# 

# Cisco Series D9510 USRM Release 2.1.4 Release Note

## **Overview**

### Introduction

The Cisco Series D9510 Universal Session and Resource Manager (USRM) release 2.1.4 succeeds and carries forward all of the enhancements and features of prior USRM releases (2.1.3, 2.1.2, 2.1.1, 2.1.0, 2.0.1, 2.0.0, 1.7.3, 1.7.2, and 1.7.1).

### Purpose

This release note is being provided for user support related to the installation and operation of USRM System Release 2.1.4.

### **Qualified Personnel**

Only appropriately qualified and skilled service personnel should attempt to install, operate, maintain, and service this product.



#### WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service this product. Otherwise, personal injury or equipment damage may occur.

### In This Document

General Information	2
Installation and Upgrade Guidelines	4
Downgrade Guidelines	10
Appendix A: New Script Usage in opt/usrm/linux-tools	11
Appendix B: Policy	15
Appendix C: Spreadsheet Import and Export	17
Appendix D: GQI v1.5 Requirements and Settings	20
Appendix E: VodSm Web Pages	21
Appendix F: Conversion from CaMgrDNCS to CaManagerPK	23

# **General Information**

#### **Additional Features**

Release 2.1.4 provides the following new features:

- Added encryption system failure counter. A new feature was added to monitor the number of Unknown Encryptor failures and allow the user to define a value at which the USRM will place this RCAS/TED pair out of service until the hardware issue has been addressed.
- Increase in the number of Ermi2 ports supported. Increased the number of supported ports to 384.
- Activity Logging enhancement. Added the Program Number Not Available count to the Activity Log.
- Enhanced log messaging. Added source address to all RmAnnounce log messages; added source address for failure to stream Lost messages; added QAM IP for announce messages; added transition state logging while in auto mode.

#### **Enhancements and Corrections**

Release 2.1.4 offers the following enhancements and corrections:

- MSA logging support. USRM 2.1.4 increases the maximum client session in MSA logging from 6 to 10. Any sessions beyond 10 are truncated.
- New version of brassd and associated components. USRM 2.1.4 includes a new version of the third-party Snmp agent used by USRM. This newer version includes defect corrections.
- VodSm default program number. The default range for program numbers under VodSm has been changed to 10000-20000 from 1000-2000.
- Added reason/Response codes in MSA logging. Added the Reason/Response code for CRReq, CRConf, SRInd, SRResp and Server Release indication in MSA messages.
- VodSm Release sent to BMS upon timeout indication. Added the option whether or not to send release indications on the server and resource timeouts.
- Maximum number of SDV programs has been increased to 1000. Increased the supported number of offered programs from 500 to 1000.
- Setting the reserved field in the Client Session Setup Confirmation as 0xFF instead of 0x00.
- Status Monitor sampling. Corrected an issue with sampling an MQAM's status.
- **•** Fix a problem with the propagation of session notifications.

- Addressed a race condition where a non-PowerKey QAM could be out of sync with the SdvSM due to certain timeout conditions that may occur during session setup.
- **Brassd Agent Watch Dog reporting.** This is now a Max log level message.
- Enhanced the error message logged for CcpEventIndErr to include the actual error code.
- HA correction for database transfer issue.
- **Corrected Status Count for Server session Status Confirm.**
- Enhancement for RFGW Edge input port control. Corrected issue with releasing sessions from an edge input.
- **Corrected issue with Copy Protection settings.** Server Add Resource Request now passes the Copy Protection setting to the OCAI interface.
- SaCaManager Asynchronous mode removed.

#### **Open Issues and Known Restrictions**

Release 2.1.4 has the following known open issues and restrictions:

- No commas, periods, or spaces can be used in any device name on the USRM.
  - Workaround: If multiple words are required, use an underscore in the place of the comma, period, or space.
- For users of Internet Explorer, logging out of the USRM webUI requires the browser to be fully closed for logout to occur, as IE caches the user.
- The version of Firefox included with DNCS 4.2 is not completely compatible with the enhanced web UI used with 2.1.4.
  - Workaround: use Internet Explorer or Firefox from alternate source to view/manipulate the USRM web UI.
- During initial configuration or any other operation that requires adding a large number of high density QAMs (e.g. 72 TSIDs or more) to a USRM database via a config file, it is recommended to add a maximum of 15 QAMs per config file.
  - Workaround: Use the new spreadsheet (CSV) import feature.
- During Service Group migration or any other operation that requires removing a large number of Service Groups containing 6000 or more STBs from a USRM database via a config file, it is recommended to remove a maximum of 20 SGs per config file.
- The pop up box for Server Sip Timeout states that the valid range is from 1 to 99999 but the field is actually limited to 10 to 99999.
- MSA does not log an error when the STB is not in the RCAS DB (0xca00004).
- MSA does not log the error when the SspTcp connection is not available. This may be due to VodSm timeouts being longer than 30 seconds.

## **Installation and Upgrade Guidelines**

#### **General Notes**

An FTP or SSH server is required to download new software to the USRM.

#### Installation Requirements

Before performing the upgrade procedure, make sure the following requirements are met:

- The desired USRM software release has already been uploaded to the FTP server.
- If the DNCS is being used as the FTP or SSH server, make sure that the desired USRM release is located in the /export/home/dncs directory.
- If the DNCS is being used as an SSH server, make sure that the Provisionkeys application has been run on each of the servers.
- A backup of the existing USRM database has been completed prior to upgrading to be prepared in case a rollback to the previous version is desired. A backup can be created from any directory in the USRM by typing **usrmbackup** at the command line prompt. The backup file will be stored in the /root directory. We recommend that this backup file be copied to and saved in a secure location in case it is needed in the future.

**Note:** A downgrade from USRM 2.1.4 to USRM 1.x requires the installation of a 1.x database as part of the procedure. If a 1.x database does not exist, all persistdata will be lost during the downgrade.

### **New Requirement**

With the introduction of VOD Session Management capabilities to the USRM, it is now required to keep track of all traffic on all GigE ports on all QAMs. With this in mind, we now require that the Edge Input IP address(es) be included for all QAMs.

If you have configuration files, the Edge Input address(es) should be added to these files.

**Note:** Failure to populate Edge Input Address(es) will result in session setup failures.

### Supervised vs. Auto Mode

USRM servers running the SdvSm application in a Cisco DNCS system should be run in Supervised mode. In this mode, the SDV Manager, which is part of the DNCS software release, provisions the USRM with information including the SDV Offered Programs table via SNMP, and also manages the servers from an HA perspective. USRM servers that run the VodSm application only should be run in Auto mode. High Availability still exists in Auto mode, but does not have a third party manager running it. All USRMs that are not in a Cisco DNCS environment should run in Auto mode.

### Release 2.1.4 from Release 2.0 – 2.1.1 Upgrade Procedure

A database change between USRM 2.0 and USRM 2.1.4 requires that the connection between the Primary and Standby Servers be removed during the upgrade. Renaming of the persistdata files for CA Managers between 2.1.1 and 2.1.4 requires a special step detailed in the procedure below (step 6).

- 1 If you have not done so already, complete the steps listed under **Installation Requirements** above.
- **2** Download the software to the USRM Standby Server using *one* of the following procedures, a or b, as appropriate.
  - **a** If you typically upgrade your USRM from the USRM Software Upgrade page:
    - From the Standby Server WebUI, select Platform -> ConfigManager -> Software Upgrade page.
    - Select **DownloadProtocol = SSH** from the drop-down menu.
    - Fill in the FTPHost, FTPUserName, FTPUserPassword, ImageDownloadString and ImageExecuteString fields with the appropriate information.
    - Click **Commit Changes** to save your changes.
    - Under InitiateDownload, select **Download**.
    - Click Commit Changes to download the software to the Standby USRM.
  - **b** If you typically upgrade your USRM from the DNCS SDV Server page:
    - From the DNCS, go to **Network Provisioning > SDV Server**.
    - Check your USRM to select it.
    - Select **Download Software** from the list at left on the screen.
    - Fill in the Image Download String and Image Execute String.
    - Select **Download/Install** to start the download process.
- **3** Terminate the USRM Standby Server process, preferably from the USRM WebUI System.Reset page.

**Note:** The Standby Server remains terminated until all of its Primary servers have been upgraded and rebooted.

- **4** Download the software to the USRM Primary Servers using *one* of the following procedures, a or b, as appropriate.
  - **a** If you typically upgrade your USRM from the USRM Software Upgrade page:
    - From the Standby Server WebUI, select Platform -> ConfigManager -> Software Upgrade page.
    - Select **DownloadProtocol = SSH** from the drop-down menu.
    - Fill in the FTPHost, FTPUserName, FTPUserPassword, ImageDownloadString and ImageExecuteString fields with the appropriate information.
    - Click **Commit Changes** to save your changes.
    - Under InitiateDownload, select **Download**.
    - Click **Commit Changes** to download the software to the Standby USRM.
  - **b** If you typically upgrade your USRM from the DNCS SDV Server page:
    - From the DNCS, go to Network Provisioning > SDV Server.
    - Check your USRM to select it.
    - Select **Download Software** from the list at left on the screen.
    - Fill in the Image Download String and Image Execute String.
    - Select **Download/Install** to start the download process.
- 5 Terminate the USRM Server process from the Reset page as follows:
  - a Select Terminate from the ServerState drop-down list.
  - **b** Click **Commit Changes**.
- 6 If the CaMgrDncs resource was used for Conditional Access, rename the CaMgrDncs persistdata files as follows:
  - **a** Open an ssh session to the Primary Server and go to the /opt/usrm/persistdata directory.
  - b Type the following to get a list of existing CA Manager files: [persistdata]# ls -ltr | grep CaMgrDncs
     A (list of) file(s) will be returned with the following format, where xyz is the
     name assigned to the particular CA Manager CaMgrDncs.xyz.bin.
  - c Change the file name as shown below. [persistdata] mv CaMgrDncs.xyz.bin CaManagerPk.xyz.bin
  - **d** Make the change for each CA Manager on the USRM, if more than one exists.
- 7 Install the rpm on the Primary Server as follows:
  - **a** In the same ssh session, go to the /tmp directory and manually install the rpm.

```
[usrm]# cd /tmp
[tmp]# rpm -Uvh usrm-2.1.3-8.i386.rpm --force
```

Note: There is one dash before Uvh and two dashes before force.

**b** Go to the /opt/usrm directory and verify that the rpm was successfully installed.

```
[tmp]# cd /opt/usrm
[usrm]# ./usrm -x
Universal Session & Resource Manager (USRM)
(c) Copyright 2006-2008 Cisco Systems, Inc., All Rights Reserved.
Configuration is VALID.
USRM Version 2.1.4-6
```

- 8 Start the PrimaryServer process as follows:
  - a From the ssh shell session in the /opt/usrm directory, start the usrm process in auto and daemon mode by typing *one* of the following, depending on whether the servers are in auto or supervised mode.
     [usrm]# ./usrm --auto -d

```
[usrm]# ./usrm --supervised -d
```

**Note:** In the examples above, there are two dashes before supervised and auto and one dash before d.

- **9** After all primary USRMs in the cluster have been upgraded, install the rpm on the Standby Server as follows:
  - **a** Open an ssh session to the Standby Server, and then go to the /tmp directory and install the rpm manually.

```
[usrm]# cd /tmp
[tmp]# rpm -Uvh usrm-2.1.3-8.i386.rpm --force
```

Note: There is one dash before Uvh and two dashes before force.

**b** Go to the /opt/usrm directory and verify that the rpm was successfully installed.

```
[tmp]# cd /opt/usrm
[usrm]# ./usrm -x
Universal Session & Resource Manager (USRM)
(c) Copyright 2006-2008 Cisco Systems, Inc., All Rights Reserved.
Configuration is VALID.
USRM Version 2.1.4-6
```

10 Start the Standby Server process.

Important: Complete the upgrade on ALL primary USRMs before proceeding.

**a** From the ssh shell session in the /opt/usrm directory, start the usrm process in Auto and daemon mode by typing *one* of the following, depending on whether the servers are in auto or supervised mode.

```
[usrm]# ./usrm --auto -d
```

[usrm]# ./usrm --supervised -d

Note: In the examples above, there are two dashes before supervised and auto and one dash before d.

#### Release 2.1.4 from Release 1.6 or 1.7 Upgrade Procedure

A database change between USRM 1.7 and USRM 2.1.4 requires that the connection between the Primary and Standby Servers be removed during the upgrade.

- 1 If you have not done so already, complete the steps listed under **Installation Requirements** above.
- 2 Download software to the USRM Standby Server as follows:
  - a From the Standby Server WebUI, select **Platform -> ConfigManager -> Software Upgrade** page.
  - **b** Select **DownloadProtocol = SSH** from the drop-down list.
  - c Fill in the FTPHost, FTPUserName, FTPUserPassword, ImageDownloadString and ImageExecuteString fields with the appropriate information.
  - d Click Commit Changes to save your changes.
  - e Under InitiateDownload, select **Download**.
  - f Click Commit Changes to download the software to the Standby USRM.
- **3** Terminate the Standby Server process, preferably from the USRM WebUI System.Reset page.

**Note:** The Standby Server remains terminated until all of its Primary servers have been upgraded and rebooted.

- 4 Download and install the software to the USRM Primary Servers as follows:
  - a From each Primary Server WebUI, select **Platform -> ConfigManager -> Software Upgrade** page.
  - **b** Select **DownloadProtocol = SSH** from the drop-down list.
  - c Fill in the FTPHost, FTPUserName, FTPUserPassword, ImageDownloadString, and ImageExecuteString fields with the appropriate information.
  - d Click **Commit Changes** to save your changes.
  - e Under InitiateDownload, select DownloadInstall.
  - f Click Commit Changes to download the software to the USRM.Note: The DownloadInstall option will cause the server to reset after the download is complete.
- 5 Install the rpm on the Standby Server as follows:
  - **a** Open an ssh session to the Standby Server, and then go to the / tmp directory and manually install the rpm.

[usrm]# cd / tmp

[tmp]# rpm -Uvh usrm-2.1.4-6.i386.rpm --force

Note: There is one dash before Uvh and two dashes before force.

**b** Go to the /opt/usrm directory and verify that the rpm was successfully installed.

```
[tmp]# cd /opt/usrm
[usrm]# ./usrm -x
Universal Session & Resource Manager (USRM)
(c) Copyright 2006-2008 Cisco Systems, Inc., All Rights Reserved.
Configuration is VALID.
USRM Version 2.1.4-6
```

**c** Start the Standby Server process.

Important: Complete the upgrade on *all* primary USRMs before proceeding.

**d** From the ssh shell session in the /opt/usrm directory, start the usrm process in Auto and daemon mode by typing *one* of the following, depending on whether the servers are in auto or supervised mode.

[usrm]# ./usrm --auto -d
[usrm]# ./usrm --supervised -d

**Note:** In the examples above, there are two dashes before supervised and auto and one dash before d.

#### Release 2.1.4 from Release 1.5 (or Earlier) Upgrade Procedure

A direct upgrade from USRM 1.5 to USRM 2.1.2 or greater is not supported. An interim upgrade to USRM 1.6 or later is required. Refer to previous release notes for those versions.

## **Downgrade Guidelines**

Database changes between USRM 1.7 and USRM 2.1.4 require that the connection between the Primary and Standby Servers be removed during the downgrade. Also, all sessions must be removed on RFGW-1 and GQI QAMs. Lastly, any QAM that was created after the upgrade to USRM 2.1.4 will have to be recreated after the downgrade (it will not be in the old persistdata files).

### Downgrading from USRM 2.1.4 to USRM 1.7

Perform the following procedure to downgrade from USRM 2.1.4 to USRM 1.7.

- 1 Locate the servers' previous USRM 1.7 database that was saved prior to the upgrade and place them in the servers' root directories, if they are not already there.
- 2 Download the software to each server according to the directions in the *Installation and Upgrade Guidelines* (on page 4).
- 3 Terminate the Standby Server.
- 4 On each Primary Server, release all sessions on all RFGW-1 and GQI QAMs.
- 5 Terminate the Primary Server.
- 6 Restore the USRM 1.7 persistdata files by opening an ssh session to the server and typing the following from any directory: usrmrestore /root/goqam.tar.bz2
- 7 Install the rpm on the Primary Server.
- 8 Initialize the Server as follows:
- [usrm]# init 6
- **9** Start the Primary server using *one* of the following startup commands, a or b, as appropriate:
  - **a** [usrm] # ./usrm --auto -d (for systems without DNCS)
  - **b** [usrm]# ./usrm --supervised -d (for systems with DNCS)

**Note:** In the examples above, there are two dashes before supervised and auto and one dash before d.

- **10** After all Primary servers in a cluster are back online, open an ssh session to the standby server and install the rpm.
- **11** Start up the Standby Server using *one* of the following startup commands, a or b, as appropriate:
  - **a** [usrm]# ./usrm --auto -d (for systems without DNCS)
  - **b** [usrm] # ./usrm --standby -d (for systems with DNCS)

Note: In the examples above, there are two dashes before standby and auto and one dash before d.

### Appendix A: New Script Usage in opt/usrm/linux-tools

This appendix describes scripting commands available with USRM Release 2.0.

#### **USRM** Platform

#### usrmbackup

This command creates a USRM database backup and causes the following files and directories to be TARed, compressed, and saved in the root directory:

- opt/usrm/ConfigFiles
- opt/usrm/persistdata
- home/dncs
- etc/sysconfig/network-scripts
- etc/sysconfig/network
- etc/hosts

You can run this command from any directory by typing **usrmbackup**. We recommend that you copy the backup file to a secure location in case of a catastrophic failure of the USRM hardware.

#### usrmrestore

Use this command to reinstall previously stored backup files onto the USRM.

This script requires you to specify the full path and filename of the backup file to be used. For example, the following usage restores the filename USRM01.25Aug2009.tar.bz2, which is stored in the root directory:

usrmrestore /root/USRM01.25Aug2009.tar.bz2

#### VOD

#### Perftail

Use this command to monitor the performance of the VOD requests. The results show the number of VOD Create and Release requests, how many succeeded and failed and why, and how many VOD sessions were active, over a series of one-minute intervals. The enumerated failures are Error 18 (no resource available), Error 32 (BMS could not build the session) and Error 6 (No Video PID in the PMT).

```
Tailing /opt/usrm/EventLog/13Jul2011_000001.txt ...
Time,ClntReqs,ClntCnfs,Succs,Fails,Err18s,Err32s,Err6s,ClntRelReqs,ClntRelCnfs,CS
ipMsgs,ActiveSessions
13:46,102,92,86,6,6,0,0,80,80,0,26
13:47,269,279,255,24,24,0,0,320,320,0,215
13:48,146,146,134,12,12,0,0,82,82,0,79
```

You can also use this script to evaluate a log file. However, the ActiveSessions count will not be correct, as this parameter is pulled real time from the running USRM software and not the log files. To use this script with a log file, use the following format:

Perftail <log filename>

You can also specify that this command run for a specified time period by using the following syntax:

perftail [-s <starttime>][-e <endtime>] [<logfile>]

#### sesstail

This command gives a listing of SSP Sessions for VOD. You can use this script to tail sessions in real time or to evaluate an existing log file. When evaluating a log file, you can specify start and end times to narrow the results of the evaluation. You must provide the full path to the log file to be evaluated.

The following are usage examples:

```
sesstail -s 10:00 -e 11:00 /opt/usrm/EventLog/09Sep2009 000000.txt
sesstail /opt/usrm/EventLog/09Sep2009 00000.txt
++++ 380ca8c00499/21 ++++
RmCreateSession
                                 2009/09/09 07:44:57.775
SspServerTxSISC
                                 2009/09/09 07:44:57.775 Rsp=0 TID=4110421
SGID=1194 nSes=1 uBW=3750000
PN=1097
RmCmdExec
                                 2009/09/09 07:44:57.775 Cmd=CreateSession
RID=172.16.4.78 Tid=668
                                 2009/09/09 07:44:57.800 Cmd=CreateSession
RmCmdSuccess
RID=172.16.4.78
SspServerRxServerReleaseRequest 2009/09/09 07:45:07.806 TID=3eb869 reason=1
RmSessionRelease
                                 2009/09/09 07:45:07.806 RID=172.16.4.78
SspServerTxServerReleaseConfirm 2009/09/09 07:45:07.807 TID=3eb869 response=0
RmCmdExec
                                 2009/09/09 07:45:07.807 Cmd=DeleteSession
RID=172.16.4.78 Tid=1
                                 2009/09/09 07:45:07.847 Cmd=DeleteSession
RmCmdSuccess
RID=172.16.4.78
 ++++ 001d09fa6301/716599 ++++
RmCreateSession
                                 2009/09/09 00:46:13.919
RmCmdExec
                                 2009/09/09 00:46:13.919 Cmd=CreateSession
RID=172.16.4.78
RmCmdSuccess
                                 2009/09/09 00:46:13.946 Cmd=CreateSession
RID=172.16.4.78
RmSessionRelease
                                 2009/09/09 00:46:17.932 RID=172.16.4.78
RmCmdExec
                                 2009/09/09 00:46:17.932 Cmd=DeleteSession
RID=172.16.4.78 Tid=1
RmCmdSuccess
                                 2009/09/09 00:46:17.967 Cmd=DeleteSession
RID=172.16.4.78
```

#### sspsistail

This command gives a listing of SSP-SIS sessions. Use this tool to display real-time SSP-SIS operations or to evaluate an event log file.

The following are examples of both usages:

```
ssptail
sspsistail
++++++++ 380ca8c003de/8 ++++++++
RmCreateSession 2009/09/09 07:43:23.980 (RID=172.16.4.78 chan=7
EdgeIn=0.0.0.0)
SspServerTxSISC 2009/09/09 07:43:23.980 (RC=0 PN=1010)
+++++++ 380ca8c003df/9 ++++++++
SspServerRxSISR 2009/09/09 07:43:24.481 (SgId=1194 BW=3750000)
RmCreateSession 2009/09/09 07:43:24.482 (RID=172.16.4.78 chan=7
EdgeIn=0.0.0.0)
SspServerTxSISC 2009/09/09 07:43:24.482 (RC=0 PN=1011)
```

Use the following command to see data from a specific event log.

sspsistail /opt/usrm/EventLog/31Aug2009\_000000.txt

#### vermtail

This command gives the statistics of Channel changes and QAM operations. Use this tool to display real-time channel change operations or to evaluate an event log file.

The following are examples of both usages:

```
Real time log tail.
vermtail
+++++++++ 0000000400 ++++++++++
VermServerRxSETUP
                  2009/08/31 14:25:44.031 (Service-Group: 1194
bit_rate=3750000)
RmCreateSession
                   2009/08/31 14:25:44.032 (sess=001d09fa6301/547245
RID=172.16.4.78 chan=6
EdgeIn=0.0.0.0)
VermServerTxRESPONSE 2009/08/31 14:25:44.032 (RC= OK)
+++++++++ 000000804 +++++++++
VermServerRxSETUP 2009/08/31 14:25:46.038 (Service-Group: 1194
bit rate=3750000)
RmCreateSession 2009/08/31 14:25:46.038 (sess=001d09fa6301/547246
RID=172.16.4.78 chan=6
EdgeIn=0.0.0.0)
VermServerTxRESPONSE 2009/08/31 14:25:46.038 (RC= OK)
+++++++++ 0000000905 +++++++++
VermServerRxSETUP
                  2009/08/31 14:25:46.540 (Service-Group: 1194
bit_rate=3750000)
RmCreateSession
                   2009/08/31 14:25:46.540 (sess=001d09fa6301/547247
RID=172.16.4.78 chan=7
EdgeIn=0.0.0.0)
VermServerTxRESPONSE 2009/08/31 14:25:46.540 (RC= OK)
```

vermtail /opt/usrm/EventLog/31Aug2009 00000.txt

#### vodsessquery

This command, run from an SSH shell on the VSM, prints all log messages on VSM, ERM, and RCAS (optional) that pertain to a given VOD session. You can run the command **vodsessquery <sessionId>** from any directory. An example is shown below.

To include the RCAS in the result, add the option **-r** before the session ID. Optionally, you can specify a date if the date of the session of interest is known. This will shorten the time it takes to search for the session.

You can find the various usages for this command using the following command:

#### Vodsessquery -h.

[root@VSM-02 linux-tools]# vodsessquery 0002de0d2614/1302298896
Checking VSM Logs for session 0002de0d2614/1302298896
Checking ERM Logs on server 192.168.12.153 for session 0002de0d2614/1302298896
Warning: Permanently added '192.168.12.153' (RSA) to the list of known hosts.
Cherking RCAS Logs for session 00:02:DE:00:26:14/1302298896
Skinning RCASL og analysis, use the -r flag to enable
VSMI (Gc: 2011/hd/kg17/41/36.392 SchlidhServerBxClntSessSetunBen: Sthin=192.168.12.192 SthMar=0x0002de0d2614 Sesid=0002de0d2614/1302298896 Vodin=192.168.12.192 TID=1621114 casid=0
VSMI (0G: 2011/04/08 12/41:36 392 V045mClientRequest Stblin=192 168 12 192 StbMac=0x0002/de0d2614/302298886 Server=192 168 12 192 TID=1621114
VSMI (0G: 2011/04/08 12:41:36 392 VodSmServerSessionSetupIndication Sthip:192 168 12 192 SthMar=0x0002de0d2614 SetId=0002de0d2614/1302298896 Server=192 168 12 192 TID=340060454 Sessindex=39270
VSMI (0G: 2011/04/08 12:41:36 392 SenTenServerTxSessionSetupIndication Stblin=192 168 12 192 StbMac=0x0002de0d2614 SesId=0002de0d2614/1302298896 Vodin=192 168 12 192 TID=340060454
VSMI (0G: 2011/04/0817/41/36.411 StorTonServerRtsServerAddResRen Server:192.168.12.192.SGID=15.BW=3750000 Sesid=0002/de0d2614/1302298896 TID=116725992 Casid=3584 tsid=0.MPN=0
VSML0G: 2011/04/08 17:41:36 411 V045mBesourceRequest Secid=0002/e0d/2614/1302298896 SGID=15 RW=3750000 Casid=3584 edgeCalifol ength-0
VSMI (0G: 2011/04/08 12:41:36 411 DiscSursTxResRes spid=15 bw=3750000 tid=340060454 Sestel=0002de0d2614/1302298896
ERM153: 2011/04/08 17:41:36 412 DiscSvcsRxBesRes exid=15 hu=3750000 tid=340060454 usrm=192 168 12 22 Sexid=0002de0d2614/1302298896
ERMISE 2011/0//08 17:41:36 412 ERRWBAR SCIEFT BW-250000 Svc-Demand (AS-2584 Secid-0002/em4/5/1/120229886
Emitists 2011/01/08 17 4130-424 Interferences and a State 1970 Section 2012 Section
Emitis: 001/01/01/01/7410-05 /1/18/05/04/54/12/001/06/04/12/05/04/04/05/04/12/16/0
Emitist 2011/01/08/17/41/-06/41/Emiting/education
Emilia 2017 04/00 17 4130-424 milling degume-section (primo)-1221000-12/00/00/2017 04/00/2017/1302230000
Enviruos 2011/04/00 17/4130424 mitchines/schure-deteining/printing/nut-azz1004.n/i/0-21133276,85304-002214000244(13023050) USMI 06: 10/11/04/00 17/4132475 Directore/Dure-from of extra response for a constraint of a constra
V3mC04. 2011/04/09 17:41-30:425 / Discovstantescullinstatios-success(0);39(0-12);0-2);0000;110-300000439;45:103111-12;2106.12:135;35:310-00020002014/1302236690
V3mC04. 2011/04/001743-0042740001114520000014460423-00001145200000041-000000000000000000000000000000
V3mC04. 2011/04/00 1741-30425 35P1(352140) 110-110/2372/34441102750000,1510-12025000000000000000000000000000000
V3mCOV.2011/04/00 1741-30425 350 FL950VEIN35EVEI-35535EU0PRES/JSEVEI-3252.000 AV4000045/HE39-0,35510-00020E00214/10/223005/JJIVAE00404EI-03 VSMICOV.2011/04/00 1741-30425 40655000560000000000000000000000000000
V3mCOV. 2011/04/00 174.30422 V003m3erve13ess3et0pmesp, no-5400004-94,resp-0-2580-40022e014, 3302230000, Exgectaminotengin-04,piivate02461614/200308986 Eriorta.Datal.one65 covid=2014.000004-94,resp-0-2580-40022e014, 3302230000, Exgectaminotengin-04,piivate0246161/200308986 Eriorta.Datal.one65 covid=2014.000004-94,resp-0-2580-40022e014, 3302230000, Exgectaminotengin-04,piivate0246161/200308986 Eriorta.Datal.one65 covid=2014.00004-94,resp-0-2580-40022e014, 3302230000, Exgectaminotengin-04,piivate0246161/200308986 Eriorta.Datal.one65 covid=2014.00004-94,resp-0-2580-40022e014, 3302230000, Exgectaminotengin-04,piivate0246161/200308986 Eriorta.Datal.one65 covid=2014.00004-94,resp-0-2580-40022e014, 33022300000 Eriorta.Datal.one65 covid=2014.00004-94,resp-0-2580-40022e014, 33022000000 Eriorta.Datal.one65 covid=2014.00004-94,resp-0-2580-40022e014, 3302200000 Eriorta.Datal.one65 covid=2014.00004-94,resp-0-2580-40022e014, 33022000000 Eriorta.Datal.one65 covid=2014.00004-94,resp-0-2580-40022e014, 33022000000 Eriorta.Datal.one65 covid=2014.00004-94,resp-0-2580-40004-94,resp-0-2580-40004-94,resp-0-2580-40004-94,resp-0-2580-40004-94,resp-0-2580-40004-94,resp-0-2580-4004-94,resp-0-2580-4004-94,resp-0-2580-4004-94,resp-0-2580-
V3mC04.2011/0/10/19/174.30426/33p0/0J3444444444533p0/0J344444444444444444444444444444444444
Envirus. 2011/04/00 1741.30-22 0 http://doi.org/10.1011/04/01.3011/04/01/04/04/04/04/04/04/04/04/04/04/04/04/04/
Envirus: 2011/04/00 17/41:30-420 https://www.anvirus.com/envirus/anvirus
ENVIDS: 2011/04/00 1/41:00.420 DISCINCINKESCON;SIGUESSUCISSUCIES(S)(0):010-010-010-010-010-010-010-010-010-010
ERM 133: 2011/04/00 1/41:30-420 MIICH24(25553)0(1);251(I=00022(20020)A(1));152(250050);MIICH21/2:104-6);MIINT=37, J0003(2000);(202111/2:1/2:10-2);J0003(2000);(202111/2:10);J0003(2000);(202111/2:10);J0003(2000);J0003(20
ENVID3: 2011/04/00 1/41:30-420 MICHIOQUEUC,UIIIC-LI44(4526550(1),IUI-172.104-6,QUEUCDEUII-12550(-00020E002014/1302298890,CH8I0=87,MEN=3730000,QDA=0.0.0.0,UDP=22/30
Erwitabi 20/08/1741:30-420 MilleSouticeReady,Salus=0,5estic=V00204000214(1302206570
ERW135: 2011/04/00 1/41:30-420 MTC/INDEXEQUIDE-DESESSIOI,RUE-1/2.10-4.0, (10=340000-59,5es)1=00/22000204/130/2230650,CHall0=07,JMPN=537,BWP=53
EXMIDS: 2011/04/001741:30-420 AMIC/INDUCUESS,CINDEL/240-482/ESSION,MDE1/210-482/ESSION/UD1/2210-482/ESSION/UD1/22104-82/ESSION/UD1
VSMLOG: 2011/04/08 1742:17.025 Sp0dpSerVerkxClientKeleasekeduest, Client=152.058, 12.152, 110=116/26332, Secia=0002de002014/1302298896, PrivateDataLen=0
VSMLOG: 2011/04/08 1742:17.025 V035MCIEINTREE38EREQUEST, LIENT=192.165.12.192, 110=116726392, Rea30n=0,5e510=00020e0d2614/1302296896
VSMLUG: 2011/04/08 1/42/17.025 V005mkeleasesession,Sesta=000/20e002614/130/2298896;Sessionindex=39270
VSMLOG: 2017/04/08 17:42:17.025 DiscSvc51xRelReq,1D=340062230,SesId=0002de0d2614/1302298896,retryCount=3,ermip=192.168.12.153
VSMLOG: 2017/04/08 17:42:17.025 VodSmClientReleaseContirm,Client=192.168.12.192,1ID=116726392,Resp=0,Sesid=0002de0d2614/1302298896
VSMLOG: 2017/04/08 17/42:17.025 SspUdpServer1xClientReleaseContirm, 1ID=116726392, Resp=0, Client=192.168.12.192, SesId=0002de0d2614/1302298896
VSMLOG: 2011/04/08 17:42:17.025 VodSmServerReleaseIndication,Server=192.168.12.192,TID=116726392,Reason=0,SesId=0002de0d2614/1302298896
VSMLOG: 2017/04/08 17/42:17.025 SpTcpServer1xServerReleaseIndication,Server=192.168.12.192,TID=116726392,SesId=0002de002614/1302298896,reason=0,PrivateDataLength=0
VSMLOG: 2011/04/08 17/42:17.025 DiscSvcsRxRelCont,status=success(0),ermip=192.168.12.154,Sesid=0002de0d2614/1302298896
ERM153: 2011/04/08 17:42:17.026 DiscSvcsRxRelReq,sesId=0002ae0d2614/1302298896,retryCount=3,srcip=192.168.12.216
ERM153: 2011/04/08 17:42:17.026 RmSessionRelease,RID=172.16.4.8,Sesid=0002de0d2614/1302298896,chan0=87
ERM153: 2011/04/08 17:42:17:026 RmCmdQueue,Cmd=DeleteSession,RID=172:16:4.8,queueDepth=2,SesId=0002de0d2614/1302298896,chan0=87
ERM153: 2011/04/08 17:42:17:026 DiscSvc5TxReiCont,status=success[0],User=192.168.12.222,SesId=0002de0d2614/1302298896
ERM153: 2011/04/08 17:42:17.026 RmCmdExec,Cmd=DeleteSession,RID=172.16.4.8,Tid=211533178,SesId=0002de0d2614/1302298896,chan0=87
ERMIS3: 2011/04/08 17:42:17:035 RmCmdSuccess,Cmd=DeleteSession,RiD=172.16.4.8,CmdTime=8ms,Sesid=0002de0d2614/1302298896,chan0=87,Tid=211533178
For further analysis, check the following logfiles on the appropriate servers:
VSMLOG: /opt/usrm/EventLog/08Apr2011_000006.txt
ERMLOG: /opt/usrm/EventLog/08Apr2011_000000.txt on 192.168.12.153

RCSLOG: on 192.168.6.1

## **Appendix B: Policy**

The simple video policy server that existed in prior versions of USRM 2.x. has been enhanced in USRM 2.1.4 with a new configuration setting in which the mode is explicitly configured. The modes are ChannelBased, GuaranteeAll, and GuaranteeHighPri.

You can enter and configure applications that will be governed by USRM Policy on the Resource manager under the ResourceManager.Application Policy tab. You can specify up to 16 separate applications for each USRM. For each application, you can also specify the minimum and maximum allowable bandwidth.

ResourceManager.Application Policy										
Priority	Applications	MinimumBandwidth (%)	MaximumBandwidth (%)							
1	VOD	50	100							
2	SDV	50	100							
Commit Changes Reload Logout										
Search	Create CSV	]								

Once the applications are configured, you can specify the policy mode on the ResourceManager.Configuration page. You can choose one of three Policy Modes: Channel Based, Guarantee All, and Guarantee Higher Priority.

PolicyMode	GuaranteeAl 🗨
GbePortProtection	Guarantee All
ResourceDeviceSelectMode	ChannelBased

**ChannelBased** mode indicates that a QAM channel is configured for a specific application. Channel based should be used for siloed applications (i.e., specific TSIDs for VOD, specific TSIDs for SDV). If a TSID is not specified for a particular application, any application can use it on a first-come, first-serve basis. If Channel Based Mode is selected, the Minimum and Maximum Bandwidth settings on the Application Policy page are not necessary, and are ignored if they are set.

TSIDs are specified for each application on the ResourceManager.QAMs.QAM xyz.QAM Channels page. The example below shows a GQAM whose first carrier on output Port 1 is VOD-only, whose fourth carrier is SDV-only and whose second and third carrier can be used by either application.

GQAM03	GQAM03.QAM Channels											
Port.Chan	Frequency (MHz)	ModulationFormat	TSID	InterleaveDepth	Mute	Admin State			Application	ReservedBandwidth (Mbps)	AllocatedBandwidth (Mbps)	
1.1	285.000000	ITUB-QAM-256	10600	i-128-1A	Unmuted	InService •	•	vod		0.000000	37.564000	
1.2	291.000000	ITUB-QAM-256	10601	i-128-1A	Unmuted	InService -	•			0.000000	37.564000	
1.3	297.000000	ITUB-QAM-256	10602	i-128-1A	Unmuted	InService -	•			0.000000	37.564000	
1.4	303.000000	ITUB-QAM-256	10603	i-128-1A	Unmuted	InService -	,	sdv		0.000000	37.564000	

Use **GuaranteeAll** or **GuaranteeHighPri** when QAM sharing between applications, such as VOD and SDV is enabled. Applications are allocated a specific percentage of total bandwidth. A percentage of minimum bandwidth and maximum bandwidth is specified for each application. These percentages apply to the total amount of bandwidth available to the service group. If a QAM or other edge device is OutOfService or otherwise unavailable, the USRM applies the percentages to the total amount of bandwidth available at the time of the service request.

**GuaranteeAll** mode allows resource requests if all minimum bandwidth guarantee configurations can be satisfied.

**GuaranteeHighPri** mode allows resource requests if higher priority minimum bandwidth guarantee configurations are satisfied. The highest priority application (i.e., first in the list) will always get its requests satisfied, bandwidth permitting. Lower priority applications will then be satisfied if possible.

### **Appendix C: Spreadsheet Import and Export**

In USRM 2.1.4, two directories are created on the USRM in the /opt/usrm/ConfigFiles directory, either manually by the user, or automatically upon writing a file for the first time. The ERM resource directory is called Qams; the SDV offered programs directory is called Sdv.

On the webUI, the spreadsheet import functionality can be accessed at ResourceManager.Resource Backup for the ERM QAM Resources, and Applications.SdvSm.Programs Backup for the SDV Offered Programs.

esourceManager Activity Log	ResourceManager.Resource Backup									
Application Policy	DeviceBackupFilename	StuttgartQams_07Apr								
Discovery Services	DeviceBackupFileUpdate	Inactive 👻								
Hub Names	SendCmdsToDevice	No 👻								
NLS	DeleteDevices	Yes 👻								
Network Config	DeviceBackupFileDirectory	ConfigFiles/Qams								



With Resource Backup, you can create a CSV file of all QAMs on a given server by selecting **Write** from the DeviceBackupFileUpdate drop-down menu. This file is written to the /opt/usrm/ConfigFiles/Qams directory. To view this file in Excel spreadsheet format, copy the file to a computer and open it in Excel. An example for a GQAM is shown below.

				Virtual		Service			Applic				Applic				Applic				Appli	
Server	MgmtipAddr	GbePort	IpAddress	Address	RfPort	Group	Freq	TSID	ation	Usage	Freq	TSID	ation	Usage	Freq	TSID	ation	Usage	Freq	TSID	cation	Usage
Stuttgart	172.16.6.4	1	172.16.15.9		1	15	285	10600	vod	Enabled	291	10601		Enabled	297	10602		Enabled	303	10603	sdv	Enabled
					2	0	333	10604		Disabled	339	10605		Disabled	345	10606		Disabled	351	10607		Disabled
					3	0	525	10608		Disabled	531	10609		Disabled	537	10610		Disabled	543	10611		Disabled
					4	0	477	10612		Disabled	483	10613		Disabled	489	10614		Disabled	495	10615		Disabled

You can also read in a file that is located in the /opt/usrm/ConfigFiles/Qams directory and apply its settings by selecting **ReadApply** in the DeviceBackupFileUpdate drop-down menu. Prior to reading and applying a file's settings, you can preview the changes that will be made by selecting **Preview** from the drop-down menu. This causes the settings about to be changed to be printed to the Eventlog. You can then open an SSH session to the server and run **usrmlogtail**, filtering on ResourceBackupChange, to view these contents.

An example is shown below. In this case, the Admin States of the ports are being placed OutOfService.

usrmlogtail ResourceBackupChange

2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=PortTable.ServiceGroupId.1, Value=15 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.2.1, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=PortTable.ServiceGroupId.2, Value=0 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.2.2,Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.2.3, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=ChannelTable.AdminState.2.4,Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.2,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.3.1, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=PortTable.ServiceGroupId.3, Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.3.2, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.3.3, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.3.4, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.3,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.4.1, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=PortTable.ServiceGroupId.4, Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.4.2, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.4,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.4.3, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.4,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=ChannelTable.AdminState.4.4, Value=OutOfService 2011/04/08 16:12:30.524 ResourceBackupChange,Dev=GQAM03,Parm=PortTable.ServiceGroupId.4,Value=0 2011/04/08 16:12:30.524 ResourceBackupChange, Dev=GQAM03, Parm=PortTable.ServiceGroupId.4, Value=0

Setting SendCmdsToDevice to **Yes** causes the USRM to provision the QAM devices with the settings in the CSV file. This only works for RFGW-1 QAMs.

Setting DeleteDevices to **No** causes the USRM to leave existing QAM resources in place when reading a file (ReadApply) whether they are in the file being read or not. If DeleteDevices is set to Yes and the USRM sees a QAM device in the USRM database that is not in the file being read, it will delete that device from the USRM database.

Programs Backup is similar to Resource Backup. The selections for ProgramsBackupFileDirectory are the same as for ResourceBackupFileDirectory (Write, ReadApply, and Preview). DeleteProgramsOnApply behaves similarly to DeleteDevices.

ourceId	Name	ServiceGroup	Zone	SrcAddr1	SrcAddr2	SrcAddr3	DestAddr	Priority	B/W	Video	UdpPort	OfferState	AdminState
1216	HBO Comedy E							1				Dynamic	InService
				172.16.17.5	172.16.17.1	172.16.17.9	232.0.0.61		3.75	MPEG-2			InService
			4	172.16.17.5			232.1.1.16						InService
			5	172.16.17.9			232.2.2.16						InService
4032	SDV Cinemax HD2							1				Dynamic	InService
				172.16.17.1			232.0.1.32		15	MPEG-2	48304		InService
5056	Action Max 4							1				Dynamic	InService
				172.16.17.13			232.0.4.56		3.75	MPEG-2	48304		InService
1217	WMAX E							1				Dynamic	InService
				172.16.17.1	172.16.17.5	172.16.17.9	232.0.0.17		3.75	MPEG-2	48304		InService

# An example of the SDV Offered Programs table in Excel spreadsheet format is shown below.

# Appendix D: GQI v1.5 Requirements and Settings

At the time of this writing, the only QAM that supports GQI v1.5 is the Arris D5 QAM. Contact your Arris representative for details on how to enable or disable announce messaging.

### **USRM Settings**

- **1** Resource Manager "normal" logging mode will log success and failure announcements along with the source IP.
- 2 ResourceAdapter.GenericQamSrm "max" logging mode will give more details to the exact failure code(s).
- **3** Qam.Sessions page status column documents the source IP for a successful session create, or reports "failure" for an unsuccessful session create.

### Appendix E: VodSm Web Pages

Use the VOD Session Manager (VodSm) configuration page to set the Session In Progress (SIP) timers for Clients and Server as well as the timeout for waiting for a response to a VOD session request.

Use the SessionTimeout parameter to define a period of time that a session will be allowed to remain on a QAM before it is torn down due to a lack of SIPs.

Use the values for MpegProgram Low and High to define a range for VOD program numbers to help differentiate between SDV programs and VOD programs that may be built on a shared QAM.

Use the MaxVodLogFileSize field to limit the size of the created MSA log if the VodLogType parameter is set to Msa.

VodSm.Configuration									
AdminState	InService 🚽								
ClientSipTimeout	70	Minutes							
ServerSipTimeout	0	Minutes							
TransactionTimeout	3000	milliseconds							
SessionTimeout	8100	Seconds							
MpegProgramLow	100								
MpegProgramHigh	999								
UseClientCA	No 💌								
ReleaseRetryCount	3								
VodLogType	Msa 💌								
VodLogStatus	OK								
VodLogRecords	3959690								
MaxVodLogFileSize	20	Mbytes							
CurrentVodLogFile	/opt/msa/msa_logs/n	nsa-vsm-0-20110712-184218.log							
Commit Changes Reload Logout									

Use the Service Groups Bandwidth screen to get a snapshot of aggregate VOD BW usage for all service groups on this particular VSM at any point in time.

VodSm.Service Groups Bandwidth										
SgIndex	ServiceGroup	ErmlpAddress	ActiveBw (Mbps)							
1	9	10.16.4.114	123.750							
2	4	10.16.4.114	135.000							
Commit Changes Reload Logout										
Search Create CSV										

The Active Sessions screen displays a listing very similar to those on an SDV system showing all active VOD sessions. It shows the Session ID, Bandwidth used, Start Time for the session, Client IP Address, and the IP address of the BMS server servicing the session. There are also columns for Service group, Last Client SIP, and Last Server SIP.

Vod Sm.	VodSm.Active Sessions													
Session	State	SessionId	AdminState	Bandwidth (Mbps)	StartTime	ClientAddress	ServerAddress	ErmAddress	ServiceGroupId	LastClientSIP	LastServerSIP			
1021	Active	001bd7641238/1310562231	InService -	3.750000	2011/07/13 09:03:51	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:51	2011/07/13 09:03:51			
3911	Active	001bd763795e/1310562235	InService 💌	3.750000	2011/07/13 09:03:55	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:55	2011/07/13 09:03:55			
5101	Active	001bd763fe15/1310562231	InService 💌	3.750000	2011/07/13 09:03:51	192.168.12.140	192.168.12.140	10.16.4.114	4	2011/07/13 09:03:51	2011/07/13 09:03:51			
9351	Active	001bd76378d4/1310562231	InService 👻	3.750000	2011/07/13 09:03:51	192.168.12.140	192.168.12.140	10.16.4.114	4	2011/07/13 09:03:51	2011/07/13 09:03:51			
10201	Active	001bd7641ab1/1310562233	InService 💌	3.750000	2011/07/13 09:03:53	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:53	2011/07/13 09:03:53			
10711	Active	001bd765997c/1310562235	InService 💌	3.750000	2011/07/13 09:03:55	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:55	2011/07/13 09:03:55			
11901	Active	001bd7641b1c/1310562235	InService 👻	3.750000	2011/07/13 09:03:55	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:55	2011/07/13 09:03:55			
12411	Active	001bd763fddc/1310562236	InService 💌	3.750000	2011/07/13 09:03:56	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:56	2011/07/13 09:03:56			
13431	Active	001bd7659a61/1310562235	InService 💌	3.750000	2011/07/13 09:03:55	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:55	2011/07/13 09:03:55			
14451	Active	001bd763fd84/1310562236	InService 💌	3.750000	2011/07/13 09:03:56	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:56	2011/07/13 09:03:56			
15131	Active	001bd763fde1/1310562236	InService 💌	3.750000	2011/07/13 09:03:56	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:56	2011/07/13 09:03:56			
15471	Active	001bd765a19f/1310562231	InService 💌	3.750000	2011/07/13 09:03:51	192.168.12.140	192.168.12.140	10.16.4.114	4	2011/07/13 09:03:51	2011/07/13 09:03:51			
15981	Active	001bd7659ad5/1310562234	InService 👻	3.750000	2011/07/13 09:03:54	192.168.12.140	192.168.12.140	10.16.4.114	4	2011/07/13 09:03:55	2011/07/13 09:03:55			
16321	Active	001bd763fe58/1310562233	InService 💌	3.750000	2011/07/13 09:03:53	192.168.12.140	192.168.12.140	10.16.4.114	9	2011/07/13 09:03:53	2011/07/13 09:03:53			

# Appendix F: Conversion from CaMgrDNCS to CaManagerPK

**Important:** Perform this procedure only when upgrading from USRM Release 2.1.0 or 2.1.1 to Release 2.1.3-7 or above.

- **1** Terminate the USRM and its backup.
- 2 Rename the CaMgrDncs persistdata files.
- **3** Open an SSH session to the Primary Server and go to the /opt/usrm/persistdata directory.
- 4 Type the following to get a list of existing CA Manager files: [persistdata]# ls -ltr | grep CaMgrDncs
- 5 A (list of) file(s) will be returned with the following format, where xyz is the name assigned to the particular CA Manager: CaMgrDncs.xyz.bin
- 6 Change the file name as shown below. [persistdata] mv CaMgrDncs.xyz.bin CaManagerPk.xyz.bin
- 7 Make the change for each CA Manager on the USRM, if more than one exists.

**Note:** See also the sections in *Installation and Upgrade Guidelines* (on page 4) for details on upgrading from releases prior to 2.1.4.

# **For Information**

### If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

# יו|ייו|יי כוsco

Cisco Systems, Inc. 5030 Sugarloaf Parkway, Box 465447 Lawrenceville, GA 30042 678 277-1120 800 722-2009 www.cisco.com

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to the this URL: **www.cisco.com/go/trademarks**. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) Product and service availability are subject to change without notice. © 2012 Cisco and/or its affiliates. All rights reserved.

August 2012 Printed in USA

Part Number 4035984 Rev A