installation Procedures in reference [1] to install the software on the new servers and add the new Network Element under the existing NOAM(s). Skip the sections of the Installation Procedure related to installing and configuring the NOAM(s). This will add a new DSR SOAM site under the existing NOAM(s).
	THIS PROCEDURE HAS BEEN COMPLETED.	

5 SITE UPGRADE EXECUTION

This section contains the procedures for upgrading an entire site - starting with the pre-upgrade activities, to upgrading the SOAMs and C-level servers, and finishing with verifying the upgrade.

To maximize the Maintenance Window usage, the procedures in this section make full use of the parallel upgrade capabilities of the DSR, while ensuring traffic continuity and redundancy.

Table 7 details the site upgrade plan, which divides the upgrade into five iterations. An iteration is defined as the complete upgrade of one or more servers, from the pre-upgrade health checks to upgrade complete. The first two iterations consist of upgrading the SOAMs - the first iteration upgrades the Standby SOAM along with the Spare SOAM, if a spare exists. The second iteration upgrades the Active SOAM.

The third iteration begins the upgrade of the C-level servers. In iteration 3, one-half of the DA-MPs, SS7-MPs, and IPFEs are upgraded. This leaves the remaining half of these server functions to handle traffic processing. If the system is configured to support PCA/PDRA, then all Spare SBR servers are also upgraded in iteration 3 (including the second Spare SBR for three-site redundancy).

The fourth iteration upgrades the second half of the DA-MPs, SS7-MPs, and IPFEs, as well as the Standby SBR(s), if equipped. For non-PCA/PDRA systems, the site upgrade is complete when iteration 4 is completed.

The fifth iteration is required only for PCA/PDRA-equipped systems. In iteration 5, the Active SBR(s) are upgraded, completing the site upgrade.

NOTE: For PCA/PDRA systems, the Spare, Standby, and Active SBRs are upgraded in separate iterations to enforce redundancy of the session data. This approach ensures that two SBRs are online at all times.

Table 7. Site Upgrade Plan

Iteration 1	Iteration 2	Iteration 3	Iteration 4	Iteration 5
Standby SOAM, Spare SOAM	Active SOAM			
		½ DA-MPs	½ DA-MPs	
		½ SS7-MPs	½ SS7-MPs	
		½ IPFEs	½ IPFEs	
		Spare SBR(s)	Standby SBR(s)	Active SBR(s)

5.1 Site Pre-Upgrade Activities

SOAM UPGRADE: Pre-Upgrade Activities

Use this section to execute pre-upgrade planning, pre-upgrade backups, pre-upgrade health checks, and to disable Site Provisioning.

This section contains the procedures for site upgrade planning, pre-upgrade backups, health checks, and disabling site provisioning.

5.1.1 Site Upgrade Planning

The upgrade of the site servers consists of a mixture of automated upgrades using the Automated Server Group upgrade feature, along with "manual" upgrades that are a little less automated.

Table 8 should be used to plan the upgrade of each site. For the server groups that will be upgraded using ASG, the only planning necessary is to record the server group name. ASG will automatically select the individual servers to be upgraded. The SS7-MP and IPFE server groups must be upgraded manually since there is only one server per server group. Planning is necessary for these server groups to ensure traffic continuity. Record the hostname of the servers to be upgraded in each iteration.

Table 8. Site Upgrade Planning Sheet.

Iteration 1		Notes
Standby SOAM Hostname: Spare SOAM Hostname:		If a Spare SOAM exists, the Spare and Standby SOAMs will be upgraded manually. Otherwise, the SOAMs will be upgraded with ASG.
Iteration 2		**Notes**
Active SOAM		The Active SOAM will be upgraded in iteration 2, either manually or by ASG.
Iteration 3		**Notes**
DA-MP Group 1		ASG will automatically select DA-MPs for upgrade
SS7-MP 1 Hostname:		Manual upgrade
SS7-MP 3 Hostname:		Manual upgrade
SS7-MP 5 Hostname:		Manual upgrade
SS7-MP 7 Hostname:		Manual upgrade
IPFE 1 Hostname:		Manual upgrade
IPFE 3 Hostname:		Manual upgrade
Spare SBR(s)		ASG will automatically select the Spare SBR(s) for upgrade
Iteration 4		**Notes**
DA-MP Group 2		ASG will automatically select DA-MPs for upgrade
SS7-MP 2 Hostname:		Manual upgrade
SS7-MP 4 Hostname:		Manual upgrade
SS7-MP 6 Hostname:		Manual upgrade
SS7-MP 8 Hostname:		Manual upgrade
IPFE 2 Hostname:		Manual upgrade
IPFE 4 Hostname:		Manual upgrade
Standby SBR(s)		ASG will automatically select the Standby SBR(s) for upgrade
Iteration 5		**Notes**
Active SBR(s)		ASG will automatically select the Active SBR(s) for upgrade

Table 9 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 9 as a guide for determining the order in which the procedures are to be executed.

Table 9: Site Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 19	0:10-0:20	0:10-0:20	Site Pre-Upgrade Backups	None
Procedure 21 or Procedure 22	0:05-0:10 0:10-0:15	0:15-0:30 0:20-0:25	Site Pre-Upgrade Health Check for Release 7.2 and later Site Pre-Upgrade Health Check for Release 7.0.1, 7.1.x	None None
Procedure 23	0:01-0:05	0:16-0:45	Disable Site Provisioning	Site Provisioning Disabled, No Traffic Impact
Procedure 24	0:01-0:05	0:17-0:50	SOAM Upgrade Pre-Checks	No Traffic Impact
Iteration 1	0:40-1:00		Standby SOAM, Spare SOAM (if equipped)	Refer to Section 5.2 for details
Iteration 2	0:40-1:00		Active SOAM	Refer to Section 5.2 for details
Iteration 3	0:40-1:00		½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Spare SBR(s)	Refer to Section 5.3 for details
Iteration 4	0:40-1:00		½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Standby SBR(s)	Refer to Section 5.4 for details
Iteration 5	0:00-1:00		Active SBR(s)	Refer to Section 5.5 for details
Procedure 30	0:02		Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 31	0:10-0:15		Site Post-Upgrade Health Check	None

5.1.2 Site Pre-Upgrade Backups

This procedure is non-intrusive and is used to perform a backup of all servers associated with the SOAM Site(s) being upgraded. It is recommended that this procedure be executed no earlier than 36 hours prior to the start of the upgrade.

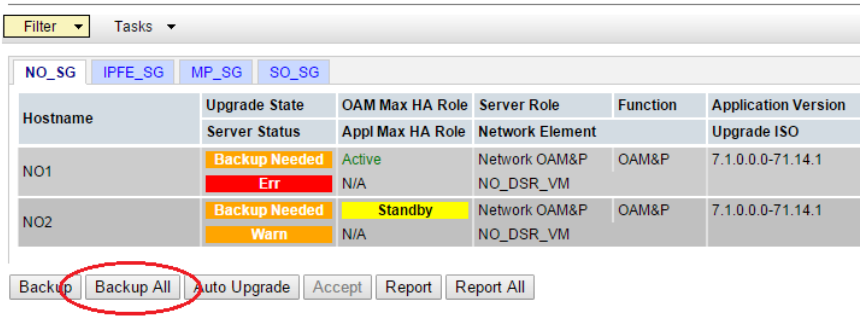
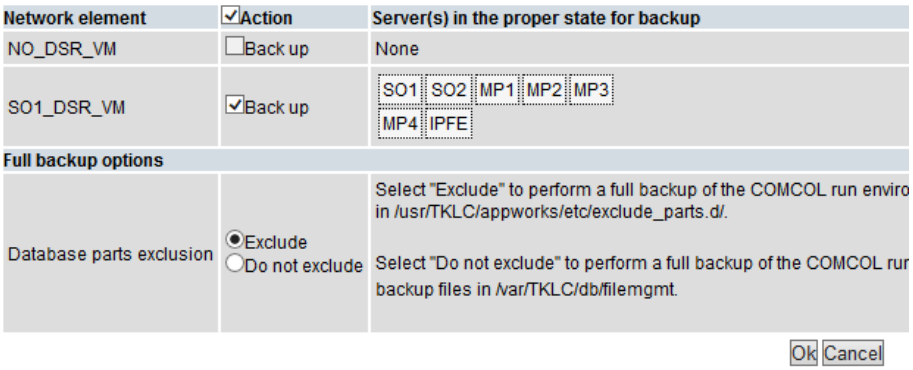
Since this backup is to be used in the event of disaster recovery, any site configuration changes made after this backup should be recorded and re-entered after the disaster recovery.

Procedure 20 is an alternate procedure that can be used to backup a site using the command line. Procedure 20 should only be used by direction of MOS.

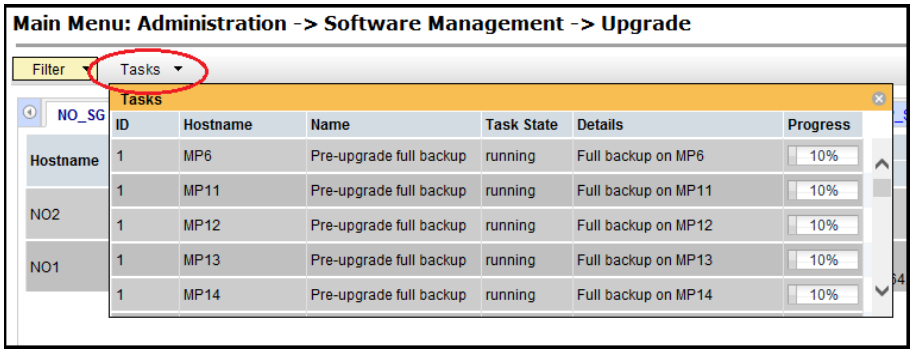
Procedure 19: Site Pre-Upgrade Backups

S T E P #	This procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	**Active SOAM VIP:** Backup Site configuration data **IMPORTANT: Required for Disaster Recovery**	Backup SOAM database. 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database** to return to the Database Status screen. 3. Click to highlight the **Active SOAM** server, and then click **Backup.** The Backup and Archive screen is displayed. **(NOTE: the Backup button will only be enabled when the Active server is selected.)** 4. Select the **Configuration** checkbox. 5. Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it. 6. Enter **Comments** (optional). 7. Click **OK**. NOTE: the Active SOAM can be determined by going to the **Status & Manage >HA** screen, and note which server is currently assigned the VIP in the "Active VIPs" field. The server having VIP assigned is the Active.
2. ☐	**Active SOAM VIP:** Save database backup **IMPORTANT: Required for Disaster Recovery**	Download and save backup files. 1. Select **Status & Manage > Files** The **Files** menu is displayed. 2. Click on the Active SOAM server tab**.** 3. Select the configuration database backup file and click the **Download** button. 4. If a confirmation window is displayed, click **Save**. 5. If the **Choose File** window is displayed, select a destination folder on the local workstation to store the backup file. Click **Save**. 6. If a **Download Complete** confirmation is displayed, click **Close**.

Procedure 19: Site Pre-Upgrade Backups

S T E P #		
	This procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
3. ☐	**Active NOAM VIP:**	Backup run environment for site being upgraded. 1. Login to the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade.** 3. Click the **Backup All** button. **Main Menu: Administration -> Software Management -> Upgrade** 
4. ☐	**Active NOAM VIP:**	The **Upgrade [Backup All]** screen is displayed. This screen displays the various Network Elements, and identifies which servers are ready for backup. 1. In the **Action** column, select the **Back up** checkbox for the Network Element to be upgraded. 2. Verify the check box for the NOAM server group is NOT checked. Note: Backing up the NOAM servers at this point will overwrite the pre-upgrade backup files that are needed for backing out the target release. Do NOT backup the NOAM servers. 3. In the **Full backup options** section, verify the 'Exclude' option is selected. 4. Click the **Ok** button. This initiates a full backup on each eligible server. 

Procedure 19: Site Pre-Upgrade Backups

S T E P #		
	This procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
5. ☐	**Active NOAM VIP:** Monitor for backup completion	Monitor the backup tasks **From the Active NOAM GUI:** 1. From the Upgrade screen, select the **Tasks** pulldown. 2. Monitor the progress of the backups until the Network Element(s) selected in step 4 are complete. 

6. ☐	**Active NOAM VIP:**
	Verify that backup files are present on each server.
		1. Log into the Active NOAM or SOAM GUI.
		2. Select **Status & Manage > Files** *(The **Files** menu is displayed)*
		3. Click on each Server tab, in turn
		4. For each Server, verify that the following (2) files have been created:
		
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		5. Repeat sub-steps 1 through 4 for each site being upgraded.

	THIS PROCEDURE HAS BEEN COMPLETED.	

5.1.3 Alternate SOAM Pre-Upgrade Backup

Procedure 20 creates a backup of some or all servers in the topology. This procedure is a manual command line alternative to the GUI backup in Procedure 19.

Procedure 20: Alternate SOAM Pre-Upgrade Backup

S T E P #	This procedure is a manual alternative backup. The procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	**Active SOAM CLI:** SSH to the Active SOAM	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active SOAM: `ssh admusr@<SOAM_VIP>`
2. ☐	**Active SOAM CLI:** Start a screen session.	Enter the following commands: `# screen` (The screen tool will create a no-hang-up shell session, so that the command will continue to execute if the user session is lost.)

Procedure 20: Alternate SOAM Pre-Upgrade Backup

S T E P #	This procedure is a manual alternative backup. The procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

3. ☐	**Active SOAM CLI:**
	Execute a backup of all servers managed from the SOAM to be upgraded.
		Execute the **backupAllHosts** utility on the Active SOAM. This utility will remotely access each specified server, and run the backup command for that server.
		
		The **--site** parameter allows the user to backup all servers associated with a given SOAM site to be upgraded:
		
		WARNING: Failure to include the --site parameter with the backupAllHosts command will result in overwriting the NOAM backup file created in Section 3.3.4. Backing out to the previous release is not possible if the file is overwritten.
		
		`$ /usr/TKLC/dpi/bin/backupAllHosts --site=<NEName>`
		
		…where **<NEName>** is the Network Element Name (**NEName**) as seen using the following command:
		
		`$ iqt NetworkElement`
		
		The following output will be generated upon execution of either of the above options:
		
		`Do you want to remove the old backup files (if exists ) from all the servers (y/[n])?y`
		
		It may take from 10 to 30 minutes for this command to complete, depending upon the number of servers and the data in the database.
		Do not proceed until the backup on each server is completed.
		
		Output similar to the following will indicate successful completion:
		
		`Script Completed. Status:`
		`HOSTNAME | STATUS`
		`----------`
		`HPC3blade02 | PASS`
		`HPC3blade01 | PASS`
		`HPC3blade03 | PASS`
		`HPC3blade04 | PASS`
		
		(Errors will also report back to the command line.)
		
		NOTE: There is no progress indication for this command; only the final report when it completes.

4. ☐	**Active SOAM CLI:**
	Exit the screen session.
		`# exit`
		
		`[screen is terminating]`
		
		NOTE: "screen -ls" is used to show active screen sessions on a server, and "screen -dr" is used to re-enter a disconnected screen session.

Procedure 20: Alternate SOAM Pre-Upgrade Backup

S T E P #	This procedure is a manual alternative backup. The procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

5. ☐	**ALTERNATIVE METHOD (Optional)**
	
	Server CLI:
	
	If needed, the Alternative backup method can be executed on each individual server instead of using the **"backupAllHosts"** script.
		ALTERNATIVE: A manual back up can be executed on each server individually, rather than using the script above. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:
		
		`$ sudo /usr/TKLC/appworks/sbin/full_backup`
		
		Output similar to the following will indicate successful completion:
		
		`Success: Full backup of COMCOL run env has completed.`
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullDBParts.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`
		
		`Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv.SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.`

6. ☐	**Active NOAM VIP:**
	
	Verify that backup files are present on each server.
		1. Log into the Active NOAM GUI using the VIP.
		2. Select **Status & Manage > Files**
		The **Files** menu is displayed
		3. Click on each server tab, in turn
		4. For each server, verify that the following (2) files have been created:
		
		`Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		`Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<time_stamp>.UPG.tar.bz2`
		
		Repeat sub-steps 1 through 4 for each site.

THIS PROCEDURE HAS BEEN COMPLETED.		

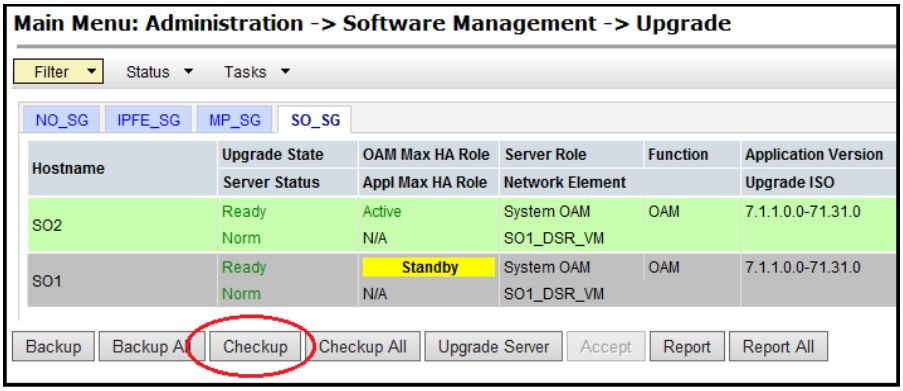
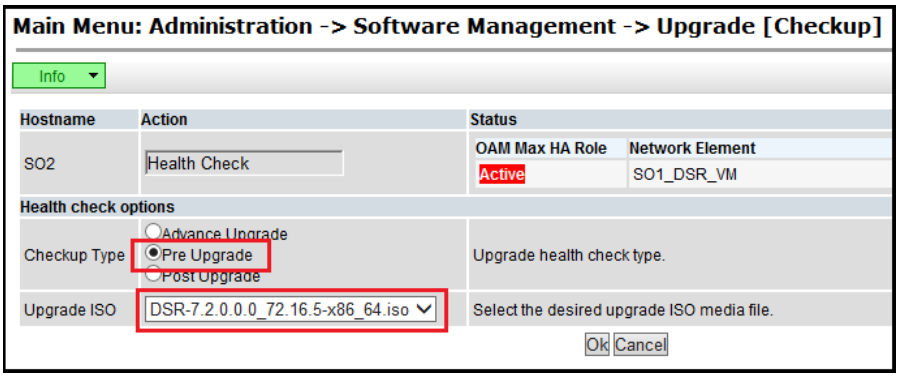
5.1.4 Site Pre-Upgrade Health Checks

This section provides procedures to verify the health of the SOAM site prior to upgrade. Procedure 21 is the primary procedure to be executed when the Active NOAM is on release 7.2 and later. Alternate release-specific procedures are provided, to be used as directed.

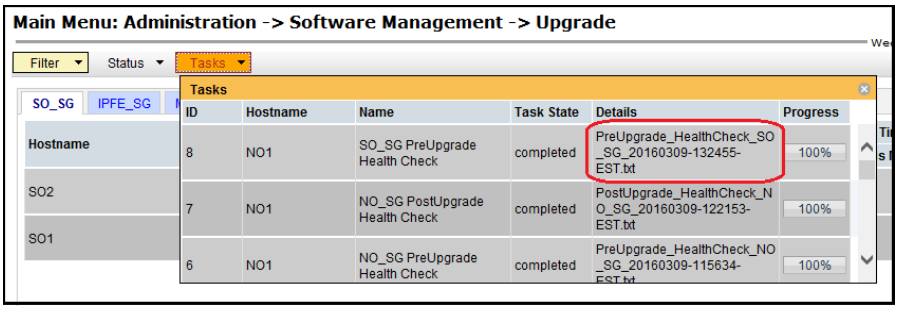
5.1.4.1 Site Pre-Upgrade Health Check for Release 7.2 and later

This procedure is used when the NOAMs are on Release 7.2 and later. The procedure is non-intrusive and performs a health check of the site prior to upgrading.

Procedure 21: Site Pre-Upgrade Health Check for Release 7.2 and later

S T E P #	This procedure performs a Health Check prior to upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1	**Active NOAM VIP:** Run health checks	This procedure will run the automated pre-upgrade Health Checks. 1. Select **Administration > Software Management > Upgrade**. The Upgrade screen is displayed. 2. Select the SOAM server group tab. 3. Select the Active SOAM.  4. Click the **Checkup** button. The Upgrade [Checkup] screen is displayed. 5. Under Health check options, select the **Pre Upgrade** option. 6. Use the Upgrade ISO pulldown to select the target release ISO. 7. Click **Ok**. Control returns to the Upgrade screen. 

Procedure 21: Site Pre-Upgrade Health Check for Release 7.2 and later

2 ☐	**Active NOAM VIP:** Monitor health check progress	Monitor for the completion of the Health Check. 1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PreUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The **Details** column will display a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. Open the report and review the results. 
3 ☐	**Active NOAM VIP:** Analyze health check results	Analyze Health Check report for failures. If the Health Check report status is anything other than “Pass”, the Health Check logs must be analyzed to determine if the upgrade can proceed. 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the file named “UpgradeHealthCheck.log” and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix J. If the health check log contains the message “Unable to execute Health Check on <Active SOAM hostname>”, perform the alternate health check in Procedure 22.
		THIS PROCEDURE HAS BEEN COMPLETED.

5.1.4.2 Site Pre-Upgrade Health Check for Release 7.0.1, 7.1.x

This procedure is an alternate health check that is used when upgrading to Release 7.3 and the Active SOAM is on Release 7.0.1 or 7.1.x. The procedure is non-intrusive and performs a health check of the site prior to upgrading.

Procedure 22: Site Pre-Upgrade Health Check for Release 7.0.1, 7.1.x

S T E P #	This procedure performs a Health Check prior to upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1. ☐	**ACTIVE SOAM CLI:**
	
	Verify SOAM pre-Upgrade Status
		Run health checks on Active SOAM.
		
		1. Use an SSH client to connect to the Active SOAM:
		
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: The static XMI IP address for each server should be available in Table 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck preUpgradeHealthCheckOnSoam`
		
		This command creates three files in `/var/TKLC/db/filemgmt/UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		`<SOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		
		If any alarms are present in the system:
		`<NOserver_name>_AlarmStatusReport_<date-time>.xml`
		
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		
		Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.
		
		3. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message. If the following message appears in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended to contact MOS for guidance.
		
		4. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

2. ☐	**ACTIVE SOAM CLI:** Capture Diameter Maintenance Status	Capture Diameter Maintenance status. 1. Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command will output a series of messages, providing Diameter Maintenance status. Capture this output and save for later use. Note: the output is also captured in /var/TKLC/db/filemgmt/UpgradeHealthCheck.log. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.

Procedure 22: Site Pre-Upgrade Health Check for Release 7.0.1, 7.1.x

3. ☐	**ACTIVE SOAM CLI:** View DA-MP Status	Capture DA-MP status. 1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established _____
4. ☐	**ACTIVE SOAM VIP:** Capture configuration on Active SOAM GUI	Export configuration data. 1. Select **Main Menu > Diameter Common > Export**. 2. Capture and archive the configuraiton data by setting the **Export Application** drop down entry to "**ALL**". 3. If SCP will be used to retrieve the export files in substep 6, select the **Export Directory - File Management Directory** radio button. 4. Click **Ok** to confirm. 5. Verify the requested data is exported using the tasks button at the top of the screen. 6. Select the File Management button to view the files available for download. Download all of the exported files to the client machine, or use the SCP utility to download the files from the Active NOAM to the client machine.
5. ☐	Capture Data for each SOAM Site	**Repeat steps 1 through 11 for each configured SOAM Site to be upgraded.**
THIS PROCEDURE HAS BEEN COMPLETED.		

5.1.5 Disable Site Provisioning

This procedure disables Site Provisioning in preparation for upgrading the site.

!! WARNING!! **THIS PROCEDURE MAY ONLY BE PERFORMED IN THE MAINTENANCE WINDOW IMMEDIATELY BEFORE THE START OF THE SOAM SITE UPGRADE.**

Procedure 23: Disable Site Provisioning

S T E P #	This procedure disables provisioning for the SOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active SOAM VIP:** Disable Site Provisioning	Disable Site Provisioning at the SOAM. 1. Log into the SOAM GUI of the site to be upgraded. 2. Select **Status & Manage > Database.** The Database Status screen is displayed. 3. Click the **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning;** a yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 004] - Site provisioning has been manually disabled**. The Active SOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
	THIS PROCEDURE HAS BEEN COMPLETED.	

SOAM UPGRADE
ACTIVE / STANDBY / SPARE

5.2 SOAM Upgrade Overview

This section contains the steps required to perform a major or incremental upgrade of the SOAMs for a DSR site.

During the site upgrade, site provisioning is disabled. Provisioning will be re-enabled at the completion of the site upgrade.

For each site in the DSR, the SOAM(s) and associated MPs and IPFEs should be upgraded within a single maintenance window.

Table 10 shows the estimated execution times for the SOAM upgrade. Procedure 25: Automated SOAM Upgrade (Active/Standby) is the recommended procedure for upgrading the SOAMs when there is no Spare. ASG will automatically upgrade the Standby SOAM, followed by the Active SOAM.

If the site does have a Spare SOAM, Procedure 26: Manual SOAM Upgrade (Active/Standby/Spare) is the recommended procedure. The manual upgrade procedure will upgrade the Standby and Spare SOAMs in parallel, followed by the Active SOAM.

Table 10: SOAM Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Iteration 1 & 2 Procedure 25	1:20-2:40	1:20-2:40	Automated SOAM Upgrade (Active/Standby)	No traffic impact
or Procedure 26	1:20-2:40	1:20-2:40	Manual SOAM Upgrade (Active/Standby/Spare)	

!! WARNING!!

THE FOLLOWING PROCEDURES MUST BE COMPLETED BEFORE THE START OF SOAM UPGRADE:

Procedure 19; [Procedure 21 or Procedure 22]; Procedure 23

5.2.1 Upgrade SOAMs

This section provides the procedures to upgrade the SOAMs. The SOAMs can be upgraded manually under user control, or automatically using the Automated Server Group Upgrade option. The recommended method for SOAM upgrade depends on the existence of a Spare SOAM. If the site includes a Spare SOAM, then the SOAMs are upgraded manually so that the Spare and Standby can be upgraded concurrently. This reduces the time required to upgrade the SOAMs.

Regardless of which SOAM upgrade option is used, Procedure 26 is required to ensure site provisioning is disabled.

If the site does *__not__* include a Spare SOAM, use the automated SOAM upgrade in Procedure 25.
If the site does include a Spare SOAM, use the manual SOAM upgrade in Procedure 26.

Procedure 24: SOAM Upgrade Pre-Checks

S T E P #		
	This procedure verifies traffic status, and verifies that Site Provisioning is disabled, in preparation for upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active SOAM VIP:** Verify Traffic status	View KPIs to verify traffic status. 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > KPIs**. 3. Inspect KPI reports to verify traffic is at the expected condition.
2. ☐	**Active SOAM VIP:** Verify Site Provisioning is disabled	Verify that Site Provisioning was properly disabled in Procedure 23. 1. In the GUI status bar, where it says *"Connected using …"*, check for the message **"Site Provisioning disabled"** If the message is present, continue with the next procedure per Table 9, otherwise, execute: Procedure 23: Disable Site Provisioning
	THIS PROCEDURE HAS BEEN COMPLETED.	

5.2.1.1 Automated SOAM Upgrade (Active/Standby)

Procedure 25 is the recommended method for upgrading the SOAMs if the site does not include a Spare SOAM. Upon completion of this procedure, proceed to the next procedure as specified in Table 9.

Procedure 25: Automated SOAM Upgrade (Active/Standby)

S T E P #		
	This procedure upgrades the SOAM(s) using the Automated Server Group Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	Upgrade SOAM Server Group	Upgrade the SOAM Server Group using the Upgrade Multiple Servers procedure with the following options: • Use the Automated Server Group Upgrade option • Select the **Serial** upgrade mode **Execute Appendix E** — Upgrade Multiple Servers Procedure After successfully completing the procedure in Appendix E, return to this point and continue with the next procedure per Table 9.
	THIS PROCEDURE HAS BEEN COMPLETED.	

NOTE: Once the Network Element SOAMs are upgraded, if any C-level server is removed from a Server Group and re-added, the server must be restored by way of Disaster Recovery procedures. The normal replication channel to the C-level server will be inhibited due to the difference in release versions.

5.2.1.2 Manual SOAM Upgrade (Active/Standby/Spare)

Procedure 26 is used to upgrade the SOAM Server Group if the site includes a Spare SOAM. If the SOAM Server Group was upgraded using Procedure 25, do not execute this procedure; continue with the next procedure per Table 9.

Procedure 26: Manual SOAM Upgrade (Active/Standby/Spare)

S T E P #		
	This procedure upgrades the SOAM(s) in a DSR using the manual upgrade method. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	Upgrade Standby and Spare SOAMs	Upgrade the Standby and Spare SOAM servers in parallel using Upgrade Multiple Servers procedure : **Execute Appendix E** - Upgrade Multiple Servers Procedure After successfully completing the procedure in **Appendix E**, return to this point and continue with the next procedure per Table 9.
2. ☐	Upgrade Active SOAM	Upgrade the Active SOAM server using Upgrade Single Server procedure : **Execute Appendix D** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix D, return to this point and continue with the next procedure per Table 9.
	THIS PROCEDURE HAS BEEN COMPLETED.	

NOTE: Once the Network Element SOAMs are upgraded, if any C-level server is removed from a Server Group and re-added, the server must be restored by way of Disaster Recovery procedures. The normal replication channel to the C-level server will be inhibited due to the difference in release versions.

5.3 Upgrade Iteration 3 Overview

Upgrade iteration 3 begins the upgrade of the site C-level servers. As shown in Table 7, iteration 3 consists of upgrading the DA-MPs, SS7-MPs, IPFEs, and Spare SBR(s), if equipped. The C-level components will be upgraded in parallel to maximize Maintenance Window usage.

Table 11 shows the estimated time required to upgrade the C-level servers for iteration 3.

Table 11: Iteration 3 Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 27	0:40-1:00	0:40-1:00	Upgrade Iteration 3	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Spare SBR(s) will be offline

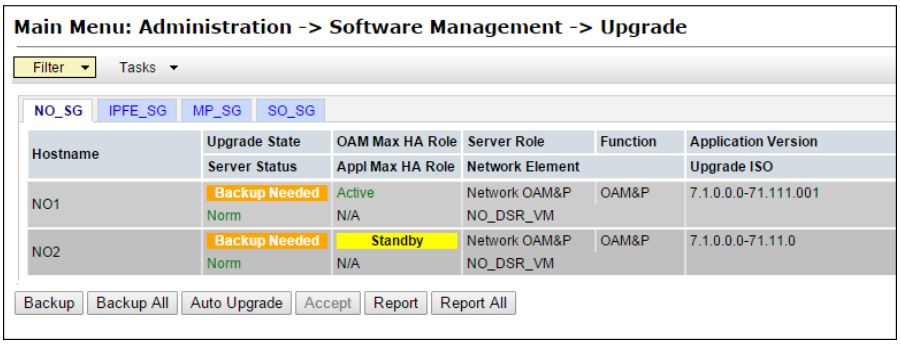
ASG DOES NOT ALLOW THE OPERATOR TO SPECIFY THE UPGRADE ORDER OF THE DA-MP SERVERS. IF A SPECIFIC ORDER IS REQUIRED TO MAINTAIN AVAILABILITY OF ANY ONE TARGET SET (I.E. ALL DA-MPS OF A TARGET SET ARE NOT SIMULTANEOUSLY UNAVAILABLE), THEN DO NOT USE ASG TO UPGRADE THE DA-MPS. ALTERNATE UPGRADE PROCEDURES ARE PROVIDED IN Appendix G.2.

NOTE: The intent of the upgrade iteration is to upgrade multiple server groups in parallel. After initiating the upgrade of a server group, proceed immediately to the next step to initiate the upgrade of the next server group.

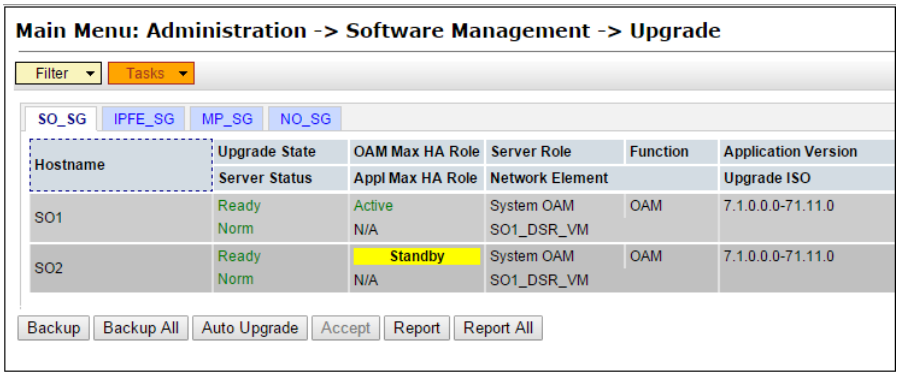
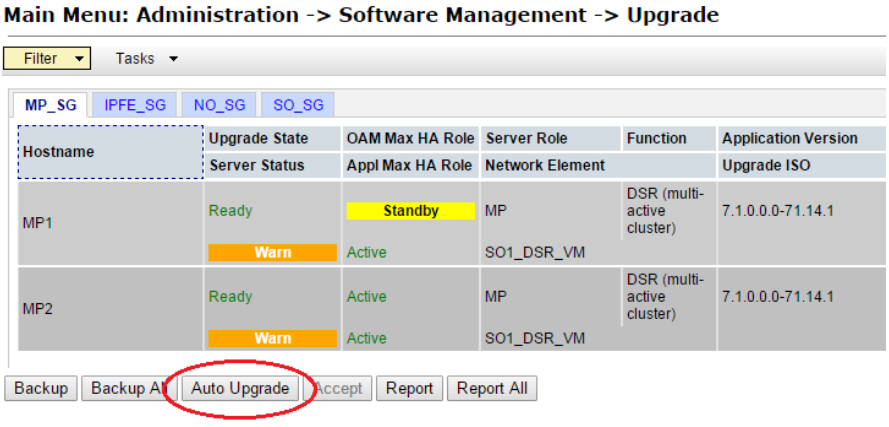
5.3.1 Upgrade Iteration 3

Procedure 27 provides the steps to upgrade ½ of the DA-MPs, ½ of the SS7-MPs, ½ of the IPFEs, and the Spare SBR(s). Refer to Table 8 for the hostnames of the servers to be upgraded in this iteration.

Procedure 27: Upgrade Iteration 3

S T E P #		
	This procedure upgrades a portion of the C-level servers for iteration 3. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** View pre-upgrade status of DA-MPs	View the pre-upgrade status of the DA-MP servers. 1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 3. Select the DA-MP Server Group tab. 4. For the DA-MP servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version.  5. If the servers are in "**Backup Needed"** state, select the servers and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**". 6. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)

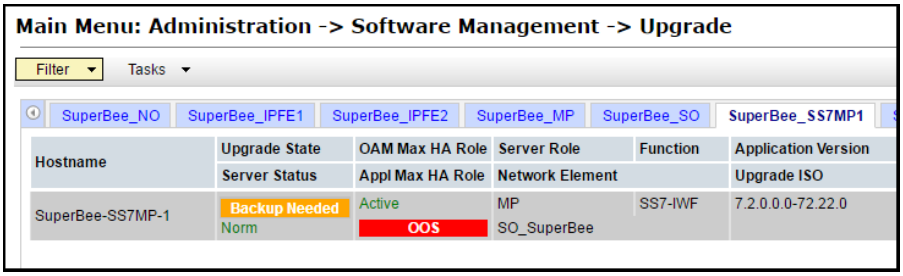
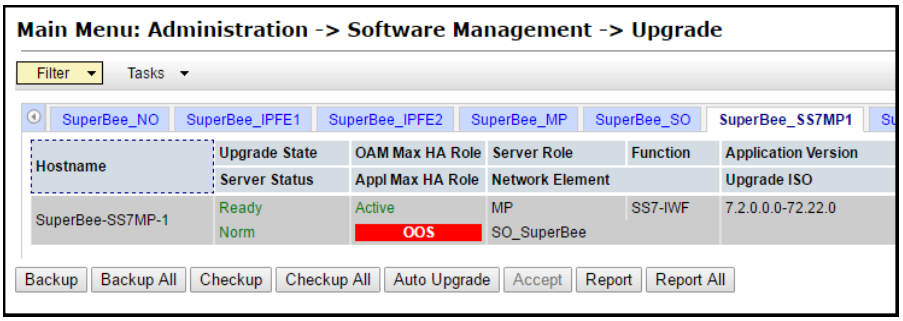
Procedure 27: Upgrade Iteration 3

2. ☐	**Active NOAM VIP:** Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the servers to be upgraded will show Upgrade Status = READY (This may take a minute). Depending on the servers being upgraded, new alarms may occur. The Upgrade Administration screen is displayed:  Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31106 (DB Merge to Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats)** or **(Lost Communication with Mate Server)**
3. ☐	**Active NOAM VIP:** Initiate DA-MP upgrade (part 1)	Initiate the Automated Server Group Upgrade option 1. To utilize the Automated Server Group upgrade option, verify that no servers in the server group are selected.  2. Click the **Auto Upgrade** button. The Upgrade [Initiate] screen is displayed.

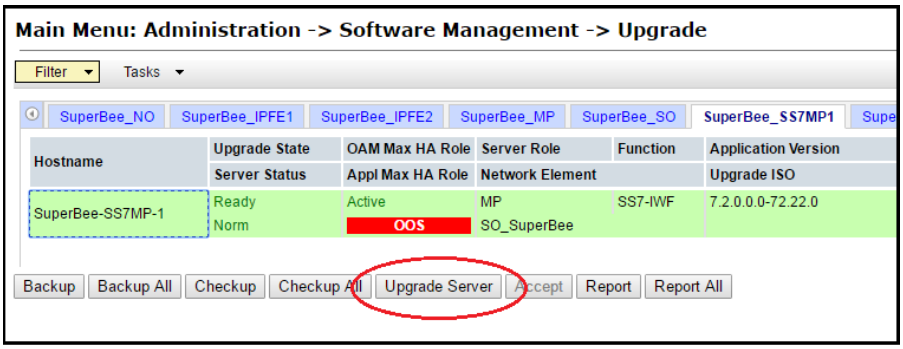
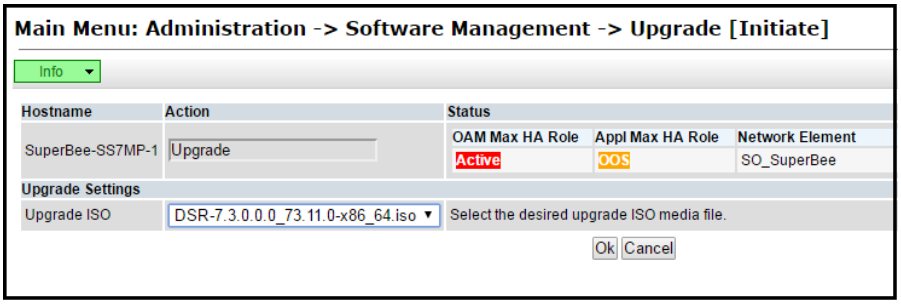
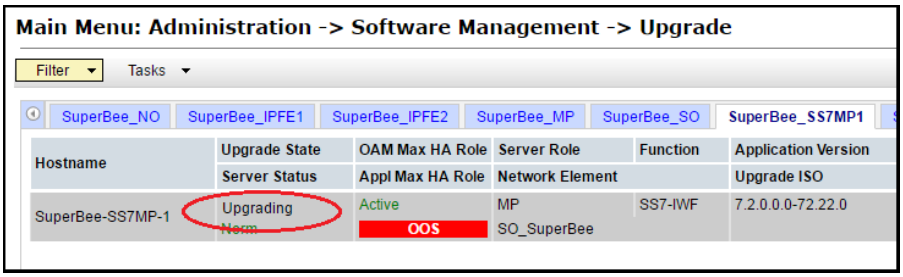
Procedure 27: Upgrade Iteration 3

4.	**Active NOAM VIP:** Initiate DA-MP upgrade (part 2)	Start the Automated Server Group Upgrade of the DA-MPs. 1. The **Upgrade Settings** section of the Initiate screen controls the behavior of the automated upgrade. Select **Bulk** Mode. 2. Select **50%** for the **Availability** setting. 3. Select the appropriate ISO from the **Upgrade ISO** pick list. 4. Click the **Ok** button to start the upgrade. **Main Menu: Administration -> Software Management -> Upgrade [Initiate]** Info Hostname / Action / Status (OAM Max HA Role / Appl Max HA Role / Network Element) MP1 — Auto upgrade — Standby / Active / SO1_DSR_VM MP2 — Auto upgrade — Active / Active / SO1_DSR_VM Upgrade Settings Mode: Bulk / Serial / Grouped Bulk — Server group upgrade mode. Select "Bulk" to upgrade servers in groups according to the availability s; Select "Serial" to upgrade servers one at a time in HA order; Select "Grouped Bulk" to upgrade servers in HA groups according to the; In all modes, any designated last server will be upgraded last. HA groups are created according to the "Application HA Role" of the ser; The HA role order is spare, observer, standby and active. Availability: 50% — Select the desired percent availability of servers in the server group duri; ('NONE' - all servers with 'Upgrade' action will be unavailable.) Upgrade ISO: DSR-7.1.0.0.0_71.14.1-x86_64.iso — Select the desired upgrade ISO media file. Ok Cancel
5.	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. 1. Observe the **Upgrade State** of the DA-MP servers. Upgrade status will be displayed under the **Status Message** column. **Main Menu: Administration -> Software Management -> Upgrade** Filter / Status / Tasks MP_SG / IPFE_SG / NO_SG / SO_SG Hostname / Upgrade State / Server Status / OAM Max HA Role / Appl Max HA Role / Server Role / Network Element / Function / Application Version / Upgrade ISO MP1 — Upgrading / Err — Standby / OOS — MP / SO1_DSR_VM — DSR (active/standby pair) — 7.2.0.0.0-72.18.0 / DSR-7.3.0.0.0_73.11.0-x86_64.iso MP2 — Pending / Err — Active / Active — MP / SO1_DSR_VM — DSR (active/standby pair) — 7.2.0.0.0-72.18.0 / DSR-7.3.0.0.0_73.11.0-x86_64.iso While the DA-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.
6.	Identify the SS7-MP Server Group(s) to Upgrade	If no SS7MPs are configured, proceed to step 14. From the data captured in Table 8, identify the SS7-MP server group(s) to upgrade in iteration 3.

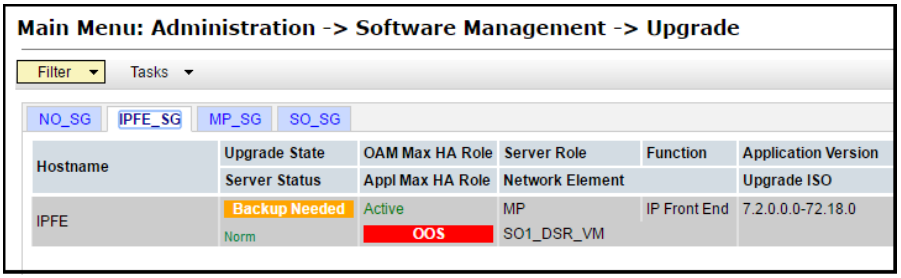
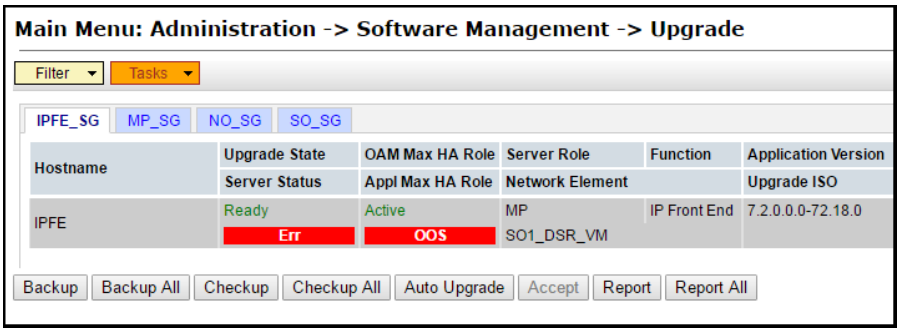
Procedure 27: Upgrade Iteration 3

7. ☐	**Active NOAM VIP:** View pre-upgrade status of SS7-MPs	View the pre-upgrade status of the SS7-MP servers. 1. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 2. Select each SS7-MP Server Group tab in turn. 3. For the SS7-MP servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version.  4. If the servers are in "**Backup Needed"** state, select the servers and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**". 5. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)
8. ☐	**Active NOAM VIP:** Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the servers to be upgraded will show Upgrade Status = READY (This may take a minute). Depending on the servers being upgraded, new alarms may occur. The Upgrade Administration screen is displayed:  Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31106 (DB Merge to Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats)** or **(Lost Communication with Mate Server)**

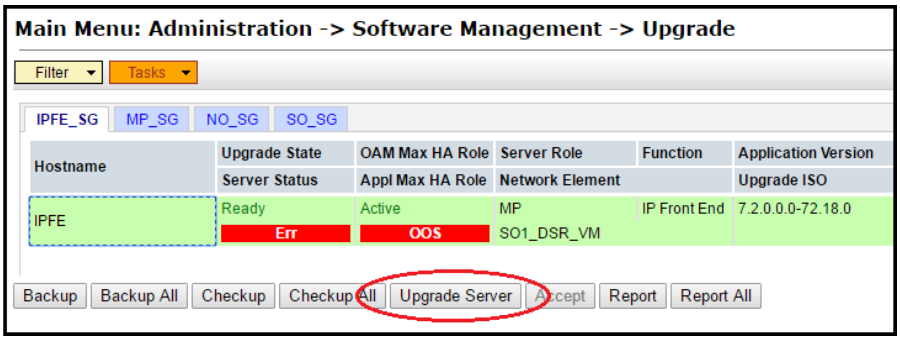
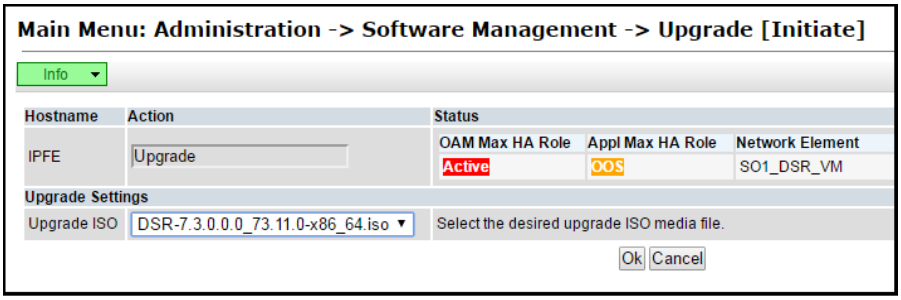
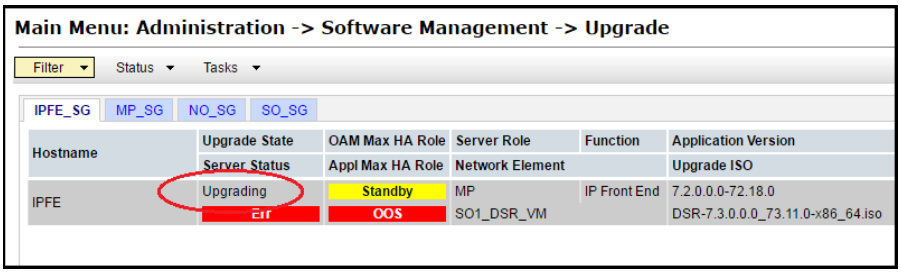
Procedure 27: Upgrade Iteration 3

9. ☐	**Active NOAM VIP:** Initiate SS7-MP upgrade (part 1)	Initiate the SS7-MP server upgrade. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click the "**Upgrade Server"** button.  The Initiate Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]**
10. ☐	**Active NOAM VIP:** Initiate SS7-MP upgrade (part 2)	Select target ISO. 1. On the **Upgrade [Initiate]** screen, select the target ISO from the Upgrade ISO picklist. 2. Click **Ok** to initiate the upgrade. 
11. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. 1. Observe the **Upgrade State** of the SS7-MP server. Upgrade status will be displayed under the **Status Message** column. 
12. ☐	Repeat for each SS7-MP	Repeat steps 6 through 11 for the next SS7-MP to be upgraded per Table 8.
13. ☐	Continue upgrade iteration 3	While the SS7-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.

Procedure 27: Upgrade Iteration 3

14. ☐	Identify the IPFE Server Group(s) to Upgrade	If no IPFEs are configured, proceed to step 21. From the data captured in Table 8, identify the IPFE server group(s) to upgrade in iteration 3.
15. ☐	**Active NOAM VIP:** View pre-upgrade status of IPFEs	View the pre-upgrade status of the IPFE servers. 1. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 2. Select each IPFE Server Group tab in turn. 3. For the IPFE servers to be upgraded in iteration 3, verify the Application Version value is the expected source software release version.  4. If the servers are in "**Backup Needed"** state, select the servers and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**". 5. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)
16. ☐	**Active NOAM VIP:** Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the servers to be upgraded will show Upgrade Status = READY (This may take a minute). Depending on the servers being upgraded, new alarms may occur. The Upgrade Administration screen is displayed:  Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31106 (DB Merge to Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats)** or **(Lost Communication with Mate Server)**

Procedure 27: Upgrade Iteration 3

17. ☐	**Active NOAM VIP:** Initiate IPFE upgrade (part 1)	Initiate the IPFE server upgrade. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click the "**Upgrade Server"** button.  The Initiate Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]**
18. ☐	**Active NOAM VIP:** Initiate SS7-MP upgrade (part 2)	Select target ISO. 1. On the **Upgrade [Initiate]** screen, select the target ISO from the Upgrade ISO picklist. 2. Click **Ok** to initiate the upgrade. 
19. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. 1. Observe the **Upgrade State** of the IPFE server. Upgrade status will be displayed under the **Status Message** column. 
20. ☐	Repeat for each IPFE	Repeat steps 14 through 19 for the next IPFE to be upgraded per Table 8.
21. ☐	Identify the SBR Server Group(s) to Upgrade	If no SBRs are configured, proceed to step 28. From the data captured in Table 8, identify the SBR server group(s) to upgrade in iteration 3.

Procedure 27: Upgrade Iteration 3

22. ☐	**Active NOAM VIP:** Verify status of Servers to be upgraded	For the SBR server group to be upgraded: 1. From the **Administration > Software Management > Upgrade** screen, select the SBR Server Group to be upgraded. 2. Verify the Application Version value is the expected source software release version for each SBR server in the selected server group. **Main Menu: Administration -> Software Management -> Upgrade** Filter ▾ Tasks ▾ EVONO | EVONODR | EVO_BPSBR_A | EVO_BPSBR_B | EVO_BPSBR_C | EVO_BPSBR_D | EVO_DAMP 3. If the server is in "**Backup Needed"** state, select the server and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**". 4. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)

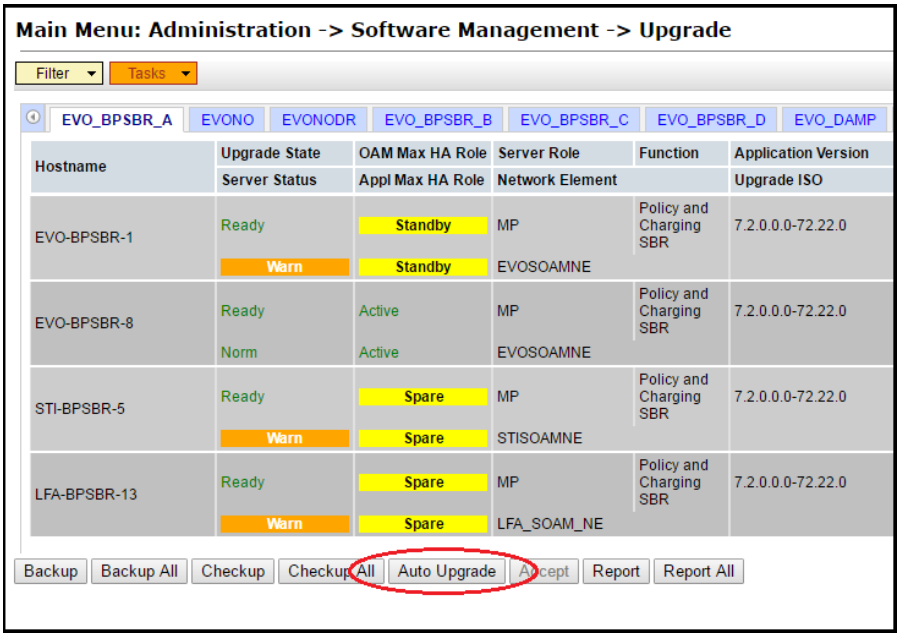
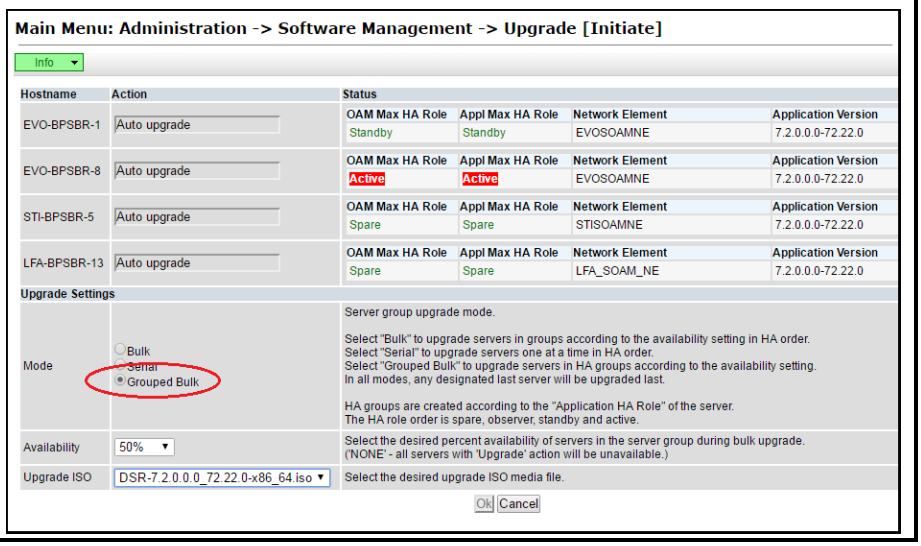
Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
EVO-BPSBR-1	Backup Needed Warn	Standby Standby	MP EVOSOAMNE	Policy and Charging SBR	7.2.0.0.0-72.22.0
EVO-BPSBR-8	Backup Needed Norm	Active Active	MP EVOSOAMNE	Policy and Charging SBR	7.2.0.0.0-72.22.0
STI-BPSBR-5	Backup Needed Warn	Spare Spare	MP STISOAMNE	Policy and Charging SBR	7.2.0.0.0-72.22.0
LFA-BPSBR-13	Backup Needed Warn	Spare Spare	MP LFA_SOAM_NE	Policy and Charging SBR	7.2.0.0.0-72.22.0

Procedure 27: Upgrade Iteration 3

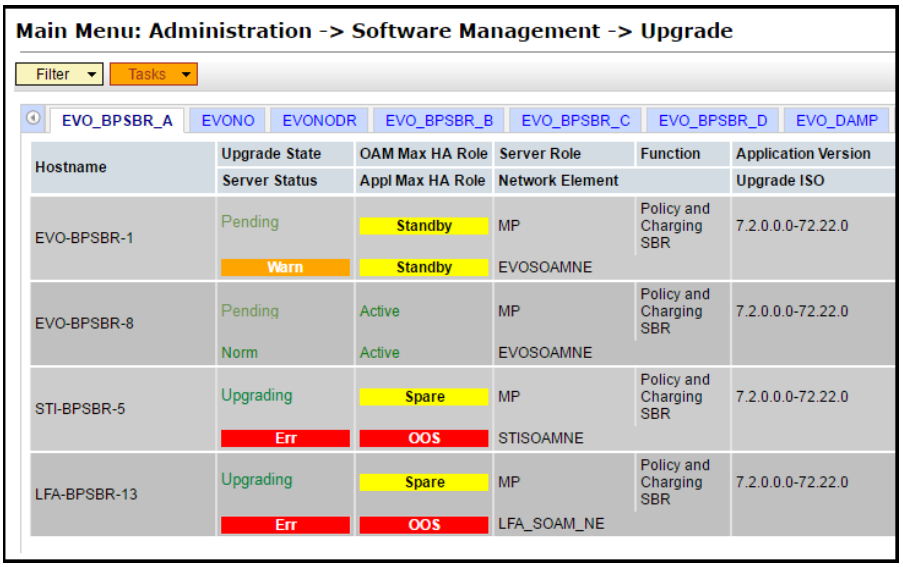
23. ☐	**Active NOAM VIP:** Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the server to be upgraded will show Upgrade Status = READY (This may take a minute). Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen is displayed: **Main Menu: Administration -> Software Management -> Upgrade** Filter Tasks EVONO EVONODR EVO_BPSBR_A EVO_BPSBR_B EVO_BPSBR_C EVO_BPSBR_D EVO_DAMP Backup Backup All Checkup Checkup All Auto Upgrade Accept Report Report All Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31106 (DB Merge to Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats)** or **(Lost Communication with Mate Server)**

Hostname	Upgrade State / Server Status	OAM Max HA Role / Appl Max HA Role	Server Role / Network Element	Function	Application Version / Upgrade ISO
EVO-BPSBR-1	Ready Warn	Standby Standby	MP EVOSOAMNE	Policy and Charging SBR	7.2.0.0.0-72.22.0
EVO-BPSBR-8	Ready Norm	Active Active	MP EVOSOAMNE	Policy and Charging SBR	7.2.0.0.0-72.22.0
STI-BPSBR-5	Ready Warn	Spare Spare	MP STISOAMNE	Policy and Charging SBR	7.2.0.0.0-72.22.0
LFA-BPSBR-13	Ready Warn	Spare Spare	MP LFA_SOAM_NE	Policy and Charging SBR	7.2.0.0.0-72.22.0

Procedure 27: Upgrade Iteration 3

24. ☐	**Active NOAM VIP:** Initiate SBR upgrade (part 1)	Initiate the Automated Server Group Upgrade option 1. To utilize the Automated Server Group upgrade option, select the SBR server group to be upgraded. 2. Verify that no servers in the server group are selected.  3. Click the **Auto Upgrade** button. The Upgrade [Initiate] screen is displayed.
25. ☐	**Active NOAM VIP:** Initiate SBR upgrade (part 2)	Start the Automated Server Group Upgrade. 1. The Upgrade **Settings** section of the Initiate screen controls the behavior of the automated upgrade. Select **Grouped Bulk** Mode. 2. Select an **Availability** setting of 50%. 3. Select the appropriate ISO from the **Upgrade ISO** pick list. 4. Click the **Ok** button to start the upgrade. 

Procedure 27: Upgrade Iteration 3

26. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. 1. Observe the **Upgrade State** of the SBR Server Group. Upgrade status will be displayed under the **Status Message** column. 
27. ☐	Repeat for each SBR Server Group	Repeat steps 21 through 26 for the next SBR Server Group to be upgraded per Table 8.

Procedure 27: Upgrade Iteration 3

28. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. See step 29 below for instructions if the upgrade fails, or if execution time exceeds 60 minutes. *Note: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade will be shown as "FAILED".* *The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.* 1. Navigate to **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 2. Sequence through the server group tabs for the server groups being upgraded. Observe the **Upgrade State** of the servers of interest. Upgrade status will be displayed under the **Status Message** column. **Main Menu: Administration -> Software Management -> Upgrade** Filter ▾ Status ▾ Tasks ▾ MP_SG | IPFE_SG | NO_SG | SO_SG | Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO | |---|---|---|---|---|---| | MP1 | Upgrading Err | Standby OOS | MP SO_DSR_VM | DSR (active/standby pair) | 7.1.0.0.0-71.6.0 DSR-7.1.0.0.0_71.8.1-x86_64.iso | | MP2 | Upgrading Err | Spare OOS | MP SO_DSR_VM | DSR (active/standby pair) | 7.1.0.0.0-71.6.0 DSR-7.1.0.0.0_71.8.1-x86_64.iso | Backup | Backup All | Auto Upgrade | Accept | Report | Report All During the upgrade, the servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **31101 (DB Replication To Slave Failure)** Alarm ID = **31106 (DB Merge To Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** Alarm ID = **31233 (HA Secondary Path Down)** Alarm ID = **31283 (Highly available server failed to receive mate heartbeats)** Alarm ID = **32515 (Server HA Failover Inhibited)** 3. The DA-MP and SBR server groups being upgraded with ASG will automatically sequence to iteration 4. Periodically monitor these servers for failures. 4. For the SS7-MP and IPFE servers being upgraded, wait for the upgrades to complete. The **Status Message** column will show "Success" after approximately 20 to 50 minutes. Do not proceed to iteration 4 until the SS7-MP and IPFE servers have completed upgrade. **NOTE: Do Not Accept any upgrade at this time.** **If any upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix I for failed server recovery procedures.**

Procedure 27: Upgrade Iteration 3

29. ☐	**Server CLI:**
	If the upgrade of a server fails:
		If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		
		It is recommended to contact MOS by referring to Appendix F of this document and provide these files.Refer to Appendix I for failed server recovery procedures.

THIS PROCEDURE HAS BEEN COMPLETED.		

5.4 Upgrade Iteration 4 Overview

Upgrade iteration 4 continues the upgrade of the site C-level servers. As shown in Table 7, iteration 4 consists of upgrading the second half of the DA-MPs, SS7-MPs, and IPFEs, as well as the Standby SBR(s), if equipped.

Table 12 shows the estimated time required to upgrade the C-level servers for iteration 4.

Table 12: Iteration 4 Upgrade Execution Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 28	0:40-1:00	0:40-1:00	Upgrade Iteration 4	½ DA-MPs, ½ SS7-MPs, ½ IPFEs, Standby SBR(s) will be offline

NOTE: The intent of the upgrade iteration is to upgrade multiple server groups in parallel. After initiating the upgrade of a server group, proceed immediately to the next step to initiate the upgrade of the next server group.

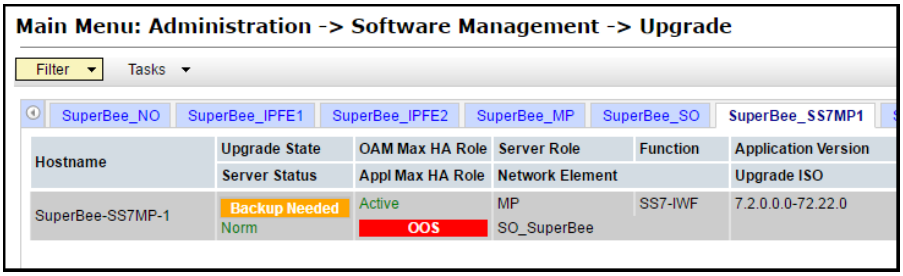
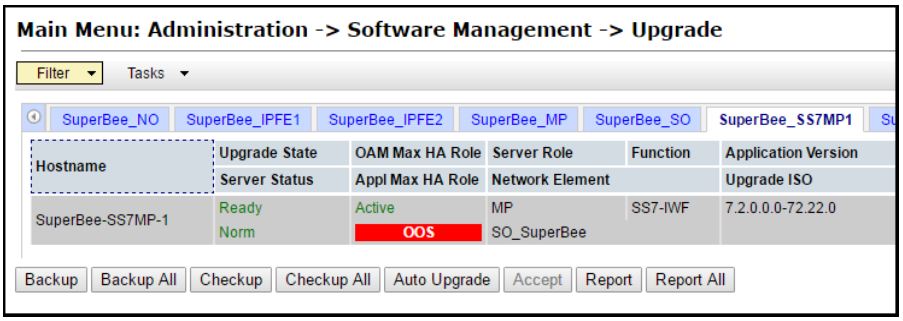
5.4.1 Upgrade Iteration 4

Procedure 28 provides the steps to upgrade ½ of the SS7-MPs, and ½ of the IPFEs. The DA-MPs and SBRs will automatically be upgraded by ASG. Refer to Table 8 for the hostnames of the servers to be upgraded in this iteration

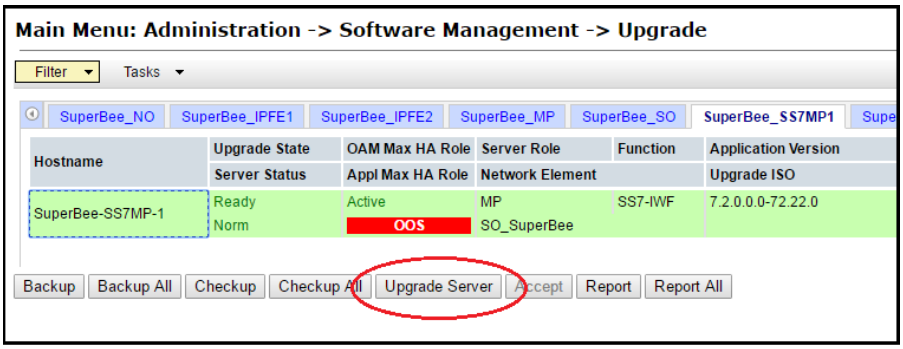
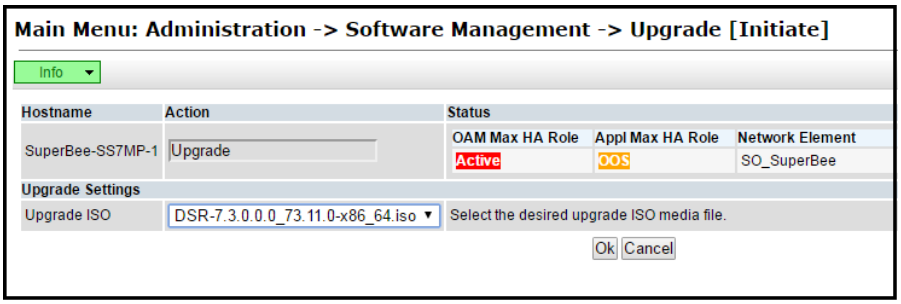
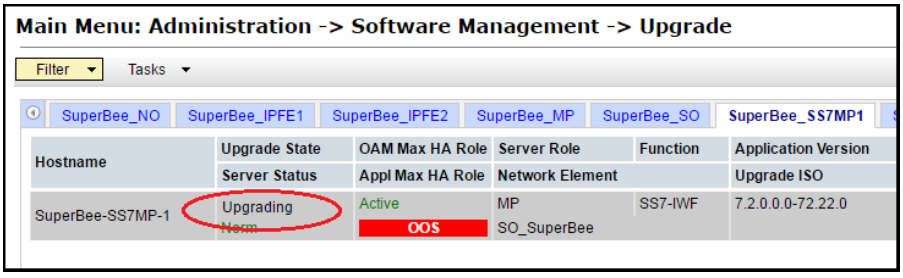
Procedure 28: Upgrade Iteration 4

S T E P #	This procedure upgrades a portion of the C-level servers for iteration 4. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	Identify the SS7-MP Server Group(s) to Upgrade	If no SS7MPs are configured, proceed to step 9. From the data captured in Table 8, identify the SS7-MP server group(s) to upgrade in iteration 4.

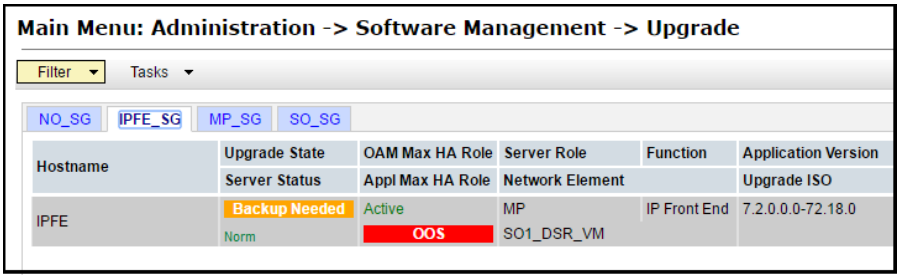
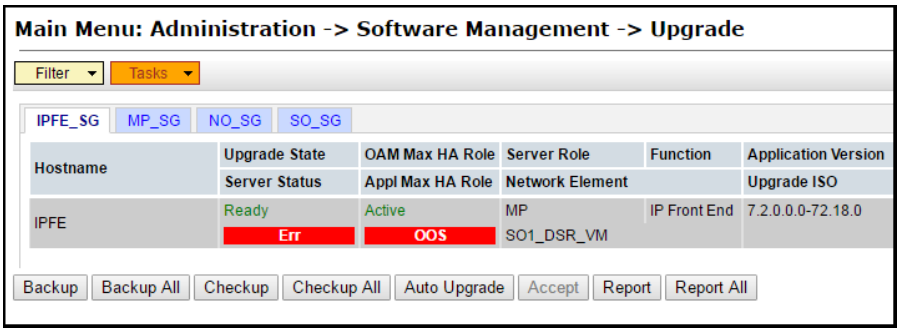
Procedure 28: Upgrade Iteration 4

2. ☐	**Active NOAM VIP:** View pre-upgrade status of SS7-MPs	View the pre-upgrade status of the SS7-MP servers. 1. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 2. Select each SS7-MP Server Group tab in turn. 3. For the SS7-MP servers to be upgraded in iteration 4, verify the Application Version value is the expected source software release version.  4. If the servers are in "**Backup Needed"** state, select the servers and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**". 5. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)
3. ☐	**Active NOAM VIP:** Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the servers to be upgraded will show Upgrade Status = READY (This may take a minute). Depending on the servers being upgraded, new alarms may occur. The Upgrade Administration screen is displayed:  Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31106 (DB Merge to Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats)** or **(Lost Communication with Mate Server)**

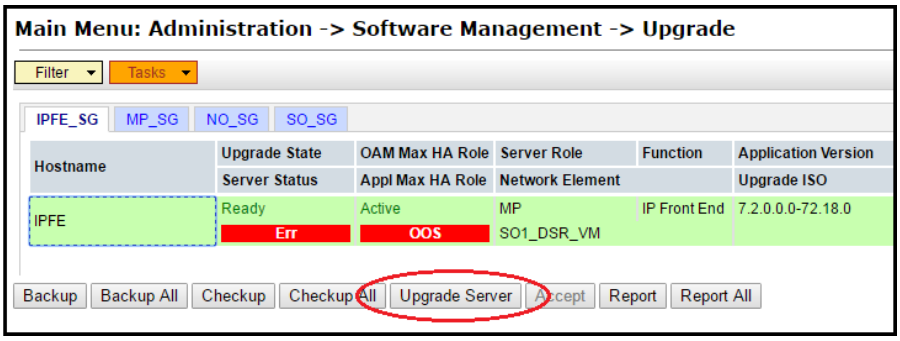
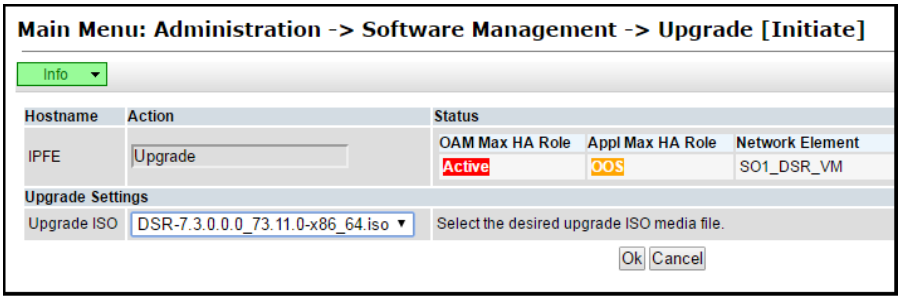
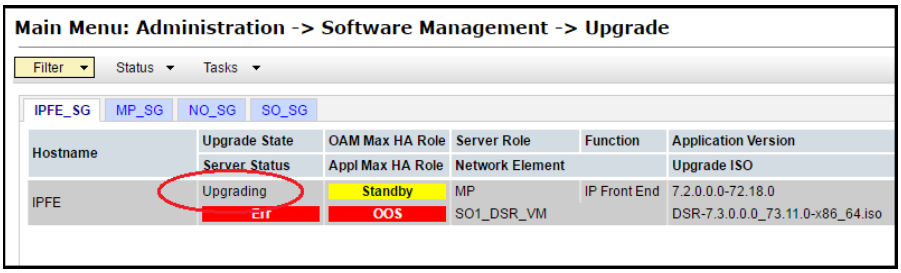
Procedure 28: Upgrade Iteration 4

4. ☐	**Active NOAM VIP:** Initiate SS7-MP upgrade (part 1)	Initiate the SS7-MP server upgrade. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click the "**Upgrade Server"** button.  The Initiate Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]**
5. ☐	**Active NOAM VIP:** Initiate SS7-MP upgrade (part 2)	Select target ISO. 1. On the **Upgrade [Initiate]** screen, select the target ISO from the Upgrade ISO picklist. 2. Click **Ok** to initiate the upgrade. 
6. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. 1. Observe the **Upgrade State** of the SS7-MP server. Upgrade status will be displayed under the **Status Message** column. 
7. ☐	Repeat for each SS7-MP	Repeat steps 1 through 6 for the next SS7-MP to be upgraded per Table 8.
8. ☐	Continue upgrade iteration 4	While the SS7-MP servers are upgrading, continue with the next step to upgrade additional C-level components in parallel.

Procedure 28: Upgrade Iteration 4

9. ☐	Identify the IPFE Server Group(s) to Upgrade	If no IPFEs are configured, proceed to step 16. From the data captured in Table 8, identify the IPFE server group(s) to upgrade in iteration 4.
10. ☐	**Active NOAM VIP:** View pre-upgrade status of IPFEs	View the pre-upgrade status of the IPFE servers. 1. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 2. Select each IPFE Server Group tab in turn. 3. For the IPFE servers to be upgraded in iteration 4, verify the Application Version value is the expected source software release version.  4. If the servers are in "**Backup Needed"** state, select the servers and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**". 5. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)
11. ☐	**Active NOAM VIP:** Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the servers to be upgraded will show Upgrade Status = READY (This may take a minute). Depending on the servers being upgraded, new alarms may occur. The Upgrade Administration screen is displayed:  Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31106 (DB Merge to Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats)** or **(Lost Communication with Mate Server)**

Procedure 28: Upgrade Iteration 4

12. ☐	**Active NOAM VIP:** Initiate IPFE upgrade (part 1)	Initiate the IPFE server upgrade. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click the "**Upgrade Server"** button.  The Initiate Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]**
13. ☐	**Active NOAM VIP:** Initiate IPFE upgrade (part 2)	Select target ISO. 1. On the **Upgrade [Initiate]** screen, select the target ISO from the Upgrade ISO picklist. 2. Click **Ok** to initiate the upgrade. 
14. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. 1. Observe the **Upgrade State** of the IPFE server. Upgrade status will be displayed under the **Status Message** column. 
15. ☐	Repeat for each IPFE	Repeat steps 9 through 14 for the next IPFE to be upgraded per Table 8.

Procedure 28: Upgrade Iteration 4

16. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. See step 17 below for instructions if the upgrade fails, or if execution time exceeds 60 minutes. *Note: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade will be shown as "FAILED".* *The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.* 1. Navigate to **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 2. Sequence through the server group tabs for the server groups being upgraded. Observe the **Upgrade State** of the servers of interest. Upgrade status will be displayed under the **Status Message** column. **Main Menu: Administration -> Software Management -> Upgrade** Filter ▾ Status ▾ Tasks ▾ MP_SG | IPFE_SG | NO_SG | SO_SG | Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role	Server Role Network Element	Function	Application Version Upgrade ISO | |---|---|---|---|---|---| | MP1 | Upgrading Err | Standby OOS | MP SO_DSR_VM | DSR (active/standby pair) | 7.1.0.0.0-71.6.0 DSR-7.1.0.0.0_71.8.1-x86_64.iso | | MP2 | Upgrading Err | Spare OOS | MP SO_DSR_VM | DSR (active/standby pair) | 7.1.0.0.0-71.6.0 DSR-7.1.0.0.0_71.8.1-x86_64.iso | Backup | Backup All | Auto Upgrade | Accept | Report | Report All During the upgrade, the servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **31101 (DB Replication To Slave Failure)** Alarm ID = **31106 (DB Merge To Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** Alarm ID = **31233 (HA Secondary Path Down)** Alarm ID = **31283 (Highly available server failed to receive mate heartbeats)** Alarm ID = **32515 (Server HA Failover Inhibited)** 3. The SBR server groups being upgraded with ASG will automatically sequence to iteration 5. Periodically monitor these servers for failures, if equipped. 4. For the DA-MP, SS7-MP and IPFE servers being upgraded, wait for the upgrades to complete. The **Status Message** column will show "Success" after approximately 20 to 50 minutes. Do not proceed to iteration 5 until the DA-MP, SS7-MP and IPFE servers have completed upgrade. **If the system does not have SBRs, the server upgrades are complete. Proceed to Procedure 30 per Table 9.**

Procedure 28: Upgrade Iteration 4

17. ☐	**Server CLI:**
	
	If the upgrade of a server fails:
		If any upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix I for failed server recovery procedures.
		
		If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`

		THIS PROCEDURE HAS BEEN COMPLETED.

5.5 Upgrade Iteration 5 Overview

Upgrade iteration 5 continues the upgrade of the site C-level servers. As shown in Table 7, iteration 5 consists of upgrading the Active SBR(s).

Table 11 shows the estimated time required to upgrade the remaining C-level servers for iteration 5.

Table 13: Iteration 4 Upgrade Execution Overview.

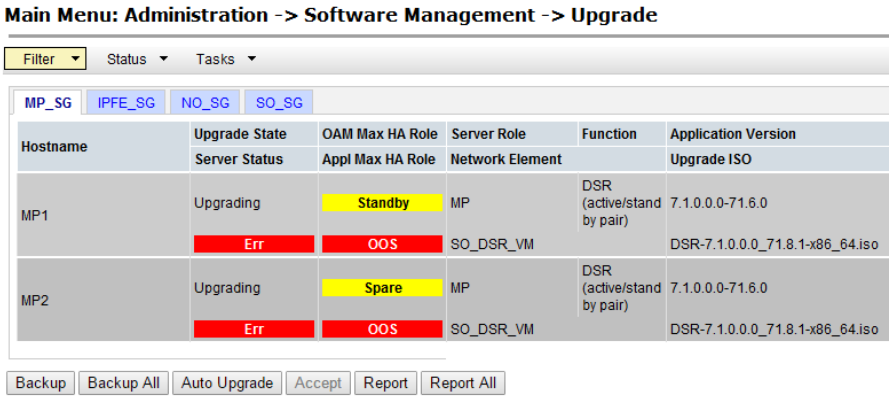
Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 29	0:40-1:00	0:40-1:00	Upgrade Iteration 5	Standby SBR will become Active; previously Active SBR will be offline for upgrade

5.5.1 Upgrade Iteration 5

Procedure 29 provides the steps to upgrade the Active SBRs. The SBRs are automatically upgraded by ASG so the task for iteration 5 is to monitor the upgrade progress. Refer to Table 8 for the hostnames of the servers upgraded in this iteration.

Procedure 29: Upgrade Iteration 5

1. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. See step 2 below for instructions if the upgrade fails, or if execution time exceeds 60 minutes. *Note: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade will be shown as "FAILED". The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.* 1. Navigate to **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 2. Sequence through the server group tabs for the server groups being upgraded. Observe the **Upgrade State** of the servers of interest. Upgrade status will be displayed under the **Status Message** column.



		During the upgrade, the servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **31101 (DB Replication To Slave Failure)** Alarm ID = **31106 (DB Merge To Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** Alarm ID = **31233 (HA Secondary Path Down)** Alarm ID = **31283 (Highly available server failed to receive mate heartbeats)** Alarm ID = **32515 (Server HA Failover Inhibited)** 3. Wait for the SBR upgrades to complete. The "Status Message" column will show "Success". This step will take approximately 20 to 50 minutes.

2. ☐	**Server CLI:**
	
	If the upgrade of a server fails:
		If any upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix I for failed server recovery procedures.
		
		If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`

		THIS PROCEDURE HAS BEEN COMPLETED.

THE FOLLOWING PROCEDURES MUST BE EXECUTED AT THE COMPLETION OF EACH SOAM SITE UPGRADE:

- **Procedure 30: Allow Site Provisioning**
- **Procedure 32: Verify Post-Upgrade Status**

AFTER ALL SOAM SITES IN THE TOPOLOGY HAVE COMPLETED UPGRADE, THE UPGRADE MAY BE ACCEPTED USING THE FOLLOWING PROCEDURE:

- **Procedure 42: Accept Upgrade**

5.6 Site Post-Upgrade Verification

The post-upgrade procedures consist of procedures that are performed after all of the site upgrades are complete. The final Health Check of the system collects alarm and status information to verify that the upgrade did not degrade system operation. After an appropriate soak time, the upgrade is accepted.

5.6.1 Allow Site Provisioning

This procedure enables Site Provisioning for the site just upgraded.

ANY PROVISIONING CHANGES MADE TO THIS SITE BEFORE THE UPGRADE IS ACCEPTED WILL BE LOST IF THE UPGRADE IS BACKED OUT

Procedure 30: Allow Site Provisioning

S T E P #	This procedure allows provisioning for SOAM and MP servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active SOAM VIP:** Enable Site Provisioning	1. Log into the SOAM GUI of the site just upgraded using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed. 3. Click the **Enable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Disable Site Provisioning**
THIS PROCEDURE HAS BEEN COMPLETED.		

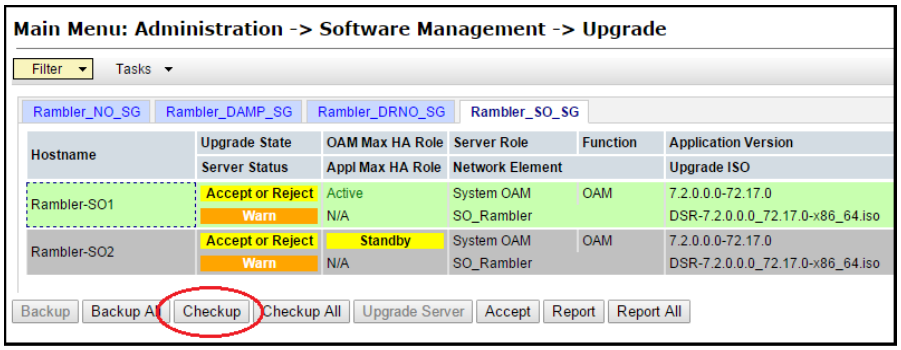
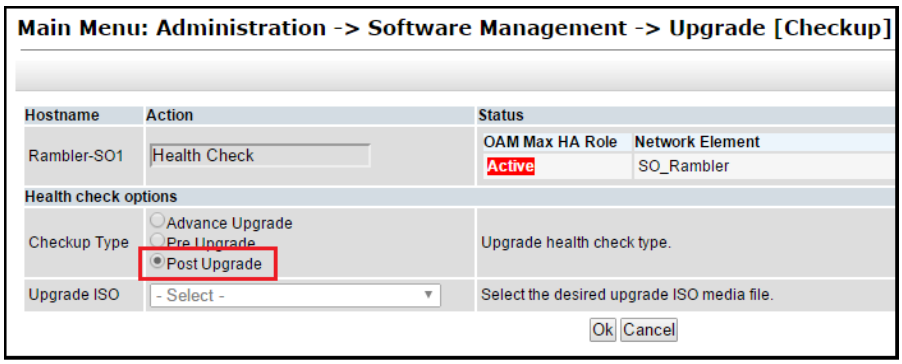
5.6.2 Site Post-Upgrade Health Checks

This section provides procedures to verify the validity and health of the site upgrade.

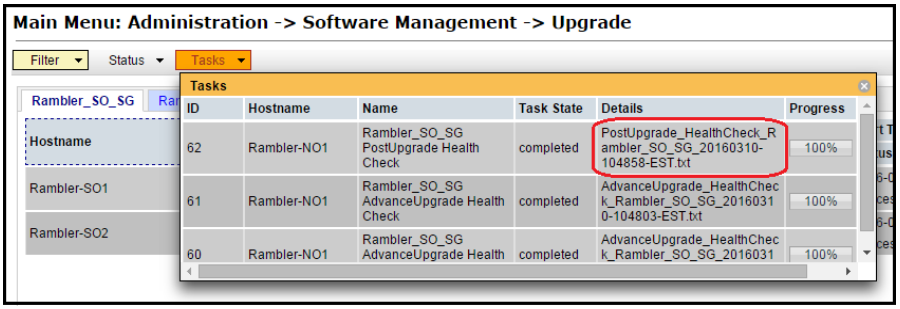
5.6.2.1 Site Post-UpgradeHealth Check

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers.

Procedure 31: Site Post-Upgrade Health Check

S T E P #	This procedure verifies Post-Upgrade site status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	**Active NOAM VIP:**	This procedure will run the automated post-upgrade Health Checks. **From the Active NOAM GUI:** 1. Select **Administration > Software Management > Upgrade**. The Upgrade screen is displayed. 2. Select the SOAM Server Group tab for the site being upgraded. 3. Select the Active SOAM.  4. Click the **Checkup** button. The Upgrade [Checkup] screen is displayed. 5. Under Health check options, select the **Post Upgrade** option. 6. Click **Ok**. Control returns to the Upgrade screen. 

Procedure 31: Site Post-Upgrade Health Check

2 ☐	**Active NOAM VIP:** Monitor health check progress	Monitor for the completion of the Health Check. **From the Active NOAM GUI:** 1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PostUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column will display a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. Open the report and review the results. 
3 ☐	**Active NOAM VIP:** Analyze health check results	Analyze Health Check failure. If the Health Check report status is anything other than “Pass”, the Health Check logs can be analyzed to determine if the upgrade can proceed. **From the Active NOAM GUI:** 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the file named “UpgradeHealthCheck.log” and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact MOS for guidance as described in Appendix J.
4 ☐	**Active SOAM VIP:** Export and archive configuration data	Export configuration data **From the Active SOAM GUI:** 1. Select **Main Menu > Diameter Common > Export** 2. Capture and archive the configuration data by choosing **Export Application** the drop down entry named “ALL”. 3. Click **Ok** to confirm. 4. If SCP will be used to retrieve the export files in step 6, select the **Export Directory** - File Management Directory radio button. 5. Verify the requested data is exported using the tasks button at the top of the screen. 6. Browse to **Main Menu >Status & Manage >Files** and download all the exported files to the client machine, or use the SCP utility to download the files from the Active SOAM to the client machine. 7. Select **Diameter > Maintenance > Applications** 8. Verify Operational Status is ‘**Available**’ for all applications
5 ☐	**Active SOAM Server:** Check if the setup previously has a customer supplied Apache certificate installed and protected with a passphrase, which was renamed before starting with upgrade.	If the setup had a customer-supplied Apache certificate installed and protected with passphrase before the start of the upgrade (refer to Procedure 2), the certification was renamed to server.crt-orig. To restore the customer-supplied certification, rename ‘server.crt-orig’ back to ‘server.crt’.

Procedure 31: Site Post-Upgrade Health Check

6 ☐	Compare data to the Pre-Upgrade health check to verify if the system has degraded after the second maintenance window.	Verify that the health check status of the upgraded site as collected from Steps 1 through 4 is the same as the pre-upgrade health checks taken in Procedure 21. If system operation is degraded, it is recommended to contact MOS.
THIS PROCEDURE HAS BEEN COMPLETED.		

5.6.2.2 Alternate SOAM Post-Upgrade Health Check

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers. This procedure is an alternative to the normal post upgrade health check in Procedure 31.

Procedure 32: Verify Post-Upgrade Status

S T E P #	This procedure verifies Post-Upgrade site status. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1. ☐	**ACTIVE SOAM CLI:**
	
	Verify SOAM post-Upgrade Status
		Run SOAM post-upgrade health check.
		
		1. Use an SSH client to connect to the Active SOAM:
		
		`ssh <SOAM XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: The static XMI IP address for each server should be available in Table 3.
		
		2. Enter the command:
		
		`$ upgradeHealthCheck postUpgradeHealthCheckOnSoam`
		
		This command creates files in `/var/TKLC/db/filemgmt/ UpgradeHealthCheck/` with the filename format:
		
		`<SOserver_name>_ServerStatusReport_<date-time>.xml`
		`<SOserver_name>_ComAgentConnStatusReport_<date-time>.xml`
		
		If any alarms are present in the system:
		`<SOserver_name>_AlarmStatusReport_<date-time>.xml`
		
		If the system is PDRA, one additional file is generated:
		`<SOserver_name>_SBRStatusReport_<date-time>.xml`
		
		Note: The same command used for pre-upgrade healthchecks "preUpgradeHealthCheckOnSoam" is also used to verify Post upgrade health status.
		
		Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.
		
		3. If the message "Server <hostname> needs operator attention before upgrade" is output, inspect the Server Status Report to determine the reason for the message. If the following message appears in the Server Status Report, the alert can be ignored: **Server <hostname> has no alarm with DB State as Normal and Process state as Kill**.
		
		Note: If any server status is not as expected, do not proceed with the upgrade. It is recommended to contact MOS for guidance.
		
		4. Keep these reports for future reference. These reports will be compared to alarm and status reports after the upgrade is complete.

2. ☐	**ACTIVE SOAM CLI:** Capture Diameter Maintenance Status	Capture Diameter Maintenance status. 1. Enter the command: `$ upgradeHealthCheck diameterMaintStatus` This command will output a series of messages, providing Diameter Maintenance status. Capture this output and save for later use. Note: the output is also captured in /var/TKLC/db/filemgmt/UpgradeHealthCheck.log. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored.

Procedure 32: Verify Post-Upgrade Status

3. ☐	**ACTIVE SOAM CLI:** View DA-MP Status	Capture DA-MP status. 1. Enter the command: `$ upgradeHealthCheck daMpStatus` This command outputs status to the screen for review. Note: The message "**FIPS integrity verification test failed**" may be output when the upgradeHealthCheck command runs. This message can be ignored. 2. Verify all Peer MPs are available 3. Note the number of Total Connections Established _____
4. ☐	Verify system health.	Verify that the health check status of the upgraded site as collected in this procedure is the same as the pre-upgrade health checks taken in Procedure 21. If system operation is degraded, it is recommended to report it to MOS.
	THIS PROCEDURE HAS BEEN COMPLETED.	

NOTE: *If another site is to be upgraded, all procedures specified by Table 9 must be executed. However, the user should be aware that mated sites should not be upgraded in the same maintenance window.*

6 BACKOUT PROCEDURE OVERVIEW

The procedures provided in this section return the individual servers and the overall DSR system to the source release after an upgrade is aborted. The backout procedures support two options for restoring the source release:

- Emergency backout
- Normal backout

The emergency backout overview is provided in Table 14. These procedures back out the target release software in the fastest possible manner, without regard to traffic impact.

The normal backout overview is provided in Table 15. These procedures back out the target release software in a more controlled manner, sustaining traffic to the extent possible.

All backout procedures are executed inside a maintenance window.

The backout procedure times provided in Table 14 and Table 15 are only estimates as the reason to execute a backout has a direct impact on any additional backout preparation that must be done.

Table 14: Emergency Backout Procedure Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 33	0:10-0:30	0:10-0:30	Backout Setup: The reason to execute a backout has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time will vary.	None.
Procedure 34	See Note	See Note	Emergency Site Backout: NOTE: Execution time of downgrading entire network is approximately equivalent to execution time taken during upgrade. 0:05 (5 minutes) can be subtracted from total time because ISO Administration is not executed during Backout procedures.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures will cause traffic loss.
Procedure 35	See Note	See Note	Emergency NOAM Backout: NOTE: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures will cause traffic loss.
Section 6.8	See Note	See Note	IDIH Backout NOTE: Execution time of downgrading the Oracle server is approximately equivalent to execution time to upgrade the server.	None
Procedure 40	0:01-0:05	Varies	Post-Backout Health Check	None

Table 15: Normal Backout Procedure Overview.

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 33	0:10-0:30	0:10-0:30	Backout Setup: The reason to execute a backout has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time will vary.	None.
Procedure 36	See Note	See Note	Normal Site Backout: NOTE: Execution time of downgrading entire network is approximately equivalent to execution time taken during upgrade. 0:05 (5 minutes) can be subtracted from total time because ISO Administration is not executed during Backout procedures.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures will cause traffic loss.
Procedure 37	See Note	See Note	Normal NOAM Backout: NOTE: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also backout procedures will cause traffic loss.
Section 6.8	See Note	See Note	IDIH Backout NOTE: Execution time of downgrading the Oracle server is approximately equivalent to execution time to upgrade the server.	None
Procedure 40	0:01-0:05	Varies	Post-Backout Health Check	None

6.1 Recovery Procedures

It is recommended to direct upgrade procedure recovery issues to MOS by referring to Appendix J of this document. Before executing any of these procedures, it is recommended to contact MOS.
Execute this section only if there is a problem and it is desired to revert back to the pre-upgrade version of the software.

Warning

Before attempting to perform these backout procedures, it is recommended to first contact MOS as described in Appendix J.

Warning

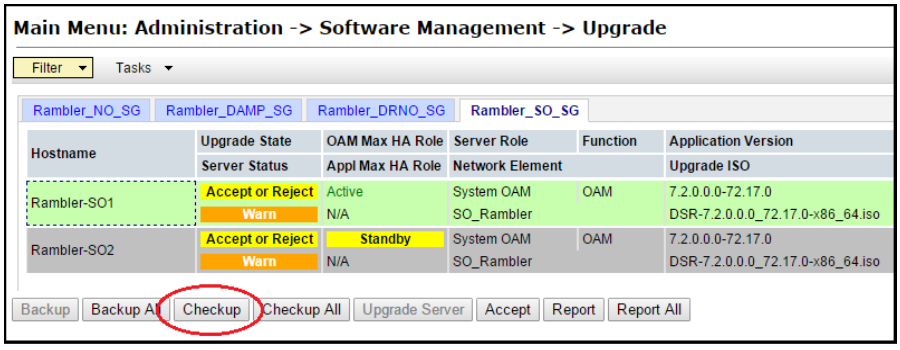
Backout procedures WILL cause traffic loss.

NOTE: These recovery procedures are provided for the backout of an Upgrade ONLY (i.e., from a failed 71.y.z release to the previously installed 7.0.w release). Backout of an initial installation is not supported.

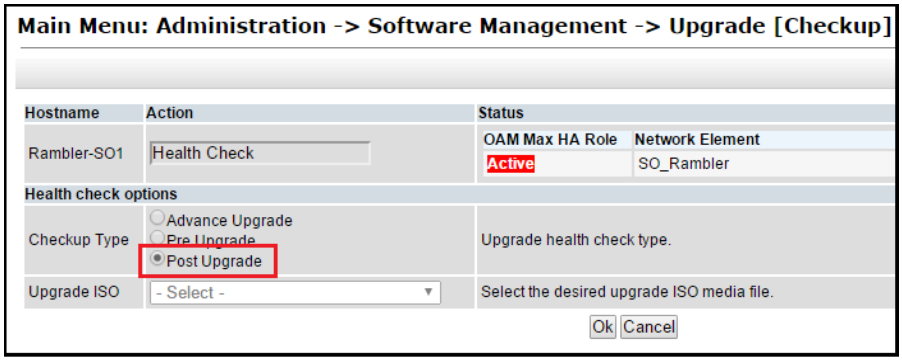
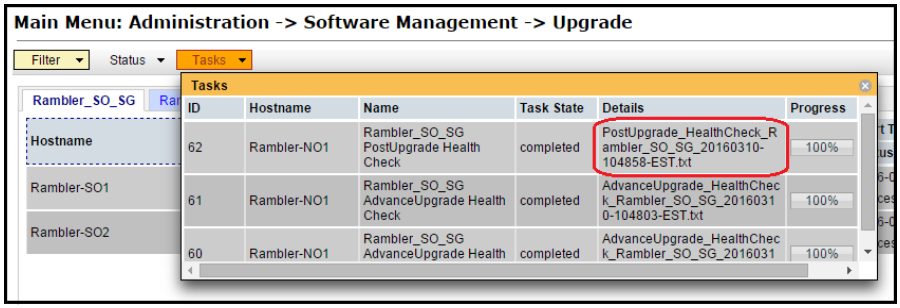
6.2 Backout Health Check

This section provides the procedure to verify that the DSR is ready for backout. The site post-upgrade Health Check is used to perform the backout Health Check.

Procedure 33: Backout Setup

S T E P #	This procedure is used to prepare a DSR system for backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	**Active NOAM VIP:**	This procedure will run the automated post-upgrade Health Checks for backout. 1. Select **Administration > Software Management > Upgrade**. The Upgrade screen is displayed. 2. Select the SOAM Server Group tab for the site being backed out. 3. Select the Active SOAM. 

Procedure 33: Backout Setup

		4. Click the **Checkup** button. The Upgrade [Checkup] screen is displayed. 5. Under Health check options, select the **Post Upgrade** option. 6. Click **Ok**. Control returns to the Upgrade screen. 
2.	**Active NOAM VIP:** Monitor health check progress	Monitor for the completion of the Health Check. 1. Click the **Tasks** dropdown to display the currently executing tasks. The Health Check task name appears as **<SOServerGroup> PostUpgrade Health Check**. 2. Monitor the Health Check task until the Task State is **completed**. The Details column will display a hyperlink to the Health Check report. 3. Click the hyperlink to download the Health Check report. Open the report and review the results. 
3.	**Active NOAM VIP:** Analyze health check results	Analyze Health Check results. If the Health Check report status is anything other than “Pass”, the Health Check logs can be analyzed to determine if the backout can proceed. 1. Select **Status & Manage > Files**. The Files screen is displayed. 2. Select the file named “UpgradeHealthCheck.log” and click **View**. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the backout. If necessary, it is recommended to contact MOS for guidance as described in Appendix J.

Procedure 33: Backout Setup

4. ☐	**Active NOAM VIP:** Identify IP addresses of servers to be backed out	1. Select **Administration > Software Management > Upgrade.** 2. Based on the "Application Version" column, identify all the hostnames that need to be backed out. 3. Select **Configuration > Servers.** 4. Using the data recorded in Table 3, note the XMI/iLO/LOM IP addresses of all the hostnames to be backed out. These are required to access the server when performing the backout. The reason to execute a backout has a direct impact on any additional backout preparation that must be done. The backout procedures **WILL** cause traffic loss. Since all possible reasons cannot be predicted ahead of time, it is recommended to contact MOS as stated in the **Warning** box above.
5. ☐	**Active NOAM VIP:** Verify backup archive files	1. Select **Status & Manage > Files**. 2. For each server to be backed out, select the server tab on the Files screen. Verify that the two backup archive files, created in section 3.3.4, are present on every server that is to be backed out. These archive files will have the format: Backup.<application>.<server>.**FullDBParts**.<role>.<date_time>.**UPG**.tar.bz2 Backup. <application>.<server>.**FullRunEnv**.<role>.<date_time>.**UPG**.tar.bz2
	THIS PROCEDURE HAS BEEN COMPLETED.	

EMERGENCY SITE BACKOUT

Use this section to perform an emergency backout of a DSR upgrade

6.3 Perform Emergency Backout

The procedures in this section perform a backout of all servers to restore the source release. An emergency backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. It is recommended to contact MOS, as stated in the warning box in Section 6.1, to verify that all corrective setup steps have been taken.

6.3.1 Emergency Site Backout

The procedures in this section backout all servers at a specific site without regard to traffic impact.

!! WARNING!! **EXECUTING THIS PROCEDURE WILL RESULT IN A TOTAL LOSS OF ALL TRAFFIC BEING PROCESSED BY THIS DSR. TRAFFIC BEING PROCESSED BY THE MATE DSR IS NOT AFFECTED.**

Procedure 34: Emergency Site Backout

S T E P #	This procedure is used to backout the DSR application software from multiple B- and C-level servers for a specific site. Any server requiring backout can be included: SOAMs, DA-MPs, SS7-MPs, IPFEs, and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	**Active NOAM VIP:** Identify all servers that require Backout	Identify all servers that require Backout (within a Site): 1. Log into the NOAM GUI using the VIP. 2. Select **Administration >Software Management >Upgrade.** The Upgrade Administration screen is displayed. 3. Identify the servers in the respective Server Groups with the target release **Application Version** value. These servers were previously upgraded but now require Backout. 4. Make note of these servers. They have been identified for backout. 5. Before initiating the backout procedure, remove all new servers and/or sites configured after upgrade was started.

Procedure 34: Emergency Site Backout

2. ☐	**Active NOAM VIP:** Disable Global Provisioning (if not already done)	Disable provisioning and configuration updates on the entire network (if not done previously): Since this step is being executed during a backout procedure, it is likely that Provisioning and Configuration updates are disabled already. If they have not been disabled, execute the following steps to disable provisioning: 1. Select **Status & Manage > Database.** The Database Status screen is displayed. 2. Click the **Disable Provisioning** button. 3. Confirm the operation by clicking **Ok** in the popup dialog box. 4. Verify the button text changes to **Enable Provisioning**. A yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 002] - Global provisioning has been manually disabled**. The Active NOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
3. ☐	**Active SOAM VIP:** Disable Site Provisioning for the site to be backed out.	Disable Site Provisioning 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed 3. Click the **Disable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Enable Site Provisioning.** A yellow information box will be displayed at the top of the view screen which states: 5. **[Warning Code 004] - Site provisioning has been manually disabled**. The Active SOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
		**!WARNING!** **STEP 4 WILL RESULT IN A TOTAL LOSS OF ALL TRAFFIC BEING PROCESSED BY THIS DSR**
4. ☐	Backout all C-level servers, as applicable	**For all configurations:** Backout all C-level servers (IPFEs, SBRs, SBRs, DA-MPs, and SS7-MPs) identified in step 1: Execute Section 6.6, Backout Multiple Servers.
5. ☐	Backout the Standby and Spare SOAM servers, as applicable	Backout the Standby and Spare DSR SOAM servers: If Standby and Spare SOAM servers are present: Execute Section 6.6, Backout Multiple Servers. If only a Spare SOAM server is present: Execute Section 6.5. Backout Single Server.
6. ☐	Backout the Active SOAM	Backout the Active DSR SOAM server: Execute Section 6.5, Backout Single Server.
7. ☐	Repeat work-around for other SOAM	Repeat step 6 on the other (now Standby) SOAM.

Procedure 34: Emergency Site Backout

8. ☐	**Active SOAM VIP:** Enable Site Provisioning	Enable Site provisioning 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Enable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Disable Site Provisioning**
	THIS PROCEDURE HAS BEEN COMPLETED.	

NOTE: If another site is to be backed out, follow all procedures in Table 14 in another maintenance window.

6.3.2 Emergency NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 35: Emergency NOAM Backout

S T E P #	This procedure is used to perform an emergency backout of the DSR application software from the NOAM servers. This procedure backs out the application software as quickly as possible, without regard to operational impact. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	Backout Standby DR NOAM server (if equipped)	Backout the Standby DR NOAM server: Execute Section 6.5 Backout Single Server.
2. ☐	Backout Active DR NOAM server (if equipped)	Backout the other DR NOAM server (now the Standby): Execute Section 6.5 Backout Single Server.
3. ☐	Backout Standby DSR NOAM server (as applicable)	Backout the Standby DSR NOAM server: Execute Section 6.5 Backout Single Server.
4. ☐	Backout Active DSR NOAM server	Backout the other DSR NOAM server (now the standby): Execute Section 6.5 Backout Single Server.
5. ☐	**Active NOAM VIP:** Enable Global Provisioning	Enable global provisioning and configuration updates on the entire network 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed. 3. Click the **Enable Provisioning** button. 4. Verify the button text changes to **Disable Provisioning**.
6. ☐	**Active NOAM VIP:** Remove 'Ready' state for any backed out server	Remove 'Ready' state 1. Select **Status & Manage > Servers**. The Server Status screen is displayed. 2. If any backed-out server Application Status is '**Disabled**', then select the server row and press the **Restart** button. 3. Select **Administration >Software Management >Upgrade** The Upgrade Administration screen is displayed. 4. If any backed-out server shows an Upgrade State of "**Ready**" or "**Success**", then select that server and press the **Complete Upgrade** button. Otherwise, skip this step. The Upgrade [Make Ready] screen will appear. 5. Click **OK**. This will now remove the Forced Standby designation for the backed-out server. NOTE: Due to backout being initiated from the command line instead of through the GUI, the following SOAP error may appear in the GUI banner. `SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]` It is safe to ignore this error message. 6. Verify the Application Version value for servers has been downgraded to the original release version.
	THIS PROCEDURE HAS BEEN COMPLETED.	

NORMAL SITE BACKOUT

Use this section to perform a normal backout of a DSR upgrade

6.4 Perform Normal Backout

The following procedures to perform a normal backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. It is recommended to contact MOS, as stated in the warning box in Section 6.1, to verify that all corrective setup steps have been taken.

6.4.1 Normal Site Backout

The procedures in this section backout all servers at a specific site.

Procedure 36: Normal Site Backout

S T E P #	This procedure is used to backout an upgrade of the DSR application software from multiple servers in the network. Any server requiring backout can be included: SOAMs, DA-MPs, SS7-MPs, IPFEs and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	**Active NOAM VIP:** Identify all servers that require Backout	Identify all servers that require Backout (within a Site): 1. Log into the NOAM GUI using the VIP. 2. Select **Administration >Software Management >Upgrade.** The Upgrade Administration screen is displayed. 3. Identify the servers in the respective Server Groups with the target release **Application Version** value. These servers were previously upgraded but now require Backout. 4. Make note of these servers. They have been identified for Backout. 5. Before initiating the backout procedure, remove all new servers and/or sites configured after upgrade was started.
2. ☐	**Active NOAM VIP:** Disable Global Provisioning (if not already done)	Disable provisioning and configuration updates on the entire network (if not done previously: Since this step is being executed during a backout procedure, it is likely that Provisioning and Configuration updates are disabled already. If they have not been disabled, execute the following steps to disable provisioning: 1. Select **Status & Manage > Database.** The Database Status screen is displayed. 2. Click the **Disable Provisioning** button. 3. Confirm the operation by clicking **Ok** in the popup dialog box. 4. Verify the button text changes to **Enable Provisioning**. A yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 002] - Global provisioning has been manually disabled**. The Active NOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**

Procedure 36: Normal Site Backout

3. ☐	**Active SOAM VIP:** Disable Site Provisioning for the site to be backed out	Disable Site Provisioning 1. Select **Status & Manage > Database** The Database Status screen is displayed 2. Click the **Disable Site Provisioning** button. 3. Confirm the operation by clicking **Ok** in the popup dialog box. 4. Verify the button text changes to **Enable Site Provisioning.** A yellow information box should also be displayed at the top of the view screen which states: **[Warning Code 004] - Site provisioning has been manually disabled**. The Active SOAM server will have the following expected alarm: Alarm ID = **10008 (Provisioning Manually Disabled)**
4. ☐	Backout the first set of C-level servers as applicable	Backout the first set of servers. The following servers can be backed out in parallel (as applicable) • Standby DA-MP for 1+1 (Active/Standby) configuration, or • ½ of all DA-MPs for N+0 (Multi-Active) configuration • Standby SBR(s) • Spare SBR(s) • ½ of all SS7-MPs • ½ of all IPFEs **NOTE: In a PCA System, the Spare SBR server is located at the mated site of the site being backed out.** Execute Section 6.6 - Backout Multiple Servers for the C-level servers identified above.
		**!WARNING!** **Failure to comply with step 5 and step 6 may result in the loss of PCA traffic, resulting in service impact**
5. ☐	**Active NOAM VIP:** Verify Standby SBR server status	If the server being backed out is the Standby SBR, execute this step. Otherwise, continue with step 6. 1. Navigate to **Main Menu -> Policy and Charging->Maintenance->SBR Status.** Open the tab of the server group being upgraded. 2. Do not proceed to step 6 until the **Resource HA Role** for the Standby server has a status of **Standby**. **Main Menu: Policy and Charging -> Maintenance -> SBR Status** Filter PCA_MATED_SITES Server Group Name / Resource Domain Name / Resource Domain Profile GTR_SBR_SG_A / PCA_SESSION / Policy and Charging Session Server Name / Resource HA Role / Congestion Level / Sub Resources Hosted GTR-SBR-1A / Active / Normal / 0,1,2,3,4,5,6,7 GTR-SBR-1B / Standby / Normal / 0,1,2,3,4,5,6,7 NSX-SBR-1Sp / Spare / Normal / 0,1,2,3,4,5,6,7

Procedure 36: Normal Site Backout

6. ☐	**Active NOAM VIP:** **Execute this Step for PCA installations only:** Verify bulk download is complete	Verify that bulk download is complete between the Active SBR in the server Group to the Standby and Spare SBRs. **From the Active NOAM GUI:** 1. Navigate to **Main Menu > Alarm & Event > View History** 2. Export the Event Log using the following filter: **Server Group**: Choose the SBR group that is in upgrade **Display Filter**: Event ID = 31127 – DB Replication Audit Complete **Collection Interval**: X hours ending in current time, where X is the time from upgrade completion of the Standby and Spare servers to the current time. 3. Wait for the following instances of Event 31127: • 1 for the Standby Binding SBR server • 1 for the Standby Session SBR server • 1 for the Spare Binding SBR server • 1 for the Spare Session SBR server • 1 for the 2nd Spare Binding SBR server, if equipped • 1 for the 2nd Spare Session SBR server, if equipped NOTE: There is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured.
7. ☐	Backout remaining C-level servers, as applicable	Backout the next set of servers. The following servers can be backed out in parallel (as applicable) • Active DA-MP for 1+1 (Active/Standby) configuration, or • ½ of all DA-MPs for N+0 (Multi-Active) configuration • Active SBR(s) • ½ of all SS7-MPs • ½ of all IPFEs Execute 6.5, Backout Single Server for each C-level server identified above.
8. ☐	Backout the Standby SOAM server	Backout the Standby DSR SOAM server: Execute Section 6.5 Backout Single Server.
9. ☐	Backout Active SOAM Server	Backout the Active DSR SOAM server: Execute Section 6.5 Backout Single Server.
10. ☐	Backout Spare SOAM Server (if applicable)	**NOTE: The Spare server is located at the mated site of the site being backed out.** Backout the spare SOAM server: Execute Section 6.5 Backout Single Server.
11. ☐	**Active SOAM VIP:** Enable Site Provisioning	Enable Site provisioning 1. Log into the SOAM GUI using the VIP. 2. Select **Status & Manage > Database.** The Database Status screen is displayed 3. Click the **Enable Site Provisioning** button. 4. Confirm the operation by clicking **Ok** in the popup dialog box. 5. Verify the button text changes to **Disable Site Provisioning**
	THIS PROCEDURE HAS BEEN COMPLETED.	

NOTE: If another site is to be backed out, follow all procedures in Table 15 in another maintenance window.

6.4.2 Normal NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 37: Normal NOAM Backout

S T E P #	This procedure is used to perform a normal backout of the DSR application software from the NOAM servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1. ☐	Backout Standby DR NOAM server (if equipped).	Backout the Standby DR NOAM server: Execute Section 6.5 Backout Single Server.
2. ☐	Backout Active DR NOAM server (if equipped).	Backout the Active DR NOAM server Execute Section 6.5 Backout Single Server.
3. ☐	Backout Standby DSR NOAM server (as applicable).	Backout the Standby DSR NOAM server: Execute Section 6.5 Backout Single Server.
4. ☐	Backout Active DSR NOAM server.	Backout the Active NOAM server: Execute Section 6.5 Backout Single Server.
5. ☐	**Active NOAM VIP:** Enable Global Provisioning	Enable global provisioning and configuration updates on the entire network 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Database** The Database Status screen is displayed. 3. Click the **Enable Provisioning** button. 4. Verify the button text changes to **Disable Provisioning**.
	THIS PROCEDURE HAS BEEN COMPLETED.	

6.5 Backout Single Server

This section provides the procedures to backout the application software on a single server.

CAUTION	**THIS PROCEDURE IS EXECUTED AS A COMPONENT OF THE EMERGENCY BACKOUT PROCEDURE (SECTION 6.3) OR THE NORMAL BACKOUT PROCEDURE (SECTION 6.4). THIS PROCEDURE SHOULD NEVER BE EXECUTED AS A STANDALONE PROCEDURE.**

Procedure 38: Backout Single Server

S T E P #		
	This procedure will backout the upgrade of DSR 7.3 application software. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**Active NOAM VIP:** Prepare the server for backout.	Perform the following steps to prepare the server for backout. 1. Select **Administration > Software Management > Upgrade**. The Upgrade Administration screen is displayed. 2. Select the server group tab containing the server to be backed out. Verify the Upgrade State is '**Accept or Reject**'. Make the server '**Backout Ready'** as follows: 3. Select **Status & Manage > HA.** The HA status screen displays. 4. Click the **Edit** button. 5. Select the server to be backed out and choose a Max Allowed HA Role value of **Standby** (unless it is a Query server, in which case the value should remain set to **Observer**). **Note: When the Active NOAM is the server being backed out, selecting OK will initiate an HA switchover, causing the GUI session to log out. Before logging into the Active OAM again, close and re-open the browser using the VIP address for the NOAM, and then clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.** 6. Click the **Ok** button. 7. The HA status screen displays. Verify the Max Allowed HA Role is set to the desired value for the server. 8. Select **Status & Manage > Server.** The server status screen is displayed. 9. Select the server to be backed out and click **Stop**. Click **Ok** to confirm the operation, then verify the Appl State changes to **Disabled**. 10. Select **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 11. Select the tab of the server group containing the server to be backed out. Verify the Upgrade State is now **Backout Ready**. (Note: It may take a couple of minutes for the status to update.)

2 ☐	**Server CLI:**
	
	SSH to server
		Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`
		
		NOTE: If direct access to the IMI is not available, then access the target server via a connection through the Active NOAM. SSH to the Active NOAM XMI first. From there, SSH to the target server's IMI address.

Procedure 38: Backout Single Server

3	**Server CLI:**
	Execute the backout
		Execute following command to find the state of the server to be backed out. :
		`$ ha.mystate`
		In the example output below, the HA state is Standby.
		`[admusr@SO2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby B2435.024 0 0127:113603.435`
		`VIP Stby B2435.024 0 0127:113603.438`
		`SbrBBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrBindingRes OOS B2435.024 0 0127:113601.918`
		`SbrSBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrSessionRes OOS B2435.024 0 0127:113601.918`
		`CacdProcessRes OOS B2435.024 0 0127:113601.918`
		`DA_MP_Leader OOS B2435.024 0 0127:113601.917`
		`DSR_SLDB OOS B2435.024 0-63 0127:113601.917`
		`VIP_DA_MP OOS B2435.024 0-63 0127:113601.917`
		`EXGSTACK_Process OOS B2435.024 0-63 0127:113601.917`
		`DSR_Process OOS B2435.024 0-63 0127:113601.917`
		`CAPM_HELP_Proc Stby B2435.024 0 0127:113603.272`
		`DSROAM_Proc OOS B2435.024 0 0128:081123.951`
		If the server being backed out is on release 7.0.1, and the state of the server is Active, then go back to step 1 above.
		`$ sudo /var/TKLC/backout/reject`
		NOTE: If backout prompts to continue, answer "**y**".
		(The reject command will create a no-hang-up shell session, so that the command will continue to execute if the user session is lost.)
		Sample output of the reject script:
		`Applications Enabled.`
		`Running /usr/TKLC/plat/bin/service_conf reconfig`
		`Remove isometadata (appRev) file from upgrade`
		`Reverting platform revision file`
		`RCS_VERSION=1.4`
		`Creating boot script: /etc/rc3.d/S89backout`
		`Rebuilding RPM database. This may take a moment...`
		`rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format`
		`Cleaning up chroot environment...`
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

4	Backout proceeds	Many informational messages are output to the terminal screen as the backout proceeds. Finally, after backout is complete, the server will automatically reboot.

5	**Server CLI:**
	SSH to server
		Use an SSH client to connect to the server (e.g. ssh, putty):
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`

Procedure 38: Backout Single Server

6 ☐	**Server CLI:**
	
	Restore the full DB run environment
		1. Execute the backout_restore utility to restore the full database run environment:
		
		`$ sudo /var/tmp/backout_restore`
		
		NOTE: If prompted to proceed, answer "**y**".
		
		NOTE: In some incremental upgrade scenarios, the backout_restore file will not be found in the `/var/tmp` directory, resulting in the following error message:
		
		`/var/tmp/backout_restore: No such file or directory`
		
		If this message occurs, copy the file from `/usr/TKLC/appworks/sbin` to /var`/tmp` and repeat sub-step 1.
		
		(The backout_restore command will create a no-hang-up shell session, so that the command will continue to execute if the user session is lost.)
		
		If the restore was successful, the following will be displayed:
		
		`Success: Full restore of COMCOL run env has completed.`
		`Return to the backout procedure document for further instruction.`
		
		If an error is encountered and reported by the utility, it is recommended to consult with MOS by referring to Appendix J of this document for further instructions.

7 ☐	**Server CLI:**
	
	Verify the backout
		1. Examine the output of the following commands to determine if any errors were reported:
		
		`$ sudo verifyBackout`
		
		The following command will show the current rev on the server:
		
		`$ appRev`
		`Install Time: Wed Feb 25 02:52:47 2015`
		`Product Name: DSR`
		`Product Release: 7.1.0.0.0_71.10.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.0.0.0_86.14.0`
		`Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64.iso`
		`ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso`
		`OS: OracleLinux 6.5`
		
		2. If the backout was not successful because other errors were recorded in the logs, it is recommended to contact MOS by referring to Appendix J of this document for further instructions.
		3. If the backout was successful (no errors or failures), then continue with the next step.

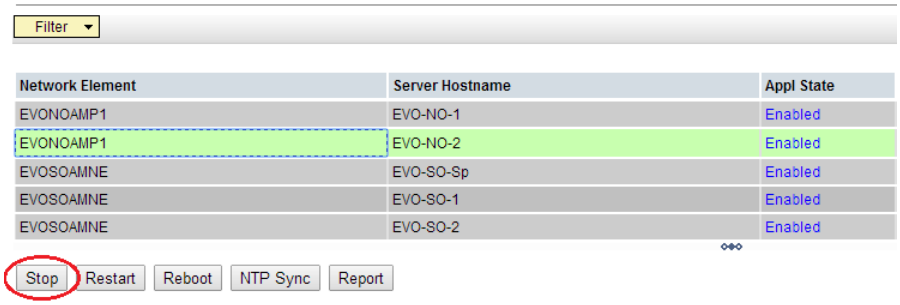
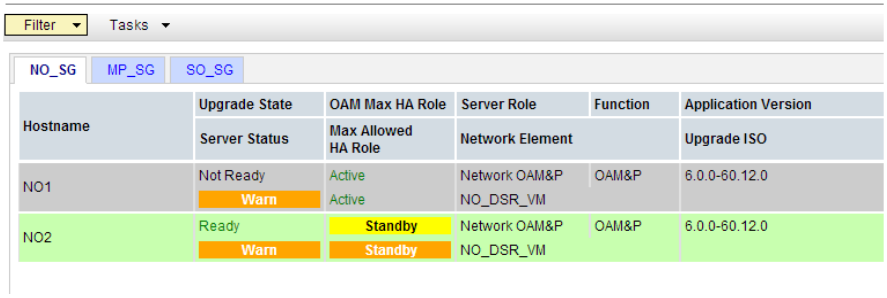
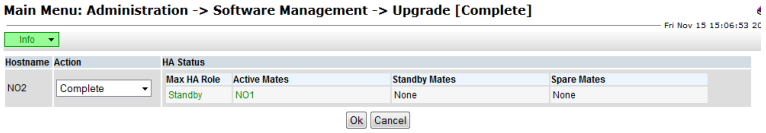
8 ☐	**Server CLI:** Reboot the server	Enter the following command to reboot the server: `$ sudo init 6` This step can take several minutes.

Procedure 38: Backout Single Server

9 ☐	**Server CLI:**
	
	Verify services restart (NOAM/SOAM only)
		If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 10.
		
		Verify OAM services have restarted.
		
		1. Wait several (approx. 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		2. SSH to the server and log in.
		
		`login as: admusr`
		`password: <enter password>`
		
		3. Execute the following command to verify the httpd service is running:
		
		`$ sudo service httpd status`
		
		4. The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored):
		
		`httpd <process IDs will be listed here> is running...`
		
		If httpd is not running, repeat sub-steps 3 and 4 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact MOS by referring to Appendix J of this document for further instructions.

10 ☐	**Active NOAM VIP:** Verify server states	Verify server state. 1. Select **Administration > Software Management > Upgrade** to observe the server upgrade status. **If the Active NOAM is on release 7.1.1 or later:** 2. If the server status is **Not Ready**, proceed to step 11; otherwise proceed to step 13. **If the Active NOAM is on release 7.0.1:** 2. If the server status is **Ready**, proceed to step 12; otherwise proceed to step 13.
11 ☐	**Active NOAM VIP:** Correct Upgrade State on backed out server **For Active NOAM on release 7.1.x or later**	Modify the backed out server to transition the Upgrade State to **Ready**. 1. Select **Status & Manage > HA** The HA status screen is displayed. 2. Click the **Edit** button. 3. Select the backed out server and choose a Max Allowed HA Role value of **Active** (unless it is a Query server, in which case the value should remain set to **Observer**). 4. Click the **Ok** button. 5. The HA status screen is displayed. Verify the Max Allowed HA Role is set to the desired value for the server. 6. Select **Status & Manage > Server.** The Server status screen is displayed. 7. If the Appl State of the server to be backed out is **Disabled**, select the server and click **Restart**. Click **Ok** to confirm the operation. Verify the Appl State updates to **Enabled**. 8. Select **Administration > Software Management > Upgrade**; The Upgrade Status screen is displayed. 9. Select the tab of the server group containing the server that was backed out. Verify the Upgrade State is now **Ready**. (Note: It may take a couple of minutes for the status to update.) **Proceed to step 13 to complete this procedure.**

Procedure 38: Backout Single Server

12	**Active NOAM VIP:** Remove Upgrade Ready status **For Active NOAM on release 7.0.1 only**	Remove Upgrade Ready status 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed. 3. If the server just backed-out shows an "**Appl State**" of **"Enabled"**, then select the server row and press the **Stop** button. **Main Menu: Status & Manage -> Server** 
13	**Active NOAM VIP:** Correct Upgrade State on backed out server **For Active NOAM on release 7.0.1 only**	Change the upgrade state for the backed out server. 1. Select **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 2. If the server just backed-out shows an Upgrade State of "**Ready**" or "**Success**", then select the backed-out server and press **Complete.** **Otherwise, skip to step 13.** **Main Menu: Administration -> Software Management -> Upgrade**  3. The **Upgrade** [**Complete]** screen will appear. Leave the Action set to hte default value of **Complete**. 4. Click **OK.** This will update the Max Allowed HA Role of the backed-out server to Active, which will cause the server's Upgrade State to move to **Not Ready**. **Main Menu: Administration -> Software Management -> Upgrade [Complete]**  The following SOAP error may appear in the GUI banner: `SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]` It is safe to ignore this error message.

Procedure 38: Backout Single Server

14 ☐	**Active NOAM VIP:** Verify application version	1. Select **Administration > Software Management > Upgrade** The Upgrade screen is displayed 2. Select the Server Group tab for the server that was backed out. **3.** Verify the **Application Version** value for this server has been downgraded to the original release version.
15 ☐	Procedure Complete	**The single server backout is now complete.** **Return to the overall DSR backout procedure step that directed the execution of this procedure.**
	THIS PROCEDURE HAS BEEN COMPLETED.	

6.6 Backout Multiple Servers

This section provides the procedures to backout the application software on multiple servers.

CAUTION

THIS PROCEDURE IS EXECUTED AS A COMPONENT OF THE EMERGENCY BACKOUT PROCEDURE (SECTION 6.3) OR THE NORMAL BACKOUT PROCEDURE (SECTION 6.4). THIS PROCEDURE SHOULD NEVER BE EXECUTED AS A STANDALONE PROCEDURE.

Procedure 39: Backout Multiple Servers

S T E P #	This procedure will backout the upgrade of DSR 7.3 application software for multiple servers. Any server requiring backout can be included: DA-MPs, SS7-MPs, IPFEs and SBRs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**Active NOAM VIP:** Prepare the server for backout. **For** Active **NOAM on release 7.1.1 and later**	**If the Active NOAM is on release 7.1.1 and later, perform this step; otherwise, proceed to step 2.** Perform the following steps to prepare the server for backout. 1. Select **Administration > Software Management > Upgrade**. The Upgrade Administration screen is displayed. 2. Select the server group tab containing the server to be backed out. Verify the Upgrade State is '**Accept or Reject**'. Make the server '**Backout Ready'** as follows: 3. Select **Status & Manage > HA.** The HA status screen displays. 4. Click the **Edit** button. 5. Select the server to be backed out and choose a Max Allowed HA Role value of **Standby** (unless it is a Query server, in which case the value should remain set to **Observer**). **Note: When the Active NOAM is the server being upgraded, selecting OK will initiate an HA switchover, causing the GUI session to log out. Before logging into the Active OAM again, close and re-open the browser using the VIP address for the NOAM, and then clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.** 6. Click the **Ok** button. 7. The HA status screen displays. Verify the Max Allowed HA Role is set to the desired value for the server. 8. Select **Status & Manage > Server.** The server status screen is displayed. 9. Select the server to be backed out and click **Stop**. Click **Ok** to confirm the operation, then verify the Appl State updates to **Disabled**. 10. Select **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 11. Select the tab of the server group containing the server to be backed out. Verify the Upgrade State is now **Backout Ready**. (Note: It may take a couple of minutes for the status to update.)

2 ☐	**Server CLI:**
	
	Login to the server(s)
		Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`
		
		NOTE: If direct access to the IMI is not available, then access the target server via a connection through the Active NOAM. SSH to the Active NOAM XMI first. From there, SSH to the target server's IMI address.

Procedure 39: Backout Multiple Servers

3 ☐	**Server CLI:**
	
	Execute the backout
		Determine the state of the server to be backed out. The server role must be either **Standby** or **Spare**. Execute following command to find the state :
		
		`$ ha.mystate`
		
		In the example output below, the HA state is Standby.
		
		`[admusr@SO2 ~]# ha.mystate`
		`resourceId role node subResources lastUpdate`
		`DbReplication Stby B2435.024 0 0127:113603.435`
		`VIP Stby B2435.024 0 0127:113603.438`
		`SbrBBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrBindingRes OOS B2435.024 0 0127:113601.918`
		`SbrSBaseRepl OOS B2435.024 0 0127:113601.918`
		`SbrSessionRes OOS B2435.024 0 0127:113601.918`
		`CacdProcessRes OOS B2435.024 0 0127:113601.918`
		`DA_MP_Leader OOS B2435.024 0 0127:113601.917`
		`DSR_SLDB OOS B2435.024 0-63 0127:113601.917`
		`VIP_DA_MP OOS B2435.024 0-63 0127:113601.917`
		`EXGSTACK_Process OOS B2435.024 0-63 0127:113601.917`
		`DSR_Process OOS B2435.024 0-63 0127:113601.917`
		`CAPM_HELP_Proc Stby B2435.024 0 0127:113603.272`
		`DSROAM_Proc OOS B2435.024 0 0128:081123.951`
		
		If the state of the server is Active, then return to step 1 above.
		
		`$ sudo /var/TKLC/backout/reject`
		
		NOTE: If backout prompts to continue, answer "**y**".
		
		(The reject command will create a no-hang-up shell session, so that the command will continue to execute if the user session is lost.)
		
		Sample output of the reject script:
		
		`Applications Enabled.`
		`Running /usr/TKLC/plat/bin/service_conf reconfig`
		`Remove isometadata (appRev) file from upgrade`
		`Reverting platform revision file`
		`RCS_VERSION=1.4`
		`Creating boot script: /etc/rc3.d/S89backout`
		`Rebuilding RPM database. This may take a moment...`
		`rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format`
		`Cleaning up chroot environment...`
		
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

4 ☐	**Server CLI:** Backout proceeds	Many informational messages are output to the terminal screen as the backout proceeds. Finally, after backout is complete, the server will automatically reboot.
5 ☐	Repeat for each server to be backed out.	Repeat steps 1 through 4 for each server to be backed out.

6 ☐	Login to the server	Use an SSH client to connect to the server (e.g. ssh, putty):
		
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`

Procedure 39: Backout Multiple Servers

7 ☐	**Server CLI:**
	
	Restore the full DB run environment
		1. Execute the backout_restore utility to restore the full database run environment:
		
		`$ sudo /var/tmp/backout_restore`
		
		If prompted to proceed, answer "**y**".
		
		NOTE: In some incremental upgrade scenarios, the backout_restore file will not be found in the `/var/tmp` directory, resulting in the following error message:
		
		`/var/tmp/backout_restore: No such file or directory`
		
		If this message occurs, copy the file from `/usr/TKLC/appworks/sbin` to /var`/tmp` and repeat sub-step 1.
		
		(The backout_restore command will create a no-hang-up shell session, so that the command will continue to execute if the user session is lost.)
		
		If the restore was successful, the following will be displayed:
		
		`Success: Full restore of COMCOL run env has completed.`
		`Return to the backout procedure document for further instruction.`
		
		If an error is encountered and reported by the utility, it is recommended to consult with MOS by referring to Appendix J of this document for further instructions.

8 ☐	**Server CLI:**
	
	Verify the backout
		1. Examine the output of the following commands to determine if any errors were reported:
		
		`$ sudo verifyBackout`
		
		The following command will show the current rev on the server:
		
		`$ appRev`
		`Install Time: Wed Feb 25 02:52:47 2015`
		`Product Name: DSR`
		`Product Release: 7.1.0.0.0_71.10.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.0.0.0_86.14.0`
		`Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64.iso`
		`ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso`
		`OS: OracleLinux 6.5`
		
		2. If the backout was not successful because other errors were recorded in the logs, it is recommended to contact MOS by referring to Appendix J of this document for further instructions.
		3. If the backout was successful (no errors or failures), then continue with the next step.

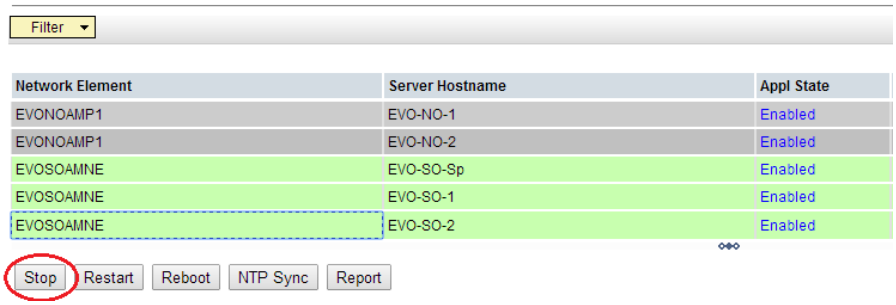
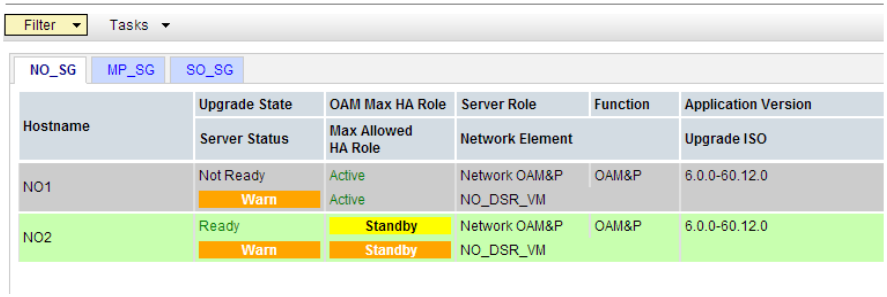
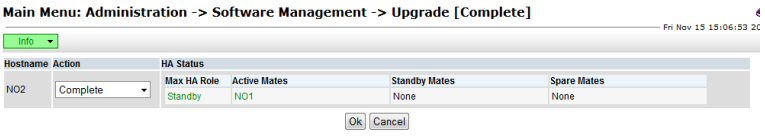
9 ☐	**Server CLI:** Reboot the server	Enter the following command to reboot the server: `$ sudo init 6` This step can take several minutes.

Procedure 39: Backout Multiple Servers

10 ☐	**Server CLI:**
	
	Verify services restart (NOAM/SOAM only)
		If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 11.
		
		Verify OAM services have restarted:
		
		1. Wait several (approx. 6 minutes) minutes for a reboot to complete before attempting to log back into the server.
		2. SSH to the server and log in.
		
		`login as: admusr`
		`password: <enter password>`
		
		3. Execute the following command to verify the httpd service is running.
		
		`$ sudo service httpd status`
		
		4. The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored):
		
		`httpd <process IDs will be listed here> is running...`
		
		If httpd is not running, repeat sub-steps 3 and 4 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact MOS by referring to Appendix J of this document for further instructions.

11 ☐	Repeat for each server backed out	Repeat steps 6 through 10 for each server backed out.
12 ☐	**Active NOAM VIP:** Verify server states	Verify server state is correct after the backout. 1. Select **Administration > Software Management > Upgrade** to observe the server upgrade status. **If the Active NOAM is on release 7.1.1 or later:** 2. If the server status is **Not Ready**, proceed to step 13; otherwise proceed to step 16. **If the Active NOAM is on release 7.0.1:** 3. If the server status is **Ready**, proceed to step 14; otherwise proceed to step 16.
13 ☐	**Active NOAM VIP:** Correct Upgrade State on backed out server **For Active NOAM on release 7.1.1 or later**	Modify the backed out server to transition the Upgrade State to **Ready**. 1. Select **Status & Manage > HA** The HA status screen is displayed. 2. Click the **Edit** button. 3. Select the backed out server and choose a Max Allowed HA Role value of **Active** (unless it is a Query server, in which case the value should remain set to **Observer**). 4. Click the **Ok** button. 5. The HA status screen is displayed. Verify the Max Allowed HA Role is set to the desired value for the server. 6. Select **Status & Manage > Server.** The Server status screen is displayed. 7. Select the server being backed out and click **Restart**. Click **Ok** to confirm the operation. Verify the Appl State updates to **Enabled**. 8. Select **Administration > Software Management > Upgrade**; The Upgrade Status screen is displayed. 9. Select the tab of the server group containing the server that was backed out. Verify the Upgrade State is now **Ready**. (Note: It may take a couple of minutes for the status to update.) **Proceed to step 16 to complete the procedure.**

Procedure 39: Backout Multiple Servers

14	**Active NOAM VIP:** Remove Upgrade Ready status **For Active NOAM on release 7.0.1 only**	Remove Upgrade Ready status 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed. 3. If the servers just backed-out show an "**Appl State"** of **Enabled**, then multi-select the server rows and press the **Stop** button. 4. Click **OK** on the confirmation dialog box. **Main Menu: Status & Manage -> Server** 
15	**Active NOAM VIP:** Correct Upgrade State on backed out server **For Active NOAM on release 7.0.1 only**	Correct the upgrade status on the backed out server. 1. Select **Administration > Software Management > Upgrade.** The Upgrade Administration screen is displayed. 2. If the servers just backed-out show an Upgrade State of "**Ready**" or "**Success**", then select the backed-out server and press the **Complete** button. If the servers just backed out show an Upgrade State of "**Not Ready**", then proceed to step 16. **Main Menu: Administration -> Software Management -> Upgrade**  3. The **Upgrade [Complete]** screen will appear. Leave the Action set to hte default value of **Complete**. 4. Click **OK.** This will update the Max Allowed HA Role of the backed-out server to Active, which will cause the server's Upgrade State to move to **Not Ready**. **Main Menu: Administration -> Software Management -> Upgrade [Complete]**  The following SOAP error may appear in the GUI banner: `SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]` It is safe to ignore this error message.

Procedure 39: Backout Multiple Servers

16 ☐	**Active NOAM VIP:** Verify application version	Verify the application version of the backed out server. 1. Select **Administration > Software Management > Upgrade** The Upgrade screen is displayed 2. Select the Server Group tab for the server that was backed out. **3.** Verify the **Application Version** value for this server has been downgraded to the original release version.
17 ☐	Procedure Complete	**The multiple server backout procedure is now complete.** **Return to the overall DSR backout procedure step that directed the execution of this procedure.**
		THIS PROCEDURE HAS BEEN COMPLETED.

6.7 Post-Backout Health Check

This procedure is used to determine the health and status of the DSR network and servers following the backout of the entire system.

Procedure 40: Post-Backout Health Check

S T E P #	This procedure performs a basic Health Check of the DSR to verify the health of the system following a backout. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Verify Server Status is Normal	Verify Server Status is Normal 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Server.** The Server Status screen is displayed. 3. Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). 4. Do not proceed with the upgrade if any server status is not **Norm**. 5. Do not proceed with the upgrade if there are any Major or Critical alarms. NOTE: It is recommended to troubleshoot if any server status is not Norm. A backout should return the servers to their pre-upgrade status.
2. ☐	**Active NOAM VIP:** Log all current alarms	Log all current alarms in the system: 1. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 2. Click the **Report** button to generate an Alarms report. 3. Save the report and print the report. Keep these copies for future reference.
		THIS PROCEDURE HAS BEEN COMPLETED.

6.8 IDIH Backout

The procedures in this section back out the Oracle, Application, and Mediation servers to the previous release.

6.8.1 Oracle Server Backout

This procedure backs out the Oracle server.

Procedure 41: Oracle Server Backout

S T E P #	This procedure performs a backout of the Oracle server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**Oracle Server CLI**
	Login to the server
		Use an SSH client to connect to the Oracle server (e.g. ssh, putty):
		`ssh <server address>`
		`login as: admusr`
		`password: <enter password>`

2 ☐	**Oracle Server CLI**
	Backout the server
		Execute the following commands to back out the server.
		`sudo /opt/xIH/plat/bin/db_rollback.sh MED`
		`sudo /opt/xiH/plat/bin/db_rollback.sh APP`

6.8.2 Mediation and Application Server Backout

The Mediation and Application servers are backed out using the disaster recovery procedure documented in [7]

7 APPENDICES

Appendix A. POST UPGRADE PROCEDURES

The procedures in this section are executed only ***AFTER*** the upgrade of ***ALL*** servers in the topology is completed.

Appendix A.1. Accept Upgrade

Detailed steps for accepting the upgrade are shown in the procedure below. TPD requires that upgrades be accepted or rejected before any subsequent upgrades may be performed. Alarm 32532 (Server Upgrade Pending Accept/Reject) will be displayed for each server until one of these two actions is performed.

An upgrade should be accepted only after it is determined to be successful as the Accept is final. This frees up file storage but prevents a backout from the previous upgrade.

NOTE: Once the upgrade is accepted for a server, that server will not be allowed to backout to a previous release.

!! WARNING!!

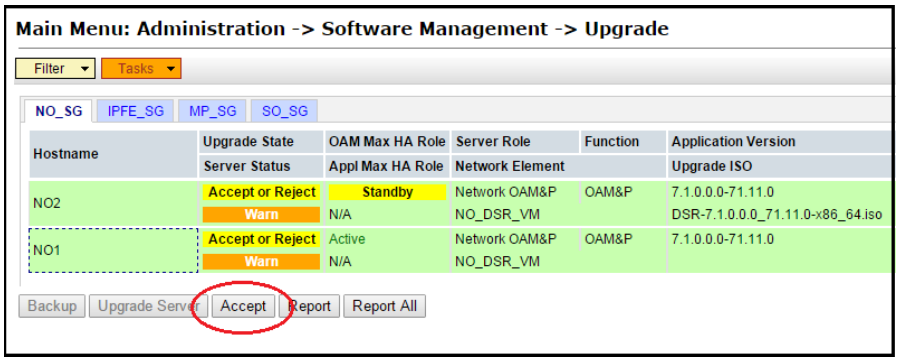
UPGRADE ACCEPTANCE MAY ONLY BE EXECUTED WITH AUTHORIZATION FROM THE CUSTOMER.

THE USER SHOULD BE AWARE THAT ONCE UPGRADE HAS BEEN ACCEPTED, IT WILL NOT BE POSSIBLE TO BACKOUT TO THE PREVIOUS RELEASE.

Procedure 42: Accept Upgrade

S T E P #	This procedure accepts a successful upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	It is recommended that this procedure be performed two weeks after the upgrade.	Verify that the upgraded system has been stable for two weeks or more. **NOTE: It will not be possible to backout after this is procedure is executed.**
2. ☐	**Active NOAM VIP:** Execute this Step if accepting a NOAM server. Log all current alarms present at the NOAM.	Log all alarms before accepting the NOAM upgrade. 1. Log into the NOAM GUI. 2. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 3. Click the **Report** button to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers will have the following expected alarm: Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
3. ☐	**Active SOAM VIP:** Execute this Step if accepting a SOAM server. Log all current alarms present at the SOAM.	Log all alarms before accepting the SOAM upgrade. 1. Log into the SOAM GUI. 2. Select **Alarms & Events > View Active.** The Alarms & Events > View Active screen is displayed. 3. Click the **Report** button to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers will have the following expected alarm: Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**

Procedure 42: Accept Upgrade

4. ☐	**Active NOAM VIP:** Accept upgrade for multiple servers	Accept the upgrade in multiple servers. 1. Log into the NOAM GUI using the VIP. 2. Select **Administration >Software Management >Upgrade.** The Upgrade Administration screen is displayed. 3. Select the server Groups tabs and select the servers (using the Ctrl button) for which upgrade is to be accepted, considering traffic, as Accept upgrade may lead to a server reboot. **4.** Click the **Accept** button  5. A confirmation dialog will warn that once accepted, the server will not be able to revert back to the previous image state. 6. Click **Ok.** The Upgrade Administration screen re-displays. **7.** Select **Alarms & Events > View** Active. The Alarms & Events > View Active screen displays. As upgrade is accepted on each server, the corresponding Alarm ID - **32532 (Server Upgrade Pending Accept/Reject)** should automatically clear.
5. ☐	Accept upgrade of the rest of the system	Repeat step 4 until the upgrade of all Servers within the system has been accepted.

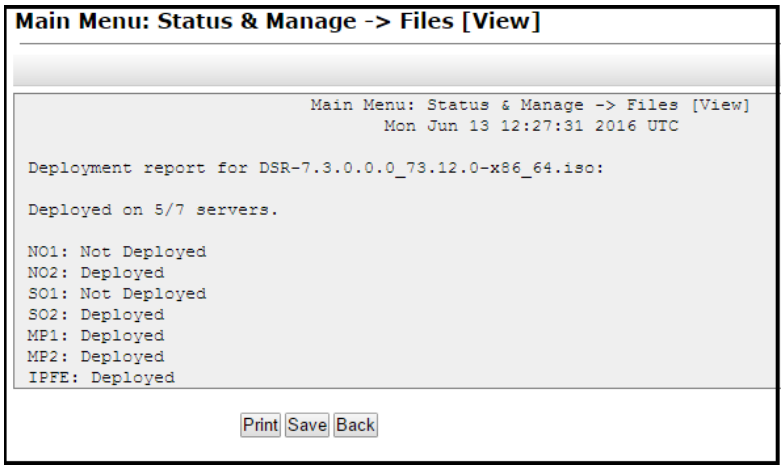
THIS PROCEDURE HAS BEEN COMPLETED.

Appendix A.2. Undeploy ISO

This procedure is run after the upgrade has been Accepted to undeploy all deployed ISOs. When an ISO is undeployed, the ISO is deleted from all servers in the topology except for the Active NOAM. On the Active NOAM, the ISO remains in the File Management Area.

This procedure can be run at anytime after the upgrade has been Accepted.

Procedure 43: Undeploy ISO

S T E P #	This procedure undeploys an ISO from the DSR servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** View files	View the files in the File Management Area on the Active NOAM. 1. Log into the NOAM GUI using the VIP. 2. Select **Status & Manage > Files.** The Files screen is displayed.
2. ☐	**Active NOAM VIP:** Start ISO undeploy	Start the ISO undeploy sequence. 1. Select an ISO that is stored in the isos directory of the File Management Area. The ISO filename will have the format: `isos/DSR-7.3.0.0.0_73.12.0-x86_64.iso` 2. Click the **Undeploy ISO** button. 3. Click **OK** in the confirmation dialog box to start the undeploy sequence. After clicking Ok the **Status & Manage > Files** screen will refresh.
3. ☐	**Active NOAM VIP:** Monitor progress	Monitor the ISO undeploy progress. 1. Select the ISO being deployed in step 2. 2. Click the **View ISO Deployment Report** button. 3. If some servers show the ISO as "Deployed", click the **Back** button on the **Files [View]** page 4. Periodically repeat sub-steps 1 thru 3 until all servers indicate "Not Deployed". 
4. ☐	**Active NOAM VIP:** Repeat as necessary	1. If there are additional ISOs in the File Management Area that need to be undeployed, repeat steps 2 and 3 as necessary.

Appendix A.3. PCA Post Upgrade Procedure

THIS PROCEDURE IS FOR PCA SYSTEMS ONLY!

Procedure 44 must be executed on PCA systems after the upgrade to DSR 7.3 is Accepted. Do not run this procedure until *after* Procedure 42 has been completed. This procedure executes the PCA top level activation script to remedy a potential PCA activation issue from earlier releases.

Procedure 44: PCA Post Upgrade Procedure

S T E P #	This procedure executes the PCA top level activation script. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM CLI:** Log into the Active NOAM	Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the Active NOAM: `ssh admusr@<NOAM_VIP>`

2. ☐	**Active NOAM CLI**
	Run PCA activation script
		Execute the top level PCA script:
		`/usr/TKLC/dsr/prod/maint/loaders/activate/load.pcaActivationTopLevel`
		At the completion of the activation script, the following message is output:
		`Execution of PCA Activation Script complete.`

3. ☐	**Active NOAM CLI** Clear cache	Execute the following command to reset the initialization caches: `clearCache`
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix B. COMMAND OUTPUTS

Not Applicable.

Appendix C. PCRF POOLING MIGRATION CHECK

If the PCA application has been activated and the PDRA feature has been enabled, a check of the PCRF Pooling Migration is **REQUIRED** prior to the start of a major upgrade to DSR 7.3.

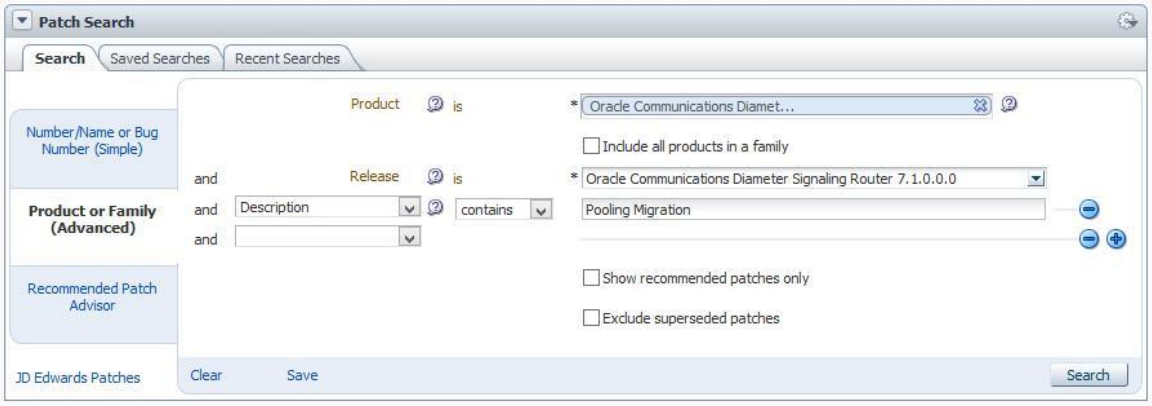
The PCRF Pooling Migration check is NOT required for a DSR 7.3 incremental upgrade.
The PCRF Pooling Migration check is NOT required for a DSR 7.1 or 7.2 to 7.3 upgrade.

Follow the steps in Procedure 45 to execute the PCRF Pooling Migration Check:

Note: If the PCRF Pooling Migration is NOT complete, this check must be repeated until PCRF Pooling Migration Tool indicates that the migration is complete.

Procedure 45: PCRF Pooling Migration Check

S T E P #		
	This procedure checks the PCRF Pooling Migration status to determine if the migration is complete. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	Download PCRF Pooling Migration Tool	Download the PCRF Pooling Migration Tool from MOS. The tool is used to determine the status of the PCRF pooling migration. 1. Navigate to the MOS site at https://support.oracle.com/ and sign in. 2. Select the **Patches & Updates** tab 3. In the Patch Search window, select the **Product or Family (Advanced)** tab on left. 4. Use the following search criteria to locate and download the migration tool (as shown in the figure below): • Product is: Oracle Communications Diameter Signaling Router (DSR) • Release is: Oracle Communications Diameter Signaling Router (DSR) 7.1.0.0.0 ○ *Note: The 7.1 Migration Tool is also valid for DSR 7.3.* • **Description contains**: Pooling Migration
2. ☐	Copy the PCRF Pooling Migration Tool	Copy the PCRF Pooling Migration Tool to the Active NOAM. `scp -p <patchfilename> admusr@<Active_NOAM>`
3. ☐	SSH to the Active NOAM	Using a SSH tool, login to the Active NOAM server. `ssh admusr@<NOAM_VIP>`
4. ☐	**Active NOAM CLI:** Move the patch file	Move the patch file to the working directory: `sudo mv <patchfilename> /usr/TKLC/dsr/tools`



Procedure 45: PCRF Pooling Migration Check

5. ☐	**Active NOAM CLI:** Change directory to the PCA tool directory	Change directories using the following command: `cd /usr/TKLC/dsr/tools/`
6. ☐	**Active NOAM CLI:** Unzip the patch	Unzip the PCRF Pooling Migration Tool using the "unzip" command. Example: `sudo unzip <patchfilename>`

7. ☐	**Active NOAM CLI:**
	
	Check the PCRF Pooling Migration Status
		Check the PCRF Pooling Migration Status using the following command:
		
		`./verifyPCRFPoolingMigration.sh --checkPCRFPoolingMigrationStatus`
		
		Sample output:
		`Preparing log directory ...`
		
		`Creating log directory...`
		`Logging is started in /var/TKLC/log/migrationStatusToolLogs/migrationStatusTool.log`
		`Preparation of log directory done.`
		
		`============= Execution of PCRF Pooling Migration Verification Tool Started ===============`
		
		`Checking host server status whether it is active NOAMP server or not.`
		`This server is Active NOAMP server.`
		
		`Application Release is 7.0.1.0.0`
		
		`PDRA/PCA application is activated on this system.`
		
		`'PCRFPooling' feature is enabled on this system.`
		
		`PCRF Pooling Migration is not required. No need to check PCRF pool migration status. Exiting ...`
		
		`PCRF Pooling Migration is completed or not required on all servers. Execute tool again with option --verifyUpgradeAllowed to check if upgrade is allowed or not.`
		
		`============= Execution of PCRF Pooling Migration Verification Tool Completed =============`

8. ☐	**Active NOAM CLI:** Verify that PCRF Pooling Migration is complete	After executing the PCRF Pooling Migration tool, determine if the PCRF Pooling Migration has completed using the following command: `./verifyPCRFPoolingMigration.sh --verifyUpgradeAllowed` **Note:** This command will inform the user if the PCRF Pooling Migration has completed. If PCRF Pooling Migration is complete, the command will print the following output: "`Upgrade is allowed.`" If PCRF Pooling Migration is **NOT** complete, the command will print the following output: "`Upgrade is not allowed.`"

Procedure 45: PCRF Pooling Migration Check

9. ☐	**Active NOAM CLI:**
	
	Estimate PCRF Pooling Migration Completion
	Optional
		If the PCRF Pooling Migration is not complete, the user may get an estimate of when the PCRF Pooling Migration will be complete.
		
		Execute the PCRF Pooling Migration Completion Estimate tool using the following command:
		
		`./verifyPCRFPoolingMigration.sh --estimateMigrationCompletionTime`
		
		Note:
		Once complete, this command will output the estimated PCRF Pooling Migration in Days, Hours, Minutes and Seconds.
		
		Example:
		`Estimated total time for migration completion for all binding servers is: 3 days 4 hours 45 minutes 34 seconds.`

	THIS PROCEDURE HAS BEEN COMPLETED.	

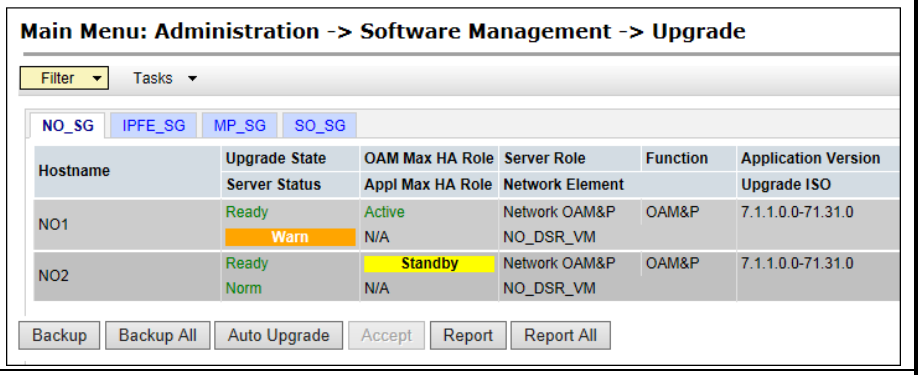
Appendix D. UPGRADE SINGLE SERVER – UPGRADE ADMINISTRATION

This Appendix provides the procedure for upgrading a DSR single server of any type (NOAM, SOAM, MP, etc).

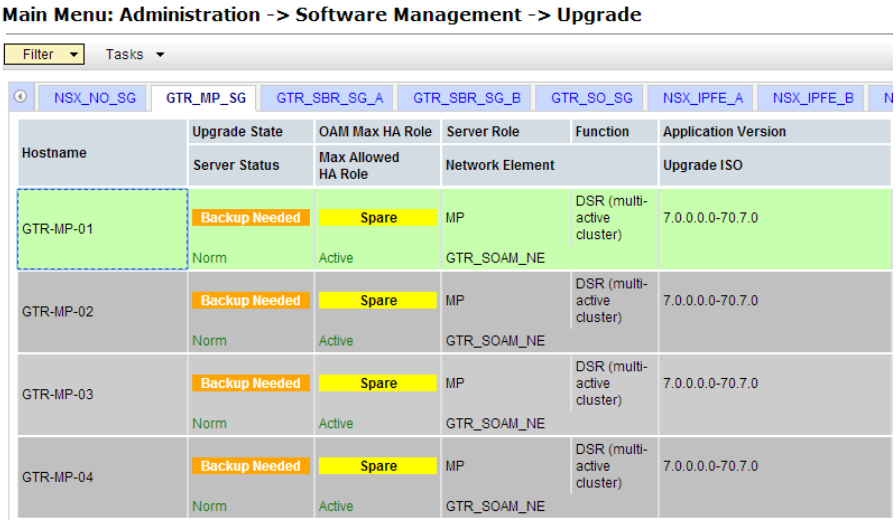
Note that this procedure will be executed multiple times during the overall upgrade, depending on the number of servers in the DSR. Make multiple copies of Appendix D to mark up, or keep another form of written record of the steps performed.

Procedure 46: Upgrade Single Server – Upgrade Administration

S T E P #		
	This procedure executes the Upgrade Single Server – Upgrade Administration steps. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	**Active NOAM VIP:** View the pre-upgrade status of Servers	View the pre-upgrade status 1. Log into the NOAM GUI using the VIP 2. Select **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed (example below): The Active NOAM server may have some or all of the following expected alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**
2 ☐	Verify status of Server to be upgraded	For the server to be upgraded: 1. Identify the server (NOAM, SOAM, MP, etc) _____(record name) 2. Verify the Application Version value is the expected source software release version. 3. From the **Administration > Software Management > Upgrade** screen, select the Server Group of the server to be upgraded.



Procedure 46: Upgrade Single Server – Upgrade Administration

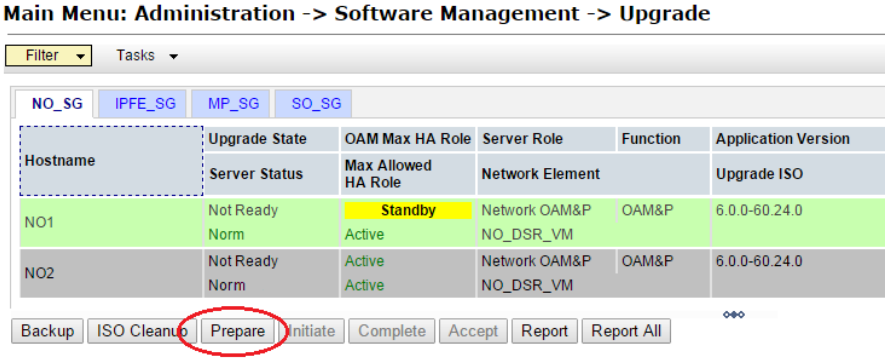


4. If the server is in the "**Backup Needed"** state, select the server and click the "**Backup**" button. On the **Upgrade [Backup]** screen, click '**Ok**'. The Upgrade State changes to "**Backup in Progress**".
5. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)

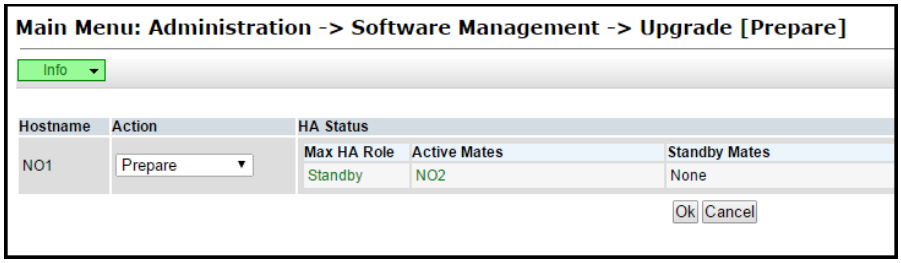
For Active NOAM on release 7.0.1:
When the backup is complete, verify the server state changes to "**Not Ready**".
Perform steps 3 thru 10.

For Active NOAM on release 7.1.1 or later:
When the backup is complete, verify the server state changes to "**Ready**".
Proceed to step 11.

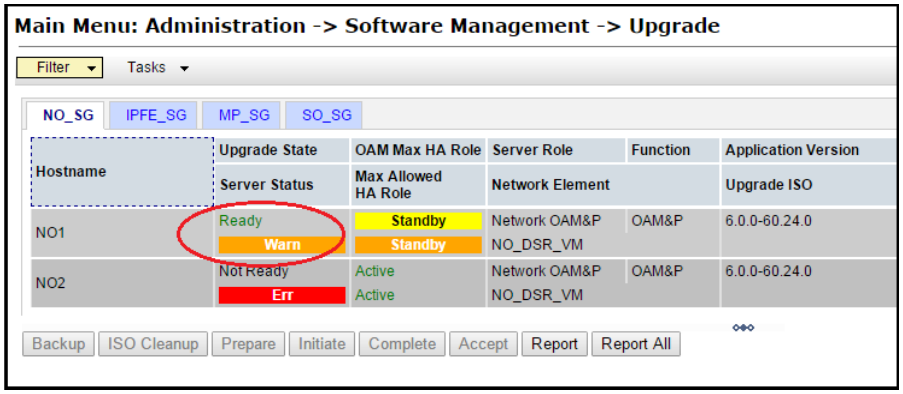
3	**Active NOAM VIP:** Prepare Upgrade (step 1) **For Active NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** For the server to be upgraded: 1. On the Upgrade form, make the server 'Upgrade Ready', by selecting the server to be upgraded, and selecting the **Prepare** button. (In this example, an NOAM with name "NO2" will be made ready for Upgrade)



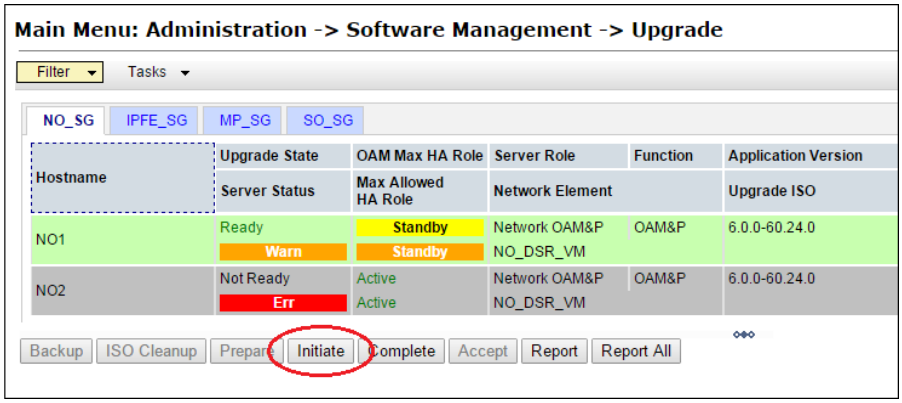
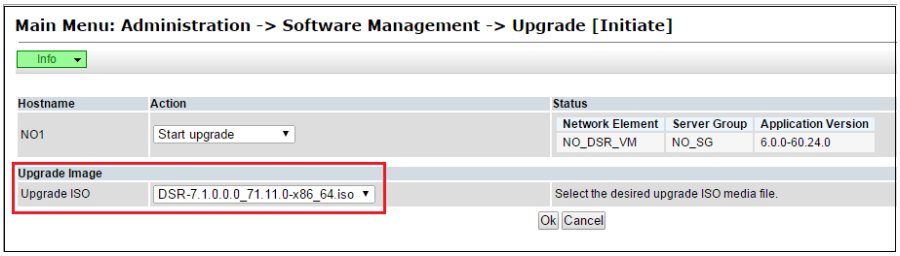
Procedure 46: Upgrade Single Server – Upgrade Administration

4 ☐	**Active NOAM VIP:** Prepare Upgrade (step 2) **For Active NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** Prepare the server for upgrade. The **Upgrade [Prepare]** form is displayed.  For the Max Ha Role: 1. Verify the selected server status **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded) 2. If the state of the server to be upgraded is as expected, select **Ok.** **NOTE: When the Active NOAM is the server being upgraded, selecting OK will initiate an HA switchover, causing the GUI session to log out. Before logging into the Active OAM again, close and re-open the browser using the VIP address for the NOAM, and then clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.** **NOTE: If the selected server is the active server in an Active/Standby pair, the Max HA Role column will display "Active" with a red background. This is NOT an alarm condition. This indicator is to make the user aware that the Make Ready action WILL cause an HA switchover.**

Procedure 46: Upgrade Single Server – Upgrade Administration

5	**Active NOAM VIP:** Verify upgrade status is "Ready **For Active NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** Verify the server upgrade status is ready. Upon preparing the selected server, the Upgrade Administration form will refresh, and the server to be upgraded will show Upgrade State = **Ready** (This may take a minute)  Depending on the server being upgraded, new alarms may occur. Servers may have a combination of the following expected alarms. NOTE: Not all servers have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats)** or **(Lost Communication with Mate Server)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31106 (DB Merge to Parent Failure)**

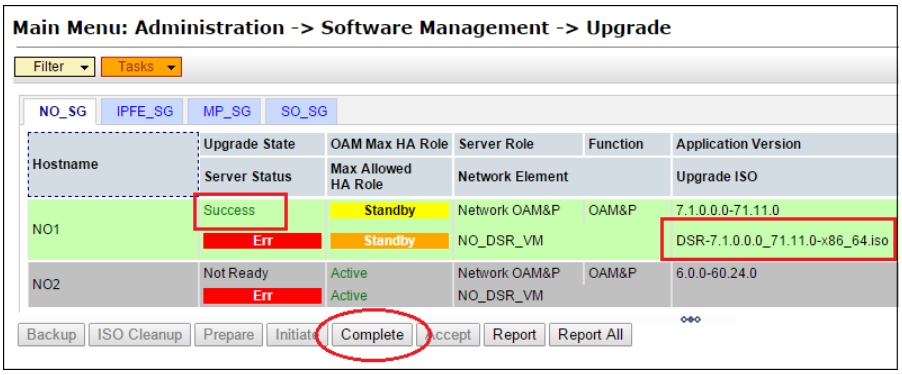
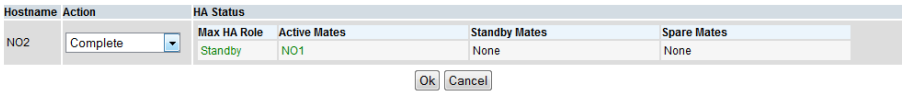
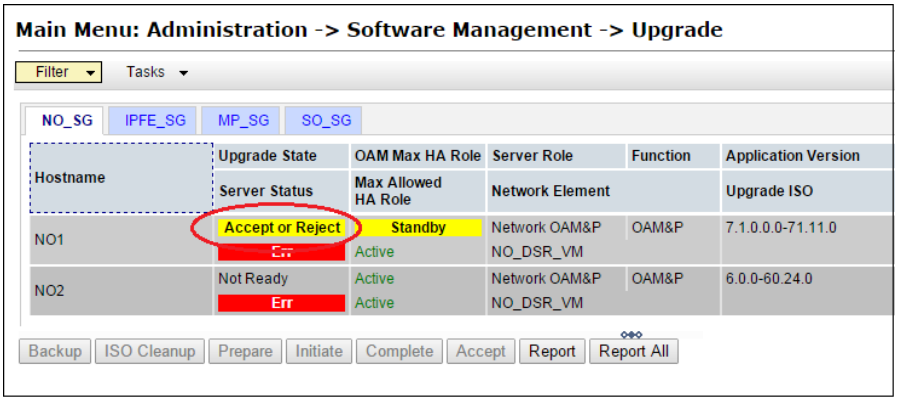
Procedure 46: Upgrade Single Server – Upgrade Administration

6 ☐	**Active NOAM VIP:** Initiate Upgrade (part 1) **For Active NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** Initiate the upgrade on the server. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click the "**Initiate"** button 
7 ☐	**Active NOAM VIP:** Initiate Upgrade (part 2) **For Active NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** Initiate the upgrade on the server. The Initiate Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]** 1. In the **Upgrade Image – Upgrade ISO** pick list, select the ISO to use in the server upgrade, 2. Click the **Ok** button. The upgrade will begin and control will return to the Upgrade Administration screen. 

Procedure 46: Upgrade Single Server – Upgrade Administration

8 ☐	**Active NOAM VIP:** View In-Progress Status (monitor) **For Active NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** View the Upgrade Administration form to monitor upgrade progress. See step 14 for an optional method of monitoring upgrade progress. See step 15 below for instructions if the Upgrade fails, or if execution time exceeds 60 minutes. *NOTE: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade will be shown as "FAILED". The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.* 1. Observe the **Upgrade State** of the server of interest. Upgrade status will be displayed under the **Status Message** column. **Main Menu: Administration -> Software Management -> Upgrade** Filter ▾ Status ▾ Tasks ▾ NO_SG IPFE_SG MP_SG SO_SG Hostname / Upgrade State / OAM Max HA Role / Server Role / Function / Application Version / Start Time Server Status / Appl Max HA Role / Network Element / Upgrade ISO / Status Message NO2: Upgrading / OOS / Network OAM&P / OAM&P / 2015-01-29 10:49:57 EST Unk / N/A / NO_DSR_VM / DSR-7.1.0.0.0_71.8.1-x86_64.iso / Upgrade is in progress NO1: Ready / Active / Network OAM&P / OAM&P / 7.1.0.0.0-71.6.0 Err / N/A / NO_DSR_VM Servers may have a combination of the following expected alarms. Note: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** Alarm ID = **31283 (Highly available server failed to receive mate heartbeats)** Alarm ID = **31106 (DB Merge To Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31233 (HA Secondary Path Down)** Alarm ID = **31101 (DB Replication To Slave Failure)** Alarm ID = **31104 (DB Replication over SOAP has failed** 2. Wait for the upgrade to complete. The "Status Message" column will show "Success". This step will take approximately 20 to 50 minutes. **If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix J for failed server recovery procedures.**

Procedure 46: Upgrade Single Server – Upgrade Administration

9	**Active NOAM VIP:** Take the upgraded server out of the upgrade ***SUCCESS*** state (part 1) **For Active NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** Take the upgraded server out of the upgrade ready state. This step applies to all servers, regardless of type. 1. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed. 2. Verify the **Application Version** value for this server has been updated to the target software release version. 3. Verify status: 4. Verify the **Upgrade State** of the server that was upgraded is **Success**. 5. Select the server that was upgraded 6. Click the **Complete** button. 
10	**Active NOAM VIP:** Take the upgraded server out of the upgrade ***SUCCESS*** state (part 2) **For Active NOAM on release 7.0.1 only**	**This step is for an Active NOAM on release 7.0.1 only.** The **Upgrade[Complete]** screen is displayed  1. Click **OK**. This completes the upgrade action on the server. The Upgrade Administration screen is displayed. 2. Wait for the screen to refresh and show the Upgrade State as **Accept or Reject.** It may take up to 2 minutes for the Upgrade State to change to **Accept or Reject**.  **Proceed to step 17 to complete this procedure.**

Procedure 46: Upgrade Single Server – Upgrade Administration

11 ☐	**Active NOAM VIP:** Initiate Upgrade (part 1) **For Active NOAM on release 7.1.1 or later**	**This step is for an Active NOAM on release 7.1.1 or later.** Initiate the server upgrade. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click the "**Upgrade Server"** button. **Main Menu: Administration -> Software Management -> Upgrade** Filter Tasks NO_SG IPFE_SG MP_SG SO_SG Hostname / Server Status / Upgrade State / Ready / Norm / OAM Max HA Role / Standby / Appl Max HA Role / N/A / Server Role / Network Element / Network OAM&P / NO_DSR_VM / Function / OAM&P / Application Version / Upgrade ISO / 7.1.0.0.0-71.6.0 NO2 Ready Norm Standby N/A Network OAM&P NO_DSR_VM OAM&P 7.1.0.0.0-71.6.0 NO1 Ready Norm Active N/A Network OAM&P NO_DSR_VM OAM&P 7.1.0.0.0-71.6.0 Backup Upgrade Server Accept Report Report All The Initiate Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]**
12 ☐	**Active NOAM VIP:** Initiate Upgrade (part 2) – Select ISO form **For Active NOAM on release 7.1.1 or later**	**This step is for an Active NOAM on release 7.1.1 or later.** Initiate the server upgrade. 1. In the **Upgrade Settings – Upgrade ISO** pick list, select the ISO to use in the server upgrade, **Note: When the Active NOAM is the server being upgraded, selecting OK will initiate an HA switchover, causing the GUI session to log out. Before logging into the Active OAM again, close and re-open the browser using the VIP address for the NOAM, and then clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.** **Note: If the selected server is the active server in an Active/Standby pair, the OAM Max HA Role column will display "Active" with a red background. This is NOT an alarm condition. This indicator is to make the user aware that the Make Ready action WILL cause an HA switchover.** 2. Click the **Ok** button. The upgrade will begin and control will return to the Upgrade Administration screen. **Main Menu: Administration -> Software Management -> Upgrade [Initiate]** Info Hostname / Action / Status / OAM Max HA Role / Network Element NO2 Upgrade Standby NO_DSR_VM Upgrade Settings Upgrade ISO DSR-7.1.0.0.0_71.8.1-x86_64.iso Select the desired upgrade ISO media file. Ok Cancel

Procedure 46: Upgrade Single Server – Upgrade Administration

13 ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. See step 14 for an optional method of monitoring upgrade progress. See step 15 below for instructions if the Upgrade fails, or if execution time exceeds 60 minutes. *NOTE: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade will be shown as "FAILED". The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.* 2. Observe the **Upgrade State** of the server of interest. Upgrade status will be displayed under the **Status Message** column. **Main Menu: Administration -> Software Management -> Upgrade** Filter Status Tasks NO_SG IPFE_SG MP_SG SO_SG Hostname / Upgrade State / OAM Max HA Role / Server Role / Function / Application Version / Start Time Server Status / Appl Max HA Role / Network Element / Upgrade ISO / Status Message NO2: Upgrading / OOS / Network OAM&P / OAM&P / 2015-01-29 10:49:57 EST Unk / N/A / NO_DSR_VM / DSR-7.1.0.0.0_71.8.1-x86_64.iso / Upgrade is in progress NO1: Ready / Active / Network OAM&P / OAM&P / 7.1.0.0.0-71.6.0 Err / N/A / NO_DSR_VM Servers may have a combination of the following expected alarms. Note: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** Alarm ID = **31283 (Highly available server failed to receive mate heartbeats)** Alarm ID = **31106 (DB Merge To Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31233 (HA Secondary Path Down)** Alarm ID = **31101 (DB Replication To Slave Failure)** Alarm ID = **31104 (DB Replication over SOAP has failed** 3. Wait for the upgrade to complete. The "Status Message" column will show "Success". This step will take approximately 20 to 50 minutes. **If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix J for failed server recovery procedures.**

Procedure 46: Upgrade Single Server – Upgrade Administration

14 ☐	**Server CLI:**
	
	Optional : View In-Progress Status from command line of server
		An optional method to view Upgrade progress from the command line:
		
		To view the detailed progress of the upgrade , access the server command line (via SSH or Console), and enter:
		
		`$ tail -f /var/TKLC/log/upgrade/upgrade.log`
		
		Once the server has upgraded, it will re-boot, and then it will take a couple of minutes for the DSR Application processes to start up.
		
		This command will show the current rev on the server:
		
		`$ appRev`
		`Install Time: Tue Jun 17 08:20:57 2014`
		`Product Name: DSR`
		`Product Release: 6.0.0_60.14.6`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.7.0.0.1_84.14.0`
		`Base Distro ISO: TPD.install-6.7.0.0.1_84.14.0-OracleLinux6.5-x86_64.iso`
		`OS: OracleLinux 6.5`

15 ☐	IF Upgrade Fails:	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		
		It is recommended to contact MOS by referring to Appendix J of this document and provide these files.Refer to 0 for failed server recovery procedures.

16 ☐	**Active NOAM VIP:** Verify post upgrade status	Verify post upgrade status 1. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed. 2. Verify the Application Version value for this server has been updated to the target software release version. **If the Active NOAM is on release 7.0.1:** Verify the Status Message indicates **Success**. **If the Active NOAm is on release 7.1.1 or later:** Verify the Upgrade State of the upgraded server is **Accept or Reject**. NO_SG | IPFE_SG | MP_SG | SO_SG Hostname / Upgrade State / Server Status / OAM Max HA Role / Appl Max HA Role / Server Role / Network Element / Function / Application Version / Upgrade ISO NO2: Accept or Reject / Warn / Standby / N/A / Network OAM&P / NO_DSR_VM / OAM&P / 7.1.0.0.0-71.6.0 / DSR-7.1.0.0.0_71.8.1-x86_64.iso NO1: Ready / Norm / Active / N/A / Network OAM&P / NO_DSR_VM / OAM&P / 7.1.0.0.0-71.6.0 Backup | Upgrade Server | Accept | Report | Report All

Procedure 46: Upgrade Single Server – Upgrade Administration

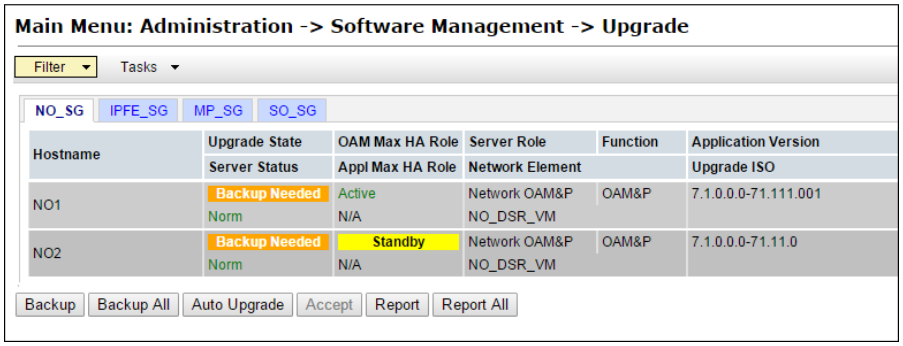
17 ☐	**Active NOAM VIP:** Verify the server was successfully upgraded	View the Post-Upgrade Status of the server: The Active NOAM or SOAM server may have some or all the following expected alarm(s): Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10010 (Stateful database not yet synchronized with mate database)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **31000 (Program impaired by S/W Fault)** Alarm ID = **31201 (Process Not Running)** for eclipseHelp process Alarm ID = **31282 (The HA manager (cmha) is impaired by a s/w fault)** Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** The Active NOAM or SOAM will have the following expected alarm until both NOAMs/SOAMs are upgraded: Alarm ID = **31233 – HA Secondary Path Down** **NOTE: Do Not Accept upgrade at this time.** This alarm is OK.
18 ☐	Procedure Complete	The single server upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of Appendix D.

Appendix E. UPGRADE MULTIPLE SERVERS – UPGRADE ADMINISTRATION

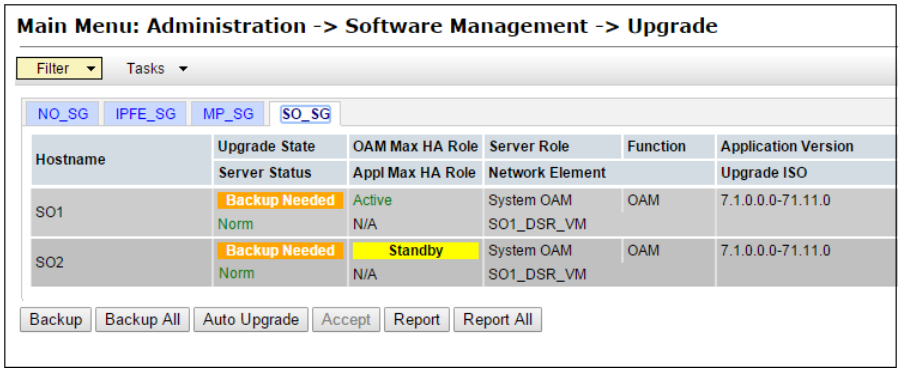
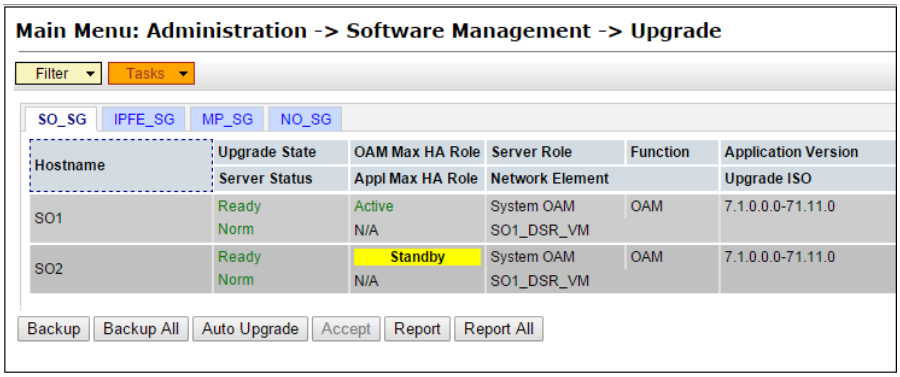
This Appendix provides the procedure for upgrading multiple servers in parallel.

Note that this procedure will be executed multiple times during the overall upgrade, depending on the number of servers in your DSR. Make multiple copies of Appendix E to mark up, or keep another form of written record of the steps performed.

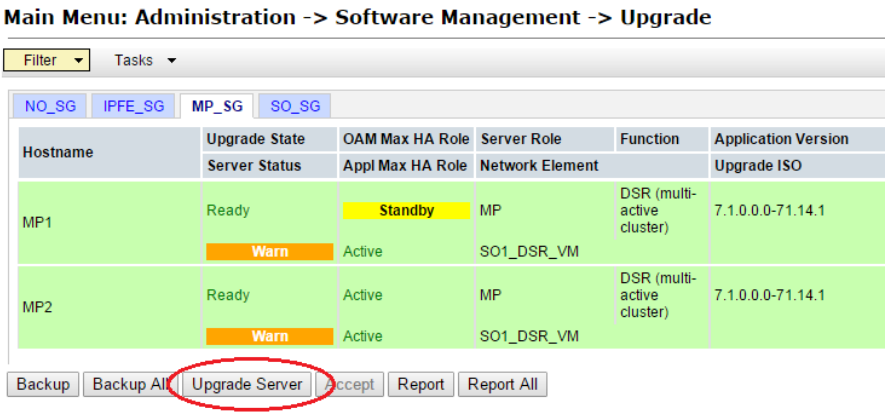
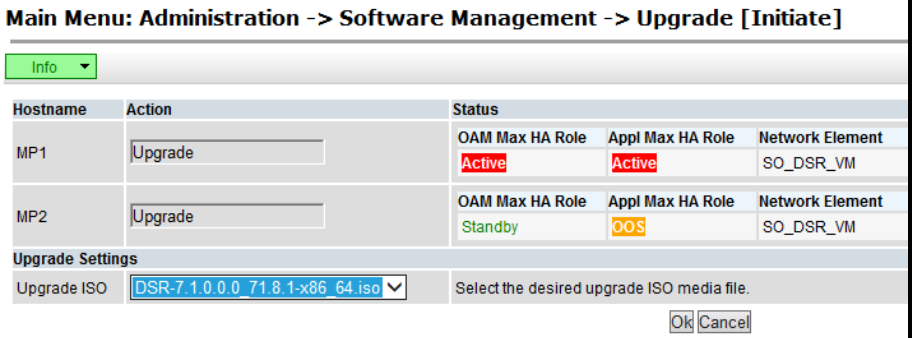
Procedure 47: Upgrade Multiple Servers - Upgrade Administration

S T E P #	This procedure executes the Upgrade Multiple Servers – Upgrade Administration steps. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1.	**Active NOAM VIP:** View the pre-upgrade status of Servers	View the pre-upgrade status of the servers. 1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed  Active NOAM server may have some or all of the following expected alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)**

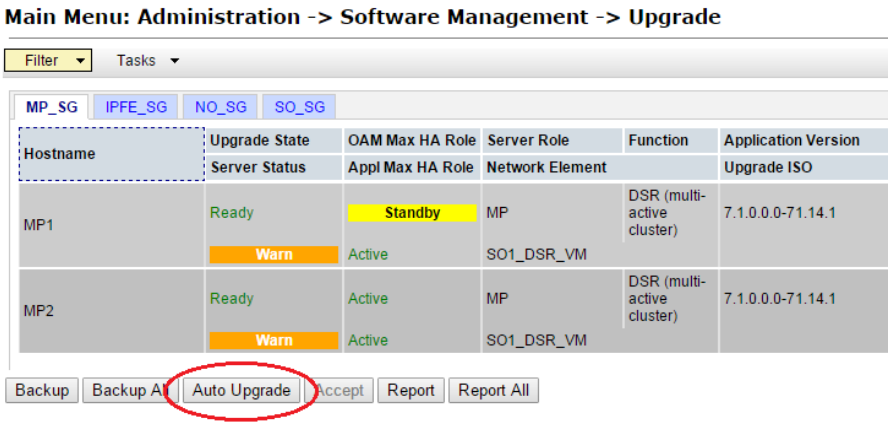
Procedure 47: Upgrade Multiple Servers - Upgrade Administration

2. ☐	**Active NOAM VIP:** Verify status of Servers to be upgraded	For the servers to be upgraded: 1. Identify the servers to be upgraded in parallel _____ (record names) 2. Select the server group associated with the servers identified in step 1. 3. Verify the Application Version value is the expected source software release version for each server to be upgraded. 4. From the **Administration > Software Management > Upgrade** screen, select the Server Group of the server to be upgraded.  5. If the server is in "**Backup Needed"** state, select the server and click the "**Backup**" button. The Upgrade State changes to "**Backup in Progress**". When the backup is complete, the Upgrade State changes to "**Ready**". 6. Verify the "OAM Max Ha Role" **is the expected condition (either Standby or Active)** (this will depend on the server being upgraded)
3. ☐	**Active NOAM VIP:** Verify Upgrade Status is "Ready"	The Upgrade Administration form will be refreshed, and the server to be upgraded will show Upgrade Status = READY (This may take a minute). Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen is displayed:  Servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **32515 (Server HA Failover Inhibited)** Alarm ID = **31101 (DB Replication to slave DB has failed)** Alarm ID = **31106 (DB Merge to Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats)** or **(Lost Communication with Mate Server)**

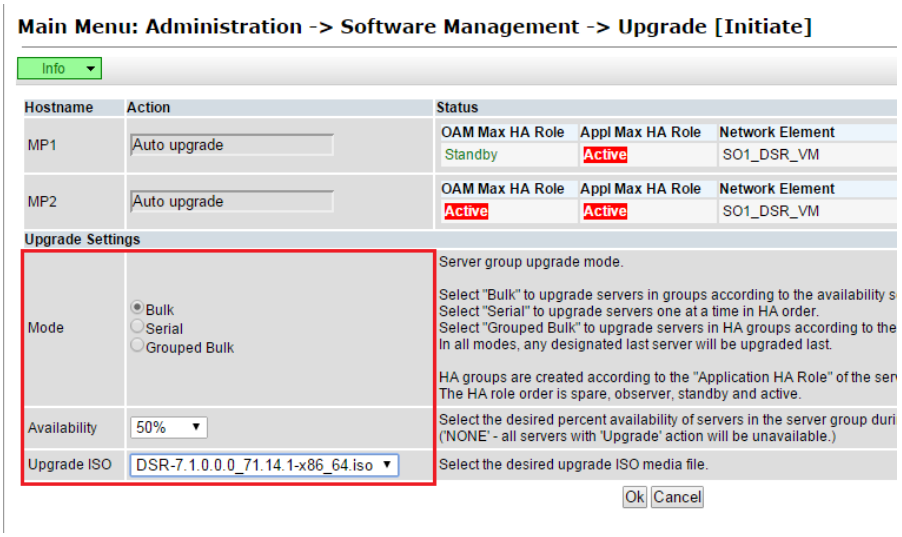
Procedure 47: Upgrade Multiple Servers - Upgrade Administration

	Determine upgrade method – manual or automatic	**To upgrade multiple servers in parallel using the manual option, execute steps 4 and 5.** **To upgrade a server group using the Automated Server Group Upgrade option, proceed to step 6.**
4. ☐	**Active NOAM VIP:** Initiate Upgrade (initiate) (part 1)	1. From the Upgrade Administration screen, select the servers to be upgraded. 2. Click the "**Upgrade Server"** button.  The Initiate Upgrade form will be displayed: **Administration > Software Management > Upgrade [Initiate]**
5. ☐	**Active NOAM VIP:** Initiate Upgrade (part 2) – Select ISO form	Start the upgrade. 1. In the **Upgrade Settings – Upgrade ISO** pick list, select the ISO to use in the server upgrade, **Note: When the Active NOAM is the server being upgraded, selecting OK will initiate an HA switchover, causing the GUI session to log out. Before logging into the Active OAM again, close and re-open the browser using the VIP address for the NOAM, and then clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.** **Note: If the selected server is the active server in an Active/Standby pair, the OAM Max HA Role column will display "Active" with a red background. This is NOT an alarm condition. This indicator is to make the user aware that the Make Ready action WILL cause an HA switchover.** 2. Click the **Ok** button. The upgrade will begin and control will return to the Upgrade Administration screen.  **Proceed to step 8 to complete this procedure.**

Procedure 47: Upgrade Multiple Servers - Upgrade Administration

6. ☐	**Active NOAM VIP:** Initiate (part 1) - **Automated Server Group Upgrade**	Initiate the Automated Server Group Upgrade option 1. To utilize the Automated Server Group upgrade option, verify that no servers in the server group are selected.  2. Click the **Auto Upgrade** button. The Upgrade [Initiate] screen is displayed.

Procedure 47: Upgrade Multiple Servers - Upgrade Administration

7. ☐	**Active NOAM VIP:** Initiate (part 2) - **Automated Server Group Upgrade**	Start the Automated Server Group Upgrade. Note: The settings to be used in this step are specified in the calling procedure. 1. The **Upgrade Settings** section of the Initiate screen controls the behavior of the automated upgrade. Select the settings that apply to the server type being upgraded. **Bulk**: Select this option for Active/Standby and multi-active server groups. For servers in an Active/Standby configuration, the Standby server is upgraded first, followed by the Active. Servers in a multi-active configuration are upgraded in parallel to the extent allowed by the Availability setting. **Serial**: Select this option to upgrade multiple servers one at a time. **Grouped Bulk**: Select this option for SBR server groups. Grouped bulk always upgrades the Spare(s), followed by the Standby, followed by the Active. **Availability**: This setting determines how many servers will remain in service while servers in the server group are upgraded. For example, a setting of 50% will ensure that *at least* half of the servers *in the server group* remain in service. Note: the Availability setting is not displayed when upgrading OAM servers. Note: The **Serial** upgrade mode is available as an alternative to Bulk and Grouped Bulk for a more conservative upgrade scenario. Serial mode will upgrade each server in the server group one at a time, and can be used on any server group type. 2. Select the appropriate ISO from the **Upgrade ISO** pick list. 3. Click the **Ok** button to start the upgrade. 

Procedure 47: Upgrade Multiple Servers - Upgrade Administration

8. ☐	**Active NOAM VIP:** View In-Progress Status (monitor)	View the Upgrade Administration form to monitor upgrade progress. See step 9 for an optional method of monitoring upgrade progress. See step 10 below for instructions if the Upgrade fails, or if execution time exceeds 60 minutes. *Note: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade will be shown as "FAILED". The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.* 1. Observe the **Upgrade State** of the servers of interest. **Main Menu: Administration -> Software Management -> Upgrade** Filter ▾ Status ▾ Tasks ▾ MP_SG | IPFE_SG | NO_SG | SO_SG | Hostname | Upgrade State / Server Status | OAM Max HA Role / Appl Max HA Role | Server Role / Network Element | Function | Application Version / Upgrade ISO | | --- | --- | --- | --- | --- | --- | | MP1 | Upgrading / Err | Standby / OOS | MP / SO_DSR_VM | DSR (active/standby pair) | 7.1.0.0.0-71.6.0 / DSR-7.1.0.0.0_71.8.1-x86_64.iso | | MP2 | Upgrading / Err | Spare / OOS | MP / SO_DSR_VM | DSR (active/standby pair) | 7.1.0.0.0-71.6.0 / DSR-7.1.0.0.0_71.8.1-x86_64.iso | Backup | Backup All | Auto Upgrade | Accept | Report | Report All During the upgrade, the servers may have a combination of the following expected alarms. NOTE: Not all servers will have all alarms: Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10073 (Server Group Max Allowed HA Role Warning)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **31101 (DB Replication To Slave Failure)** Alarm ID = **31106 (DB Merge To Parent Failure)** Alarm ID = **31107 (DB Merge From Child Failure)** Alarm ID = **31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)** Alarm ID = **31233 (HA Secondary Path Down)** Alarm ID = **31283 (Highly available server failed to receive mate heartbeats)** Alarm ID = **32515 (Server HA Failover Inhibited)** 2. Wait for the upgrades to complete. The **Upgrade State** column will transition through "**Upgrading**", "**Rebooting**", "**Not Ready**", and finally "**Accept or Reject**". This step will take approximately 20 to 50 minutes. **If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to Appendix J for failed server recovery procedures.**

Procedure 47: Upgrade Multiple Servers - Upgrade Administration

9. ☐	Server CLI:
	
	Optional : View In-Progress Status from command line of server
		Optional method to view Upgrade progress from a command line:
		
		To view the detailed progress of the upgrade –
		Access the server command line (via ssh or Console), and:
		
		`$ tail -f  /var/TKLC/log/upgrade/upgrade.log`
		
		Once a server is upgraded, it will re-boot, and then it will take a couple of minutes for the DSR Application processes to start up.
		
		This command will show the current rev on the upgraded servers:
		
		`[admusr@NO1 ~]$ appRev`
		`Install Time: Wed Feb 25 02:52:47 2015`
		`Product Name: DSR`
		`Product Release: 7.1.0.0.0_71.10.0`
		`Base Distro Product: TPD`
		`Base Distro Release: 7.0.0.0.0_86.14.0`
		`Base Distro ISO: TPD.install-7.0.0.0.0_86.14.0-OracleLinux6.5-x86_64.iso`
		`ISO name: DSR-7.1.0.0.0_71.10.0-x86_64.iso`
		`OS: OracleLinux 6.5`
		
		If the upgrade fails – do not proceed. It is recommended to consult with MOS on the best course of action. Refer to 0 for failed server recovery procedures.

10. ☐	IF Upgrade Fails**:**	If a server upgrade fails, access the server command line (via ssh or Console), and collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		
		It is recommended to contact MOS by referring to Appendix J of this document and provide these files. Refer to 0 for failed server recovery procedures.

11. ☐	**Active NOAM VIP:** Verify post upgrade status	Verify post-upgrade status 1. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed. 2. Verify the Application Version value for the servers has been updated to the target software release version. 3. Verify the Status Message indicates success. 4. Verify the Upgrade State of the upgraded servers is Accept or Reject.
12. ☐	Verify the servers were successfully upgraded	View Post-Upgrade Status of the server: The Active SOAM server may have some or all the following expected alarm(s): Alarm ID = **10008 (Provisioning Manually Disabled)** Alarm ID = **10010 (Stateful database not yet synchronized with mate database)** Alarm ID = **10075 (The server is no longer providing services because application processes have been manually stopped)** Alarm ID = **31000 (Program impaired by S/W Fault)** Alarm ID = **32532 (Server Upgrade Pending Accept/Reject)** NOTE: Do Not Accept upgrade at this time. This alarm is OK.
13. ☐	Procedure Complete.	The multiple servers upgrade is now complete. Return to the DSR upgrade procedure step that directed the execution of Appendix E.
		THIS PROCEDURE HAS BEEN COMPLETED

Appendix F. IDIH UPGRADE AT A SITE

In IDIH release 7.1 and later, the mediation and application instance data is stored in the Oracle Database. This allows the Application and Mediation servers to be upgraded by performing a fresh installation. Upon completion of the upgrade, the mediation and application guests will automatically restore the configuration data from the Oracle database.

Table 16 shows the elapsed time estimates for IDIH upgrade.

Table 16: IDIH Upgrade Execution Overview

Procedure	Elapsed Time (hr:min)		Procedure Title	Impact
	This Step	Cumulative		
Procedure 48	1:15-1:45	1:15-1:45	Oracle Guest Upgrade	None
Procedure 49	0:30-0:45	1:45-2:30	Upgrade the Mediation and Application Guests	None

Appendix F.1. Oracle Guest Upgrade

The Oracle Guest is upgraded first.

Procedure 48: Oracle Guest Upgrade

S T E P #	This procedure performs the IDIH Oracle Guest upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

1 ☐	**IDIH CLI:**
	
	Perform system health check
		Perform a system health check on the Oracle guest.
		
		1. Login in to the Oracle guest as the admusr user.
		
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		
		2. Execute the analyze_server.sh script.
		
		`$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i`
		
		Sample output:
		`[admusr@cat-ora ~]$ /usr/TKLC/xIH/plat/bin/analyze_server.sh -i`
		`13:24:52: STARTING HEALTHCHECK PROCEDURE`
		`13:24:52: date: 03-17-15, hostname: cat-ora`
		`13:24:52: TPD VERSION: 7.0.0.0.0-86.14.0`
		`13:24:52: ------------------------------------------------`
		`13:24:52: Checking disk free space`
		`13:24:52: No disk space issues found`
		`:`
		`:`
		`13:25:02: All tests passed!`
		`13:25:02: ENDING HEALTHCHECK PROCEDURE WITH CODE 0`
		
		If the output indicates a status failure, do not proceed with the upgrade. It is recommended to contact MOS for guidance.

Procedure 48: Oracle Guest Upgrade

<table>
<tr><td>2
☐</td><td>IDIH CLI:

Shutdown Mediation guest</td><td>Shutdown the Mediation guest in preparation for the Oracle guest upgrade.

1. Login in to the Mediation guest as admusr user.

ssh <IDIH IP address>
login as: admusr
password: <enter password>

2. Shutdown the Mediation guest.

$ sudo init 0

The Active SOAM server may have some or all of the following expected alarms:
Alarm ID = 19800 Communication Agent Connection Down
Alarm ID = 11511 Unable to connect via Comagent to remote DIH server with hostname

The Active NOAM server may have some or all of the following expected alarms:
Alarm ID = 19800 Communication Agent Connection Down</td></tr>
<tr><td>3
☐</td><td>IDIH CLI:

Shutdown Application guest</td><td>Shutdown the Application guest in preparation for the Oracle guest upgrade.

1. Login in to the Application guest as admusr user.

ssh <IDIH IP address>
login as: admusr
password: <enter password>

2. Shutdown the Application guest.

$ sudo init 0

The Active SOAM server may have some or all of the following expected alarms:
Alarm ID = 19800 Communication Agent Connection Down
Alarm ID = 11511 Unable to connect via Comagent to remote DIH server with hostname

The Active NOAM server may have some or all of the following expected alarms:
Alarm ID = 19800 Communication Agent Connection Down</td></tr>
<tr><td>4
☐</td><td>Move Oracle ISO.</td><td>Use a file transfer tool to copy the Oracle ISO to the Oracle guest as admusr.

Example:
$ scp oracle-7.2.0.0.0_72.21.0-x86_64.iso
admusr@<ora-guest-ip>:/var/TKLC/upgrade</td></tr>
<tr><td>5
☐</td><td>IDIH CLI:

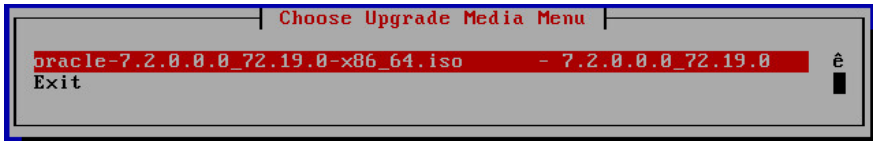
Start Oracle guest upgrade</td><td>The Oracle guest is upgraded using the Platform Configuration utility.

1. Launch the platform configuration utility.

$ sudo su - platcfg

2. In the resulting menu, select Maintenance > Upgrade > Initiate Upgrade.

3. At the ISO selection menu, select the target release Oracle ISO and press the Enter key.

  </td></tr>
</table>

Procedure 48: Oracle Guest Upgrade

6 ☐	**IDIH CLI:** Monitor upgrade progress	The platform configuration menu will exit and the guest will reboot when the upgrade completes. To view the detailed progress of the upgrade, access the server command line (via SSH or Console), and enter: `$ tail -f  /var/TKLC/log/upgrade/upgrade.log` Once the server has upgraded, it will re-boot, then it will take a couple of minutes for the Oracle processes to start up.

7 ☐	**IDIH CLI:**
	
	Perform system health check
		Wait a few minutes to allow the Oracle guest to stabilize after the reboot, and then repeat step 1 to perform the post-upgrade system health check.
		
		Note: the following warnings are expected due to the mediation and app servers being shutdown.
		
		`Warning: mediation server is not reachable (or ping response exceeds 3 seconds)`
		`Warning: app server is not reachable (or ping response exceeds 3 seconds)`

	THIS PROCEDURE HAS BEEN COMPLETED	

Appendix F.2. Upgrade the Mediation and Application Guests

The Mediation and Application Guest upgrade is similar to the installation procedure.

Procedure 49: Upgrade the Mediation and Application Guests

S T E P #	This procedure performs the IDIH Mediation and Application server upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	
1 ☐	**CLOUD GUI:** Remove existing Application Server	1. Use the hpyervisor-specific procedure to remove the current iDIH Application and iDIH Mediation guests.
2 ☐	**CLOUD GUI:** Deploy the latest application and mediation guest images	1. Use the hypervisor-specific procedure to deploy the latest Application and Mediation guests. 2. Configure the iDIH mediation and application guests to reflect the guest profile in the installation document [1].

3 ☐	**IDIH CLI:**
	
	Configure the network rules file
		1. Login in to the iDIH Mediation guest as the admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		2. Generate the net rules file
		`$ sudo udevadm trigger --subsystem-match=net`
		3. Update the net rules file. Replace the default interface names “eth0” with “xmi” and “eth1” with “int”. For the Mediation guest, rename the third interface from “eth2” to “imi”.
		`$ sudo vi /etc/udev/rules.d/70-persistent-net.rules`
		 
		4. Reboot the server:
		`$ sudo init 6`
		5. Repeat sub-steps 1 thru 4 for the application guest.

Procedure 49: Upgrade the Mediation and Application Guests

S T E P #	This procedure performs the IDIH Mediation and Application server upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

4 ☐	**IDIH CLI:**
	
	Configure the network interfaces for the mediation guest.
		1. Login in to the iDIH Mediation guest as the admusr user.
		`ssh <IDIH IP address>`
		`login as: admusr`
		`password: <enter password>`
		2. Configure the xmi network with its ip address and netmask.
		`$ sudo netAdm add -device=xmi -address=x.x.x.x -netmask=x.x.x.x -onboot=yes -bootproto=none`
		3. Configure the default route.
		`$ sudo netAdm add -route=default -device=xmi -gateway=x.x.x.x`
		4. Configure the int network its ip address and netmask.
		`$ sudo netAdm add -device=int -address=10.254.254.3 -netmask=255.255.255.224 -onboot=yes -bootproto=none`
		5. Ping the oracle guest to verify network connectivity
		`$ ping oracle`
		6. Configure the imi network with its ip address and netmask. *(mediation guest only)
		`$ sudo netAdm add -device=imi -address=x.x.x.x -netmask=x.x.x.x -onboot=yes -bootproto=none`
		7. Repeat sub-steps 1 thru 5 for the application guest.

5 ☐	**IDIH CLI:**
	
	Configure the network time protocol for the mediation and application guests.
		1. On the iDIH Mediation guest, launch the platform configuration menu.
		`$ sudo su - platcfg`
		2. From the platform configuration menu, configure ntpserver1 with the ip address supplied for NTP. Select:
		`Network Configuration -> NTP -> Edit -> ntpserver1`
		Select “Yes” when prompted to restart NTP.
		3. Exit the network configuration menu.
		4. To configure the Oracle VM hostname, select:
		`Server Configuration -> Hostname -> Edit`
		Note: the Mediation and Application guest hostnames should follow the format ‘xxxx-med’ and ‘xxxx-app’, where ‘xxxx’ can be any valid hostname characters.
		5. Exit the platform configuration menu.
		6. Repeat sub-steps 1 through 5 for the iDIH Application guest.

6 ☐	**IDIH CLI** Run the application guest post installation scipt.	1. On the iDIH application guest, run the post installation script and monitor the script until it completes. `$ sudo /opt/xIH/apps/install.sh`

Procedure 49: Upgrade the Mediation and Application Guests

S T E P #	This procedure performs the IDIH Mediation and Application server upgrade. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE**	

7 ☐	**IDIH CLI:**
	
	Run the mediation post installation script.
		1. On the iDIH mediation guest, run the post installation script and monitor the script until it completes.
		
		`$ sudo /opt/xIH/mediation/install.sh`
		
		2. Reconfigure the hostname in the comcol database.
		
		`$ sudo su - tekelec`
		`$ sudo iset -fnodeName=\`hostname\` -fhostName=\`hostname\` NodeInfo where 1=1`

8 ☐	**IDIH CLI:** Run the healthcheck scripts on the mediation and application guests.	After the post installation script has completed on the application guests. Run the healthcheck script on the application and mediation guests. `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i`

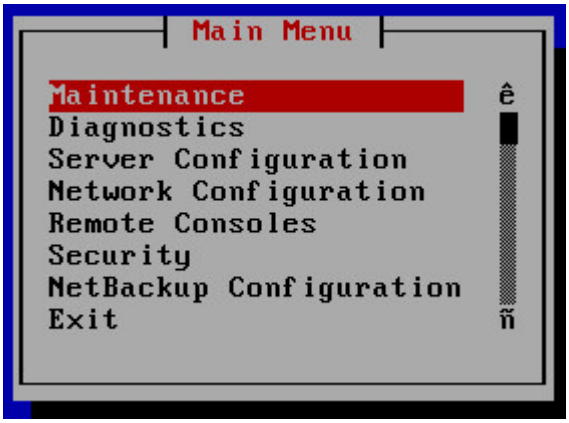
Appendix G. ALTERNATE SERVER UPGRADE PROCEDURES

The procedures in this section provide alternative ways of upgrading various server types, using an array of differing methods. All of the procedures in this section are secondary to the upgrade methods provided in Section 4 and Section 5. These procedures should be used only when directed by MOS or by other procedures within this document.

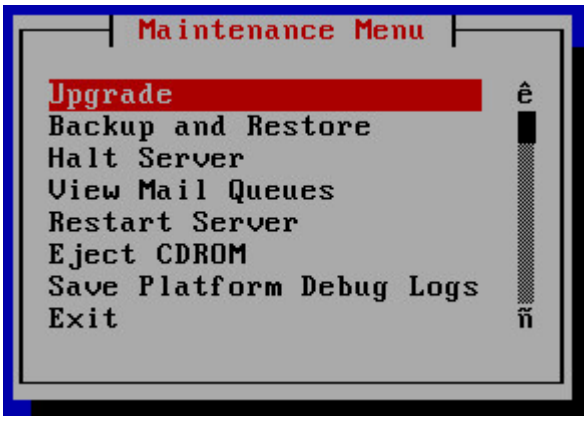
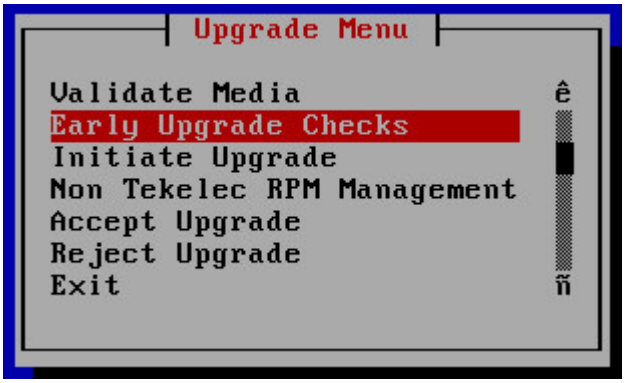
Appendix G.1. Server Upgrade using platcfg

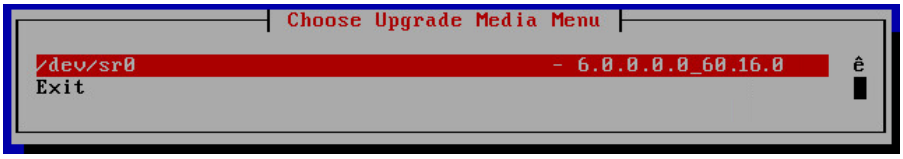
The procedure provided in this appendix enables a server to be upgraded using the Platform Configuration (platcfg) utility. This procedure should be used only under the guidance and direction of MOS.

Procedure 50: Server Upgrade Using Platcfg

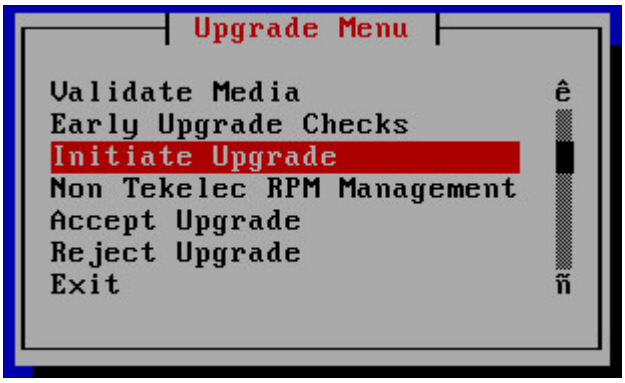
S T E P #		
	This procedure upgrades a server using the platcfg utility. NOTE: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	Login to the server to be upgraded	Use the SSH command (on UNIX systems - or putty if running on Windows) to log into the server to be upgraded: `ssh admusr@<server_ip>`
2 ☐	Enter the platcfg menu	Switch to the platcfg user to start the configuration menu. `$ sudo su - platcfg` From the Main Menu, select **`Maintenance`** 

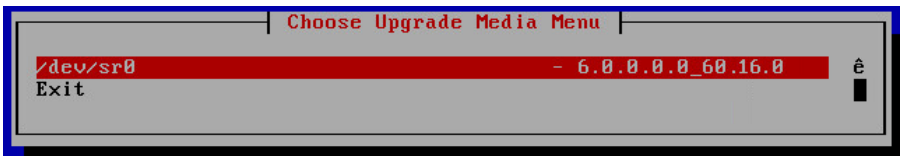
Procedure 50: Server Upgrade Using Platcfg

3 ☐	Select Upgrade	From the Maintenance Menu, select **Upgrade** 
4 ☐	Select Early Upgrade Checks	From the Upgrade Menu, select **Early Upgrade Checks** 

5 ☐	Select the Upgrade Media	1. From the Choose Upgrade Media Menu, select the desired target media. This will initiate the early upgrade checks in the console window.
		 
		Informational messages will be displayed as the checks progress. At the end of a successful test, a message similar to the following will appear:
		`Running earlyUpgradeChecks() for Upgrade::EarlyPolicy::`
		`TPDEarlyChecks upgrade policy...`
		`Verified server is not pending accept of previous upgrade`
		`Hardware architectures match`
		`Install products match.`
		`Verified server is alarm free!`
		`Early Upgrade Checks Have Passed!`
		2. Verify early upgrade checks pass. In case of errors, it is recommended to contact MOS.
		3. Press 'q' to exit the screen session and return to the platcfg menu.
		4. From the Choose Upgrade Media Menu, select **Exit.**

Procedure 50: Server Upgrade Using Platcfg

6 ☐	Initiate the upgrade	From the Upgrade Menu, select **Initiate Upgrade**. 

7 ☐	Select the Upgrade Media	The screen will display a message that it is searching for upgrade media. Once the upgrade media is found, an Upgrade Media selection menu will be displayed similar to the example shown below.
		
		From the Choose Upgrade Media Menu, select the desired target media. This will initiate the server upgrade.
		 
		Many informational messages will come across the terminal screen as the upgrade proceeds.
		
		Finally, after upgrade is complete, the server will reboot.
		
		`A reboot of the server is required.`
		`The server will be rebooted in 10 seconds`

8 ☐	SSH to the upgraded server	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server just upgraded: `ssh admusr@<server_IP>` (Answer 'yes' if you are prompted to confirm the identity of the server.)

9 ☐	Check for upgrade errors	Examine the upgrade logs in the directory /var/TKLC/log/upgrade and verify that no errors were reported.
		
		`grep -i error /var/TKLC/log/upgrade/upgrade.log`
		
		Examine the output of the above command to determine if any errors were reported.
		
		If the upgrade fails, collect the following files:
		
		`/var/TKLC/log/upgrade/upgrade.log`
		`/var/TKLC/log/upgrade/ugwrap.log`
		`/var/TKLC/log/upgrade/earlyChecks.log`
		`/var/TKLC/log/platcfg/upgrade.log`
		
		It is recommended to contact MOS by referring to Appendix J of this document and provide these files.

Procedure 50: Server Upgrade Using Platcfg

10 ☐	Verify the upgrade	Check the upgrade log for the upgrade complete message
		
		`grep "UPGRADE IS COMPLETE" /var/TKLC/log/upgrade/upgrade.log`
		
		Verify that the message "**UPGRADE IS COMPLETE**" is displayed. If not, it is recommended to contact MOS.
		
		`[admusr@NO2 ~]$ grep "UPGRADE IS COMPLETE" /var/TKLC/log/upgrade/upgrade.log`
		`1407786220::  UPGRADE IS COMPLETE`

		THIS PROCEDURE HAS BEEN COMPLETED.

Appendix G.2. Manual DA-MP Upgrade Procedure

Procedure 51 is used to upgrade the DA-MP Server Group manually. This procedure is provided as an alternative to the normal DA-MP upgrade procedures in Section 5.

Procedure 51 must be executed for all configured DA-MPs of a site, regardless of how the DA-MPs are grouped for upgrade. So if 16 DA-MPs are upgraded four at a time, then Procedure 51 must be executed four distinct times.

Procedure 51: Manual DA-MP Upgrade Procedure

S T E P #	This procedure upgrades the DA-MP servers using the manual upgrade method. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	Identify all the DA-MPs to be upgraded together	From the data captured in Table 3, 1. Identify the "DSR (multi-active cluster)" Server Group to be upgraded.
2. ☐	Upgrade DA-MP servers as identified in step 1	Upgrade up to (½) one half (no more than 50%) of the DA-MP servers in parallel using the Upgrade Multiple Servers procedure : **NOTE: When using the manual server upgrade method, it is recommended that the DA-MP Leader be upgraded in the last group of servers to minimize DA-MP Leader role changes.** **Execute Appendix E : Upgrade Multiple Servers** After successfully completing the procedure in Appendix E, return to this point and continue with the next step.
3. ☐	Repeat for all servers identified in Step 1 of this procedure.	Repeat step 2 of this procedure for the remaining DA-MP servers.
THIS PROCEDURE HAS BEEN COMPLETED.		

Appendix G.3. Manual SBR Upgrade Procedure

Procedure 52 is used to upgrade the SBR Server Group manually. This procedure is provided as an alternative to the normal SBR upgrade procedures in Section 5.

Note: Before upgrading the Active SBR, it is imperative that the database audit of the Spare and Standby servers complete successfully. Failure to comply could result in a loss of session data.

Procedure 52: Manual SBR Upgrade Procedure

S T E P #	This procedure upgrades an SBR Server Group using the manual upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED TO CONTACT MOS AND **ASK FOR UPGRADE ASSISTANCE.**	
1. ☐	**Active NOAM VIP:** Identify the SBR Server Group(s) to Upgrade	Identify the Active, Standby, and Spare SBR servers. 1. From the data captured in Table 3, identify the server group(s) to upgrade. One server group can be executed at a time or multiple server groups can be executed simultaneously. 2. Log into the NOAM GUI using the VIP. 3. Navigate to **Main Menu > Policy and Charging >Maintenance > SBR Status.** Open each server group chosen in sub-step 1. Note which server is Active, Standby and Spare (as designated by the Resource HA Role) for each server group chosen for upgrade. The following figure provides an example: **GTR-SBR-1A - Active** **GTR-SBR-1B - Standby** **GTR-SBR-1Sp - Spare** **Main Menu: Policy and Charging -> Maintenance -> SBR Status** Filter PCA_MATED_SITES Server Group Name / Resource Domain Name / Resource Domain Profile GTR_SBR_SG_A / PCA_SESSION / Policy and Charging Session Server Name / Resource HA Role / Congestion Level / Sub Resources Hosted GTR-SBR-1A / Active / Normal / 0,1,2,3,4,5,6,7 GTR-SBR-1B / Standby / Normal / 0,1,2,3,4,5,6,7 NSX-SBR-1Sp / Spare / Normal / 0,1,2,3,4,5,6,7 **NOTE: SBR servers have two High Availability policies: one for controlling replication of session or binding data, and one for receipt of replicated configuration data from the NOAM and SOAM GUIs. During this upgrade procedure, ONLY the High Availability policy for replication of session or binding data is important. This means that the SBR Status screen MUST be used to determine the High Availability status (Active, Standby, or Spare) of SBR servers. The HA Status screen and the OAM Max HA Role column on the Upgrade screen must NOT be used because they only show the status of the configuration replication policy.** **Because the two High Availability policies run independently, it is possible that a given server might be Standby or Spare for the session and binding replication policy, but Active for the configuration replication policy. When this happens, it is necessary to ignore warnings on the Upgrade screen about selecting what it views as the Active server (for the configuration replication policy).**

Procedure 52: Manual SBR Upgrade Procedure

2. ☐	**Active NOAM VIP:** Upgrade Spare SBR Server identified in step 1 of this procedure.	**NOTE: The Spare SBRs of this server group will be located at different sites.** 1. Upgrade the Spare SBR server using the Upgrade Single Server procedure : **Execute Appendix D**—Upgrade Single Server Procedure After successfully completing the procedure in Appendix D, return to this point to monitor server status. **From the Active NOAM GUI:** 2. Navigate to **Main Menu > Policy and Charging > Maintenance > SBR Status**. Open the tab of the server group being upgraded. NOTE: After executing Appendix D, the Spare SBR will temporarily disappear from the SBR Status screen. When the server comes back online, it will reappear on the screen with a status of "Out of Service". 3. Monitor the **Resource HA Role** status of the Spare server. Wait for the status to transition from "Out of Service" to "Spare". 4. If the system is equipped with a second Spare SBR server, repeat sub-steps 1 thru 3 for the other spare. Caution: Do not proceed to step 3 until the **Resource HA Role** of the Spare SBR server returns to "**Spare**".
3. ☐	Upgrade Standby SBR Server identified in step 1 of this procedure.	Upgrade the Standby SBR server using the Upgrade Single Server procedure : **Execute Appendix D -** Upgrade Single Server Procedure After successfully completing the procedure in **Appendix D**, return to this point and continue with the next step.
		**!WARNING!** **Failure to comply with step 4 and step 5 may result in the loss of PCA traffic, resulting in service impact**
4. ☐	**Active NOAM VIP:** Verify Standby SBR server status	1. Navigate to **Main Menu > Policy and Charging >Maintenance > SBR Status.** Open the tab of the server group being upgraded. NOTE: After executing Appendix D, the Standby SBR will temporarily disappear from the SBR Status screen, and the Spare server will assume the Standby role. When the upgraded server comes back online, it will reappear on the screen with a status of "Out of Service". 2. Monitor the **Resource HA Role** status of the upgraded server. Wait for the status to transition from "Out of Service" to "Standby". Caution: Do not proceed to step 5 until the **Resource HA Role** of the upgraded server transitions to "**Standby**".

Procedure 52: Manual SBR Upgrade Procedure

5. ☐	**Active NOAM VIP:** Verify bulk download completes	Verify that the bulk download from the Active SBR to the Standby and Spare SBRs completes. 1. Navigate to **Main Menu > Alarm & Event > View History** 2. Export the Event Log using the following filter: **Server Group**: Choose the SBR group that is in upgrade **Display Filter**: Event ID = 31127 – DB Replication Audit Complete **Collection Interval**: X hours ending in current time, where X is the time from upgrade completion of the Standby and Spare servers to the current time. 3. Wait for all instances of Event 31127: • 1 for the Standby binding SBR • 1 for the Standby session SBR • 1 for the Spare binding SBR • 1 for the Spare session SBR • 1 for the 3rd site Spare binding SBR (if equipped) • 1 for the 3rd site Spare session SBR (if equipped) NOTE: There is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured.
6. ☐	Upgrade Active SBR Server as identified in Step 1 of this procedure	Upgrade the Active SBR server using the Upgrade Single Server procedure : **Execute Appendix D** -- Single Server Upgrade Procedure After successfully completing the procedure in Appendix D, return to this point and continue with the next step.
7. ☐	Repeat for all SBR Server Groups with Active, Standby in Site 1 and Spare in Site 2	Repeat steps 1 through 6 for all remaining binding and session server groups to be upgraded.
THIS PROCEDURE HAS BEEN COMPLETED.		

Appendix H. EXPIRED PASSWORD WORKAROUND PROCEDURE

This appendix provides the procedures to handle password expiration during upgrade. Procedure 53 is a temporary workaround to allow an expired password to be used on a non-upgrade site. This procedure is provided as a workaround when a password expires after the NOAM has been upgraded and before all sites have been upgraded.

The workaround must be removed using Procedure 54 after the site is upgraded. Failure to remove the workaround will inhibit password aging on the server.

Appendix H.1. Inhibit Password Aging

This procedure enacts a workaround that inhibits password aging on the SOAM. This procedure should be used only when the following conditions apply:

- An upgrade is in progress
- The NOAMs have been upgraded, but one or more sites have not been upgraded
- A login password has expired on a non-upgraded site

Once the workaround is enacted, no passwords will expire at that site. It is expected that the workaround will be removed once the site is upgraded.

Procedure 53: Expired Password Workaround Procedure

S T E P #	This procedure disables password aging on a server, allowing "expired" credentials to be used for login. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

1 ☐	**Active SOAM CLI:**
	SSH to Active SOAM server
		Disable password aging.
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active SOAM of the first non-upgraded site:
		`ssh admusr@<SOAM_VIP>`
		(Answer 'yes' if prompted to confirm the identity of the server.)
		2. Create a text file with the following content (exactly as formatted):
		`[production]`
		`aw.policy.pwchange.isExpired =`
		`aw.policy.db.checkPw =`
		`[development : production]`
		`[test : development]`
		3. Save the file as:
		`/var/TKLC/appworks/ini/pw.ini`
		4. Change the file permissions:
		`$ chmod 644 pw.ini`
		5. Execute the following command:
		`$ sudo clearCache`
		NOTE: For each server on which this workaround is enacted, the old "expired" password must be used for login. The new password that is used on the NOAM will not work on these servers.

Procedure 53: Expired Password Workaround Procedure

2 ☐	Repeat for Standby SOAM	Repeat step 1 for the Standby SOAM
3 ☐	Repeat for all non-upgraded sites	Repeat steps 1 and 2 for all non-upgraded sites.
	THIS PROCEDURE HAS BEEN COMPLETED.	

Appendix H.2. Enable Password Aging

This procedure removes the password expiration workaround that is enabled by Procedure 53.

Procedure 54: Expired Password Workaround Removal Procedure

S T E P #	This procedure removes the password aging workaround and re-enables password aging on a server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	

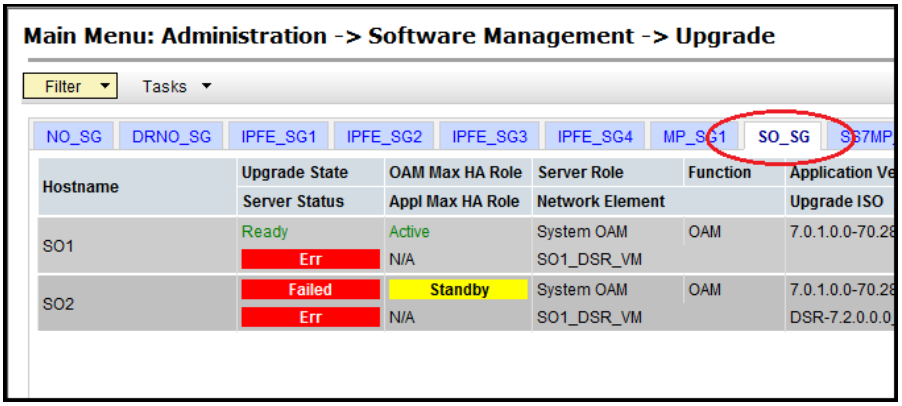
1 ☐	**Active SOAM CLI:**
	SSH to Active SOAM server
		1. Use the SSH command (on UNIX systems – or putty if running on windows) to login to the Active SOAM of the first non-upgraded site:
		`ssh admusr@<SOAM_VIP>`
		(Answer 'yes' if prompted to confirm the identity of the server.)
		2. Delete the pw.ini file:
		`$ sudo rm /var/TKLC/appworks/ini/pw.ini`
		3. Execute the following command:
		`$ sudo clearCache`

2 ☐	Repeat for Standby SOAM	Repeat step 1 for the Standby SOAM
3 ☐	Repeat for all non-upgraded sites	Repeat steps 1 and 2 for all non-upgraded sites.
	THIS PROCEDURE HAS BEEN COMPLETED.	

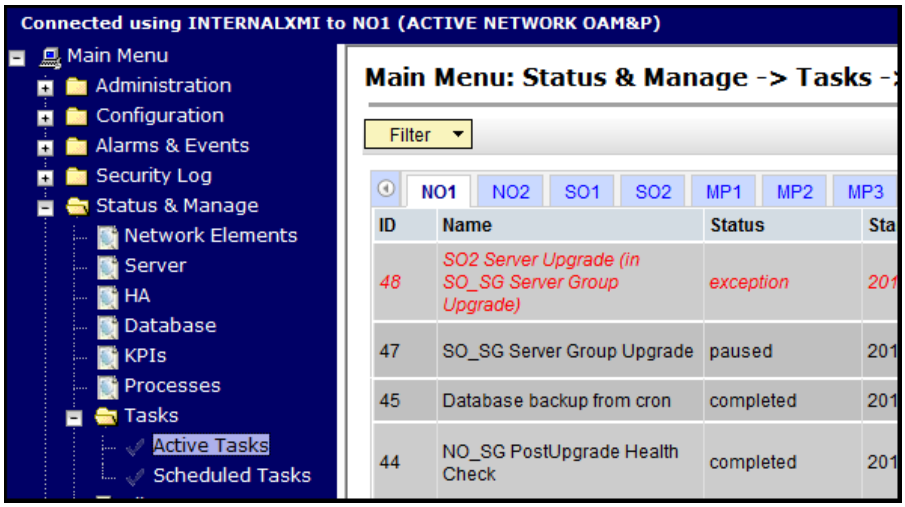
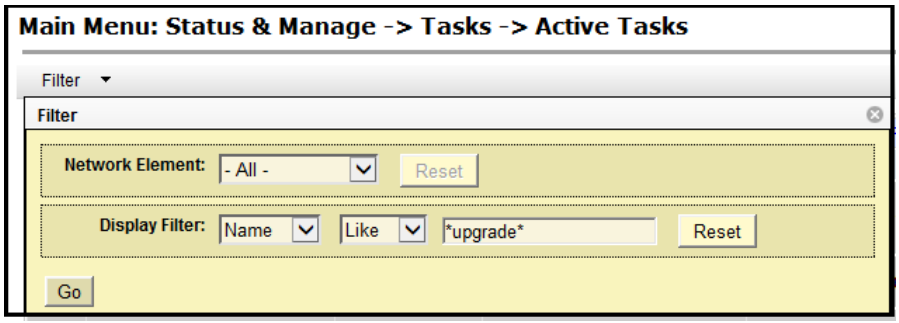
Appendix I. RECOVERING FROM A FAILED UPGRADE

This procedure provides the steps required to recover a server after a failed upgrade. Due to the complexity of the DSR system and the nature of troubleshooting, it is recommended to contact MOS for guidance while executing this procedure.

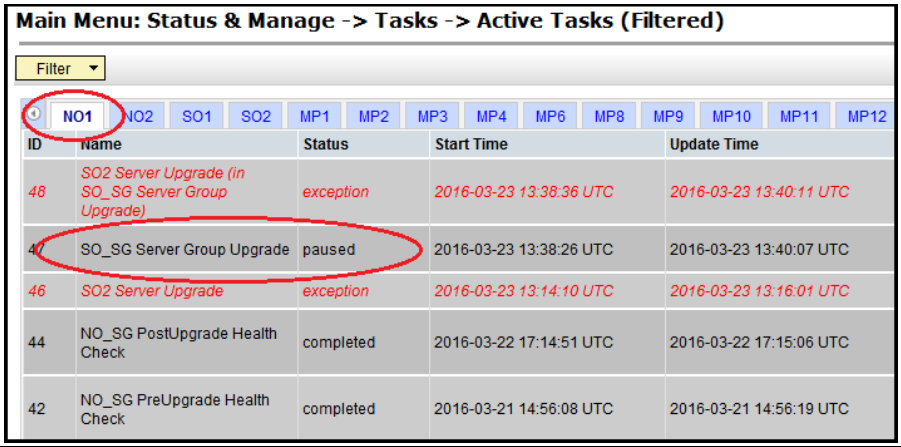
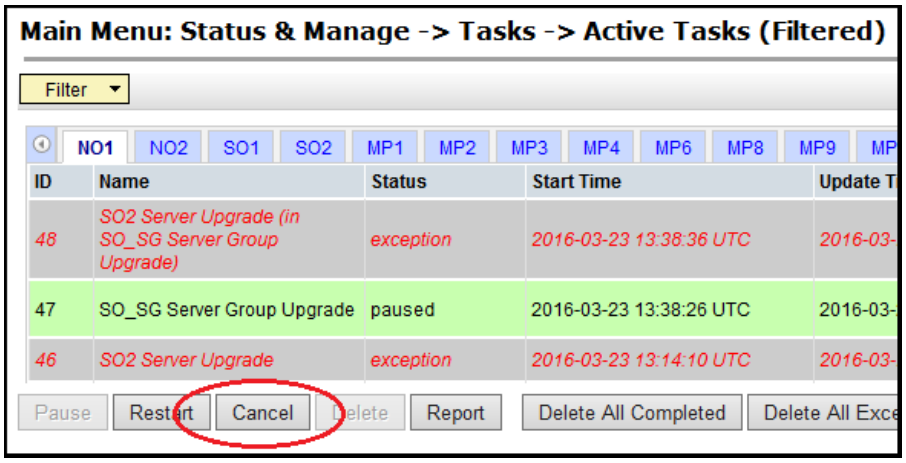
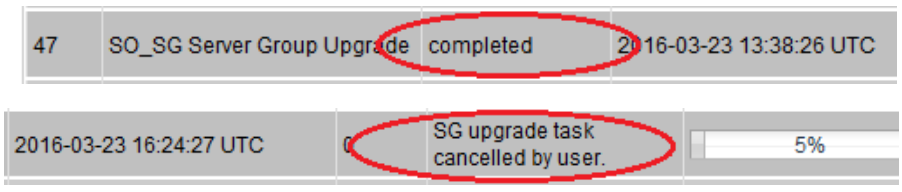
Procedure 55: Recovering from a Failed Upgrade

S T E P #		
	This procedure provides the basic steps for returning a server to a normal state after an upgrade failure. Note that the server will be returned to the source release by this procedure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, IT IS RECOMMENDED **TO CONTACT MOS AND ASK FOR UPGRADE ASSISTANCE.**	
1 ☐	**Active NOAM VIP:** Select affected server group	From the Upgrade screen, select the server group containing the failed server. 1. Log into the NOAM GUI using the VIP. 2. Navigate to **Administration > Software Management > Upgrade** The Upgrade Administration screen is displayed 3. Select the server group tab for the server to be recovered. 
		• **If the failed server was upgraded using the "Upgrade Server" option, then skip to step 7 of this procedure** • **If the failed server was upgraded using the "Auto Upgrade" option, then continue with step 2 of this procedure.**

Procedure 55: Recovering from a Failed Upgrade

2 ☐	**Active NOAM VIP:** View Active Tasks	Navigate to the Active Tasks screen to view the tasks. 1. Navigate to **Status & Manage > Tasks > Active Tasks** The Active Tasks screen is displayed. 
3 ☐	**Active NOAM VIP:** Search for upgrade task	Use the filter to locate the server group upgrade task. From the Active NOAM GUI: 1. Click the Filter dropdown and enter the following filter values: a. Network Element: **All** b. Display Filter: **Name Like *upgrade*** 2. Click the **Go** button. 

Procedure 55: Recovering from a Failed Upgrade

4	**Active NOAM VIP:** Identify the upgrade task	In the search results list, locate the **Server Group Upgrade** task. 1. If not already selected, select the tab displaying the hostname of the Active NOAM server. 2. Locate the task for the **Server Group Upgrade**. It will show a status of "paused". 
5	**Active NOAM VIP:** Cancel the upgrade task	Cancel the **Server Group Upgrade** task. 1. Click the Server Group Upgrade task to select it. It will become highlighted on the screen. 2. Click the **Cancel** button to cancel the task. 3. Click **OK** on the confirmation dialog box to confirm the cancellation. 
6	**Active NOAM VIP:** Verify task cancellation	Verify the Server Group Upgrade task is canceled. 1. On the Active Tasks screen, verify the task that was canceled in step 5 shows a status of "**completed**". 

Procedure 55: Recovering from a Failed Upgrade

7 ☐	**Failed server CLI:**
	Inspect upgrade log
		Login to the failed server to inspect the upgrade log for the cause of the failure.
		
		1. Use an SSH client to connect to the failed server:
		
		`ssh <XMI IP address>`
		`login as: admusr`
		`password: <enter password>`
		
		Note: The static XMI IP address for each server should be available in Table 3.
		
		2. View or edit the upgrade log at `/var/TKLC/log/upgrade/upgrade.log` for clues to the cause of the upgrade failure.
		3. If the upgrade log contains a message similar to the following, inspect the early upgrade log at `/var/TKLC/log/upgrade/earlyChecks.log` for additional clues.
		
		`1440613685::Early Checks failed for the next upgrade`
		`1440613691::Look at earlyChecks.log for more info`

		• Although outside of the scope of this document, the user is expected to use standard troubleshooting techniques to clear the alarm condition from the failed server. • If troubleshooting assistance is needed, it is recommended to contact MOS as described in Appendix J - Accessing My Oracle Support • **DO NOT PROCEED TO STEP 8 OF THIS PROCEDURE UNTIL THE ALARM CONDITION HAS BEEN CLEARED!**

8 ☐	**Failed Server CLI:**
	Verify Platform alarms are cleared
		Verify all Platform alarms have been cleared from the failed server.
		
		1. Use the alarmMgr utility to verify that all Platform alarms have been cleared from the system.
		
		`$ sudo alarmMgr --alarmstatus`
		
		Example output:
		`[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus`
		`SEQ: 2 UPTIME: 827913 BIRTH: 1458738821 TYPE: SET ALARM:`
		`TKSPLATMI10|tpdNTPDaemonNotSynchronizedWarning|1.3.6.1.4.1.323.5.3.18`
		`.3.1.3.10|32509|Communications|Communications Subsystem Failure`
		
		***** user troubleshoots alarm and is able to resolve NTP sync issue and clear alarm *****
		
		`[admusr@SO2 ~]$ sudo alarmMgr --alarmstatus`
		`[admusr@SO2 ~]$`

9 ☐	**Active NOAM VIP:** Re-execute the server upgrade	Return to the upgrade procedure being executed when the failure occurred. Re-execute the upgrade for the failed server using the "**Upgrade Server**" option. **Note: Once a server has failed while using the Automated Server Group Upgrade option, the "Auto Upgrade" option cannot be used again on that server group. The remaining servers in that server group must be upgraded using the "Upgrade Server" option.**

Appendix J. ACCESSING MY ORACLE SUPPORT (MOS)

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*. When calling, there are multiple layers of menus selections. Make the selections in the sequence shown below on the Support telephone menu:

1. For the first set of menu options, select 2, "New Service Request". You will hear another set of menu options.
2. In this set of menu options, select 3, "Hardware, Networking and Solaris Operating System Support". A third set of menu options begins.
3. In the third set of options, select 2, "Non-technical issue". Then 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, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the 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

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.