Oracle® Communications Application Session Controller

Maintenance Release Guide
Release 3.7.0
Formerly Net-Net OS-E

2016

ORACLE

Notices

Contents

About this guide MRG ORACLE

The 3.7.0 Maintenance Release Guide provides information about the contents of maintenance releases related to OS-E 3.7.0. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release of the ASC from prior releases. When applicable, this guide contains explanations of defect fixes to the software and step-by-step instructions, if any, for how to enables these fixes on your system. This guide contains explanations of adaptations including conceptual information and configuration steps.

Purpose of this Document

Designed as a supplement to the main documentation set supporting ASC 3.7.0, this document informs you of changes made to the ASC software in the maintenance releases of 3.7.0. Consult this document for content specific to maintenance releases. For information about general ASC features, configuration, and maintenance, consult the Related Documentation listed in the section below and then refer to the applicable document.

Organization

The 3.7.0 Maintenance Release Guide is organized chronologically by maintenance release number, started with the oldest available maintenance release and ending with the most recently available maintenance release.

This document contains a Maintenance Release Availability Matrix, showing when and if given maintenance releases have been issued and the date of issue. Each available maintenance release constitutes one chapter of this guide.

In certain cases, a maintenance release will not have been made generally available. These cases are noted in the Maintenance Release Availability Matrix. When Oracle has not made a maintenance release available, there will be no corresponding chapter for that release. Therefore, you might encounter breaks in the chronological number of maintenance release.

Maintenance Release Availability Matrix

The table below lists the availability for version 3.7.0 maintenance releases.

Mainenance release number	Availability Notes
3.7.0M1	October 31, 2013
3.7.0M2	February 22, 2014
3.7.0M3	March 1, 2015
3.7.0M4	May 17, 2016

Related Documentation

The following is a list of the documents that make up the ASC documentation set for this release:

- Oracle Communications Application Session Controller System and Installation Commissioning Guide
- Oracle Communications Application Session Controller System and Intsallation Commissioning Guide Releaes 3.7.0M4
- Oracle Communications Application Session Controller Management Tools
- Oracle Communications Application Session Controller System Administration Guide
- Oracle Communications Application Session Controller Session Services Configuration Guide
- Oracle Communications Application Session Controller Objects and Properties Reference
- Oracle Communications Application Session Controller System Operations and Troubleshooting
- Oracle Communications Application Session Controller Release Notes
- Oracle Communications Application Session Controller Web Services SOAP REST API
- Oracle Communications Application Session Controller Installation Guide

Revision History

This section contains a revision history for this document.

Date	Description
October 2013	• Includes 3.7.0M1 adaptations.
March 2014	• Includes 3.7.0M2 adaptations. • Updates the Netra X3-2 for Acme Packet Support section to include ASC-specific cabling and configuration information.
February 2015	• Updates the "Overriding Next Hop and Previous Hop IPs of Web Endpoints" section (introduced in 3.7.0M1) with a more thorough explanation. • Adds "WebRTC Video Issues" to the Known Problems and Restrictions in 3.7.0M2. • Adds a note to the "Augmented ICE Overview regarding ASC default behavior. • Corrects various typographical errors.
March 2015	• Includes 3.7.0M3 adaptations.
June 2015	• Updates version of certified OVM support to 3.3.1. • Adds KVM on OL7 to list of supported VM platforms.
October 2015	• Adds "Diffie-Hellman Logjam Attack Defense" to Known Problems and Restrictions in 3.7.0M1, 3.7.0M2, and 3.7.0M3.
May 2016	• Includes 3.7.0M4 adaptations.
July 2016	• Updates the version number of Oracle Linux on which you can install the ASC.

1

Release 3.7.0M1

This section describes all of the new adaptations added to the OS-E in release 3.7.0M1, including new features, configuration objects and properties, and MIBs.

3.7.0M1 ASC System Files

The 3.7.0M1 ASC system files available for individual download are as follows:

- Oracle Communications Application Session Controller E3.7.0m1 Installation Image Supertar
- Oracle Communications Application Session Controller E3.7.0m1 Installation USB image
- Oracle Communications Application Session Controller E3.7.0m1 Installation ISO image
- Oracle Communications Application Session Controller E3.7.0m1 VMWare VMX/VMDK file
- Oracle Communications Application Session Controller E3.7.0m1 Xen server image
- Oracle Communications Application Session Controller E3.7.0m1 HyperV OVA file
- Oracle Communications Application Session Controller E3.7.0m1 LCR Import Tool
- Oracle Communications Application Session Controller E3.7.0m1 Embedded LCR Import Tool
- Oracle Communications Application Session Controller E3.7.0m1 Samples Kit
- Oracle Communications Application Session Controller E3.7.0m1 Archive Viewer Application
- Oracle Communications Application Session Controller E3.7.0m1 Weblogic SDK file
- Oracle Communications Application Session Controller E3.7.0m1 License Document

New Features

- WebRTC Enhancements
- Licensing Enhancements
- Netra X3-2 Server for Acme Packet Support
- Call-Control-Call Multiple Session Configuration Support
- Overriding Next Hop and Previous Hop IPs of Web Endpoints
- Dynamic Events Endpoint Redundancy
- Show Ethernet Status Provider Update

Licensing Enhancements

As of release 3.7.0M1, the OS-E comes with a default license, default_license.xml, installed. You no longer need feature licenses unless you are using any of the following codecs:

- AMRWB
- AMRNB
- G723
- G729
- GSM-AMR

Note: Do not run the license fetch command to replace or update your existing license without contacting your Oracle representative first.

Update to Config Setup

The config setup command has been updated to allow you to configure session capacity for all licensed features.

The command now looks as follows:

```
OS-E>config setup
set box\hostname:
config box\interface:
set box\cli\prompt:
set features\media-sessions:
...
```

The "cxc.setup" script that is run when you issue the config setup command has been extended to prompt you to configure each capacity to match what you have purchased.

Upgrading Changes for Pre-3.7.0M1 Releases

When you upgrade the OS-E from pre-3.7.0M1 versions, the default_license.xml license is applied first and the old license file from the previous release follows. This ensures the session capacity for all features from the old license overrides the new default license.

WebRTC Enhancements

The OS-E's WebRTC support has been enhanced to include augmented ICE as well as DTLS encryption.

Augmented ICE Overview

In addition to ICE, the OS-E also supports augmented ICE. In ICE the OS-E strips the candidates from the SDP while in augmented ICE the OS-E preserves all candidates received from a WebRTC endpoint. This provides the WebRTC endpoints the option to either anchor media on the OS-E or not.

Note: By default, augmented ICE is disabled on the OS-E. If you are using augmented ICE for a particular session, enable it on that named **session-config-pool** > **entry** only. Leave the **default-session-config** object's augmented ICE setting disabled so as to not affect all named sessions, which can cause an adverse negative impact.

Configuring Augmented ICE

If you are configuring the OS-E for augmented ICE you must complete the configuration procedure for ICE plus some additional configuration.

1. Click the Configuration tab and select either default-session-config or session-config-pool > entry.
2. Click Configure next to media.
3. augmented-ice—Set to enabled to enable augmented ICE.
4. Click Set. You are returned to the media object.

5. Click Configure next to in-encryption.
6. mode—Select pass-thru from the drop-down list.
7. Click Set. You are returned to the media object.
8. Click Configure next to out-encryption.
9. mode—Select pass-thru from the drop-down list.
10. Click Set. Update and save the configuration.

What is DTLS?

In addition to SDES-SRTP, the OS-E also supports Datagram Transport Layer Security (DTLS) as a method for encryption. DTLS works similarly to SDES-SRTP in that encryption keys are exchanged in the SDP offer and answer using the crypto attribute and the OS-E supports DTLS on a per call-leg basis.

For more information on DTLS, visit http://tools.ietf.org/html/rfc4347.

Configuring In-Leg Encryption

This section describes how to configure encryption on the OS-E.

Although the OS-E supports encryption, it does not require it from WebRTC endpoints. If an endpoint does not support encryption, it does not include a crypto key in its answer SDP and RTP is automatically used to transport media.

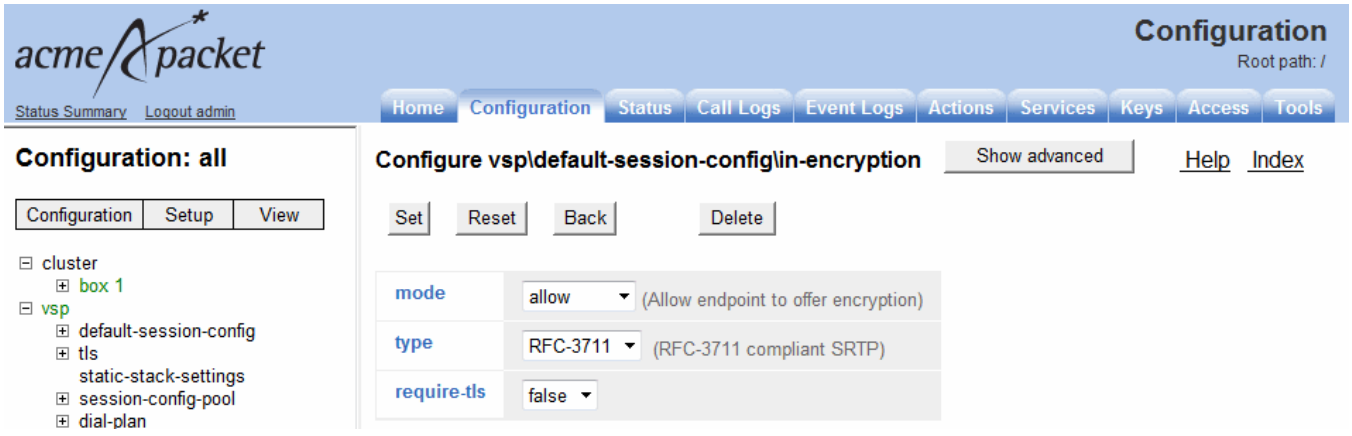
Because the OS-E always sends media encrypted out, you must configure the in-leg to allow encryption and the out-leg to require it.

You can configure the OS-E to use SDES-SRTP, DTLS, or specify multiple and let the WebRTC endpoint decide which type of encryption to use.

Note: You must configure encryption-preferences when type is set to multiple or the OS-E does not perform encryption.

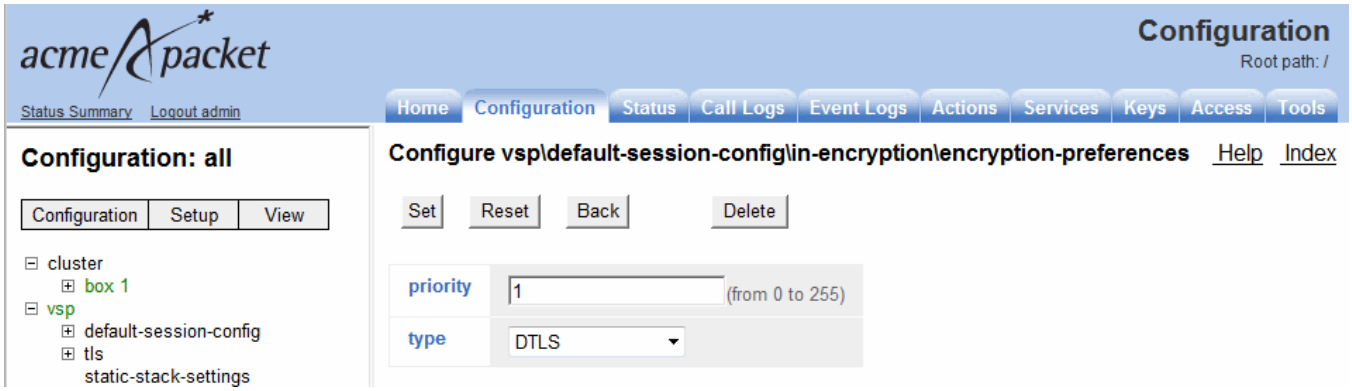
To configure in-leg encryption:

1. Click the Configuration tab and select either default-session-config or session-config-pool > entry.
2. Click Configure next to in-encryption.



3. mode—Select allow from the drop-down list. This allows the OS-E to receive encryption on the in-leg.
4. type—Select the type of encryption you want to use from the drop-down list.
   - RFC3711—Use the SDES-SRTP protocol for encryption.
   - DTLS—Use the DTLS protocol for encryption.
   - multiple—Both SDES-SRTP and DTLS are offered for encryption. Using the encryption-preferences property, assign each protocol a priority and the type of encryption used depends upon the WebRTC endpoint.

5. If you set type to multiple, click Add encryption-preferences and click Edit.



6. priority—Enter a 1.
7. type—Select DTLSfrom the drop-down list.

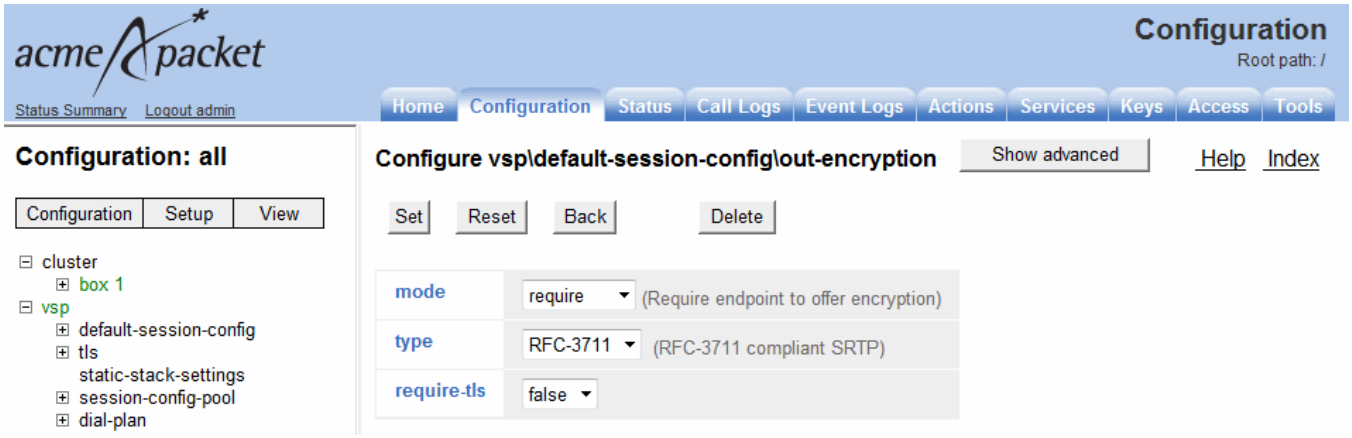
Note: Always give DTLS a priority of 1 and RFC-3711 a priority of 2.

8. Click Set.
9. Click Add encryption-preferences and click Edit.
10. priority—Enter a 2.
11. type—Select RFC3711from the drop-down list.
12. Click Set. Update and save the configuration.

Configuring Out-Leg Encryption

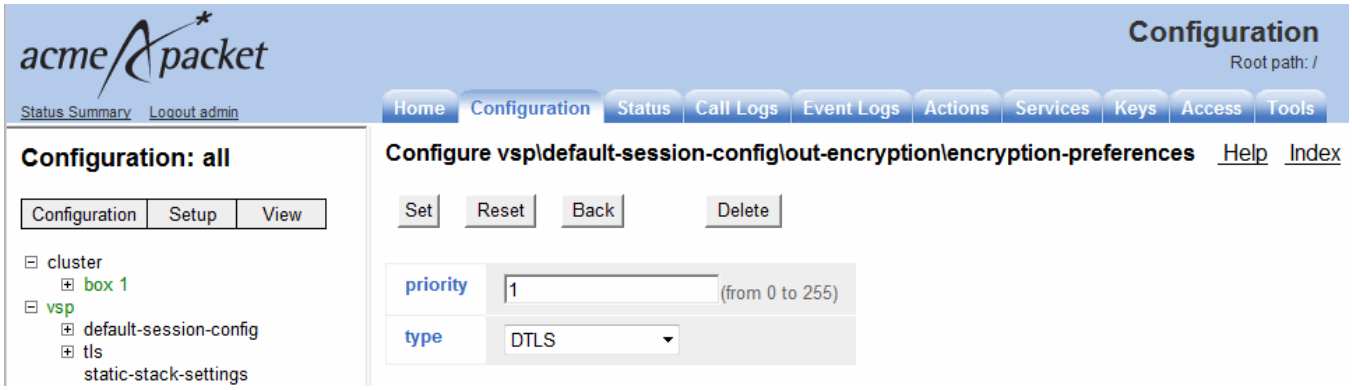
To configure out-leg encryption:

1. Click the Configuration tab and select either default-session-config or session-config-pool > entry.
2. Click Configure next to out-encryption.



3. mode—Select require from the drop-down list. This allows the OS-E to offer encryption.
4. type—Select the type of encryption you want to use from the drop-down list.
   - RFC3711—Use the SDES-SRTP protocol for encryption.
   - DTLS—Use the DTLS protocol for encryption.
   - multiple—Both SDES-SRTP and DTLS are offered for encryption. Using the encryption-preferences property, assign each protocol a priority and the type of encryption used depends upon the WebRTC endpoint.

5. If you set type to multiple, click Add encryption-preferences and click Edit.



6. priority—Enter a 1.
7. type—Select DTLSfrom the drop-down list.

Note: Always give DTLS a priority of 1 and RFC-3711 a priority of 2.

8. Click Set.
9. Click Add encryption-preferences and click Edit.
10. priority—Enter a 2.
11. type—Select RFC3711from the drop-down list.
12. Click Set. Update and save the configuration.

show ice-dtls-status

Displays information per call leg for sessions using DTLS encryption.

Sample Output

```
OS-E>show ice-dtls-status

        session-id: 0x4c40106b423123b
               leg: 1
            stream: 0
           address: 172.30.12.82:24472
            remote: 172.30.12.82:24352
              type: 1-RTP
              role: Passive
             state: Succeed
```

Properties

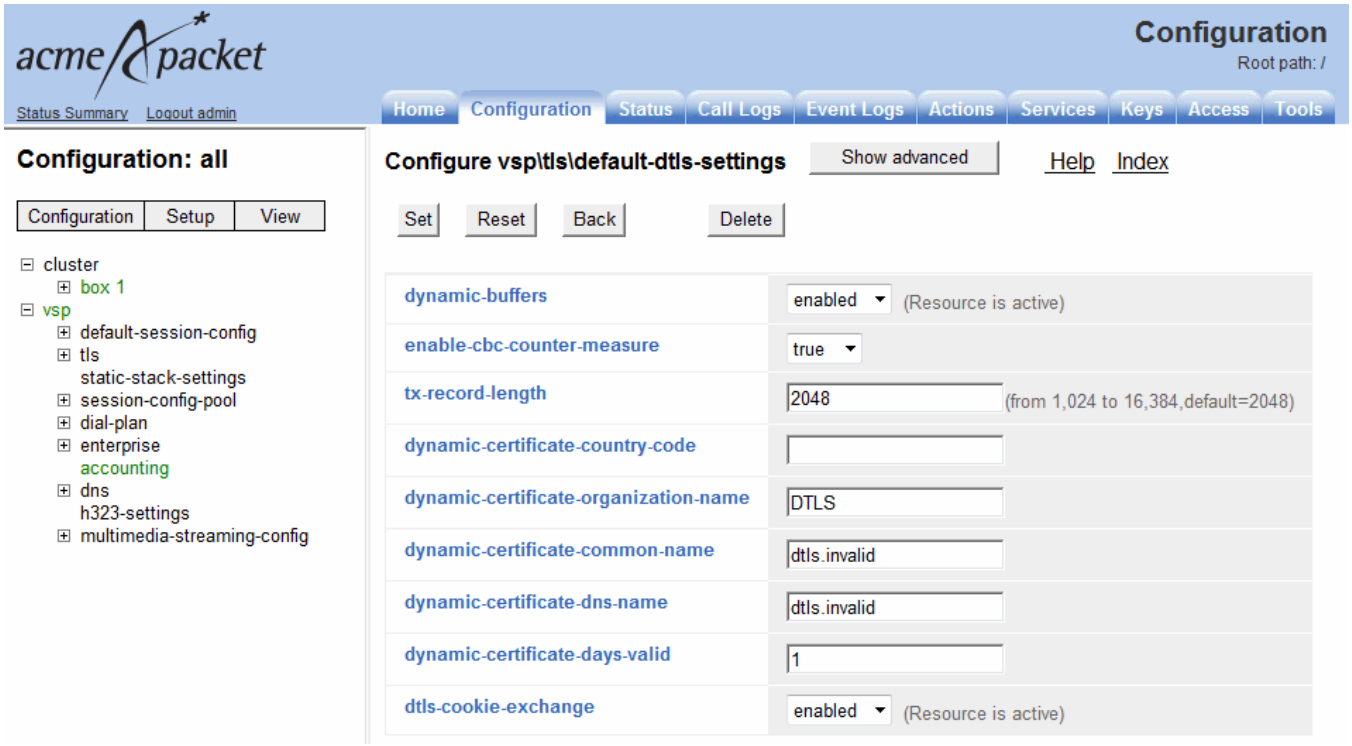
- session-id: The unique ID of the OS-E session.
- leg: Specifies in-leg (0) or out-leg (1).
- stream: The media stream index, audio (0) or video (1).
- address: The local OS-E IP and port for this DTLS socket.
- remote: The remote peer IP and port for this DTLS socket.
- type: Specifies the type of ICE port, either RTP (1) or RTCP (2).
- role: Specifies the DTLS role, either Passive or Active.
- state: The state of the DTLS socket, either Connected, Listening, Succeeded, or Closed.

Disabling the DTLS Cookie Exchange

For WebRTC to work, you must configure the OS-E to stop exchanging cookies during the DTLS negotiation.

To stop the DTLS cookie exchange:

1. Click the Configuration tab and select the vsp > tls object.
2. Click Configure next to default-dtls-settings.



3. dtls-cookie-exchange—Set to disabled to stop exchanging cookies during the DTLS negotiation.
4. Click Set. Update and save the configuration.

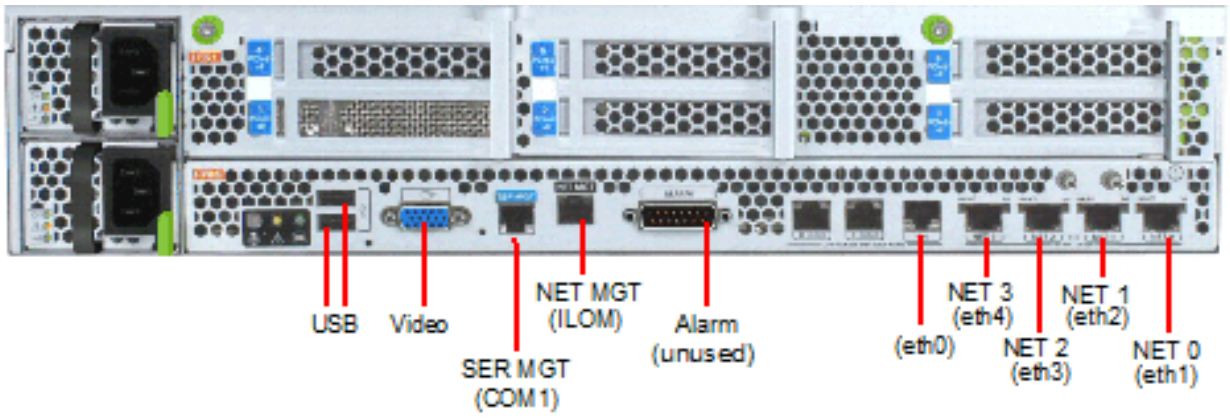
Netra Server X3-2 for Acme Packet Support

The OS-E supports the Netra X3-2 for Acme Packet.

This section explains how to cable the server.

Cabling the Netra Server X3-2 for Acme Packet

After mounting the Netra Server X3-2 for Acme Packet in an equipment rack and installing all components into it, connect all appropriate data cables to the ports before powering the system up and configuring it. This section describes how to make data cable connections.



Oracle recommends using Category 6 (or better) for all Ethernet connections.

You can install and remove Ethernet and 1000BASE-T cables while the Netra Server X3-2 for Acme Packet is operational. Not every port needs to be utilized for proper operation. However, when a cable is disconnected and the link is lost, an alarm is generated.

Available Connections

Please read all of the information pertaining to each of the available connections prior to cabling the Netra Server X3-2 for Acme Packet.

Port	Description	You Need:
NET (0-3)	10 GigE ports - labeled Net 3, Net 2, Net 1 and Net 0 (left to right) - enable you to connect the Netra Server X3-2 for Net-Net to your network.	A Category 6 (or better) Ethernet cable to connect to the NET 0 port to your network Network parameters such as an IP address (can be provided by DHCP services or assigned a static address in the OS) Additional Category 6 (or better) Ethernet cables and Ethernet addresses as needed for additional connections to NET 1 - 3
NET MGT	Provides a 10/100BASE-T Ethernet connection to the SP through an RJ-45 connector. This port provides support connections to the SP using the Oracle ILOM CLI and Web interface. By default, this port is configured to use DHCP to automatically obtain an IP address. Alternatively, you can assign a static IP address to this port. To use this port, it must have its network settings configured. Once configured, use the NET MGT port IP address to log in to the SP using a browser or secure shell.	Category 6 (or better) Ethernet cable to connect the NET MGT port to your network IP address for this port (required from DHCP or a static address)
SER MGT (COM1)	Provides a TIA/EIA-232 serial Oracle/Cisco standard connection to the SP through an RJ-45 connector. Default settings for this port are: 8N1: eight data bits, no parity, one stop bit 115200 baud Disable hardware flow control (CTS/RTS) Disable software flow control (XON/XOFF)	A terminal device (e.g., terminal, connection to a terminal server, or computer such as a laptop running terminal emulation software) A cable to connect the terminal device to the SER MGT (COM1) port
USB	Provides USB connections to the service processor (SP). The USB ports are hot pluggable, so you can connect/disconnect USB cables from these ports and peripheral devices without affecting server operations.	USB keyboard USB mouse Note: Maximum USB cable length: 5 meters
VIDEO	Provides a temporary video connection to the SP.	VGA monitor HDB-15 video cable with a maximum cable length of 6 meters (19.7 feet)

Local Console Cabling Procedure

This section explains how to physically make a console connection to the Netra Server X3-2 for Acme Packet. Administration console may be connected to either the ILOM (NET MGT), the local VGA+USB console ports, or the

local SER MGT (COM1) serial console port. When configuring bootloader parameters, set the console to VGA if ILOM or VGA+USB are used, or COM1 if SER MGT is used. The bootloader is accessible on all console ports, but only input from the active console port can be recognized by the Netra Server X3-2 for Acme Packet.

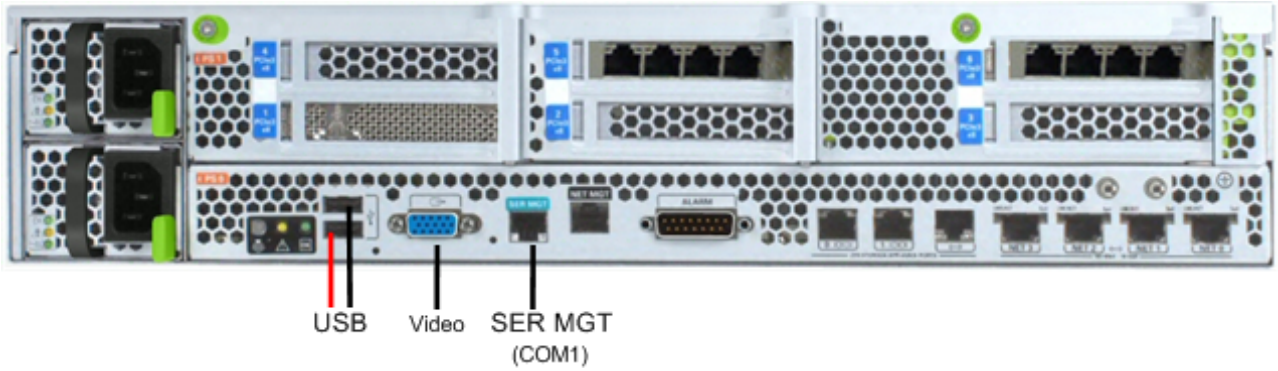
Note: DO NOT configure COM2 in the bootparams menu.

- To cable a serial console connection:
  - Serial console cable with an RJ-45 connector
- To cable a USB and Video Connection:
  - DB-15 video cable with a maximum cable length of 6 meters (19.7 feet)
  - USB cable with a maximum cable length of 6 meters (19.7 feet)
  - USB keyboard

  In the following procedure, you have the option to either cable a serial connection or to cable a USB/Video connection.

  To cable a local console connection:

1. Locate the appropriate cable(s) to connect to the Netra Server X3-2 for Acme Packet.
2. To cable a serial connection, insert the serial console cable into the SER MGT (COM1) port.



Connecting to USB, VGA and SER MGT (COM1) Ports

Note: Refer to the Netra Server X3-2 hardware documentation for information on how to configure your terminal application to connect to the console, and how to establish communications with the Netra Server X3-2 for Acme Packet.

3. To cable a USB/Video connection, insert the 15-pin connector on the end of the video cable into the Video port. Then insert the USB cable from the mouse and keyboard into the USB ports.
4. Lead the cables neatly away from the rear panel.
5. Plug in the cables to their respective destination components.

ILOM Cabling Procedure

This section explains how to make a connection to the Netra Server X3-2 for Acme Packet ILOM port. For a remote permanent connection to the SP over the ILOM connection, use the rear panel NET MGT port.

Refer to the Netra Server X3-2 for Acme Packet hardware documentation for information on how to configure your Web browser application to connect to the console, and how to establish communications with the Netra Server X3-2 for Acme Packet.

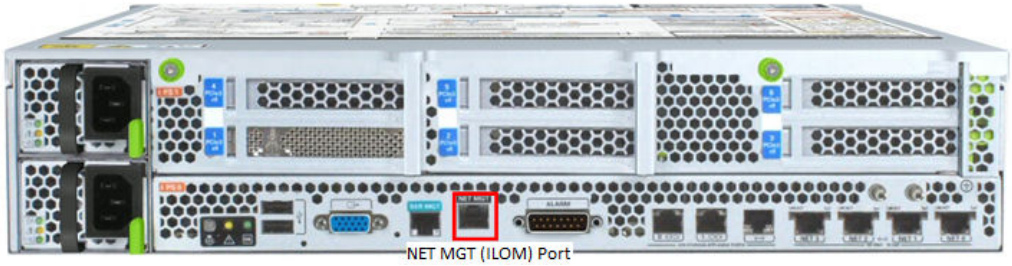
Note: Keep Ethernet cables separated from power cables by at least 60mm where possible and never run them in the same channel of the rack without segregation.

Prerequisites:

- Category 6 (or better) Ethernet cable with RJ-45 jacks

To cable an ILOM connection:

1. Locate the cable to connect to the Netra Server X3-2 for Acme Packet.
2. Plug the RJ-45 connector into the ILOM port.



3. Lead the cable neatly away from the rear panel.
4. Connect the other end of the cable to the LAN.

Commissioning OS-E on the Netra Server X3-2

To commission the OS-E on a Netra Server X3-2 with two configured hard drives (HD), you must ensure the OS-E is set to load on the same HD from which the Netra Server X3-2 is configured to boot.

By default, the Netra Server X3-2 matches the Logical Volumes to the physical HDs in the following way:

- **sdb = HDD0 disk**
- **sdc = HDD1 disk**

By default, the OS-E matches the Logical Volumes to the physical HDs in the following way:

- **sda = HDD0 disk**
- **sdb = HDD1 disk**

There are three ways to configure the Logical Volumes:

- SDC is the bootable Logical Volume
- SDB and SDC are configured as one virtual drive, allowing for redundancy
- SDB is the bootable Logical Volume

Note: When configure the server this way you must manually change the default install device.

Once Logical Volume is configured, you must disable the Netra Server X3-2's internal USB port to avoid errors during boot up.

Configuring Logical Volume

This section explains the three ways to configure Logical Volume for the OS-E on the Netra Server X3-2.

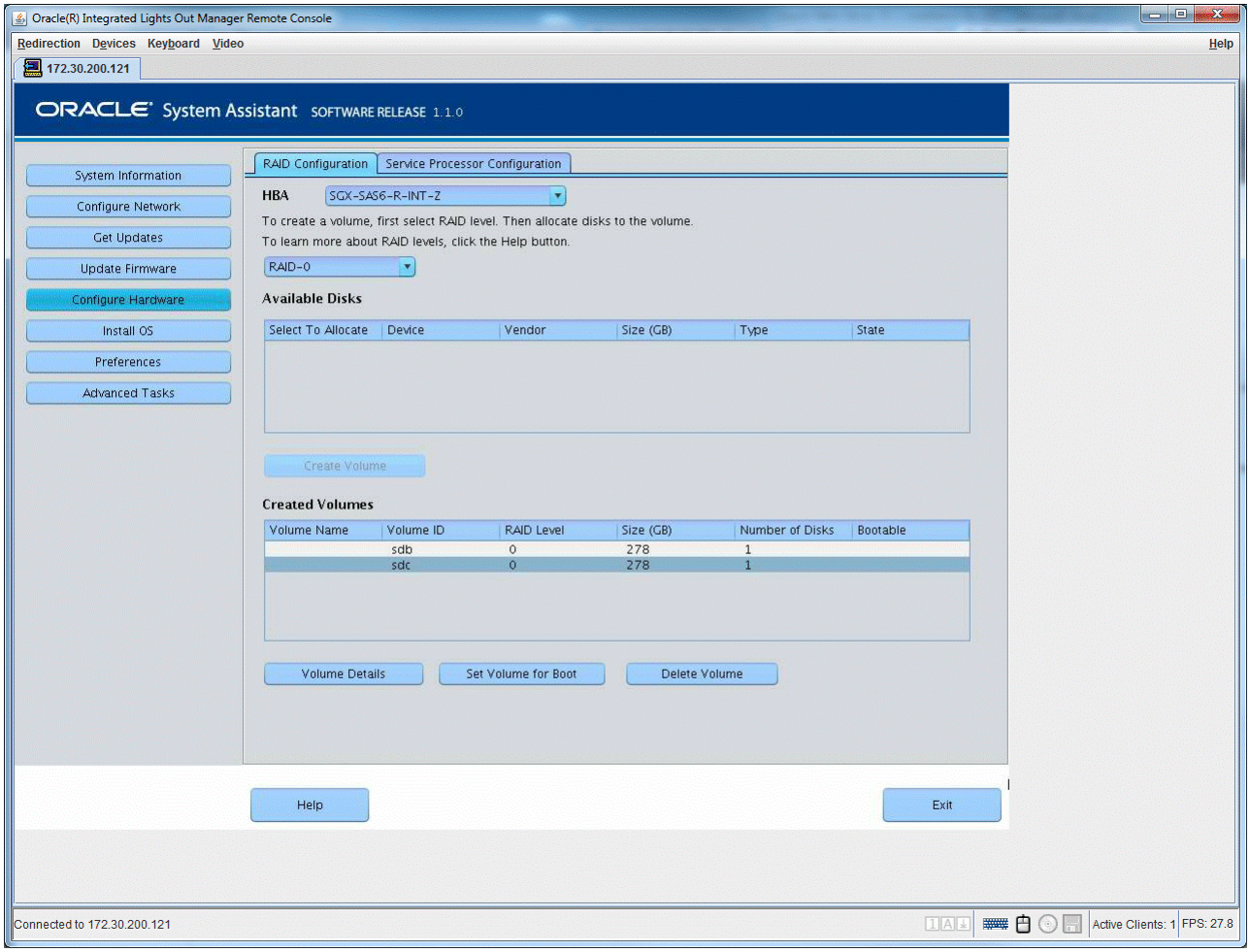
The OS-E software is written to a USB stick using the BMC tool. For more information on how to create a USB commissioning stick, see the *Oracle Communications System Installation and Commissioning Guide*.

Configuring sdc As the Bootable Drive

Configuring the sdc drive as the bootable Logical Volume:

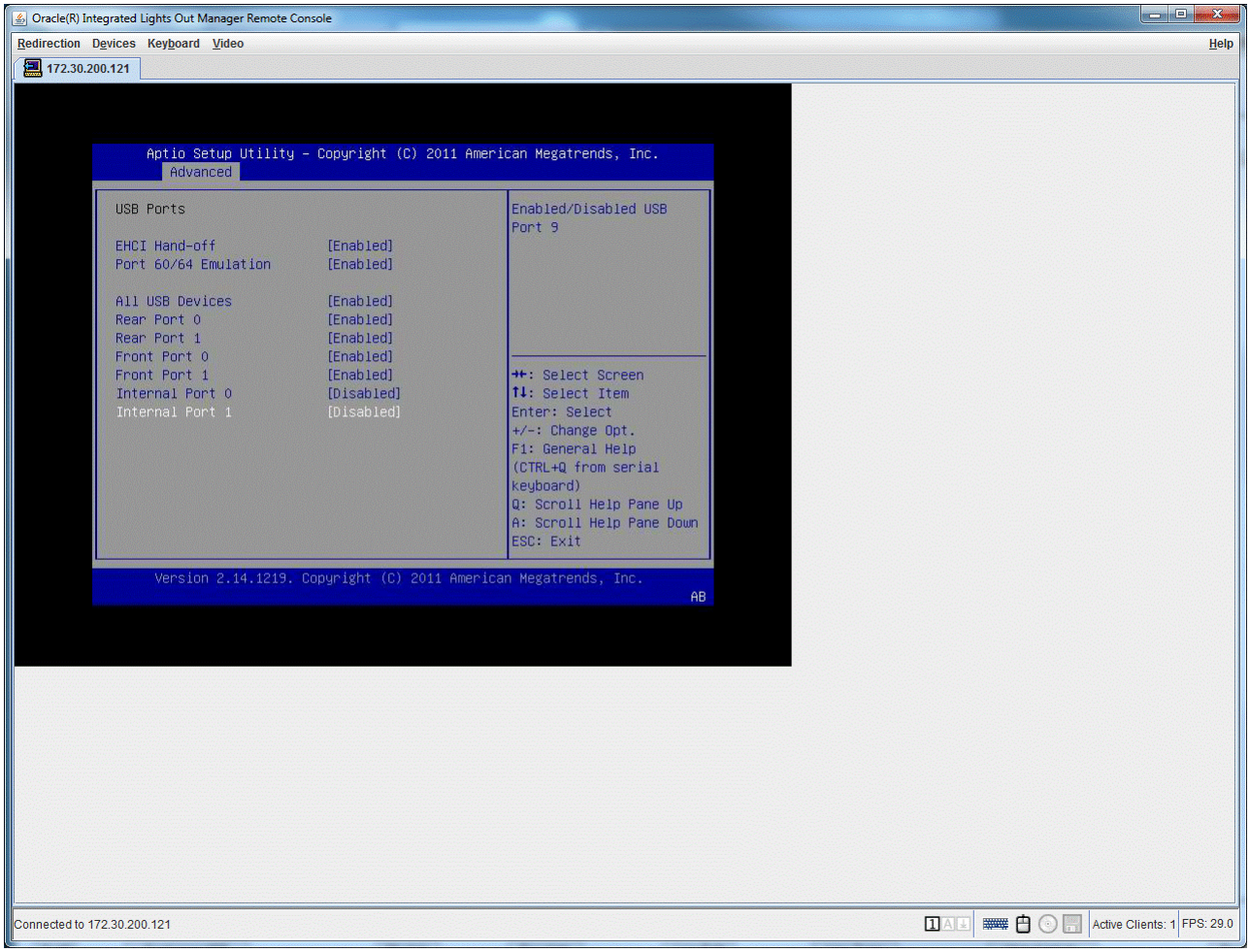
Note: The default installation behavior is to install the OS-E onto /dev/sdb (HDD1) and to use /dev/sda (HDD0 disk) as a data drive. When you commission the Netra X3-2 using the default behavior, the sdc drive must be set to Bootable or the OS-E installation does not boot.

1. Press F9 upon initial bootup to enter Oracle System Assistant.



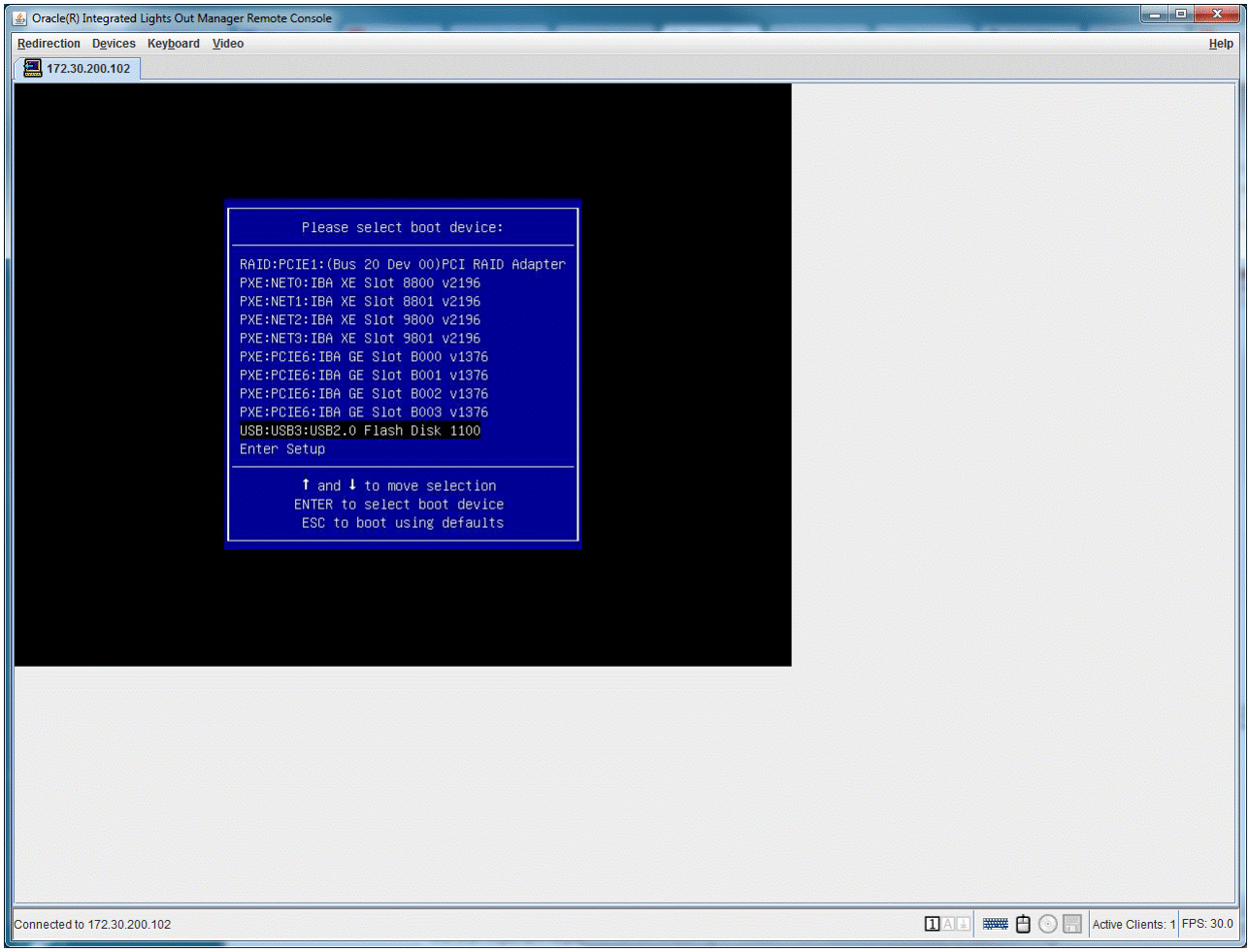
2. Click **Configure Hardware**.
3. Select the HBA from the drop-down list.
4. Configure your RAID settings.
5. Set the sdc Volume as Bootable.
6. Insert the USB commissioning drive.
7. Exit the Oracle System Assistant and reboot the server.
8. When the system has restarted, you must disable the internal USB ports. Press F2 to enter Setup.

9. Select **Advanced/USB** ports.



10. Disable both internal USB ports.
11. Press **esc**, save, exit, and reboot.
12. When the system has restarted, press F8 to enter the Boot Popup Menu.

13. Select the USB as the bootable device from the Boot Popup Menu and press Enter.



14. Press Y <Enter> when the system warns you that the first hard-drive will be reformatted.

The USB installer proceeds to unpack and install. When complete, the system restarts using the same RAID controller Logical Volume as the boot device.

Once the localhost login: prompt appears you can login and configure the OS-E.

15. Unmount the USB stick using the **unmount usb** action. Remove the USB and set aside as a Rescue stick.

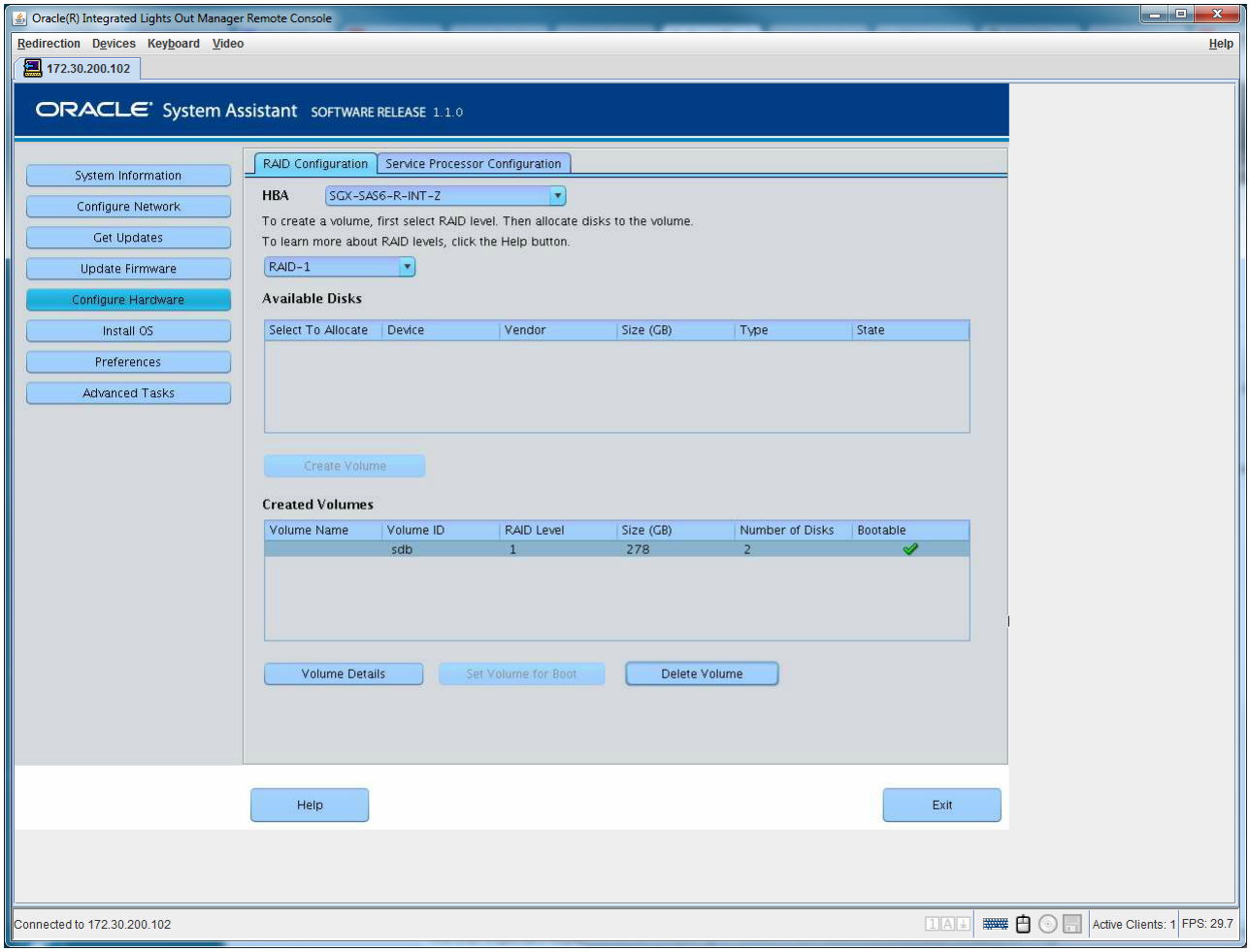
16. Run the 'config setup' script to configure basic IP connectivity and services.

Once you have finished configuring the system, you must reboot, enter Setup (F2), and reenable the internal USB ports.

Configuring sdc and sdb As One Virtual Drive

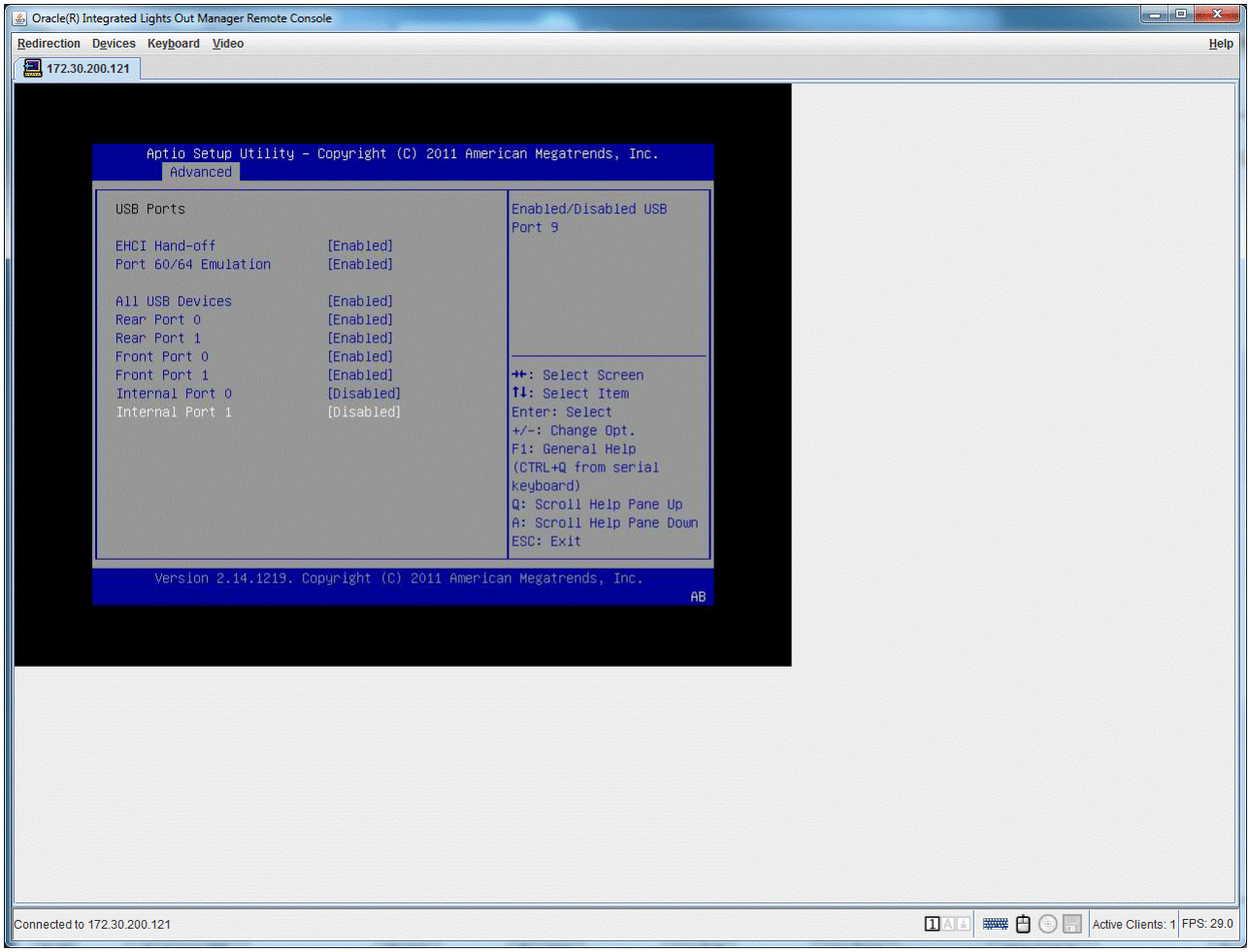
Configuring the sdc and sdb drives as one bootable virtual drive:

1. Press F9 upon initial bootup to enter Oracle System Assistant.



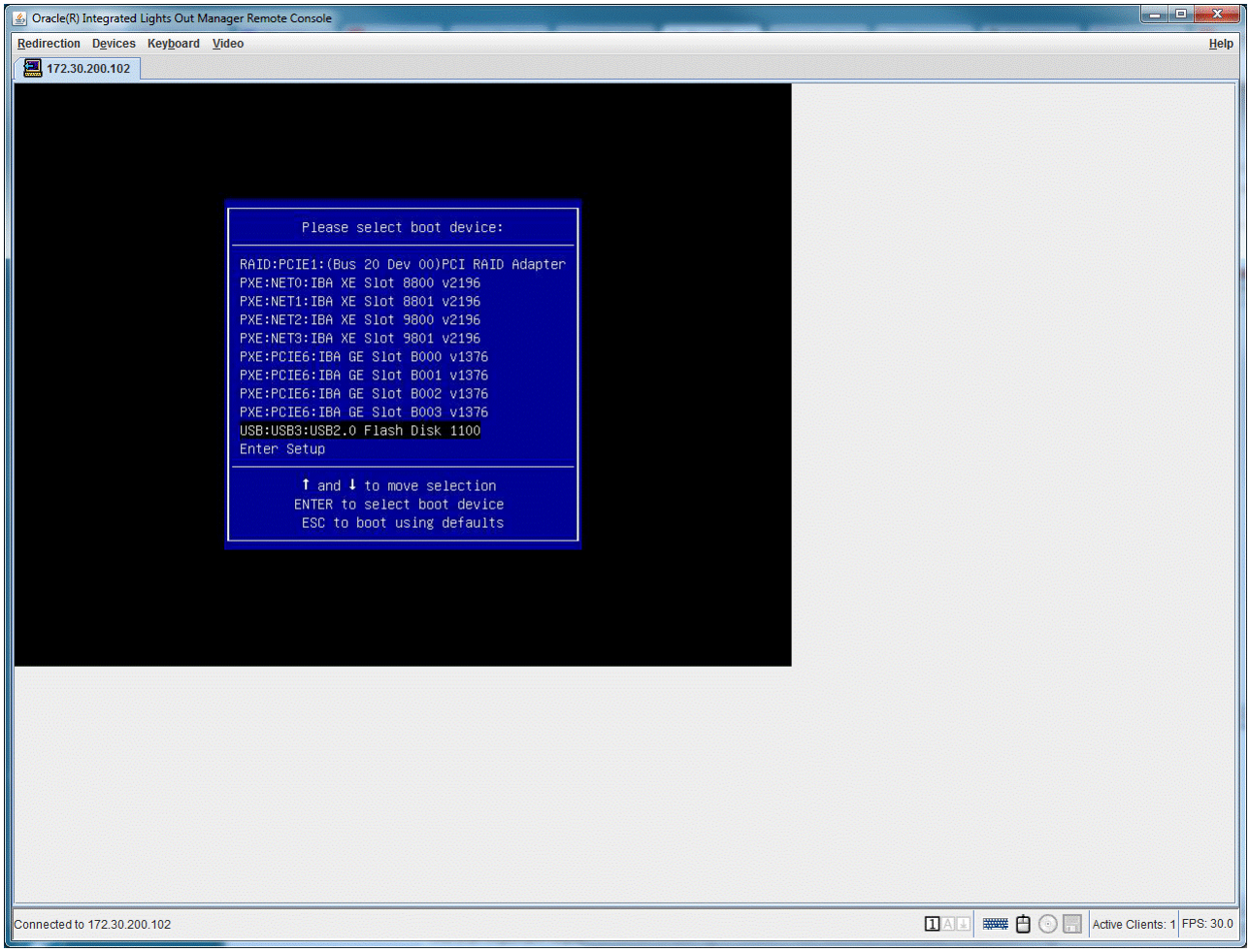
2. Click **Configure Hardware**.
3. Select the HBA from the drop-down list.
4. Configure your RAID settings.
5. Ensure only one Logical Volume is configured and set as Bootable.
6. Insert the USB commissioning drive.
7. Exit the Oracle System Assistant and reboot the server.
8. When the system has restarted, you must disable the internal USB ports. Press F2 to enter Setup.

9. Select **Advanced/USB** ports.



10. Disable both internal USB ports.
11. Press **esc**, save, exit, and reboot.
12. When the system has restarted, press F8 to enter the Boot Popup Menu.

13. Select the USB as the bootable device from the Boot Popup Menu and press Enter.



14. Press Y <Enter> when the system warns you that the first hard-drive will be reformatted.

    The USB installer proceeds to unpack and install. When complete, the system restarts using the same RAID controller Logical Volume as the boot device.

    Once the localhost login: prompt appears you can login and configure the OS-E.

15. Unmount the USB stick using the **unmount usb** action. Remove the USB and set aside as a Rescue stick.

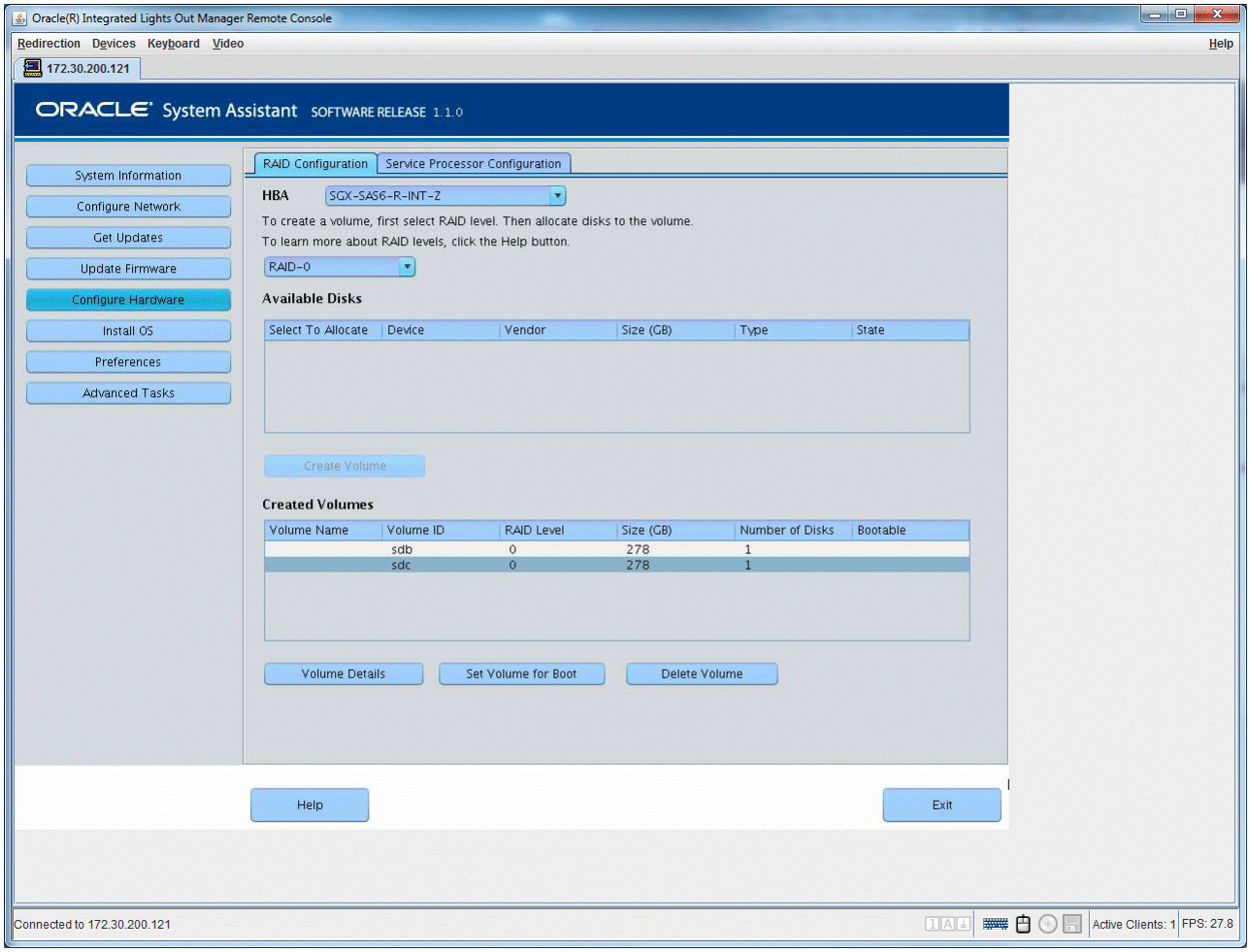
16. Run the 'config setup' script to configure basic IP connectivity and services.

Once you have finished configuring the system, you must reboot, enter Setup (F2), and reenable the internal USB ports.

Configuring sdb as the Bootable Drive

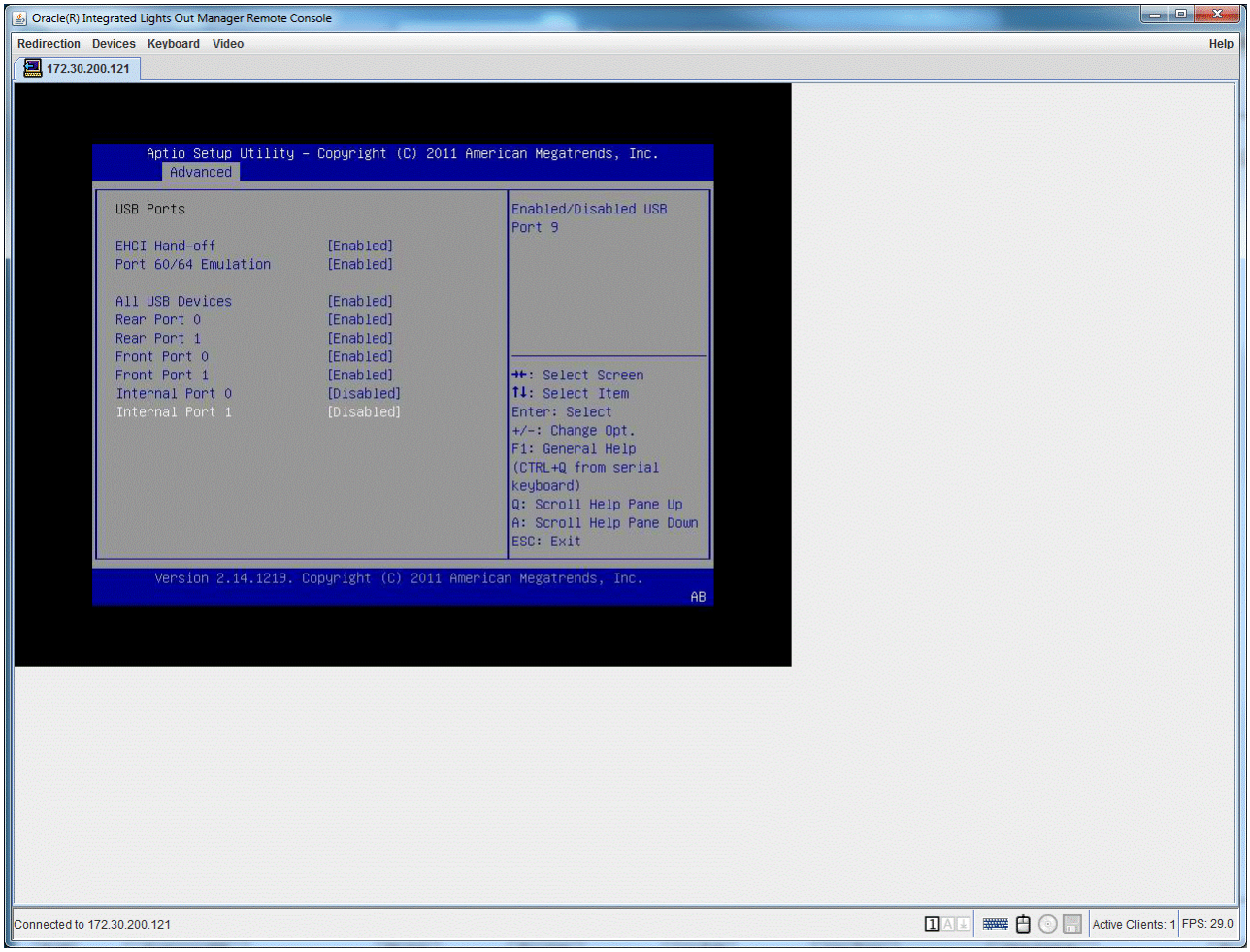
Configuring the sdb as the bootable drive:

1. Press F9 upon initial bootup to enter Oracle System Assistant.



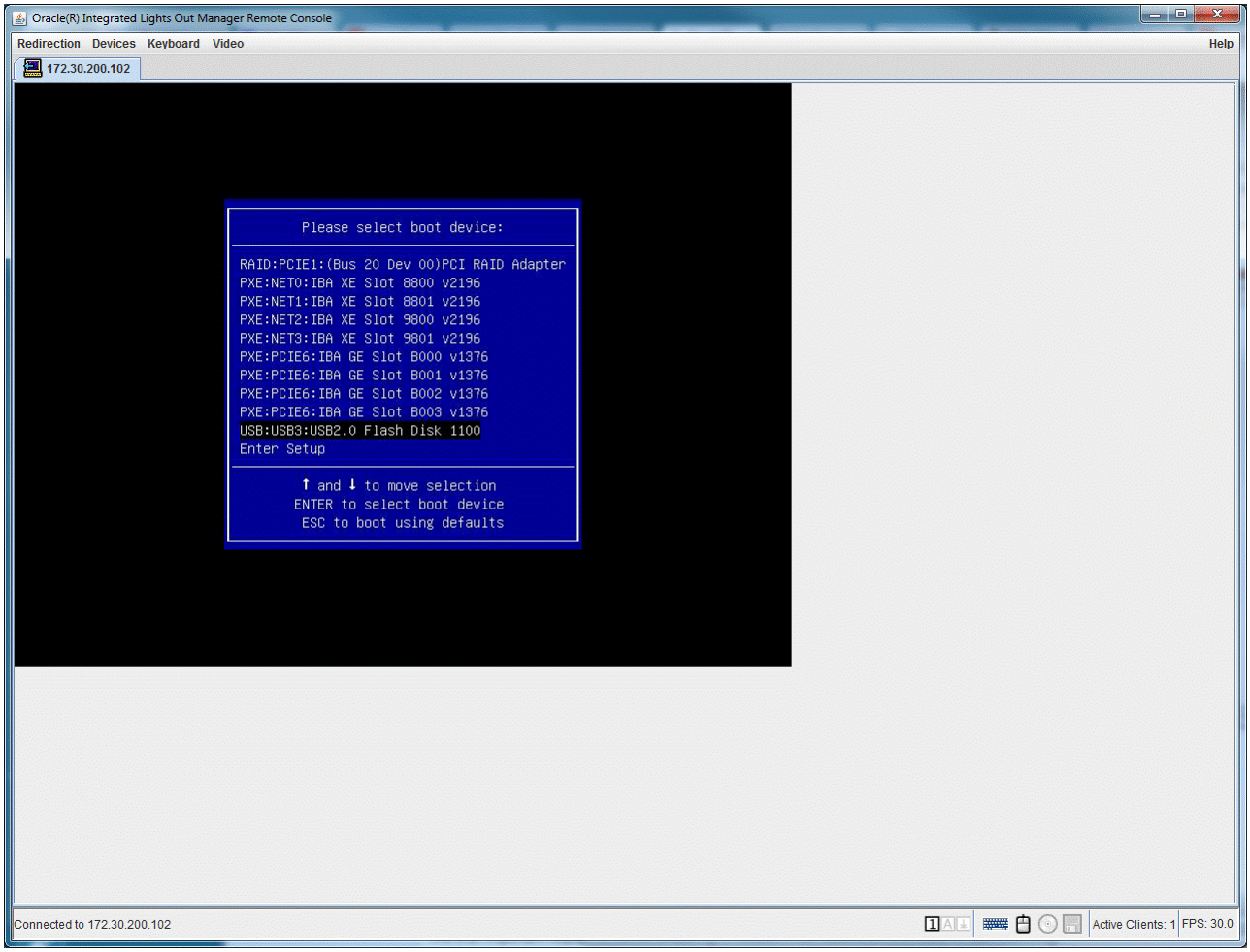
2. Click Configure Hardware.
3. Select the HBA from the drop-down list.
4. Configure your RAID settings.
5. Set the sdb Volume as Bootable.
6. Insert the USB commissioning drive.
7. Exit the Oracle System Assistant and reboot the server.
8. When the system has restarted, you must disable the internal USB ports. Press F2 to enter Setup.

9. Select **Advanced/USB** ports.



10. Disable both internal USB ports.
11. Press **esc**, save, exit, and reboot.
12. When the system has restarted, press F8 to enter the Boot Popup Menu.

13. Select the USB as the bootable device from the Boot Popup Menu and press Enter.



14. Change the default install device as follows:

```
Would you like to change the default install devices[y|n]
y
Available disks are:
--------------------
/dev/sdb( 298.9 GB )
/dev/sda( 298.9 GB )
--------------------
System drive [/dev/sdb]> /dev/sda
Data drive [/dev/sda]> /dev/sdb
```

15. Press Y <Enter> when the system warns you that the first hard-drive will be reformatted.

    The USB installer proceeds to unpack and install. When complete, the system restarts using the same RAID controller Logical Volume as the boot device.

    Once the localhost login: prompt appears you can login and configure the OS-E.

16. Unmount the USB stick using the **unmount usb** action. Remove the USB and set aside as a Rescue stick.
17. Run the 'config setup' script to configure basic IP connectivity and services.

Once you have finished configuring the system, you must reboot, enter Setup (F2), and reenable the internal USB ports.

Call-Control-Call Multiple Session Config Support

The OS-E allows you to specify multiple session-configs for a call initiated by the call-control-call action.

Update to Call-Cantrol-Call

The call-control-callaction has been updated to include an additional-session-config argument. This is where you specify additional session-configs to support the different endpoint types.

call-control-call

Initiates a call using To and From SIP URIs you provide.

You can set the OS-E to add post-dial digits to a call-control call action. Append the string postd=digits to the user portion of the to parameter. The following example shows the OS-E adding post-dial digits 12345@acmepacket.com to a call.

Syntax

```
call-control-call <to> <from> [requestId] [originatorFirst] [async]
[transport] [config] [content-type] [body] [additional-session-config]
```

Arguments

- <to>—The destination SIP URI of the call.
- <from>—The originating SIP URI of the call.
- [requestId]—A unique identifier provided by an external application. This value can be used to identify the call in subsequent events and actions. If a requestId is specified, there is a corresponding XML element in the event messages generated for the session.
- [originatorFirst]—When enabled (the default), the originating party is connected first. When disabled, the called party is connected first.
- [async]—When enabled, causes the OS-E to return a response immediately without waiting for the action to complete. When disabled (the default), the OS-E waits for the action to complete before returning a response.
- [transport]—The transport method to use for the call. This can be set to any, TCP, UDP, or TLS.
- [config]—The session-config on the OS-E to use to process a call. Use the full path to the session-config.
- [session-id]—The optional session ID for the session.
- [content-type]—The content type of the message body of the initial call.
- [body]—The message body of the initial call.
- [additional-session-config]—Any additional session-configs the OS-E can use to support different endpoint types. Separate session-configs with a semi-colon (;).

Performance and Capacity Improvements

The OS-E has been updated to take advantage of the benefits that come with some new hardware platforms to improve its performance and capacity.

This feature takes advantage of new hardware technologies to achieve better performance and capacity on the OS-E.

The Linux kernel provides scaling features that help distribute the networking traffic load across a multi-processor system, thereby yielding better performance. The following Linux kernel features are being used to achieve better RTP performance and call capacity:

- Receive Side Scaling
- Receive Packet Steering
- Receive Flow Steering
- Transmit Packet Steering

In addition to the kernel features, the sizing of the Ethernet Rx ring has proven to yield better performance under heavy traffic load. Therefore an optimization of the Ethernet Rx Ring is also part of the performance and capacity improvements made to OS-E.

Overriding Next Hop and Previous Hop IPs of Web Endpoints

When the ASC anchors media, the networks on which the two endpoints (caller and callee) reside may be unknown. In these cases, nominal network addresses can be used to steer the media correctly through the ASC by performing media service route lookups. This ensures that the media resources are allocated from a media interface that can reach the endpoint.

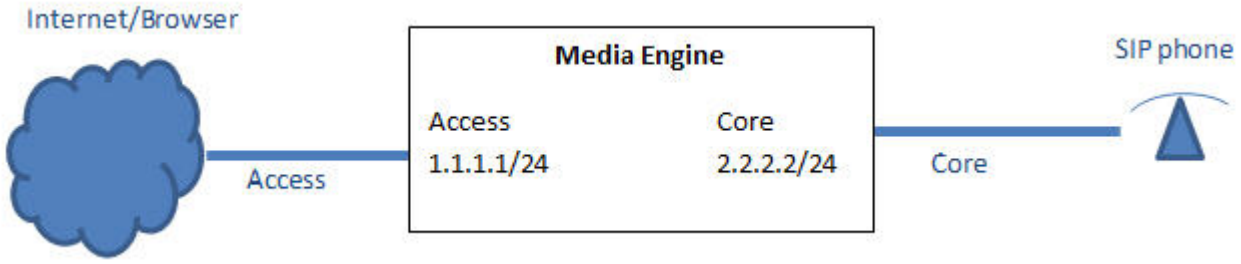
The following named variables have been created to configure the nominal network addresses (and optionally ports) used to steer media through the ASC.

- inleg.source.ip
- inleg.source.port
- outleg.source.ip
- outleg.source.port

These named variables are used to steer media through the ASC by providing nominal network addresses to perform a media service route lookup, allocating media resources on an interface that can reach the remote endpoint. The **inleg.source.ip** and **outleg.source.ip** values can be wet to the IP address of the ASC media interface to force media resource allocation from that specific interface. These values can also be used to specify a network IP address (for example, 1.1.1.1) for cases where the ASC has multiple media interfaces on the same subnet for load balancing purposes.

Note: For information on configuring named variables, see Using Regular Expressions in the *Oracle Communications Application Session Controller Objects and Properties Reference Guide*.

The following example shows the ASC residing on a customer network that has an access side (Internet) and core side (SIP network).



Configuring a Browser to SIP Call

When an Internet browser makes a call to a SIP phone residing on the customer core network, the ASC uses the 'web-to-sip' session-config call flow. Adding these named variables to the existing 'web-to-sip' session-config steers the media from the 'access' to the 'core' networks.

Note: The endpoint initiating the call resides on the 'inleg' and the endpoint receiving the call is on the 'outleg'.

To steer the media correctly for this call flow, the **inleg.source.ip** can be configured as 1.1.1.1 and the **outleg.source.ip** can be configured as 2.2.2.2. Configuring the named variables this way forces the allocation of media resources from the 'access' interface (1.1.1.1) to reach the browser, and the 'core' interface (2.2.2.2) to reach the SIP phone.

The following example shows how to add named variables to an existing 'web-to-sip' session-config.

```
config vsp
 config session-config-pool
```

```
  config entry web-to-sip
   config named-variables
    config named-variable inleg.source.ip
     set value 1.1.1.1
    return
    config named-variable outleg.source.ip
     set value 2.2.2.2
    return
   return
  return
 return
return
```

Configuring a SIP to Browser Call

When a SIP phone makes a call to an Internet browser residing on the customer core network, the ASC uses the 'sip-to-web' session-config call flow. Adding these named variables to the existing 'sip-to-web' session-config steers the media from the 'core' to the 'access' networks.

Note: The endpoint initiating the call resides on the 'inleg' and the endpoint receiving the call is on the 'outleg'.

To steer the media correctly for this call flow, the **inleg.source.ip** can be configured as 2.2.2.2 and the **outleg.source.ip** can be configured as 1.1.1.1. Configuring the named variables this way forces the allocation of media resources from the 'core' interface (2.2.2.2) to reach the SIP phone, and the 'access' interface (1.1.1.1) to reach the browser.

The following example shows how to add named variables to an existing 'sip-to-web' session-config.

```
config vsp
 config session-config-pool
  config entry sip-to-web
   config named-variables
    config named-variable inleg.source.ip
     set value 2.2.2.2
    return
    config named-variable outleg.source.ip
     set value 1.1.1.1
    return
```

Configuring a Browser to Browser Call

When an Internet browser makes a call to another Internet browser, the ASC uses either the 'web-to-web-anchored' or 'web-to-web-anchor-conditional' session-config call flows. If you require media steering for these calls, use the **inleg.source.ip** and **outleg.source.ip** named variables.

Note: The endpoint initiating the call resides on the 'inleg' and the endpoint receiving the call is on the 'outleg'.

Since both endpoints in this call flow reside on the Internet, specify the ASC's 'access' interface (1.1.1.1) for both the **inleg.source.ip** and **ourleg.source.ip**.

The following example shows how to add named variables to an existing 'web-to-web-anchored' session-config.

```
config vsp
 config session-config-pool
  config entry web-to-web-anchored
   config named-variables
    config named-variable inleg.source.ip
     set value 1.1.1.1
    return
    config named-variable outleg.source.ip
     set value 1.1.1.1
    return
```

Dynamic Events Endpoint Redundancy Overview

The ASC supports redundancy for dynamic events endpoints.

The ASC supports dynamic event endpoints to register to the ASC's Web Service. This allows third-party applications to specify which endpoints the ASC should alert when events occur.

To support the dynamic event endpoint registration feature, the ASC supports a redundant dynamic events endpoint server.

Note: Only one redundant server, acting as a load balancer, can be configured for each dynamic event endpoint server.

Update to Dynamic-Event-Service

The dynamic-event-service registeraction has been updated to include a backupEndpointargument. This is where you specify the endpoint registration that is being modified, the endpoint to be used as a backup, and, optionally, the priority of the backup.

dynamic-event-service register

This action allows a web application to register itself by using the OS-E's Web Service REST and SOAP clients.

Syntax

```
dynamic-event-service register <endpoint> [channels] [xml-format] [time-to-
live] [connect-timeout] [read-timeout] [character-set] [request-style]
[include-channels-in-events]
```

```
dynamic-event-service keepalive <registration-id>
```

```
dynamic-event-service unregister <registration-id>
```

Arguments

- <endpoint>—The application endpoint that receives events.
- [channels]—The channels for which the endpoint is getting events.
- [xml-format]—The XML format used by this server. This can be either simplified (the default) or legacy
- [time-to-live]—The time to live, in minutes, for the keepalive on this registration. The default is untilRestart, meaning the registration stays alive until the system is restarted.
- [connect-timeout]—The connect timeout, in milliseconds, for the endpoint. The default is 1000.
- [read-timeout]—The read timeout, in milliseconds, for the endpoint. The default is 1000.
- [character-set]—The character set to use when forming requests to this endpoint. This can be utf-8 (the default) or iso-8859-1.
- [request-style]—The style to use when sending events to this listener. This can be SOAP (the default), XML, or JSON.
- [include-channels-in-events]—Whether channels are included in events. This is enabled by default.
- [backupEndpoint]—The dynamic events endpoint server to be used as a backup.

```
NNOS-E> dynamic-event-service unregister reg-150
```

Show Ethernet Status Provider Update

The show ethernet -v status provider has been updated to include the following fields:

- rx-ring:The current Ethernet Rx ring size.
- rx-ring-max: The maximum allowed Ethernet Rx ring size.

- tx-ring: The current Ethernet Tx ring size.
- tx-ring-max: The maximum allowed Ethernet Tx ring size.

Sample Output

```
NNOS-E>show ethernet -v

       name: eth0
       link: up
      speed: 1Gb
     duplex: full
    autoneg: enabled
  supported:
 advertised:
       port: TP
transceiver: internal
    rx-ring: 0
rx-ring-max: 0
    tx-ring: 0
tx-ring-max: 0
```

Accessing the Action Editor

The Action Editor can now be accessed via the Web Services portal.

The Action Editor is in the ws-tools.zip file.

To access the ws-tools.zip file:

1. Log into the Web Services portal at http://n.n.n.n:port where n.n.n.n:port is the IP and port where the web-service configuration object is enabled.
2. Click the SOAP link.
3. Click the Tools link.
4. Click the Editors link.
5. Download and upzip the wstools.zip file.

New Configuration Objects in Release 3.7.0M1

This section provides a summary of the new configuration objects added to the 3.7.0M1 release.

default-dtls-settings

Sets the certificate file, requirements, and passphrase to be used for DTLSl when a certificate is not specified.

Syntax

```
config vsp tls default-dtls-settings
```

Properties

allow-sslv2 (Advanced) Specifies whether the OS-E can negotiate Secure Socket Layer Version 2 sessions with a peer. By default, the OS-E only supports SSLv3 or TLSv1. If you require SSLv2 for interoperability, set this property to true.

Note: Oracle does not recomment you use SSLv2 as it suffers serious security holes.

- Default: false
- Values: true | false

allow-sslv3 (Advanced) Specifies whether the OS-E can negotiate Secure Socket Layer Version 3 sessions with a peer.

- Default: true
- Values: true | false

allow-tlsv1 (Advanced) Specifies whether the OS-E can negotiate Transport Layer Security Version 1 sessions with a peer. (TLSv1 is the IETF-approved version of SSLv3.)

- Default: true
- Values: true | false

allow-null-cipher (Advanced) Specifies whether to use a null string in the client Hello. This setting is ignored if you have a value set in the cipher-config-string property.

Note: This property should never be enabled in a production environment, as it disables encryption. It is for debugging purposes only. If you do enable the null cipher, the client must list only the null cipher in its client Hello. Because the null cipher disables encryption, if any alternative is listed, the server uses it.

- Default: disabled
- Values: enabled | disabled

dynamic-buffers Specifies whether to use dynamic buffers, an enhancement to the OpenSSL library. When enabled, the OS-E allocates and frees transmit and receive buffers as needed, allowing support for many more TLS connections. When disabled, the OS-E allocates both a transmit and a receive buffer at connection time, and holds the buffers open until the connection is dropped.

- Default: enabled
- Values: enabled | disabled

enable-cbc-counter-measure Enables or disables an OpenSSL strategy the OS-E uses when sending TLS records. The strategy is designed to prevent an attack on cipher block chaining (CBC) ciphers, which have a vulnerability in some SSL implementations. When false, the protection is disabled.

- Default: true
- Values: true | false

cipher-config-string (Advanced) Sets ciphers using the OpenSSL method.

Note: Do not change this parameter unless instructed to by technical support personnel.

- Default: There is no default setting.

tx-record-length Sets the record length for TLS packets. By setting the length to a value less than the default (2048 bytes), you reduce the amount of memory required on transmit.

- Default: 2048
- Min: 1024 | Max: 16384

certificate-file (Advanced) Specifies the name of the certificate file used to establish connections made with this object. The OS-E supports the following certificate formats: PKCS#12: Public Key Cryptography Standard #12 format, often from Microsoft IIS Version 5 (binary). PEM: Privacy Enhanced Mail format, from any OpenSSL-based web server (ASCII).

- Default: There is no default setting.

passphrase-tag (Advanced) Specifies the passphrase associated with the certificate file. Use this property if the certificate file is encrypted to have its private key information protected. This passphrase must match the string that the certificate was encrypted with.

- Default: There is no default setting.

peer-certificate-verification (Advanced) Specifies whether the OS-E requests a certificate from a peer and the action in takes in response to the peer's response.

- Default: required-not-verified
- Values:
- none - The OS-E does not request a certificate from a peer. The OS-E allows the connection whether or not peer presents a certificate. (If the peer does present, the OS-E ignores the certificate.)
- if-presented - The OS-E requests a certificate from the peer. If the peer presents, the certificate must pass verification for the connection to proceed. If the peer does not present, the OS-E allows the connection. Use this setting only when the OS-E functions as a server.
- required - The OS-E requests a certificate from the peer. If no certificate is presented, or if the presented certificate does not pass verification, the OS-E terminates the connection.
- required-not-verified - The OS-E requests a certificate from the peer. If no certificate is presented, the OS-E terminates the connection. Any certificate presented is accepted without any verification.

use-default-ca (Advanced) Specifies whether to use the default revocation list(s) configured in the default-ca object.

- Default: true
- Values: true | false

specific-ca-file Specifies a CA file, and optionally a password, that should be used in addition to, or instead of, the default CA file(s).

- Default: There is no default setting.

use-default-crl (Advanced) Specifies whether to use the default revocation list(s) configured in the default-crl object.

- Default: true
- Values: true | false

specific-crl-file Specifies a CRL file, and optionally a password, that should be used in addition to, or instead of, the default CA file(s).

- Default: There is no default setting.

required-peer-name (Advanced) Specifies a name that must appear in the presented certificate. If you do not set this property, the OS-E does not check the presented name.

If you do specify a name, it must appear in either the DNS field of the altSubjectName field or in the Common Name field. To verify the peer, the OS-E first checks to see whether there is an entry in the DNS field of the altSubjectName field. If there is, the OS-E compares it to the required-peer-name. If it matches, the OS-E allows the connection (and performs no further peer-name checks). If the names do not match, the OS-E does not allow the connection (and performs no further peer-name checks). If there is no entry in the DNS field, the OS-E checks the Common Name field. If there is a match, the OS-E allows the connection. If the presented name does not match the required name, the OS-E rejects the connection. You can use wildcards to express the name.

- Default: There is no default setting.

dynamic-certificate-country-code Specifies the country code of the dynamically-generated certificate used for multiplexed DTLS connections.

- Default: There is no default setting.

dynamic-certificate-organization-name Specifies the organization name of the dynamically-generated certificate used for multiplexed DTLS connections.

- Default: DTLS

dynamic-certificate-common-name Specifies the common name of the dynamically-generated certificate used for multiplexed DTLS connections.

- Default: dtls.invalid

dynamic-certificate-dns-name Specifies the DNS name of the dynamically-generated certificate used for multiplexed DTLS connections.

- Default: dtls.invalid

dynamic-certificate-days-valid Specifies the number of days the dynamically-generated certificate used for multiplexed DTLS connections is valid.

- Default: 1
- Values: Min: 0 | Max: 4294967296

dtls-cookie-exchange When enabled, the OS-E forces a cookie exchange during the DTLS negotiation. This is intended to prevent DoS attacks.

Note: This property must be set to disabled in a WebRTC environment.

- Default: enabled
- Values: enabled | disabled

New Configuration Properties in Release 3.7.0M1

This section provides a summary of the new configuration properties added in release 3.7.0M1.

in-encryption

The following properties have been added to the in-encryption object in 3.7.0M1.

Syntax

```
config vsp default-session-config in-encryption
config vsp session-config-pool <entry> in-encryption
```

Properties

encryption-preferences Creates a prioritized list of encryption types to offer or accept.

Note: Always give DTLS a priority of 1 and RFC3711 a priority of 2.

media

The following properties have been added to the media object in 3.7.0M1.

Syntax

```
config vsp default-session-config media
config vsp session-config-pool <entry> media
```

Properties

augmented-ice Specifies whether the OS-E attempts augmented ICE.

- Default: disabled
- Values: enabled | disabled

os

The following properties have been added to the os object in 3.7.0M1.

Syntax

```
config box os
```

Properties

receive-packet-steering Enables Receive Packet Steering (RPS), which distributes the processing of received packets across available CPUs in the system and provides greater performance during high call rates.

- Default: enabled
- Values: enabled | disabled

receive-flow-steering Enables Receive Flow Steering (RFS), which associates receive packets with a particular flow. Unique flows are defined by a packet's IP addresses and ports and are assigned CPUs for processing. With RFS enabled, the processing of receive packets is distributed to the CPU that is handling that flow, providing greater performance during high call rates. The rx-flow-entries property controls the size of the Rx flow table. This value represents the maximum number of concurrent flows supported by the system. The default, automatic allows the system to automatically configure the number of entries for optimum performance. You have the option to override the automatic setting and configure a specific number of Rx flow entries.

- Default: enabled automatic
- Values: enabled | disabled

transmit-packet-steering Enables Transmit Packet Steering (TPS), which distributes the processing of transmitted packets across the available CPUs in the system and provides greater performance during high call rates.

- Default: enabled
- Values: enabled | disabled

ethernet-rx-ring-size When set to default-value, the Rx ring size does not change from its default setting. When set to automatic, each Ethernet receive ring size is optimized for better performance. When set to custom, you specify the Ethernet Rx ring size. If the custom size exceeds the maximum size supported by the Ethernet hardware then the custom size is set to the maximum supported Rx ring size.

- Default: automatic
- Values: automatic | default-value | custom-value <value>

out-encryption

The following properties have been added to the out-encryption object in 3.7.0M1.

Syntax

```
config vsp default-session-config in-encryption
config vsp session-config-pool <entry> in-encryption
```

Properties

encryption-preferences Creates a prioritized list of encryption types to offer or accept.

Note: Always give DTLS a priority of 1 and RFC3711 a priority of 2.

MIB Changes in Release 3.7.0M1

This section describes changes that have been applied to Management Information Base (MIB) object definitions.

New MIB Tables in Release 3.7.0M1

MIB Table Name	Description
iceDtlsStatus	The status of ICE DTLS connections.

Changed MIB Tables in Release 3.7.0M1

MIB Object Name	Description
certificates	ADDED: certificatesAllowDTLSV1, certificatesDefaultDTLS
dynamicEventServices	ADDED: dynamicEventServicesBackupEndpoint, dynamicEventServicesBackupFailureAverage, dynamicEventServicesBackupFailureAverage, dynamicEventServicesBackupFailureMaximum, dynamicEventServicesBackupFailureMinimum, dynamicEventServicesBackupFailures, dynamicEventServicesBackupLastFailed, dynamicEventServicesBackupLastFailed, dynamicEventServicesBackupLastFailMessage, dynamicEventServicesBackupLastSuccess, dynamicEventServicesBackupRequests, dynamicEventServicesBackupResponseAverage, dynamicEventServicesBackupResponseMaximum, dynamicEventServicesBackupResponseMinimum
ethernet	ADDED: ethernetRxRing, ethernetRxRingMax, ethernetTxRing, ethernetTxRingMax

Known Problems and Restrictions in 3.7.0M1

Receiving Call-Control-Created Events

To receive call-control-created events when a call is parked, you must set the vsp > session-config > third-party-call-control > inhibited-created-event-on-park property to disabled.

Diffie-Hellman Logjam Attack Defense

The defense against the Diffie-Hellman Logjam attack, as originally referenced in the Net-Net OS-E 3.7.0 Release Notes, has a different workaround in 3.7.0M1.

The Diffie-Hellman Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography, allowing the attacker to read and modify any data passed over the connection.

This attack is similar to the FREAK attack, but is due to a flaw in the TLS protocol rather than an implementation vulnerability. It attacks a Diffie-Hellman key exchange rather than an RSA key exchange. When using the ASC Web Management System, the attack affects any server that supports CHE_EXPORT ciphers and affects all modern web browsers.

Note: For more information on the Diffie-Hellman Logjam attack, see *https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000*.

To protect against the Logjam vulnerability:

1. Log into the ASC CLI.
2. Type shell to open the Linux shell.
3. Open the file */usr/java/jrel.7/lib/security/java.security* in an editor.
4. Set the property **jdk.tls.disabledAlgorithms** (found at the end of the file) to DH, DHE.

```
jdk.tls.disabledAlgorithms=DH, DHE
```

5. Restart the ASC.

2

Release 3.7.0M2

This section describes all of the new adaptations added to the ASC in release 3.7.0M2, including new features, configuration objects and properties, and MIBs.

3.7.0M2 ASC System Files

The 3.7.0M2 ASC system files available for individual download are as follows:

- Oracle Communications Application Session Controller E3.7.0m2 Installation Image Supertar
- Oracle Communications Application Session Controller E3.7.0m2 Installation USB image
- Oracle Communications Application Session Controller E3.7.0m2 Installation ISO image
- Oracle Communications Application Session Controller E3.7.0m2 VMWare VMX/VMDK file
- Oracle Communications Application Session Controller E3.7.0m2 Xen server image
- Oracle Communications Application Session Controller E3.7.0m2 HyperV OVA file
- Oracle Communications Application Session Controller E3.7.0m2 LCR Import Tool
- Oracle Communications Application Session Controller E3.7.0m2 Embedded LCR Import Tool
- Oracle Communications Application Session Controller E3.7.0m2 Samples Kit
- Oracle Communications Application Session Controller E3.7.0m2 Archive Viewer Application
- Oracle Communications Application Session Controller E3.7.0m2 Weblogic SDK file
- Oracle Communications Application Session Controller E3.7.0m2 License Document

New Features

- Media Loss Detection
- TURN Server Support for WebRTC
- Partial Trickle ICE Support

Media Loss Detection

The ASC supports media loss detection, which determines when there is a loss of media on a session call-leg. When enabled, all relevant media sessions anchored on the ASC are monitored for media activity at a configured interval. When the ASC detects a loss of media, an event is generated indicating the session-id, call-leg, media stream index, type of media stream, and the timestamp of the last RTP packet received. An additional event is generated once media has resumed.

Media loss is assumed when there is no change to the Rx packet count during a media monitor interval.

You can either configure media loss detection on a per-session basis or on-demand via the call-control-media-loss-start and call-control-media-loss-stop actions.

Note: Media streams placed on hold are not monitored for the duration that they are on hold. Monitoring resumes once the session is taken off hold.

Configuring Media Loss Detection

You can configure media loss detection for a session via the session-config > in-media-loss-detection and out-media-loss-detection properties. You can also use on-demand media loss detection using the call-control-media-loss-start and call-control-media-loss-stop actions.

Note: The call-control-media-loss-start action takes precedence over the session-config media loss detection configuration.

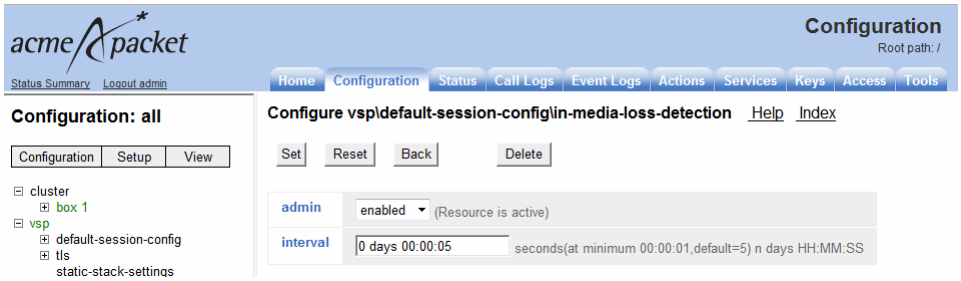
Configuring Media Detection Loss for a Session-Config

The session-config > in-media-loss-detection and out-media-loss-detection objects configure call-leg media loss monitoring. When these properties are enabled for a session, any media session call-legs matching this session-config are monitored for a loss of media.

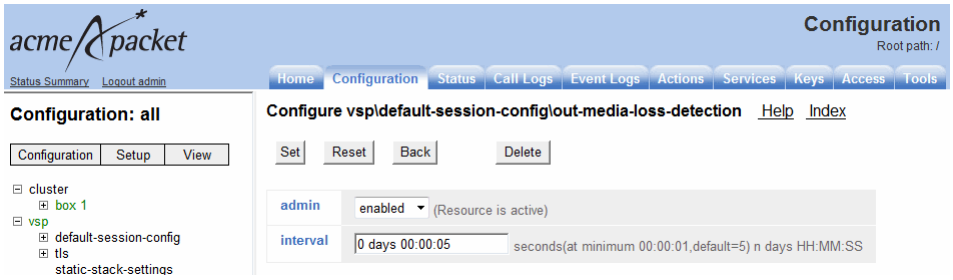
A session's media must be anchored on the ASC for media loss detection to work.

To enable in-leg and out-leg media detection loss:

1. Click the Configuration tab and select either default-session-config or session-config-pool > entry.
2. Click Configure next to in-media-loss-detection.



3. admin—Set to enabled to enable in-leg media loss detection. The default value is disabled.
4. interval—Set the interval, in seconds, to monitor for a loss of media on the in-leg. This value dictates how quickly the loss-of-media or resumption-of-media is detected and an event is generated. The default interval is 5 seconds.
5. Click Set. You are returned to the session-config object.
6. Click Configure next to out-media-loss-detection.



7. admin—Set to enabled to enable out-leg media loss detection. The default value is disabled.
8. interval—Set the interval, in seconds, to monitor for a loss of media on the out-leg. This value dictates how quickly the loss-of-media or resumption-of-media is detected and an event is generated. The default interval is 5 seconds.
9. Click Set. Update and save the configuration.

Initiating and Terminating On-Demand Media Loss Detection

You can initiate and terminate on-demand media loss detection via the call-control-media-loss-start and call-control-media-loss-stop actions.

call-control-media-loss-start

Initiates on-demand media loss detection for the call-leg of a specified session.

Syntax

```
call-control-media-loss-start <handle> [interval]
```

Arguments

- <handle>—Specify the call-leg handle on which to start monitoring for a loss of media.
- [interval]—Specify the interval, in seconds, to monitor for a loss of media. This value indicates how quickly the loss of media or resumption of media is detected and an event generated. The default value is 5 seconds.

call-control-media-loss-stop

Terminates the on-demand monitoring of a specified call-leg for the loss of media.

Syntax

```
call-control-media-loss-stop <handle>
```

Arguments

- <handle>—Specify the call-leg handle on which to stop monitoring for a loss of media.

WebRTC Enhancements in 3.7.0M2

The ASC's WebRTC support has been enhanced to include Traversal Using Relays around NAT (TURN) protocol support and partial trickle ICE support .

TURN Server Support for WebRTC

The ASC supports the TURN protocol for WebRTC. The TURN protocol assists clients located behind NAT devices to reach peers. In cases where clients and peers cannot create a direct communication path (for example, if both endpoints are behind individual NATs), it is necessary for an intermediate network device to relay data. The ASC TURN Server acts as a communication-enabling alternative for such cases, relaying data between the NAT-hidden clients. When used with ICE, the ASC TURN Server relay transport addresses are included in SDP ICE candidates received from clients. For more information on TURN, visit http://tools.ietf.org/search/rfc5766.

STUN Methods Required for the ASC's TURN Support

The following STUN methods are required for the ASC's TURN Support:

- Allocate
- Send
- Data

STUN Attributes Required for the ASC's TURN Support

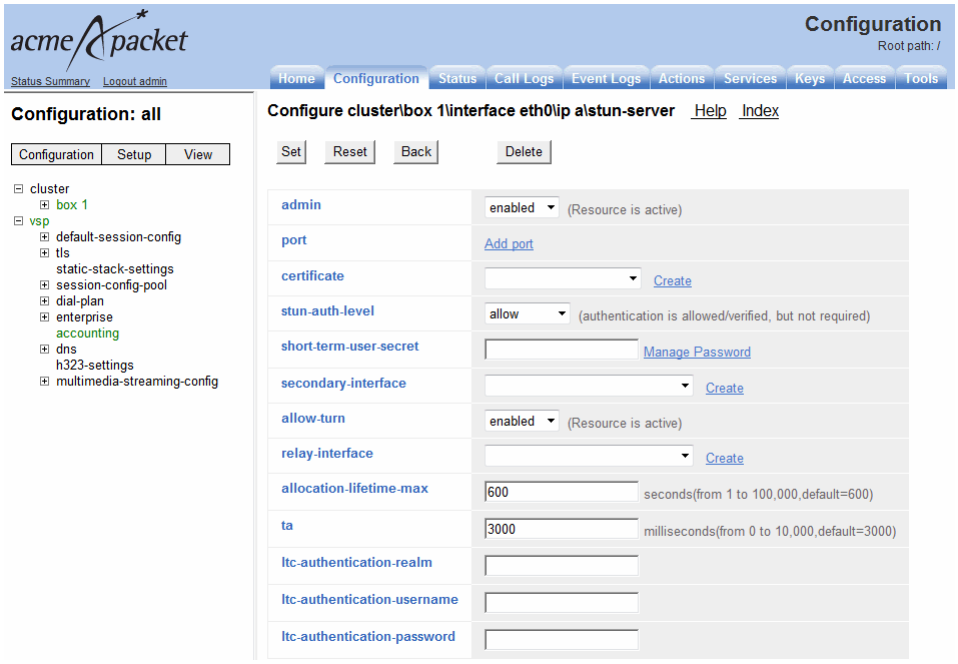
The following STUN attributes are required for the ASC's TURN support:

- LIFETIME
- DATA
- REQUESTED-TRANSPORT

Configuring TURN

To enable the TURN server on the ASC, you must enable STUN, and configure several properties within the **stun-server** object.

1. Click the **Configuration** tab and select the cluster > box > interface > ip object on which you are configuring TURN.
2. Click Configure next to stun-server.



3. admin—Set to enabled to enable STUN.
4. allow-turn—Set to enabled.
5. relay-interface—Select an interface provisioned with media ports.
6. ltc-authentication-realm— Specify the realm to use for STUN LTC authentication.
7. ltc-authentication-username— Specify a username for STUN LTC authentication.
8. ltc-authentication-password— Specify a password for STUN LTC authentication.
9. Click Set. Update and save the configuration.

Viewing TURN Server Information

Three show commands allow you to view TURN server information: show turn-allocations, show turn-destinations, show stun-server.

show turn-allocations

Provides information for each TURN client allocated server relay port. WebRTC endpoints typically allocate a relay port for each media stream.

Sample Output

```
ASC>show turn-allocations

            server-port: 172.44.10.60:3478
                   user: TurnMike@TurnRealm
                 client: 10.1.26.32:56863
      client-transport: UDP
             relay-port: 172.44.10.60:20975
       relay-transport: UDP
     destination-count: 1
client-to-peer-packets: 61489
```

```
  client-to-peer-bytes: 5822176
peer-to-client-packets: 61585
  peer-to-client-bytes: 5512977
         bandwidth-max: 150 kbits-per-second
      allocation-time: 07:12:02.147705 Tue 2014-01-21
              duration: 1177 seconds
             remaining: 503 seconds
```

Properties

- server-port: The IP and port of the TURN server listener.
- user: The user and realm of TURN LTC.
- client: The IP and port of the TURN client.
- client-transport: The transport method used for client/server communication.
- relay-port: The IP and port of the TURN relay for this Allocation.
- relay-transport: The transport method used for server/peer communication.
- destination-count: The number of TURN destinations for this Allocation.
- client-to-peer-packets: The number of packets relayed from client to peer for this Allocation.
- client-to-peer-bytes: The number of bytes relayed from client to peer for this Allocation.
- peer-to-client-packets: The number of packets relayed from peer to client for this Allocation.
- peer-to-client-bytes: The number of bytes relayed from peer to client for this Allocation.
- bandwidth-max: Currently not supported.
- allocation-time: The time the Allocation was created and/or refreshed.
- duration: The duration of the TURN Allocation.
- remaining: The time remaining for the TURN Allocation.

show turn-destinations

Provides information for each TURN peer associated with a TURN client.

Sample Output

```
ASC>show turn-destinations

            index: 1
      turn-client: 10.1.26.32:56864
 turn-allocation: 0xd1c27f75
       turn-relay: 172.44.10.60:20927
 relay-transport: UDP
        turn-peer: 172.44.10.60:20972
  channel-number: 16384
chan-expire-time: 07:32:02.972915 Tue 2014-01-21
   chanRemaining: 561 seconds
dest-permissions: Allowed
perm-expire-time: 07:32:02.972915 Tue 2014-01-21
   permRemaining: 261 seconds
   dest-anchored: true
```

Properties

- index: The index of this Destination

  Note: An Allocation can have multiple destinations.

- turn-client: The IP and port of the TURN client.
- turn-allocation: The handle of the Allocation owning this Destination.
- turn-relay: The IP and port of the TURN relay for this Destination.
- relay-transport: The transport uesd for server/peer communication.
- turn-peer: The IP and port of the TURN relay for this Destination.

- channel-number: The TURN channel number for this Destination (a value of 0 means unused).
- chan-expire-time: The time the TURN channel expires.
- chanRemaining: The time remaining before the TURN channel expires.
- dest-permissions: Permissions installed by the TURN client for this Destination.
- perm-expire-time: The time Permissions expire.
- permRemaining: The time remaining before Permissions expire.
- dest-anchored: Indicates if media is anchored for this TURN relay.

show stun-server

Provides information regarding the STUN server and, if configured, the TURN server. When you enter this action with a -v to display verbose information, the ASC displays information regarding the TURN server associated with the STUN server.

Sample Output

```
ASC> show stun-server  -v

                               index: 0
                              ifindex: 1
                            transport: UDP
                           ip-address: 172.44.10.60
                                 port: 3478
                      turn-redirector: disabled
                    secondary-ifindex: 0
                        relay-ifindex: 1
                relay-allocation-count: 2
                              connects: 0
                           disconnects: 0
                           rx-requests: 6065
                          tx-responses: 5394
                    tx-error-responses: 671
                              discards: 12
                   rx-binding-requests: 553
                  tx-binding-responses: 451
             tx-binding-error-responses: 102
                   rx-allocate-requests: 244
                  tx-allocate-responses: 122
            tx-allocate-error-responses: 122
                    rx-send-indications: 334
                    tx-app-relayed-data: 146669093
                    rx-app-relayed-data: 146141259
                    tx-data-indications: 423
                    tx-lite-framed-data: 146138511
             message-integrity-failures: 0
                   fingerprint-failures: 0
                    rx-refresh-requests: 2614
                   tx-refresh-responses: 2321
             tx-refresh-error-responses: 293
          rx-create-permission-requests: 33
         tx-create-permission-responses: 33
tx-create-permission-error-responses: 0
               rx-channel-bind-requests: 2621
              tx-channel-bind-responses: 2467
         tx-channel-bind-error-responses: 154
             rx-channel-data-indications: 146668771
             tx-channel-data-indications: 146138511
```

Properties

- index: This index of this STUN server.
- ifindex: The interface index used for this STUN server.

- transport: The transport method used for this STUN server.
- ip-address: The IP address used for this STUN server listener.
- port: The port used for this STUN server listener.
- turn-redirector: Indicates if the TURN redirector is enabled (not currently supported)
- secondary-ifindex: The secondary interface index used for STUN server change-address.
- relay-ifindex: The interface index used for the TURN server relay.
- relay-allocation-count: The number of TURN Allocations in use by the TURN server.
- connects: Not currently supported.
- disconnects: Not currently supported.
- rx-requests: The number of STUN/TURN requests received.
- tx-responses: The number of STUN/TURN success responses sent.
- tx-error-responses: The number of STUN/TURN error responses.
- discards: The number of STUN/TURN messages discarded.
- rx-binding-requests: The number of TURN binding requests received.
- tx-binding-responses: The number of TURN binding success responses sent.
- tx-binding-error-responses: The number of TURN binding error responses sent.
- rx-allocate-requests: The number of TURN Allocate requests received.
- tx-allocate-responses: The number of TURN Allocate success responses sent.
- tx-allocate-error-responses: The number of TURN Allocate error responses sent.
- rx-send-indications: The number of TURN send indications received from a TURN client.
- tx-app-relayed-data: The total number of TURN encapsulated relay messages data sent.
- rx-app-relayed-data: The total number of TURN encapsulated relay messages data received.
- tx-data-indications: The number of TURN data indications sent to a TURN client.
- tx-lite-framed-data: The number of TURN channel data indications transmitted.
- message-integrity-failures: The number of STUN/TURN messages with improper authentication received.
- fingerprint-failures: Not currently supported.
- rx-refresh-requests: The number of TURN refresh requests received.
- tx-refresh-responses: The number of TURN refresh success responses sent.
- tx-refresh-error-responses: The number of TURN refresh error responses sent.
- rx-create-permission-requests: The number of TURN permission requests received.
- tx-create-permission-responses: The number of TURN permission success responses sent.
- tx-create-permission-error-responses: The number of TURN permission error responses sent.
- rx-channel-bind-requests: The number of TURN binding requests received.
- tx-channel-bind-responses: The number of TURN binding success responses sent.
- tx-channel-bind-error-responses: The number of TURN binding success responses sent.
- rx-channel-data-indications: The number of TURN data channel messages received from a TURN client.
- tx-channel-data-indications: The number of TURN data channel messages sent to a TURN client.

Partial Trickle ICE Support

The ASC supports a limited version of trickle ICE.

What is Trickle ICE?

Trickle ICE is a draft extension to RFC 5245 that allows ICE agents to incrementally exchange remote candidate information. Trickle ICE support considerably reduces call setup time by allowing ICE to run before the candidate harvesting phase has completed by sending empty or partial media candidate lists in the SDP.

ASC Trickle ICE Limitations

The ASC currently supports only a partial implementation of trickle ICE.

The following are ASC trickle ICE limitations:

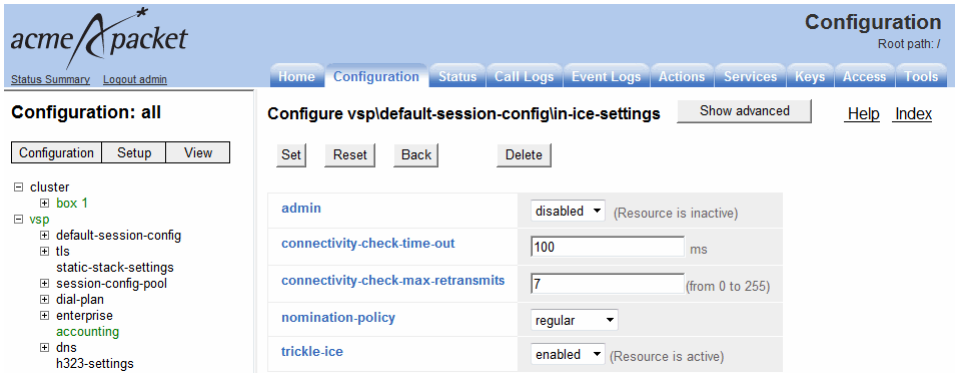
- The ASC supports only incomplete or empty candidate lists in the SDP offer/answer model. There is no support for incremental candidate exchanges.

  Note: Despite this limitation, call setup time is reduced and ICE can run to completion in call scenarios where the ASC is reachable from the trickle ICE endpoint and the media is anchored.
- Trickle ICE is not supported in augmented ICE scenarios. If both trickle ICE and augmented ICE are configured, disable augmented ICE to achieve the best possible performance.

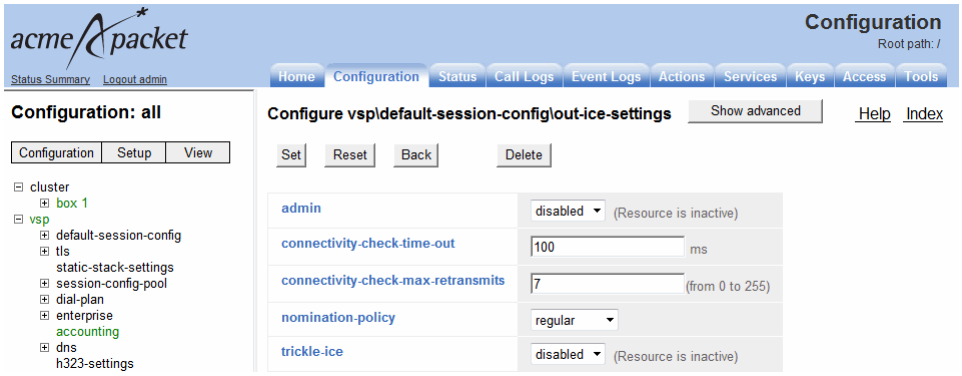
Configuring Trickle ICE

To configure trickle ICE on the ASC, you must enable the **in-ice-settings** and **in-ice-settings** > **trickle-ice**parameter.

1. Click the Configuration tab and select either default-session-config or session-config-pool > entry.
2. Click Configure next to in-ice-setting.



3. trickle-ice—Set to enabled or disabled to determine if trickle ICE is offered and supported on each call leg.
4. Click Set. You are returned to the session-config object.
5. Click Configure next to out-ice-setting.



6. trickle-ice—Set to enabled or disabled to determine if trickle ICE is offered and supported on each call leg.
7. Click Set. Update and save the configuration.

Viewing Trickle ICE Information

Three show commands allow you to view trickle ICE information: show ice-local-candidates, show ice-remote-candidates, show ice-candidate-pair-status.

show ice-local-candidates

Displays ICE information for the local candidates used by each state machine.

Sample Output

```
ASC>show ice-local-candidates
session-id           leg      checklist  transport                componentID
type  priority             foundation
----------           ---      ---------  ---------                -----------
----  --------             ----------
```

```
0x8c4ef6081de8c26   1         0          172.44.10.55:20676 UDP    1
host  2130706431           1
                                         172.44.10.55:20677 UDP    2
host  2130706430           1
0x8c4ef6081df913f   0         0          172.44.10.55:23836 UDP    1
host  2130706431           1
                                         172.44.10.55:23837 UDP    2
host  2130706430           1
```

Properties

- session-id: The ID of the session that owns the ICE state machine.
- leg: The call-leg on which the ICE state machine is running.
- checklist: The checklist number that owns the candidate. This is also known as the media description index.
- transport: The IP, port, and transport protocol of the candidate.
- componentID: The ICE component ID. This value is an integer.
- type: The ICE candidate type. This can be either host, srflx, prflx, or relay.
- priority: The candidate priority.
- foundation: The foundation string.

show ice-remote-candidates

Displays ICE information for the remote candidates received from the remote peer.

Sample Output

```
ASC>show ice-remote-candidates
session-id          leg     checklist  transport                componentID
type  priority             foundation
----------          ---     ---------  ---------                -----------
----  --------             ----------
0x8c4ef6081de8c26   1        0         172.44.10.57:22656 UDP    1
host  2130706431           1
                                       172.44.10.57:22657 UDP    2
host  2130706430           1
0x8c4ef6081df913f   0        0         172.44.10.57:22938 UDP    1
host  2130706431           1
                                       172.44.10.57:22939 UDP    2
host  2130706430           1
```

Properties

- session-id: The ID of the session that owns the ICE state machine.
- leg: The call-leg on which the ICE state machine is running.
- checklist: The checklist number that owns the candidate. This is also known as the media description index.
- transport: The IP, port, and transport protocol of the candidate.
- componentID: The ICE component ID. This value is an integer.
- type: The ICE candidate type. This can be either host, srflx, prflx, or relay.
- priority: The candidate priority.
- foundation: The foundation string.

show ice-candidate-pair-status

Displays information and state for each ICE candidate pair.

Sample Output

```
ASC>show ice-candidate-pair-status
session-id          leg     checklist  local
remote                    state      componentID nominated
----------          ---     ---------  -----
```

```
------                         -----      ----------- ---------
0x8c4ef6081de8c26   1          0          172.44.10.55:20676 UDP
172.44.10.57:22656 UDP    Succeeded  1           true
                                        172.44.10.55:20677 UDP
172.44.10.57:22657 UDP    Succeeded  2           true
0x8c4ef6081df913f   0          0          172.44.10.55:23836 UDP
172.44.10.57:22938 UDP    Succeeded  1           true
                                        172.44.10.55:23837 UDP
172.44.10.57:22939 UDP    Succeeded  2           true
```

Properties

- session-id: The session ID on which ICE is running.
- leg: The call leg on which ICE is running.
- checklist: The checklist that owns the candidate pair. This is also known as the media description index.
- local: The local candidate in the pair.
- remote: The remote candidate in the pair.
- state: The pair state. This can be either Frozen, Waiting, Succeeded, or Failed.
- componentID: The componentID of the pair. This value is an integer.
- nominated: Specifies whether or not this pair has been nominated for media transmission.

New Configuration Objects in Release 3.7.0M2

This section provides a summary of the new configuration objects added to the 3.7.0M2 release.

in-media-loss-detection

Configures in-leg media loss detection settings.

Syntax

```
config default-session-config in-media-loss-detection
config session-config-pool entry name in-media-loss-detection
```

Properties

admin Enable or disable media loss detection on this call leg.

- Default: disabled
- Values: enabled | disabled

interval Set the interval, in seconds, in which to check for media loss on this call leg.

- Default: 5

out-media-loss-detection

Configures out-leg media loss detection settings.

Syntax

```
config default-session-config out-media-loss-detection
config session-config-pool entry name out-media-loss-detection
```

Properties

admin Enable or disable media loss detection on this call leg.

- Default: disabled
- Values: enabled | disabled

interval Set the interval, in seconds, in which to check for media loss on this call leg.

- Default: 5

New Configuration Properties in Release 3.7.0M2

This section provides a summary of the new configuration properties added in release 3.7.0M2.

certificate

The following properties have been added to the certificate object in 3.7.0M2.

Syntax

```
config vsp tls certificate name
```

Properties

dynamic-certificate-days-before Secondary Property. Specifies how many days a dynamic certificate is marked as valid before its creation date. For example, if a certificate is created on February 25 and the value of this property is 7, the certificate is valid starting February 18.

- Default: 7
- Min: 0 / Max: 4294967296

dynamic-certificate-days-required Secondary Property. Specifies how many days a dynamic certificate is marked as valid after its creation date. For example, if a certificate is created on February 25 and the value of this property is 7, the certificate is valid through March 4.

- Default: 7
- Min: 0 / Max: 4294967296

New Properties 3.7.0M2 - default-dtls-settings

The following properties have been added to the default-dtls-settings object in 3.7.0M2.

Syntax

```
config vsp tls default-dtls-settings
```

Properties

dynamic-certificate-days-before Secondary Property. Specifies how many days a dynamic certificate is marked as valid before its creation date. For example, if a certificate is created on February 25 and the value of this property is 7, the certificate is valid starting February 18.

- Default: 7
- Min: 0 / Max: 4294967296

dynamic-certificate-days-required Secondary Property. Specifies how many days a dynamic certificate is marked as valid after its creation date. For example, if a certificate is created on February 25 and the value of this property is 7, the certificate is valid through March 4.

- Default: 7
- Min: 0 / Max: 4294967296

default-outgoing-settings

The following properties have been added to the default-outgoing-settings object in 3.7.0M2.

Syntax

```
config vsp tls default-outgoing-settings
```

Properties

dynamic-certificate-days-before

Secondary Property. Specifies how many days a dynamic certificate is marked as valid before its creation date. For example, if a certificate is created on February 25 and the value of this property is 7, the certificate is valid starting February 18.

- Default: 7
- Min: 0 / Max: 4294967296

dynamic-certificate-days-required

Secondary Property. Specifies how many days a dynamic certificate is marked as valid after its creation date. For example, if a certificate is created on February 25 and the value of this property is 7, the certificate is valid through March 4.

- Default: 7
- Min: 0 / Max: 4294967296

New Properties 3.7.0M2 - in-ice-settings

The following properties have been added to the in-ice-settings object in 3.7.0M2.

Syntax

```
config vsp default-session-config in-ice-settings
config vsp session-config-pool entry name in-ice-settings
```

Properties

trickle-ice

Enables or disables trickle ICE on the in-leg.

- Default: disabled
- Values: enabled | disabled

New Properties 3.7.0M2 - media

The following properties have been added to the media object in 3.7.0M2.

Syntax

```
config vsp default-session-config media
config vsp policies session-policies policy name rule name session-config
media
config vsp dial-plan dial-prefix entryName session-config media
config vsp dial-plan route name session-config media
config vsp dial-play source-route name session-config media
config vsp session-config-pool entry name media
```

Properties

dtls-passthru-latching

Secondary Property. Specifies whether ASC latches media based on observed DTLS traffic.

- Default: enabled
- Values: enabled | disabled

dtls-passthru-threshold Secondary Property. Specifies required number consecutive DTLS messages from same origin before media latch.

- Default: 2
- Min: 0 / Max: 4294967296

New Properties 3.7.0M2 - out-ice-settings

The following properties have been added to the out-ice-settings object in 3.7.0M2.

Syntax

```
config vsp default-session-config out-ice-settings
config vsp session-config-pool entry name out-ice-settings
```

Properties

trickle-ice Enables or disables trickle ICE on the out-leg.

- Default: disabled
- Values: enabled | disabled

New Properties 3.7.0M2 - stun-server

The following properties have been added to the stun-server object in 3.7.0M2.

Syntax

```
config cluster box number interface ethx ip name stun-server
configu cluster box number interface ethx vlan number ip name stun-server
config box interface ethx ip name stun-server
config box interface ethx vlan number ip name stun-server
```

Properties

ltc-authentication-realm Specifies the realm allocated for STUN LTC authentication.

ltc-authentication-username Specifies the username for STUN LTC authentication.

ltc-authentication-password Specifies the password for STUN LTC authentication.

MIB Changes in Release 3.7.0M2

This section describes changes that have been applied to Management Information Base (MIB) object definitions.

New MIB Tables in Release 3.7.0M2

MIB Table Name	Description
iceCandidatePairStatus	The status of an ICE candidate pair.
iceLocalCandidates	The local ICE candidates.
iceRemoteCandidates	The remote ICE candidates
selfSignedCertificateFactory	Self-signed certificate factory statistics.
turnDestinations	TURN server destination status.

Changed MIB Tables in Release 3.7.0M2

MIB Object Name	Description
dynamicEventServices	ADDED: dynamicEventServicesEventQueueDepth, dynamicEventServicesIdleSenderThreads, dynamicEventServicesMaxEventQueueDepth, dynamicEventServicesMaxSenderThreads, dynamicEventServicesQueueRejected
iceDtlsStatus	ADDED: iceDtlsStatusPassThruCount, iceDtlsStatusRuleUpdateDone
mediaSessionRecord	ADDED: mediaSessionRecordMediaLossDetectionIn, mediaSessionRecordMediaLossDetectionOut
stunServer	ADDED: stunServerRelayAddress, stunServerRxChannelBindRequests, stunServerRxChannelDataIndications, stunServerRxCreatePermissionRequests, stunServerRxRefreshRequests, stunServerTurnServer, stunServerTxChannelBindErrorResponses, stunServerTxChannelBindResponses, stunServerTxChannelDataIndications, stunServerTxCreatePermissionErrorResponses, stunServerTxCreatePermissionResponses, stunServerTxRefreshErrorResponses, stunServerTxRefreshResponses
turnAllocations	ADDED: turnAllocationsRxAllocateRequests, turnAllocationsRxChannelbindRequests, turnAllocationsRxChanneldataIndications, turnAllocationsRxCreatepermissionRequests, turnAllocationsRxRefreshRequests, turnAllocationsRxSendIndications, turnAllocationsTxAllocateResponses, turnAllocationsTxChannelbindResponses, turnAllocationsTxChanneldataIndications, turnAllocationsTxCreatepermissionResponses, turnAllocationsTxDataIndications, turnAllocationsTxRefreshResponses

Known Problems and Restrictions in 3.7.0M2

ASCTrickle ICE Support Limitations

The ASC currently supports only a partial implementation of trickle ICE.

The following are ASC trickle ICE limitations:

- The ASC supports only incomplete or empty candidate lists in the SDP offer/answer model. There is no support for incremental candidate exchanges.

  Note: Despite this limitation, call setup time is reduced and ICE can run to completion in call scenarios where the ASC is reachable from the trickle ICE endpoint and the media is anchored.
- Trickle ICE is not supported in augmented ICE scenarios. If both trickle ICE and augmented ICE are configured, disable augmented ICE to achieve the best possible performance.

WebRTC Video Issues

If a call is initiated from a separate third-party ASC in a WebRTC environment, there is a chance the call may have issues rendering video.

By adding the following attributes to the OFFER SDP, you allow video frame feedback and loss recovery, which may fix these video issues:

```
a=rtcp-fb:* nack
a=rtcp-fb:* nack pli
a=rtcp-fb:* ccm fir
```

Update the **header-settings** > **altered-body** in the appropriate session-config (web-to-sip, sip-to-web, web-to-web-anchored, or web-to-web-anchored-conditional) to include the above attributes into the OFFER SDP.

```
   config header-settings
    config altered-body #
```

```
     set altered-body (.*)m=video(.*) "\1m=video\2\ba=rtcp-fb:* nack\ba=rtcp-
fb:* nack pli\ba=rtcp-fb:* ccm fir" custom
    return
   return
```

Diffie-Hellman Logjam Attack Defense

The defense against the Diffie-Hellman Logjam attack, as originally referenced in the Net-Net OS-E 3.7.0 Release Notes, has a different workaround in 3.7.0M2 (same as 3.7.0M1).

The Diffie-Hellman Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography, allowing the attacker to read and modify any data passed over the connection.

This attack is similar to the FREAK attack, but is due to a flaw in the TLS protocol rather than an implementation vulnerability. It attacks a Diffie-Hellman key exchange rather than an RSA key exchange. When using the ASC Web Management System, the attack affects any server that supports CHE_EXPORT ciphers and affects all modern web browsers.

Note: For more information on the Diffie-Hellman Logjam attack, see *https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000*.

To protect against the Logjam vulnerability:

1. Log into the ASC CLI.
2. Type shell to open the Linux shell.
3. Open the file */usr/java/jrel.7/lib/security/java.security* in an editor.
4. Set the property **jdk.tls.disabledAlgorithms** (found at the end of the file) to DH, DHE.

   ```
   jdk.tls.disabledAlgorithms=DH, DHE
   ```
5. Restart the ASC.

3

Release 3.7.0M3

This section describes all of the new adaptations added to the ASC in release 3.7.0M3, including new features, configuration objects and properties, and MIBs.

3.7.0M3 ASC System Files

The 3.7.0M3 ASC system files available for individual download are as follows:

- Oracle Communications Application Session Controller E3.7.0m3 Installation Image Supertar
- Oracle Communications Application Session Controller E3.7.0m3 Installation USB image
- Oracle Communications Application Session Controller E3.7.0m3 Installation ISO image
- Oracle Communications Application Session Controller E3.7.0m3 VMWare VMX/VMDK file
- Oracle Communications Application Session Controller E3.7.0m3 Xen server image
- Oracle Communications Application Session Controller E3.7.0m3 HyperV OVA file
- Oracle Communications Application Session Controller E3.7.0m3 LCR Import Tool
- Oracle Communications Application Session Controller E3.7.0m3 Embedded LCR Import Tool
- Oracle Communications Application Session Controller E3.7.0m3 Samples Kit
- Oracle Communications Application Session Controller E3.7.0m3 Archive Viewer Application
- Oracle Communications Application Session Controller E3.7.0m3 Weblogic SDK file
- Oracle Communications Application Session Controller E3.7.0m3 License Document

New Features

- MSRP Interworking
- Configuring Static DTLS Certificates
- Call Management Enhancements
- Full Trickle ICE Support
- TURN Over TCP/TLS Support
- Certified Platforms for the ASC
- Data Channel Support
- TURN Implementation Updates
- Replacing Failed or Unconfigured Drives On the Oracle Netra X3-2

MSRP Interworking

The ASC now supports Message Session Relay Protocol (MSRP) interworking.

MSRP interworking allows communication between WebRTC and Rich Communication Suite (RCS) endpoints. This protocol is used for transmitting a series of instant message chats and file transfers within the context of a session.

For more information on MSRP, see *https://tools.ietf.org/html/rfc4975*.

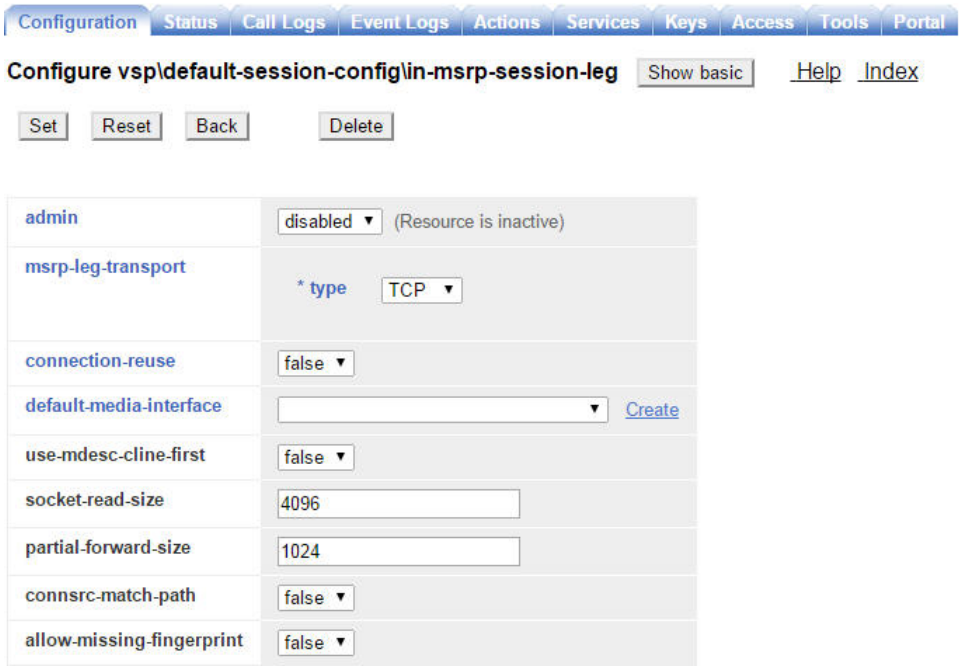
Configuring MSRP Interworking

To enable MSRP interworking on the ASC, you must configure the **in-msrp-session-leg** and **out-msrp-session-leg** objects.

Configuring In-Leg MSRP Interworking

To configure in-leg MSRP interworking:

1. Click the **Configuration** tab and select either **default-session-config** or **session-config-pool** > **entry**.
2. Click **Configure** next to **in-msrp-session-leg**.



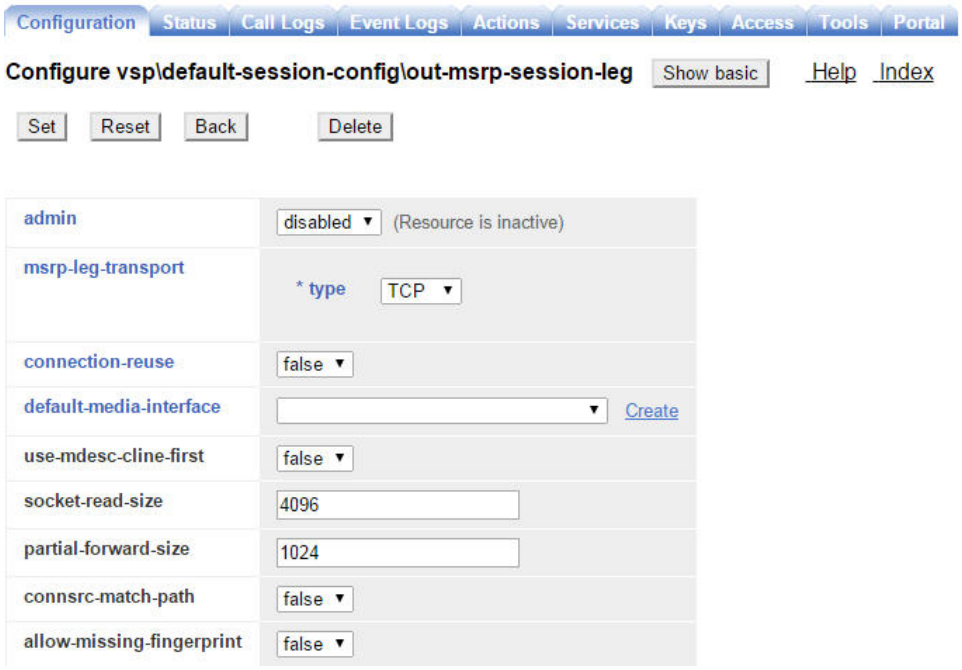
3. **admin**—Set to enabled to enable MSRP interworking.
4. **msrp-leg-transport**—Specify the MSRP transport method for RCS or WebRTC.
5. **connection-reuse**—Not supported in Release 3.7.0M3.
6. **default-media-interface**—Specify the local media interface to use for MSRP if svc-routing fails to locate the appropriate interface.
7. Click **Set**. Update and save the configuration.

Configuring Out-Leg MSRP Interworking

To configure out-leg MSRP interworking:

1. Click the **Configuration** tab and select either **default-session-config** or **session-config-pool** > **entry**.

2. Click **Configure** next to **out-msrp-session-leg**.



3. **admin**—Set to enabled to enable MSRP interworking.
4. **msrp-leg-transport**—Specify the MSRP transport method for RCS or WebRTC.
5. **connection-reuse**—Not supported in Release 3.7.0M3.
6. **default-media-interface**—Specify the local media interface to use for MSRP if svc-routing fails to locate the appropriate interface.
7. Click **Set**. Update and save the configuration.

Viewing MSRP Interworking Statistics

The ASC provides four show commands that allow you to view MSRP interworking statistics: **show active-msrp-sessions**, **show msrp-connections**, **show msrp-listeners**, **show msrp-stats**.

show active-msrp-sessions

Displays information regarding active MSRP session statistics

Sample Output

```
SIP>show active-msrp-sessions

Active MSRP Sessions:
-----------------------------------------------------------------------


    session-handle: 0xC7C634F3
        inleg-type: Msrp
       inleg-state: CONNECTED
       outleg-type: Msrp
      outleg-state: CONNECTED
 caller-session-id: mhnb1ad02f
       caller-path: msrp://wscAddress.invalid:2855/mhnb1ad02f;ws
 called-session-id: 2511644601
       called-path: msrp://10.138.238.49:53847/2511644601;tcp
       create-time: 12:09:59.163681 Thu 2014-10-30
          duration: 24 seconds
```

```
-------------------------------------------------------------------
Total Active MSRP Sessions:           1
```

Properties

- session-handle: The handle for this session.
- inleg-type: The type of endpoint of the in-leg session.
- inleg-state: The state of the in-leg session endpoint.
- outleg-type: The type of endpoint of the out-leg session.
- outleg-state: The state of the out-leg session endpoint.
- caller-session-id: The session ID of the calling endpoint.
- caller-path: The path of the calling endpoint.
- called-session-id: The session ID of the called endpoint.
- called-path: The path of the called endpoint.
- create-time: The time this session was created.
- duration: The length, in seconds, of this session.

show msrp-connections

Displays statistics regarding all of the connections used by the current MSRP sessions.

Sample Output

```
SIP>show msrp-connections
-------------------------------------------------------------------------------
Process Proto LocalAddress        RemoteAddress       State     Direction
RefCount
-------------------------------------------------------------------------------
SIP     TCP   10.138.236.35:23365 10.138.238.49:53847 Connected Answer
1
SIP     WS    10.138.236.35:23385 10.138.238.49:53848 Connected Originate
1
```

Properties

- Process: The signaling process being used for this connection.
- Proto: The media transport protocol being used for this connection.
- LocalAddress: The local IP address and port.
- RemoteAddress: The remote IP address and port.
- State: The state of the connection.
- Direction: The current direction of media transfer.
- RefCount: Not currently supported. This value should always be 1.

show msrp-listeners

Displays information listing all ports on the ASC interface that are waiting for MSRP connections.

Sample Output

```
SIP>show msrp-listeners
-----------------------------------------------------------------------
Process Proto Address              Connections Rejected Current Timeouts
-----------------------------------------------------------------------
SIP     WS    10.138.236.35:23385     0        0       1        0
```

Properties

- Process: The signaling process being used for this port.
- Proto: The media transport protocol being used for this port.

- Address: The IP address for this port.
- Connections: The number of connections available on this port.
- Rejected: The number of connections rejected by this port.
- Current: The number of current connections on this port.
- Timeouts: The number of timeouts that have occurred on this port.

show msrp-stats

Displays information regarding MSRP interworking statistics.

Sample Output

```
SIP>show msrp-stats

          totalSessions: 4
       totalConnections: 2
 totalActiveConnections: 1
totalPassiveConnections: 1
             RxRequests: 4
            RxResponses: 4
             TxRequests: 4
            TxResponses: 4
    RxMessagesDiscarded: 0
  RxMessagesPartialRead: 0
       RxMessagesFailed: 0
       TxMessageRetries: 0
       TxTcpWriteErrors: 0
       TxMessagesFailed: 0
         ListenerErrors: 0
     SessionEstTimeouts: 0
        UserMsgsExpired: 0
```

Properties

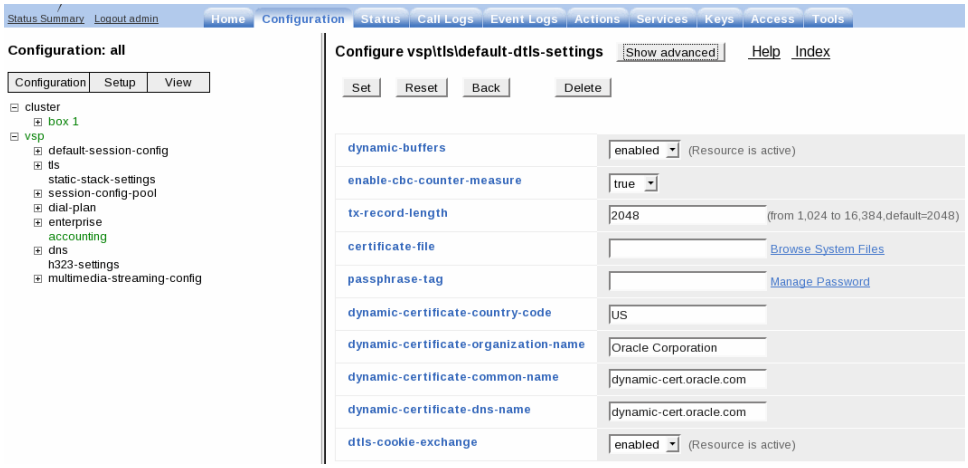
- totalSessions: The total number of MSRP sessions since the system was last started.
- totalConnections: The total number of connections since the system was last started.
- totalActiveConnections: The total number of connections created by the ASC.
- totalPassiveConnections: The total number of connections initiated by MSRP.
- RxRequests: The total number of MSRP request messages received by the ASC.
- RxResponses: The total number of MSRP responses messages received by the ASC.
- TxRequests: The total number of MSRP request messages forwarded by the ASC.
- TxResponses The total number of MSRP response messages forwarded by the ASC.
- RxMessagesDiscarded: The total number of MSRP messages discarded by the ASC regardless of reason.
- RxMessagesPartialRead: The total number of partial MSRP messages read. If this value is anything but zero, the ASC is using partial-forwarding.
- RxMessagesFailed: The total number of MSRP messages the ASC has been unable to be read.
- TxMessageRetries: The total number of attempts to forward MSRP messages (usually due to slow connection establishment).
- TxTcpWriteErrors: The total number of times the ASC encountered an error while attempting to forward an MSRP message.
- TxMessagesFailed: The total number of MSRP messages not forwarded by the ASC due to an error condition.
- ListenerErrors: The total number of MSRP listener-related errors.
- SessionEstTimeouts: The total number of times an MSRP session failed to be established.
- UserMsgsExpired: Not currently supported.

Configuring Static DTLS Certificates

When you implement Datagram Transport Layer Security (DTLS) in a WebRTC environment, you must configure a static certificate via the **default-dtls-settings** configuration object.

To configure a static DTLS certificate:

1. Click the **Configuration** tab and select the **vsp > tls** object.
2. Click **Configure** next to **default-dtls-settings**.



3. **certificate-file**—Specify the name of the certificate file used to establish connections made with this object. The ASC supports the following certificate formats: PKCS#12: Public Key Cryptography Standard #12 format, often from Microsoft IIS Version 5 (binary), PEM: Privacy Enhanced Mail format, from any Open SSL-based web server (ASCII).
4. **passphrase-tag**—Specify the passphrase associated with the certificate file. Use this property if the certificate file is encrypted to have its private key information protected. This passphrase must match the string that the certificate was encrypted with.
5. Click **Set**. Update and save the configuration.

Note: For more information on configuring certificates see the *Oracle Communications OS-E Objects and Properties Reference Guide*.

Execute the show certificates -v action to verify that the certificate is working.

Call Management API Enhancements

As a way to support the ASC as a controlling agent, several API actions have been created to allow for more granular control over media sessions.

The following API actions have been created:

- call-create
- call-alerting
- call-accept
- call-reject
- call-modify
- call-hold
- call-held
- call-retrieve
- call-retrieved
- call-destroy

- trickle-ice-update

call-create

Creates a media session that includes the underlying media subsystem. The ASC performs a route lookup and if it determines the destination endpoint is a media endpoint, no signaling is generated. However, if the ASC determines the destination endpoint is SIP, H.323, or MSS, it uses the existing infrastructure for establishing a call to an endpoint of that type to establish the out-leg for the session.

Syntax

```
call-create <to-uri> <from-uri> [request-id] <prev-hop> <next-hop> <media-specification> [named-configs] [session-config]
```

Arguments

- <to-uri>—The destination endpoint.
- <from-uri>—The source endpoint.
- [request-id]—The string returned in all events associated with this session.
- <prev-hop>—The address of the media source.
- <next-hop>—The address of the media destination.
- <media-specification>—The media specification (initial-offer-SDP).
- [named-configs]—A list of one or more associated named session-configs.

call-create-result

After the **call-create** action has been executed, the initial-offer-SDP is processed by the media subsystem to generate the actual-offer-SDP. If enabled, a **call-connecting-event** is generated and the action completes, returning a **call-create-result**.

Fields

- <to-uri>—The URI of the destination endpoint.
- <from-uri>—The URI of the source endpoint.
- <session-id>—The media session identifier.
- <request-id>—The string returned in all events associated with this session.
- <in-leg-handle>—The handle identifying the inbound call-leg.
- <out-leg-handle>—The handle identifying the outbound call-leg.
- <media-specification>—The media specification (actual-offer-SDP).

call-alerting

This action may be initiated after **call-create** has completed. In the case of a multi-protocol session, this action is invoked to alert the destination endpoint that an incoming call is being received.

Syntax

```
call-alerting <out-leg-handle> <media-type> [media-specification]
```

Arguments

- <out-leg-handle>—The handle identifying the call-leg that is alerting.
- <media-type>—The mime type of the media specification (initial-answer-SDP).
- [media-specification]—The media specification (initial-provisional-SDP).

call-alerting-result

After the **call-alert** action has been executed, if the initial-provisional-SDP has been provided, it is injected into the media sub-system, resulting in the actual-provisional-SDP being forwarded to the in-leg. After the action completes it returns the **call-alerting-result**.

Fields

- <session-id>—The identifier of the session created by the **call-create**.
- <out-leg-handle>—The handle identifying the call-leg indicating that it is alerting.
- <result-id>—The string returned in all events associated with this session.
- <media-specification>—The provisional media specification forwarded to the in-leg (actual-provisional-SDP).

call-accept

This action may be initiated in response to either a **call-connecting-event** or after a **call-create** has completed. The ASC injects the initial-answer-SDP media specification into the media session and the provides the resulting actual-answer-SDP to the peer endpoint.

Syntax

```
call-accept <out-leg-handle> <media-type> <media-specification>
```

Arguments

- <out-leg-handle>—The handle identifying the call-leg accepting the call invitation.
- <media-type>—The mime type of media specification (initial-answer-SDP).
- <media-specification>—The answer media specification (initial-answer-SDP).

call-accept-result

Once the **call-accept** action is is executed and has completed, a **call-accept-result** is returned.

Fields

- <session-id>—The identifier of the session created by the **call-create**.
- <out-leg-handle>—The handle identifying the call-leg accepting the call invitation.
- <request-id>—The string returned in all events associated with this session.
- <media-specification>—The answer media specification forwarded to the in-leg (actual-answer-SDP).

call-reject

This action may be initiated in response to a **call-connecting-event** and causes the media session to be terminated. The action completes immediately and does not provide structured results. The initiator of the action or signaling event creating the media session is notified appropriately.

Syntax

```
call-reject <out-leg-handle> <response-code> [response-phrase]
```

Arguments

- <out-leg-handle>—The handle identifying the call-leg that is rejecting the call invitation.
- <response-code>—The RFC 3261 code for why the call was rejected.
- [response-phrase]—A text string summarizing the reason the call is being rejected.

call-modify

This action may be initiated following either a **call-connected-event** or after completion of a **call-accept** or a **call-create** action. The ASC injects the initial-offer-SDP media specification provided into the media session and the resulting actual-offer-SDP is forwarded to the appropriate peer in accordance with the endpoint type.

Syntax

```
call-modify <call-leg-handle> <media-type> <media-specification>
```

Arguments

- <call-leg-handle>—The handle identifying the call-leg indicating a need for media re-negotiation.
- <media-type>—The mime type of media specification (initial-answer-SDP).
- <media-specification>—The offer media specification (initial-offer-SDP).

call-modify-result

Once the **call-modify** action is executed and completes, a **call-modify-result** is returned.

Fields

- <session-id>—The identifier of the session created by the **call-create**.
- <call-leg-handle>—The handle identifying the call-leg requesting media re-negotiation.
- <request-id>—The string returned in all events associated with this session.
- <media-specification>—The offer media specification forwarded to the peer call-leg (actual-offer-SDP).

call-hold

This action may be initiated following a **call-connected-event** or after completion of a **media-session-accept** action. When executed, this action notifies the peer endpoint that a hold has been requested and completes immediately. No structured results are returned.

Syntax

```
call-hold <call-leg-handle>
```

Arguments

- <call-leg-handle>—The handle of the call-leg indicating a desire to place the remote endpoint on hold.

call-held

This action may be initiated following a **call-held-event** or is invoked when the peer endpoint has indicated via signaling that the endpoint has entered the held state. This action completes immediately and does not return structured results.

Syntax

```
call-held <call-leg-handle>
```

Arguments

- <call-leg-handle>—The handle of the call-leg indicating it has entered the held state.

call-retrieve

This action may be initiated following a **call-held-event** or after a **call-hold** action has completed. When executed, this action notifies the peer endpoint that a retrieve has been requested and completes immediately. No structured results are returned.

Syntax

```
call-retrieve <call-leg-handle>
```

Arguments

- <call-leg-handle>—The handle of the holding call-leg indicating a desire to terminate the hold.

call-retrieved

This action may be initiated following a **call-retrieved-event** or is invoked when the peer endpoint has indicated via signaling that the endpoint is no longer in the held state. This action completes immediately and does not return structured results.

Syntax

```
call-retrieved <call-leg-handle>
```

Arguments

- <call-leg-handle>—The handle of the held call-leg indicating the hold has been terminated.

call-destroy

Terminates a media session resulting in all endpoints being disconnected.

Syntax

```
call-destroy <call-leg-handle> <response-code> [response-phrase]
```

Arguments

- <call-leg-handle>—The handle of the call-leg indicating a desire to terminate the session.
- <response-code>—An RFC 3261 code indicating why the call is being terminated.
- [response-phrase]—A text string summarizing the reason the call is being terminated.

call-destroy-result

Once the **call-destroy** action is executed and completes, a **call-destroy-result** is returned.

Fields

- <session-id>—The identifier of the session created by the **call-create**.

trickle-ice-update

This action behaves as if the trickle-ice-media-specification had been received via a SIP INFO request.

Syntax

```
trickle-ice-update <call-leg-handle> <media-type> <trickle-ice-media-
specification>
```

Arguments

- <call-leg-handle>—The handle identifying the holding call-leg providing the trickle-ice update.
- <media-type>—The mime type of media specification (initial-answer-SDP).
- <trickle-ice-media-specification>—The offer media specification forwarded to the peer call-leg (incremental-SDP).

trickle-ice-update-result

After the **trickle-ice-update** action has been executed, the media specification is processed and the resulting media specification, which would have been forwarded in a SIP INFO, is returned in the **trickle-ice-update-result**.

Fields

- <session-id>—The identifier of the session created by the **call-create**.
- <call-leg-handle>—The handle identifying the call-leg requesting media re-negotiation.
- <request-id>—The string returned in all events associated with this session.
- <media-specification>—The offer media specification forwarded to the peer call-leg (actual-incremental-SDP).

Full Trickle ICE Support

In release 3.7.0M2, the ASC supported a limited version of trickle Interactive Connectivity Establishment (ICE). As of release 3.7.0M3, trickle ICE is fully supported.

For information on configuring and monitoring trickle ICE on the ASC, see *Partial Trickle ICE Support* in this guide.

For more information on trickle ICE, see *https://tools.ietf.org/html/draft-ietf-mmusic-trickle-ice-01*.

TURN Over TCP Support

As of release 3.7.0M3, the ASC fully supports Traversal Using Relay NAT (TURN) over Transmission Control Protocol (TCP). For more information on configuring TURN, see *TURN Server Support for WebRTC* in *WebRTC Enhancements in 3.7.0M2*.

For more information on the TURN protocol, see *https://tools.ietf.org/html/rfc5766*.

Certified Platforms

Several platforms have been tested and certified for use with the ASC.

The following platforms have been certified for use with the ASC:

- Sun Netra X3-2
- HPDL360 G7
- HPDL585 G7
- HPDL320 G8
- HPDL360 G8
- Cisco C200

The following VM platforms have been certified for use with the ASC:

- OVM 3.3.1
- VMware ESXi 5.5
- XEN 3.4.3
- KVM on OL7

Data Channel Support

The ASC now supports data channels for anchored media.

Data channels use the Stream Control Transmission Protocol (SCTP) protocol as a generic transport service which allows web browsers to exchange non-media data between peers.

For more information on data channels, visit *https://tools.ietf.org/html/draft-ietf-rtcweb-data-channel-11*.

Note: You must have the **session-config > media > anchor** property enabled for data channels to work properly. For more information on this property, see the *Oracle Communications OS-E Objects and Properties Reference Guide*.

TURN Updates

The ASC's TURN server implementation has been updated to comply with RFC5766. These updates include:

- Newly required Session Traversal Utilities for NAT (STUN) methods
- Newly required STUN attributes
- A non-STUN message
- An action to purge TURN Allocations

For more information on the TURN protocol, see *https://tools.ietf.org/html/rfc5766*.

STUN Attributes Required For the ASC's TURN Support

The following STUN attributes are required for the ASC's TURN support.

- CHANNEL-NUMBER
- LIFETIME
- XOR-PEER-ADDRESS
- DATA
- XOR-RELAYED-ADDRESS
- EVEN-PORT
- REQUESTED-TRANSPORT
- DONT-FRAGMENT
- RESERVATION-TOKEN

STUN Methods Required for the ASC's TURN Support

The following STUN Methods are required for the ASC's TURN support.

- Allocate
- Refresh
- Send
- Data
- CreatePermission
- ChannelBind

Non-STUN TURN Message

The ASC supports the non-STUN **ChannelData** TURN message. This message carries application data between the TURN client and the server. Use of this message is optional for the client but required for the server if a channel has been bound to a remote peer.

Purging TURN Allocations

The turn-allocation-purge action allows you to remove TURN Allocations.

turn-allocation-purge

This action allows you to manually remove TURN Allocations. Per RFC5766, TURN clients that no longer want to use an Allocation are encouraged to delete the Allocation via a TURN Refresh request with a requested lifetime of 0. However, some TURN clients currently do not remove Allocations and these remain in the ASC until they expire.

Note: Ensure you remove only unused Allocations. Removing valid and in-use Allocations disrupts a WebRTC call using the ASC's TURN server.

Syntax

```
turn-allocation-purge [turn-client]
```

Arguments

- [turn-client]—The TURN client's IP address and port.

Note: By default, the **turn-allocation-purge** action purges all TURN Allocations, unless otherwise specified.

Replacing Failed or Unconfigured Drives On the Oracle Netra X3-2

This section describes replacing failed drives and fixing drives that have become "Unconfigured" on a Netra X3-2.

Replacing a Failed Drive

When a drive within an LSI Raid controller on the Netra X3-2 fails, you can replace it with a new factory replacement.

Note: Oracle recommends configuring logical drives consisting of no more than two physical drives for Raid1 (mirrored).

To check the state of drives and logical drives, use the **show raid-drive-status** and **show raid-logical-drive-status** status commands. When a physical drive completely fails, it no longer appears when you execute the **show raid-drive-status** command and the drive displays a red LED indicating a problem.

Also, when the **show raid-drive-status** command displays media errors, you may need to replace that drive.

If you need to replace a drive, physically remove the defective drive and replace it with a factory default replacement drive. Upon installation, the replacement drive triggers an automatic rebuild. During the rebuild process, the **show raid-drive-status** shows that drive in the **Rebuild** state and the **show raid-logical-drive-status** continues to show that logical drive in the **Degraded** state until the rebuild is complete.

To show the progress of a rebuild, execute the **show raid-missing-drives** command.

For more information on the **show raid-drive-status**, **show raid-logical-drive-status**, and **show raid-missing-drives** status commands, see the *Oracle Communications OS-E Objects and Properties Reference Guide*.

Fixing an Unconfigured Drive

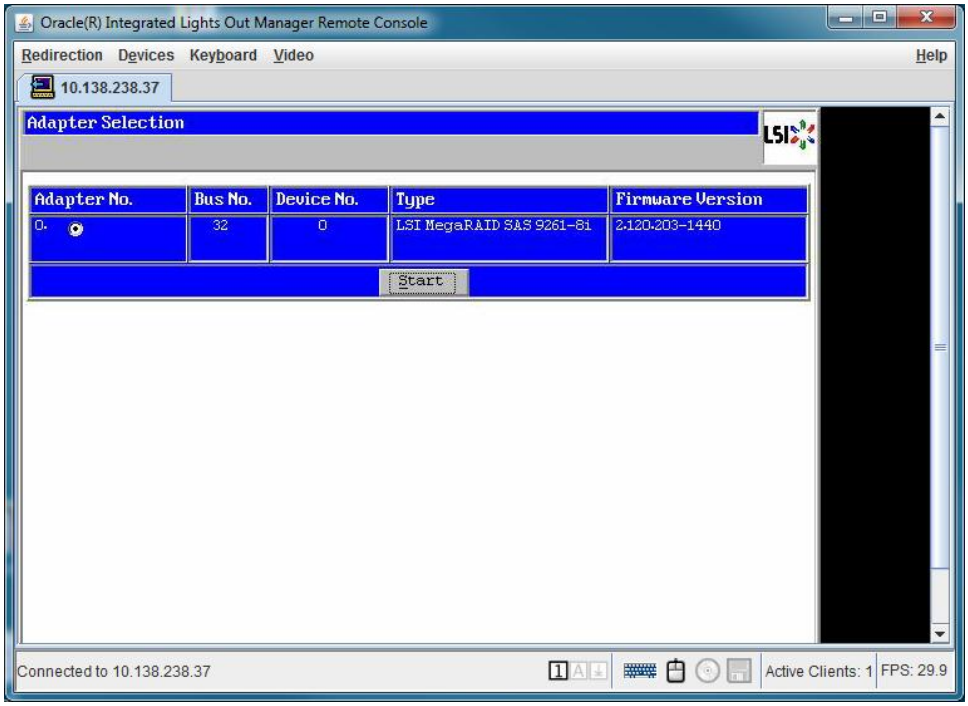
For various reasons, a drive may inadvertently enter into an **Unconfigured** state (for example if someone removes and reinserts an existing drive).

To fix an unconfigured drive:

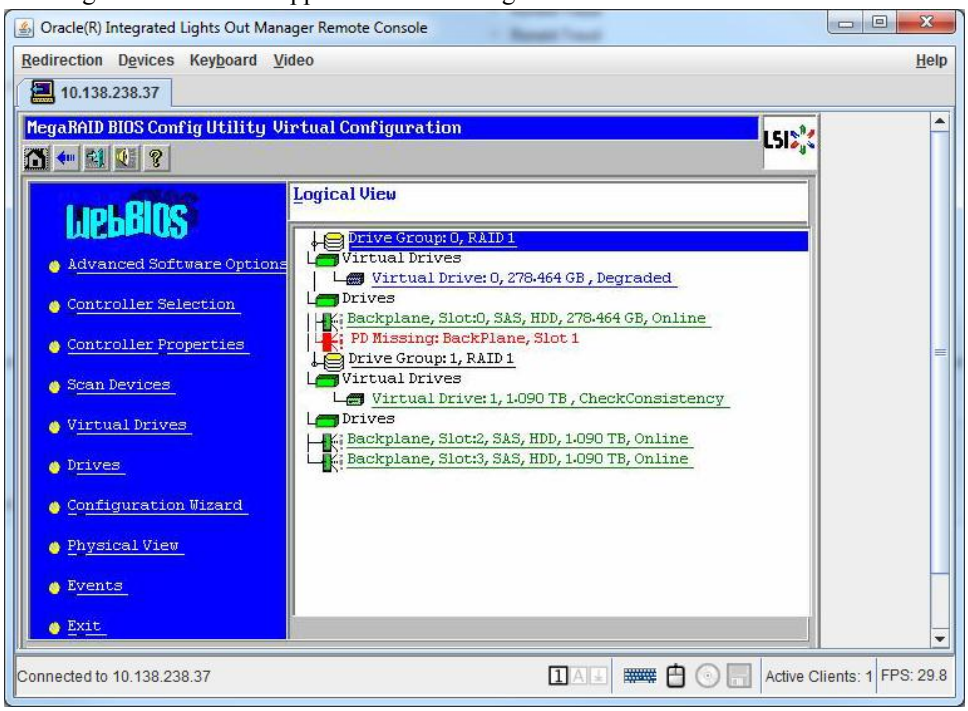
1. Attach a mouse, VGA monitor, and keyboard to the server.
2. Execute a restart cold from the CLI.

The system reboots.

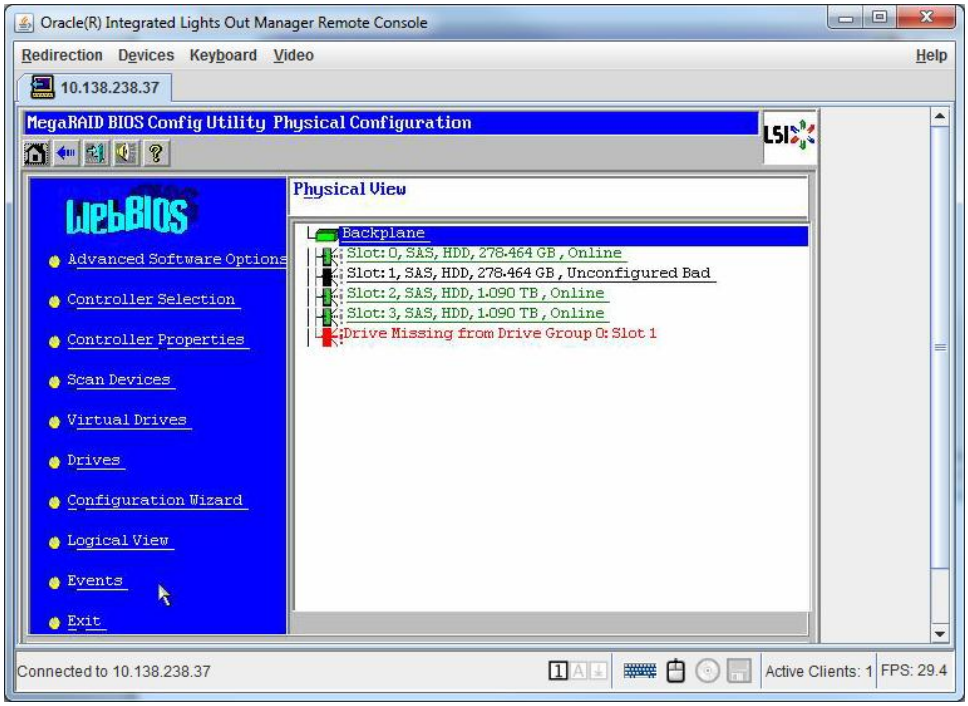
3. Enter <Ctrl><H> at the prompt to access the LSI MegaRAID utility WebBIOS.
   The Adapter Selection screen appears.



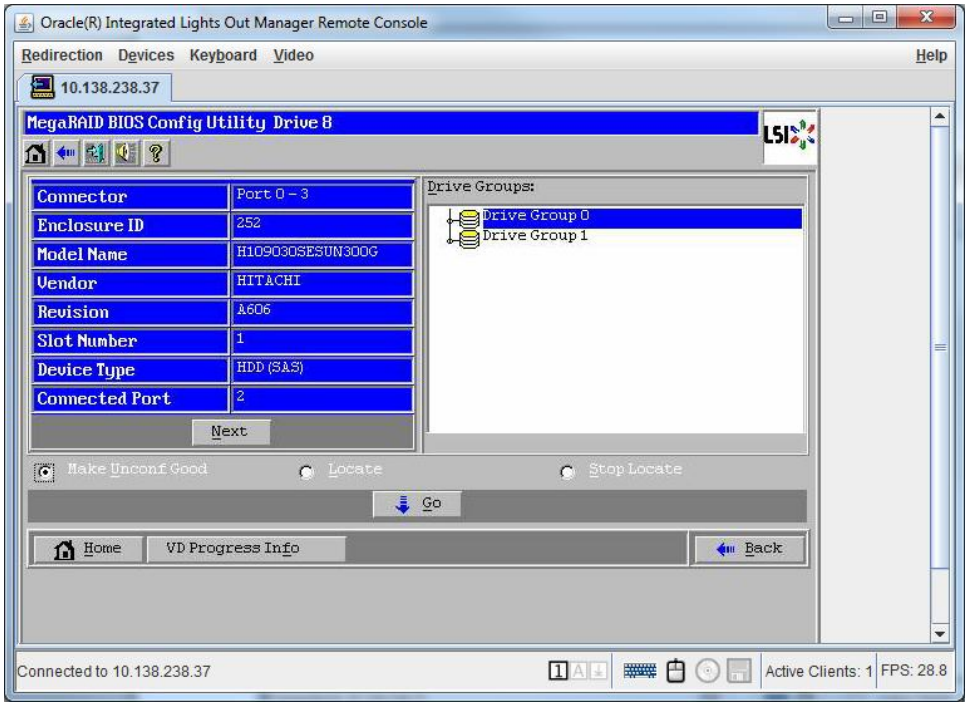
4. Click **Start** to select the adapter.
   The Logical View screen appears. Note the Degraded state of Virtual Drive 0 and the error message for Slot 1.



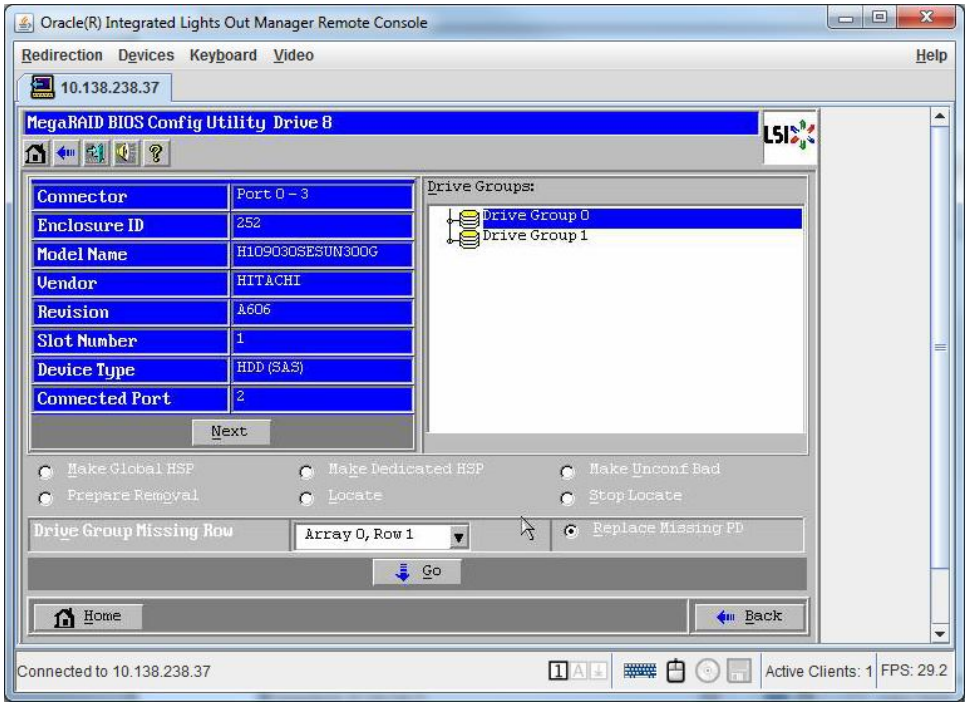
5. Select **Physical View** and select the drive marked as **Unconfigured Bad**.



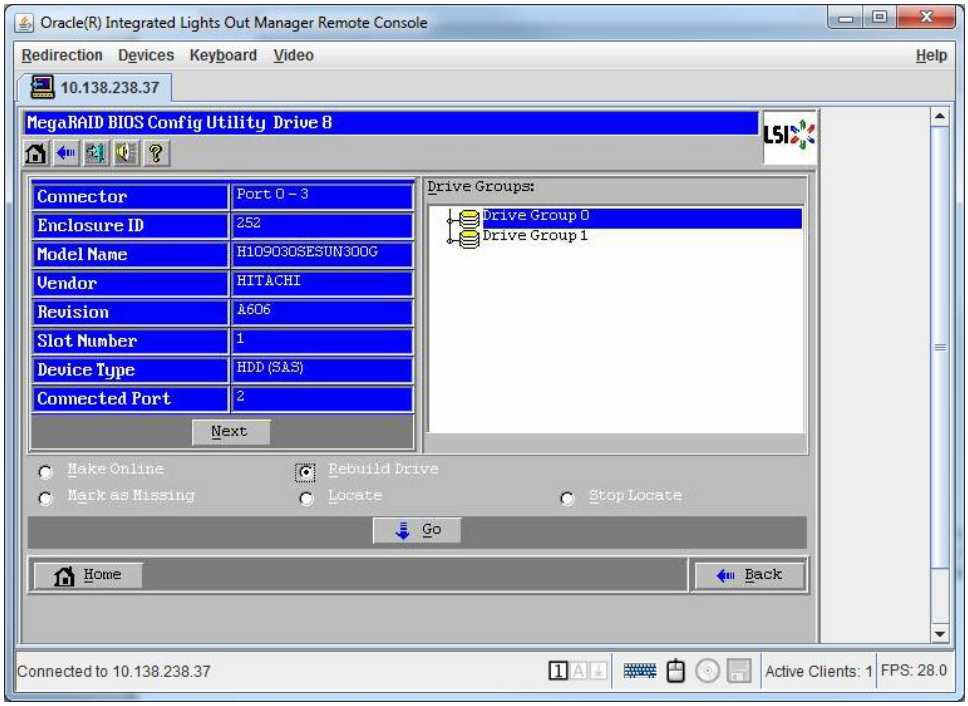
6. Select **Make Unconf Good** and click **Go**.



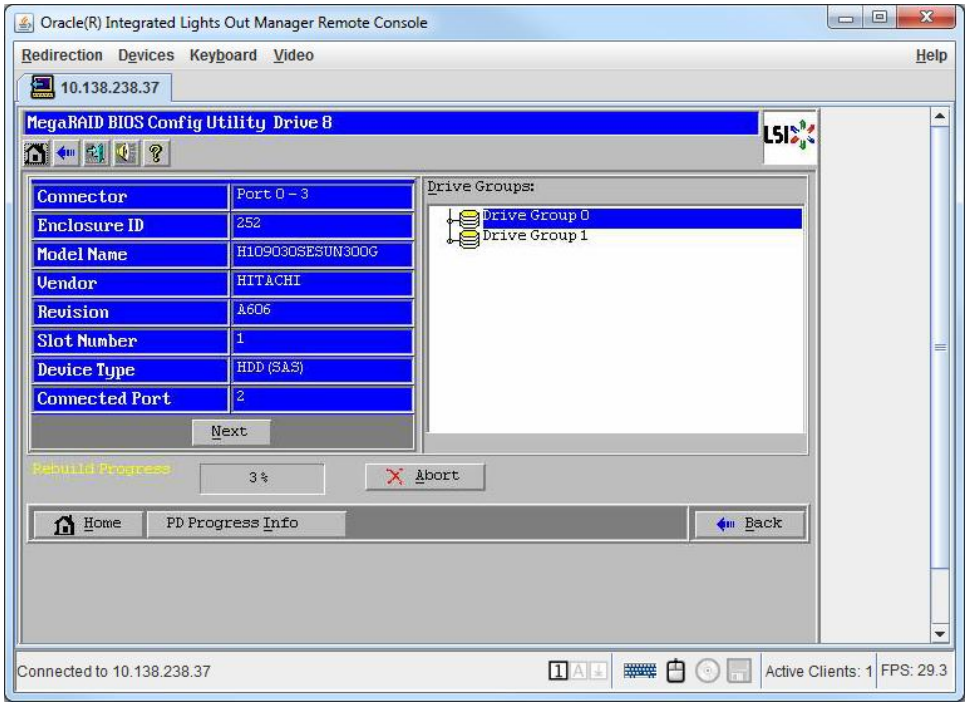
7. Select **Replace Missing PD** and click **Go**.



8. Select **Rebuild Drive** and click **Go**.



A screen showing the rebuild progress appears.



You can exit the WebBIOS and the drive continues to rebuild.

9. Select the Home screen and exit from the utility.
10. Execute a <**ctrl**><**alt**><**delete**> when prompted to reboot.
    You can use the **show raid-missing-drives** status command to see the progress of the rebuild.

New Configuration Objects in Release 3.7.0M3

This section provides a summary of the new configuration objects in release 3.7.0M3.

in-msrp-session-leg

Configures in-leg MSRP interworking.

Syntax

```
config default-session-config in-msrp-session-leg
config session-config-pool entry name in-msrp-session-leg
```

Properties

admin	Enable or disable MSRP interworking on this call leg. • Default: disabled • Values: enabled | disabled
msrp-leg-transport	Specify the MSRP transport method for RCS or WebRTC. • Default: TCP • Values: TCP | TLS | WS | WSS
connection-reuse	Not supported in Release 3.7.0M3.
default-media-interface	Specify the local media interface to use for an MSRP connection if svc-routing fails to locate the appropriate interface.

- Default: There is no default setting

use-mdesc-cline-first (Advanced) Specify whether the MSRP session manager attempts to use the SDP c-line (before using the path attribute) to learn the remote MSRP endpoint's media IP address.

- Default: false
- Values: true | false

socket-read-size (Advanced) Specify the MSRP socket read size to use when assembling incoming MSRP messages.

- Default: 4096
- Min: 0 / Max: 4294967296

partial-forward-size (Advanced) Specify the threshold for forwarding buffered MSRP message content bytes.

- Default: 1024
- Min: 0 / Max: 429967296

connsrc-match-path (Advanced) Specify whether the ASC allows incoming MSRP connections even when a remote address does not match the SDP path attribute.

- Default: false
- Values: true | false

allow-missing-fingerprint (Advanced) Specify whether the ASC allows an MSRP secure connection even when the SDP fingerprint attribute is missing.

- Default: false
- Values: true | false

out-msrp-session-leg

Configures out-leg MSRP interworking.

Syntax

```
config default-session-config out-msrp-session-leg
config session-config-pool entry name out-msrp-session-leg
```

Properties

admin Enable or disable MSRP interworking on this call leg.

- Default: disabled
- Values: enabled | disabled

msrp-leg-transport Specify the MSRP transport method for RCS or WebRTC.

- Default: TCP
- Values: TCP | TLS | WS | WSS

connection-reuse Not supported in Release 3.7.0M3.

default-media-interface Specify the local media interface to use for an MSRP connection if svc-routing fails to locate the appropriate interface.

- Default: There is no default setting

use-mdesc-cline-first (Advanced) Specify whether the MSRP session manager attempts to use the SDP c-line (before using the path attribute) to learn the remote MSRP endpoint's media IP address.

- Default: false
- Values: true | false

socket-read-size (Advanced) Specify the MSRP socket read size to use when assembling incoming MSRP messages.

- Default: 4096
- Min: 0 / Max: 4294967296

partial-forward-size (Advanced) Specify the threshold for forwarding buffered MSRP message content bytes.

- Default: 1024
- Min: 0 / Max: 429967296

connsrc-match-path (Advanced) Specify whether the ASC allows incoming MSRP connections even when a remote address does not match the SDP path attribute.

- Default: false
- Values: true | false

allow-missing-fingerprint (Advanced) Specify whether the ASC allows an MSRP secure connection even when the SDP fingerprint attribute is missing.

- Default: false
- Values: true | false

New Configuration Properties in Release 3.7.0M3

This section provides a summary of the new configuration properties added to the 3.7.0M3 release.

cluster

The following property has been added to the **cluster** object in 3.7.0M3.

Syntax

```
config cluster
```

Properties

action-timeout-addon (Advanced) Specifies how many milliseconds to add to the manager action timeout value.

Note: Do not configure this property unless explicitly told to do so by Oracle support.

- Default: 0
- Min: 0 / Max: 300000

event-settings

The following property has been added to the **event-settings** object in 3.7.0M3.

Syntax

```
configure vsp default-session-config event-settings
configure vsp session-config-pool entry name event-settings
```

Properties

event-filter Configures a filter which allows you to specify the event classes that this session is allowed to emit.

- Default: There is no default setting.

New Properties 3.7.0M3 - policy-group

The following property has been added to the **policy-group** object in 3.7.0M3.

Syntax

```
config external-services policy-group
```

Properties

connection-mode Specifies the manner in which connections between the ASC and WSDL server are established and maintained.

- Default: persistent 10 /covws/callouts?wsdl
- Values:
- persistent <inactivity-time> <keepalive-page> - Connections are initiated at boot time and maintained using periodic keepalives. Specify an activity timeout (between 2 and 120 seconds) and a keepalive page.
- lingering - Connections are made on demand then linger until broken by the remote server.
- transient - Connections are made on demand then broken when a response is received.

third-party-call-control

The following property has been added to the **third-party-call-control** object in 3.7.0M3.

Syntax

```
config vsp default-session-config third-party-call-control
config vsp session-config-pool entry name third-party-call-control
config vsp policies session-policies policy name rule name session-config
third-party-call-control
config vsp dial-plan dial-prefix entryName session-config third-party-call-
control
config vsp dial-plan route name session-config third-party-call-control
config vsp dial-plan source-route name session-config third-party-call-control
```

Properties

inhibit-anchored-update Specifies whether a re-INVITE message is generated and sent to the destination server to update the SDP for a third-party initiated call.

Note: This property is valid only when the **session-config > media > anchor** configuration property is enabled.

- Default: disabled
- Values: enabled | disabled

MIB Changes in Release 3.7.0M3

This section describes changes that have been applied to the Management Information Base (MIB) object definitions.

New MIB Tables in Release 3.7.0M3

MIB Table Name	Description
msrpStats	MSRP statistics.

Changed MIB Tables in Release 3.7.0M3

MIB Object Name	Description
activeMsrpSessions	• CHANGED: activeMsrpSessionsInLegState range • CHANGED: activeMsrpSessionsInLegState syntax from INTEGER to OCTET STRING • CHANGED: activeMsrpSessionsOutLegState range • CHANGED: activeMsrpSessionsOutLegState syntax from INTEGER to OCTET STRING
iceCandidatePairStatus	• ADDED: iceCandidatePairStatusRemoteMid
licenseDetails	• ADDED: licenseDetailsDefault, licenseDetailsHidden, licenseDetailsMax, licenseDetailsMin, licenseDetailsSecondary
msrpConnections	• ADDED: msrpConnectionsRefCount
processes	• processesAwaitingRunLevelResponse
systemInfo	• ADDED: systemInfoBaseDirectory, systemInfoUserSpace

Known Problems and Restrictions in 3.7.0M3

USB Installation Workaround

The USB install does not recognize the RAID array and cannot be used to install the code.

To mitigate this issue, turn the USB stick into a rescue stick and the installation succeeds.

Route Server Interworking Issue

In H.323/SIP interworking environments, route server lookups may fail, preventing the call from routing correctly.

Call-Control-Custom Action Conflict

A SIP fault occurs when you use the **call-control-custom** command and your configuration includes the **request-uri-specification** object.

Leave the **request-uri-specification** object unconfigured if you must use the **call-control-custom** command.

Diffie-Hellman Logjam Attack Defense

The defense against the Diffie-Hellman Logjam attack, as originally referenced in the Net-Net OS-E 3.7.0 Release Notes, has a different workaround in 3.7.0M3 (same as 3.7.0M1 and 3.7.0M2 except when using version 3.7.0M3P4 or later).

The Diffie-Hellman Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography, allowing the attacker to read and modify any data passed over the connection.

This attack is similar to the FREAK attack, but is due to a flaw in the TLS protocol rather than an implementation vulnerability. It attacks a Diffie-Hellman key exchange rather than an RSA key exchange. When using the ASC Web Management System, the attack affects any server that supports CHE_EXPORT ciphers and affects all modern web browsers.

Note: For more information on the Diffie-Hellman Logjam attack, see *https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000*.

For users on ASC versions 3.7.0M3P1, P2, and P3 to protect against the Logjam vulnerability:

1. Log into the ASC CLI.
2. Type shell to open the Linux shell.
3. Open the file */usr/java/jrel.7/lib/security/java.security* in an editor.
4. Set the property **jdk.tls.disabledAlgorithms** (found at the end of the file) to DH, DHE.

```
jdk.tls.disabledAlgorithms=DH, DHE
```

5. Restart the ASC.

For users on ASC versions 3.7.0M3P4 and later to protect against the Logjam vulnerability:

1. Select the **box > interface > ip > web** object.
2. Set the **ciphers** property to the following:

```
TLS_RSA_WITH_AES_128_CVC_SHA, TLS_RSA_WITH_AES_256_CVC_SHA,
TLS_RSA_WITH_3DES_EDE_CVC_SHA, TLS_RSA_WITH_RC4_128_SHA
```

   Note: If the ASC is part of a cluster configuration, set the **cipher** property in the **cluster > vrrp > vinterface > ip > web** object as well.

3. Click **Set**. Update and save the configuration. No restart is necessary and the changes take effect shortly.

4

Release 3.7.0M4

This section describes all of the new adaptations added to the ASC in release 3.7.0M4, including new features, configuration objects and properties, and MIBs.

3.7.0M4 ASC System Files

The 3.7.0M4 ASC system files available for individual download are as follows:

- Oracle Communications Application Session Controller E3.7.0m4 Installation Repository

Note: In prior releases, there were multiple ASC system files, but as of release 3.7.0M4, they have been consolidated into one file.

New Features

- ASC on Oracle Linux
- Certified Platforms for the ASC
- TURN Server Long Term Credentials
- Flexible MSRP Message Matching
- OPUS Codec Support

ASC On Oracle Linux

Starting with release 3.7.0M4, the ASC runs on Oracle Linux and uses yum to install and update RPM files. In prior releases, the ASC install package came with its own custom kernel. You must have Oracle Linux installed on your hardware prior to installing the ASC software.

Note: While the ASC operates under Oracle Linux, it is not certified to operate under other Linux environments.

You must have Oracle Linux Release 7.2 or higher to install the ASC. For more information on installing Oracle Linux, see *https://docs.oracle.com/cd/E52668_01/E54695/E54695.pdf*.

Due to the fact that the installation and upgrade procedures are significantly different in release 3.7.0M4 than in the other 3.7.0Mx releases, a 3.7.0M4 version of the installation guide has been created. The *Oracle Communications Application Session Controller System Installation and Commissioning Guide Release 3.7.0M4* is now available with the 3.7.0 doc set.

Certified Platforms

Several platforms have been tested and certified for use with release 3.7.0M4 of the ASC.

The following platforms have been certified for use with release 3.7.0M4 of the ASC:

- Sun Netra X5-2
- Sun Server X5-2
- Sun Netra X3-2
- HP DL160 G9
- NN2610
- NN2620

The following VM platforms have been certified for use with release 3.7.0M4 of the ASC:

- OVM 3.2.8
- VMware ESXi 5.5
- Xen 3.4.3
- KVM on OL7

TURN Server Long Term Credentials

The ASC supports TURN server Long Term Credentials (LTC). You can configure one of the following three types of LTC:

- original—LTC authentication with username and password statically configured on the ASC. These credentials are manually configured in the WebRTC browser.

  Note: For security reasons, Oracle does not recommend setting this value to **original**, as credentials can be extracted from the WebRTC browser.
- uberti—Follows the "draft-uberti-behave-turn-rest-00" document which uses a standard REST API for obtaining access to TURN services via ephemeral credentials. For more information on the "draft-uberti-behave-turn-rest-00" document, see *https://tools.ietf.org/html/rfc7635*.
- SDKv1—Follows the RFC 7635 document which uses OAuth 2.0 to obtain and validate ephemeral tokens that can be used for authentication. By using ephemeral tokens, you can ensure that access to a STUN server can be controlled even if the tokens are compromised. For more information on RFC 7635, see *https://tools.ietf.org/html/rfc7635*.

  Note: SDKv1 is not completely RFC 7635 compliant due to the fact that WebRTC browser support is required and does not exist.

When you configure either the **uberti** or**SDKv1** LTC types, you must configure a secret password. For increased security, ASC uses a two-part password mechanism for passwords shared with other devices (also known as shared secrets). You must configure both a password and a tag. An enterprise or RADIUS server, for example, probably has a configured password that ASC must use to access the server. This shared secret is the password. The tag is not the password itself, but rather a user-configurable name used to access the real password. By managing shared secrets, you can maintain the secrecy of the other passwords on other devices. An administrator can set up the tags and passwords; end users can work with the configuration files and use the password tag, without having access to the password itself.

ASC uses a password store to maintain the actual password known to the other device. Using a password store allows the shared passwords to be stored outside of, and not displayed in, the configuration file. Password tags are stored in the ASC configuration.

This password mechanism applies only to cases of ASC using a shared secret. It does not apply to passwords created for users under the **access** object. (These are stored as hashed data, never as plaintext.)

For more information on configuring secret passwords and tags, see “Understanding Passwords and Tags” in the *Oracle Communications Application Session Controller Objects and Properties Reference* guide.

Configuring TURN Server Long Term Credentials

You configure TURN long term credentials (LTC) via the **stun-server** configuration object.

To configure TURN server LTC:

1. Click the **Configuration** tab and select the **cluster > box > interface > ip** object on which you are configuring TURN.
2. Click **Configure** next to **stun-server**.
3. **type**—Specifies the type of LTC authentication to use. The ASC supports the following three types of LTC authentication:
   - **original**—LTC authentication with username and password statically configured on the ASC. These credentials are manually configured in the WebRTC browser.

     Note: For security reasons, Oracle does not recommend setting this value to **original**, as credentials can be extracted from the WebRTC browser.
   - **uberti**—Follows the "draft-uberti-behave-turn-rest-00" document which uses a standard REST API for obtaining access to TURN services via ephemeral credentials. For more information on the "draft-uberti-behave-turn-rest-00" document, see *https://tools.ietf.org/html/rfc7635*.
   - **SDKv1**—Follows the RFC 7635 document which uses OAuth 2.0 to obtain and validate ephemeral tokens that can be used for authentication. By using ephemeral tokens, you can ensure that access to a STUN server can be controlled even if the tokens are compromised. For more information on RFC 7635, see *https://tools.ietf.org/html/rfc7635*.

     Note: SDKv1 is not completely RFC 7635 compliant due to the fact that WebRTC browser support is required and does not exist.
4. **ltc-authentication-realm**—Specify the realm to use for STUN LTC authentication.
5. **ltc-auth-provider-pw-ttl**—Enter the private secret shared with the TURN LTC Authentication Provider.
6. **ltc-auth-provider-pw-ttl**—Specify the lifetime length for the shared password.
7. Click **Set**. Update and save the configuration.

Flexible MSRP Message Matching

The ASC gives you the option to choose the criteria on which to validate received MSRP messages. When the ASC receives a MSRP message, the MSRP session manager checks the configured match criteria to verify the message belongs to the MSRP session associated with the connection transporting the MSRP message.

You can choose to match on the following criteria:

- scheme
- host
- port
- transport
- sessionId

Configuring Flexible MSRP Message Matching

This section describes configuring flexible MSRP Message matching.

1. Click the **Configuration** tab and select either **default-session-config** or **session-config-pool > entry**.
2. Click **Configure**next to either **in-msrp-session-leg** or **out-msrp-session-leg**.
3. **message-match-criteria**—Select the criteria on which you want to match MSRP messages.
4. Click **Set**. Update and save the configuration.

Opus Codec Support

The ASC now supports transcoding of the Opus codec.

New Configuration Objects in Release 3.7.0M4

There are no new configuration objects in release 3.7.0M4.

New Configuration Properties in Release 3.7.0M4

This section provides a summary of the new configuration properties added in release 3.7.0M4.

features

The following property has been added to the **features** object in 3.7.0M4.

Syntax

```
config features
```

Properties

opus Sets the maximum concurrent number of Opus encoders and decoders for playout, announcements, mixing, or transcoding.

- Default: 200000
- Min: 0 / Max: 200000

stun-server

The following property has been added to the **stun-server** object in 3.7.0M4.

Syntax

```
config cluster box number interface ethx ip name stun-server
config cluster box number interface ethx vlan integer ip name stun-server
config cluster vrrp vinterface vxID ip name stun-server
config cluster vrrp vinterface vxID vlan integer ip name stun-server
config box interface ethx ip name stun-server
config box interface ethx vlan number ip name stun-server
```

Properties

ltc-authentication Specifies the type of TURN server long term credentials (LTC) to use.

- Default: original
- Values:
  - original—LTC authentication with username and password statically configured on the ASC. These credentials are manually configured in the WebRTC browser.

    Note: For security reasons, Oracle does not recommend setting this value to original, as credentials can be extracted from the WebRTC browser.
  - uberti—Follows the "draft-uberti-behave-turn-rest-00" document which uses a standard REST API for obtaining access to TURN services via ephemeral credentials. For more

information on the "draft-uberti-behave-turn-rest-00" document, see *https://tools.ietf.org/html/rfc7635*.

- SDKv1—Follows the RFC 7635 document which uses OAuth 2.0 to obtain and validate ephemeral tokens that can be used for authentication. By using ephemeral tokens, you can ensure that access to a STUN server can be controlled even if the tokens are compromised. For more information on RFC 7635, see *https://tools.ietf.org/html/rfc7635*.

New Properties 3.7.0M4 - third-party-call-control

The following property has been added to the **third-party-call-control** object in 3.7.0M4.

Syntax

```
config vsp default-session-config third-party-call-control
config vsp policies session-policies policy name rule name session-config
third-party-call-control
config vsp dial-plan dial-prefix entryName session-config third-party-call-
control
config vsp dial-plan route name session-config third-party-call-control
config vsp dial-plan source-route name session-config third-party-call-control
config vsp session-config-pool entry name third-party-call-control
```

Properties

flash-detect Specifies whether or not you want the ASC to detect Flash Publish and Subscribe events.

- Default: enabled
- Values: enabled | disabled

MIB Changes in Release 3.7.0M4

This section describes changes that have been applied to the Management Information Base (MIB) object definitions.

New MIB Tables in Release 3.7.0M4

There are no new MIB tables in release 3.7.0M4.

Changed MIB Tables in Release 3.7.0M4

MIB Object Name	Description
mx	• CHANGED: mxInterfaceStart syntax from InterfaceName to EthernetName
systemInfo	• ADDED: systemInfoAscRpmName, systemInfoInstallMethod, systemInfoLinuxDistribution
turnAllocations	• ADDED: turnAllocationsLtcAuthPwCreateTime, turnAllocationsLtcAuthPwExpireTime, turnAllocationsLtcAuthType
turnServer	• ADDED: turnServerLtcAuthType, turnServerLtcPwTtl, turnServerLtcSecretTag

Known Problems and Restrictions in Release 3.7.0M4

Inaccurate Call Duration Value In Some CDRs

When the ASC receives a 302 Redirect message during a call, the call curation is inaccurately reported as 0 in the CDR for the call.

ASC Incorrectly Modifies Response Reason

When a server responds with a "403 Authentication Failure, the ASC incorrectly changes the response to "403 Forbidden", causing some endpoints to stop sending requests.

500 Server Internal Error Returned For Some REGISTER Messages

When **max-proxy-transactions-per-vsp** is set to 0, the ASC creates a proxy pool with too few items. If the pool entries exhaust, the ASC returns a "500 server internal error" to additional incoming REGISTER messages.