



Dialogic® PowerMedia™ XMS

Installation and Configuration Guide

Copyright and Legal Notice

Copyright © 2012-2019 Dialogic Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Corporation at the address provided below.

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see <http://www.dialogic.com/company/terms-of-use.aspx> for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 3300 Boulevard de la Côte-Vertu, Suite 112, Montreal, Quebec, Canada H4R 1P8.

Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.

Dialogic, Dialogic Pro, DialogicOne, Dialogic Buzz, Brooktrout, BorderNet, PowerMedia, PowerVille, PowerNova, ControlSwitch, I-Gate, Veraz, Cantata, TruFax, and NMS Communications, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 3300 Boulevard de la Côte-Vertu, Suite 112, Montreal, Quebec, Canada H4R 1P8. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Table of Contents

1. Welcome	15
Related Information	15
2. PowerMedia XMS Installation	16
Installing PowerMedia XMS	16
System Requirements	16
Reference Configurations	17
Supported Virtual Machines	18
Cloud Environments	18
Available Application Technologies	19
Supported Web Browsers	19
SIP Softphone	19
PowerMedia XMS Installation Package Policy	20
ISO Method	21
Getting and Burning the .ISO File	21
Bootting the System from the DVD	22
Setting the IP Address	22
Completing the Installation	23
RPM Method	23
Reserved Ports	25
RPM Installation and Script Options	26
3. PowerMedia XMS Admin Console	28
Using PowerMedia XMS Admin Console	28
CentOS HTTPS Setup for Console Use	28
Guidelines for Installing a Permanent Security Certificate	30
Console Login	30
4. PowerMedia XMS Configuration	32
Configuring PowerMedia XMS	32
System	33
General	33
Services	34
Time	36
Backup/Restore	37
Upgrade	38
NFS Mount Points	39
Maintenance	40
Account Manager	40
Diagnostics	43
Audit Logs	46
Network	47
Interface Configuration	48
DNS Configuration	49
NAT Configuration	50
License	51
License Manager	51
Protocol	65
SIP	65
RTP	72
Codecs	76
Profiles	76

Settings	80
MSML.....	81
MSML Configuration	81
MSML Advanced Configuration.....	85
VXML	86
VXML Interpreter Configuration	86
VXML Application Configuration	91
RESTful API	92
RESTful Media API	93
RESTful API Credentials.....	94
NETANN	95
Routing	95
HTTP Client.....	97
Speech.....	98
Providers	98
Profiles.....	101
MSRP	103
Fax	104
Tones	105
Basic Tone Definitions	106
CPA Tone Definitions	108
CPA Profiles	110
Media.....	113
Media Configuration	113
Media Management.....	115
CDR.....	117
CDR Query	117
CDR Configuration	121
SNMP.....	125
Configuration	125
High Threshold Configuration	129
Reports	131
Monitor	134
Dashboard	135
Call Groups.....	136
Graph	136
Options	142
Secure Storage	142
Options	145
Downloads.....	146
5. PowerMedia XMS Troubleshooting	148
PowerMedia XMS Log Files	148
Retrieving PowerMedia XMS Logs.....	148
Linux RTC Device Verification.....	149
Virtual Memory Increase between Application Restarts	149
Contacting Dialogic Technical Services and Support	149
6. XMSTool RESTful Utility.....	150
XMSTool RESTful Utility.....	150
Call Control Models	150
Prerequisites	151
Starting XMSTool.....	151
XMSTool Utility Modes	152

Demo/Simple Mode	152
Accessing XMSTool using CLI	153
Advanced Mode.....	154
Basic Operation and Commands	157
Receiving an Inbound Call	157
Making an Outbound Call.....	158
Playing a File into a Call	158
Establishing a Conference	159
Additional XMSTool Commands	161
Using XMSTool to Record Macros/Demos	163
7. Third Party ASR and TTS Engine Notes.....	165
Nuance	165
8. Appendix A: ISO Method for Remote Installation.....	167
VMware ESXi	167
9. Appendix B: SNMP.....	168
List of Standard MIBs.....	168
List of Standard Traps	168
Enterprise (Proprietary) MIB	169
Enterprise (Proprietary) Traps	169
Enterprise (Proprietary) Variables	173
10. Appendix C: CDR	175
List of CDR Fields.....	176
CDR Management.....	179
Naming Convention of CDR Files.....	182
Format of CDR files.....	182
CDR-Related SNMP Traps and Their Meaning.....	183
11. Appendix D: Sample Use Cases	184
Script Location	184
Start/Stop Service and Application	184
Check Status of Service	184
Check/Install License	185
MSML Configuration.....	186
Tone Configuration	187
Codec Configuration.....	188
12. Appendix E: SIP OPTIONS Ping Processing	192
13. Appendix F: Dashboard Counters	193
CDR Server.....	193
Fax Service.....	194
HTTP Client.....	195
MRCP Client	196
MSML Server.....	198
MSRP Server.....	200
NETANN Server	201
RESTful API Server	201
VXML Server.....	202
XMS Server.....	203
XMS System	206

Revision History

Revision	Release Date	Notes
05-2704-020 (Updated)	October 2019	<p>RPM Method: Added a note about minimum version of glibc and gperftools.</p> <p>Fax: Updated the section.</p> <p>CDR: Updated the CDR Configuration section.</p> <p>Downloads: Updated the section.</p>
05-2704-020 (Updated)	July 2019	<p>RPM Method: Added a note in the RPM Installation and Script Options section.</p> <p>License: Updated the License Types and License Configuration sections.</p>
05-2704-020 (Updated)	May 2019	<p>RPM Method: Added a note about supported repositories.</p> <p>MSML: Updated the MSML Advanced Configuration section.</p> <p>Protocol: Updated the SIP section.</p>
05-2704-020	March 2019	<p>Updates to support PowerMedia XMS Release 4.0.</p> <p>System Requirements: Updated the Operating System section, added the Reference Configurations section, and updated the Supported Virtual Machines section.</p> <p>RPM Method: Added the Advanced Options section to RPM Installation and Script Options.</p> <p>System: Updated the Diagnostics section.</p> <p>License: Updated the License Manager section.</p> <p>MSML: Updated the MSML Configuration section.</p> <p>Speech: Added the section.</p> <p>HTTP Client: Updated the section.</p> <p>Fax: Updated the section.</p> <p>NETANN: Updated the section.</p> <p>VXML: Updated the VXML Interpreter Configuration section.</p> <p>RESTful API: Updated the section.</p> <p>Protocol: Updated the SIP section.</p> <p>Codecs: Updated the Profiles section.</p> <p>Monitor: Updated the Graph section.</p> <p>SNMP: Updated the High Threshold Configuration section.</p> <p>CDR: Updated the CDR Configuration section.</p>

Revision	Release Date	Notes
		<p>Reports: Updated the section.</p> <p>Secure Storage: Added the section.</p> <p>Appendix B: SNMP: Updated the Enterprise (Proprietary) Traps section.</p> <p>Appendix E: SIP OPTIONS Ping Processing: Updated the section.</p>
05-2704-019 (Updated)	February 2019	Media : Updated the Media Configuration section.
05-2704-019 (Updated)	October 2018	Options : Added the Server Mode section.
05-2704-019 (Updated)	September 2018	<p>MRCP Client: Updated the Speech Server Configuration section.</p> <p>Codecs: Updated the Audio Codecs section.</p> <p>Media: Updated the Media Configuration section.</p> <p>Downloads: Updated the section.</p> <p>PowerMedia XMS Troubleshooting: Updated the section.</p>
05-2704-019 (Updated)	May 2018	<p>Browser Support for WebRTC: Updated the section.</p> <p>MSML: Updated the MSML Advanced Configuration section.</p> <p>Appendix B: SNMP: Updated the section.</p> <p>Appendix F: Dashboard Counters: Updated the section.</p>
05-2704-019 (Updated)	February 2018	<p>SNMP: Updated the High Threshold Configuration section.</p> <p>PowerMedia XMS Troubleshooting: Updated the PowerMedia XMS Log Files section.</p>
05-2704-019 (Updated)	December 2017	<p>System: Updated the Services section.</p> <p>Media: Updated the Media Configuration section and added the Manage Undelivered Recordings section.</p>
05-2704-019 (Updated)	November 2017	<p>Network: Updated the NAT Configuration section.</p> <p>Appendix C: CDR: Updated the List of CDR Fields section.</p>
05-2704-019	October 2017	<p>Updates to support PowerMedia XMS Release 3.5.</p> <p>System Requirements: Added note in the Operating System section.</p> <p>System: Updated the Account Manager section and added the Set the Password Policy section.</p>

Revision	Release Date	Notes
		<p>License: Updated the section.</p> <p>Codecs: Updated the section.</p> <p>Media: Updated the Media Management section.</p> <p>Monitor: Removed the Graphs and Configuration sections and added the Graph section.</p> <p>Reports: Added the section.</p> <p>Appendix B: SNMP: Updated the Enterprise (Proprietary) Traps section.</p> <p>Appendix F: Dashboard Counters: Added the section.</p>
05-2704-018 (Updated)	August 2017	<p>System Requirements: Added httpd requirement and note in the Operating System section.</p> <p>PowerMedia XMS Admin Console: Updated the Guidelines for Installing a Permanent Security Certificate section.</p> <p>MRCP Client: Updated the Speech Server Configuration section.</p> <p>Codecs: Updated the Audio and Video sections.</p>
05-2704-018	June 2017	<p>Updates to support PowerMedia XMS Release 3.4.</p> <p>System: Updated the NFS Mount Points section.</p>
05-2704-017 (Updated)	June 2017	<p>System: Updated the OS Services in the Services section.</p>
05-2704-017	May 2017	<p>Updates to support PowerMedia XMS Release 3.3.</p> <p>RPM Method: Updated the Reserved Ports section.</p> <p>Tones: Added the CPA Tone Definitions and CPA Profiles sections.</p>
05-2704-016 (Updated)	February 2017	<p>MSML: Updated the MSML Advanced Configuration section with Parallel Processing of Overlapped INFO parameter.</p>
05-2704-016	November 2016	<p>Updates to support PowerMedia XMS Release 3.2.</p> <p>RPM Method: Added a note about Reverse Path Filtering.</p> <p>System:</p> <ul style="list-style-type: none"> • Added the OS Services in the Services section. • Removed a note from the Services section regarding XMS returning a 486 Busy Here message when the console is starting. • Added a note regarding the proper usage of the Backup/Restore feature.

Revision	Release Date	Notes
		<ul style="list-style-type: none"> Added a note to Restore Backup section regarding what settings are not saved or restored. Added the NFS Mount Points section. Updated the Diagnostics section. Updated the Audit Logs section. <p>License: Updated the section.</p> <p>MSML: Updated the section.</p> <p>MSRP: Updated the section.</p> <p>Protocol: Updated the SIP section. Added the RTP Timeout section.</p> <p>Codecs: Added the HMP Bulk Delay Settings section.</p> <p>Monitor: Updated the Graphs section with SIP and HTTP meters to plot. Updated the descriptions of the meters in the Graphs section.</p> <p>SNMP: Updated the High Threshold Configuration section.</p> <p>CDR: Added the Manage Columns in the CDR Query section. Updated the CDR Configuration section.</p> <p>Appendix B: SNMP: Updated the <code>xmsLicenseHighThreshMet</code> and <code>xmsServiceStatusChanged</code> trap types.</p> <p>Appendix E: SIP OPTIONS Ping Processing: Added the section.</p>
05-2704-015	August 2016	<p>Supported Virtual Machines: Added support for ESXi 6.x.</p> <p>Monitor: Updated the Graphs section to add the SIP meters.</p>
05-2704-014 (Updated)	June 2016	<p>RPM Method: Added a note regarding versions of JavaScript that are compatible with VXML.</p>
05-2704-014 (Updated)	May 2016	<p>Supported Virtual Machines: Added the recommended number of VMs.</p> <p>PowerMedia XMS Configuration: Updated the connection timeout parameter descriptions.</p> <p>Appendix B: SNMP: Updated the Enterprise (proprietary) Traps section.</p>
05-2704-014	March 2016	<p>Updates to support PowerMedia XMS Release 3.1.</p> <p>System Requirements: Updated the operating system requirements.</p> <p>PowerMedia XMS Installation Package Policy: Updated</p>

Revision	Release Date	Notes
		<p>the section.</p> <p>ISO Method: Updated the section.</p> <p>RPM Method: Added a note for enabling the libtiff-tools package repository.</p> <p>System:</p> <ul style="list-style-type: none"> Removed the Mode section. Upgrade: Added a note about the location of the xms_install.log file. Removed the NFS Mount Points section. <p>Network: Removed the Proxy Configuration section.</p> <p>HTTP Client: Added the DNS Cache Timeout parameter.</p> <p>VXML: Updated the section.</p> <p>Protocol:</p> <ul style="list-style-type: none"> Updated the Session Timeout parameter and added the Enable User Agent parameter in the SIP section. Added the Media Route Profiles section in the RTP section for multi-NIC support. <p>CDR: Updated the section.</p> <p>PowerMedia XMS Troubleshooting:</p> <ul style="list-style-type: none"> Updated the RemoteRtftool section and added the Other Parmes parameter. Added Virtual Memory Increase between Application Restarts section. <p>Appendix A: ISO Method for Remote Installation: Added the section.</p> <p>Appendix D: Sample Use Cases: Moved content to appendix.</p>
05-2704-013	October 2015	<p>Updates to support PowerMedia XMS Release 3.0.</p> <p>Welcome: Updated the Related Information.</p> <p>Installing PowerMedia XMS: Updated the System Requirements and Reserved Ports.</p> <p>PowerMedia XMS Admin Console: Updated the OpenSSL version in the Guidelines for Installing a Permanent Security Certificate section.</p> <p>License: Added information about activating a license using the License Node ID.</p> <p>MSML: Updated the MSML Configuration and MSML Advanced Configuration sections.</p> <p>VXML: Added a note to the VXML Application Configuration section.</p>

Revision	Release Date	Notes
		<p>Tones: Added the CPA Tone Definitions section.</p> <p>Fax: Added the Fax section.</p> <p>Monitor: Updated the Monitor section.</p> <p>SNMP: Updated the High Threshold Configuration section.</p> <p>CDR: Added the CDR Query section.</p> <p>Appendix C: CDR: Added new call data to List of CDR Fields table. Updated sample CDR in Format of CDR Files section.</p>
05-2704-012 (Updated)	June 2015	<p>System: Added details for filter pattern to Audit Logs page.</p> <p>Network: Added details for Remote NAT Traversal parameter to NAT Configuration page.</p> <p>Protocol: Added Key Rotation parameter to RTP page.</p>
05-2704-012	February 2015	<p>Updates to support PowerMedia XMS Release 2.4.</p> <p>Installing PowerMedia XMS: Updated list of supported processors.</p> <p>System: Added viewer option to Account Manager page. Added new Audit Logs page.</p> <p>Network: Added new Proxy Configuration page.</p> <p>License: Updated to include MRB in the licensed features.</p> <p>HTTP Client: Added Low Speed Threshold and Low Speed Timeout parameters to HTTP Client Configuration page.</p> <p>MSRP: Removed Max Sessions parameter from MSRP Configuration page.</p> <p>Protocol: Added Enable SIP Precondition parameter to SIP page. Added SRTP parameters to RTP page.</p> <p>Codecs: Added Video Encoder Sharing parameter to Video page.</p> <p>Monitor: Updated Graphs page with different views for meters. Added new Configuration page.</p> <p>SNMP: Added CDR Disk Usage parameter to High Threshold Configuration page.</p> <p>CDR: Added new section.</p> <p>Options: Added WebGUI Session Timeout parameter to Web Console Options page.</p> <p>CLI Command Scripts: Added new section.</p> <p>Appendix B: SNMP: Added new traps to Enterprise (proprietary) Traps table. Added new variables to</p>

Revision	Release Date	Notes
		Enterprise (proprietary) Variables table. Appendix C: CDR : Added new section.
05-2704-011	January 2015	<p>PowerMedia XMS Installation Package Policy: Added new section.</p> <p>RPM Method: Added table of reserved ports.</p> <p>System: Added note about CPU load to General page. Added note about call attempts to Services page.</p> <p>Network: Added Remote NAT Traversal parameter to NAT Configuration page.</p> <p>MSML: Removed Advanced Digit Pattern parameter from MSML Advanced Configuration page.</p>
05-2704-010	October 2014	<p>Updates to support PowerMedia XMS Release 2.3.</p> <p>Login to the Console: Added details for using admin login.</p> <p>System: Added new parameters to Diagnostics page.</p> <p>Network: Updated with details on IPv6.</p> <p>MSML: Updated with details on RTP and RTCP. Updated DTMF Detection Mode options. Updated value options under Media Mode parameter.</p> <p>MRCP Client: Updated parameters. Added note describing support for v1 and v2 speech servers.</p> <p>NETANN: Added Max Active Talkers parameter.</p> <p>VXML: Changed OutOfBand drop-down list option to SIP INFO for Default Input Mode parameter. Added new Default Timeout Settings (seconds) and Default Locale Settings tables.</p> <p>MSRP: Added new section.</p> <p>Protocol: Updated with details on IPv6. Updated with details on Type of Service parameter.</p> <p>Routing: Added cross-reference to App ID section on RESTful API page.</p> <p>Monitor: Changed Meters section name to Monitor. Added new Call Groups and Graphs pages.</p> <p>SNMP: Added new section.</p> <p>Appendix B: SNMP: Added new section.</p>
05-2704-009	May 2014	<p>Installing PowerMedia XMS: Updated list of supported operating systems and added new section for supported virtual machines.</p> <p>RPM Method: Added note that SELinux is not supported and should be disabled.</p>

Revision	Release Date	Notes
		<p>MRCP Client: Updated note about MRCP sessions.</p> <p>Third Party ASR and TTS Engine Notes: Added new section.</p>
05-2704-008	March 2014	<p>Updates to support PowerMedia XMS Release 2.2.</p> <p>System: Updated with Graceful Shutdown on Services page.</p> <p>Network: Added new NAT Configuration page.</p> <p>NETANN: Added new section.</p> <p>Monitor: Added new section.</p> <p>Troubleshooting PowerMedia XMS: Updated with Linux RTC Device Verification section.</p>
05-2704-007	January 2014	<p>System: Added new Diagnostics page.</p> <p>Routing: Updated with details on regular expressions.</p> <p>Media: Updated with details on absolute paths.</p>
05-2704-006	October 2013	<p>Updates to support PowerMedia XMS Release 2.1.</p> <p>Installing PowerMedia XMS: Added new sections for WebRTC.</p> <p>System: Updated Services and Account Manager pages.</p> <p>VXML: Added new parameters.</p> <p>MSML: Updated parameters.</p>
05-2704-005	March 2013	<p>System: Updated with details on Time page.</p> <p>VXML: Updated with clarification that VXML is audio-only.</p>
05-2704-004	February 2013	<p>Updates to support PowerMedia XMS Release 2.0.</p> <p>Configuring PowerMedia XMS: Added new MRCP Client, VXML, RESTful API, and HTTP Client menus. Removed the Diagnostics menu.</p> <p>System: Added new Upgrade and NFS Mount Points pages.</p> <p>MRCP Client: Added new section.</p> <p>HTTP Client: Added new section.</p> <p>VXML: Added new section.</p> <p>MSML: Added new configuration parameters.</p> <p>RESTful API: Added new section.</p> <p>Troubleshooting PowerMedia XMS: Updated with log file details for troubleshooting.</p> <p>XMSTool RESTful Utility: Updated download instructions</p>

Revision	Release Date	Notes
		in the Starting XMSTool section. Removed start command from the Demo/Simple Mode section. Updated the Basic Operation and Commands and Additional XMSTool Commands sections.
05-2704-003	August 2012	RPM Method : Added information about the perl-core package. XMSTool RESTful Utility : Updated the Starting XMSTool and Demo/Simple Mode sections.
05-2704-002	July 2012	Updates to support PowerMedia XMS Release 1.1. This is a 64-bit only release. RPM Method : Added new section. Configuring PowerMedia XMS : Added new Time and Backup/Restore pages to Systems menu. Added new Network menu. Renamed the Interface menu to Protocol. XMSTool RESTful Utility : Added new section.
05-2704-001	March 2012	Initial release of this document.
Last modified: October 2019		

Refer to www.dialogic.com for product updates and for information about support policies, warranty information, and service offerings.

1. Welcome

This Installation and Configuration Guide provides information about installing, configuring, administering, and maintaining the Dialogic® PowerMedia™ Extended Media Server (also referred to herein as "PowerMedia XMS" or "XMS").

Refer to the *Dialogic® PowerMedia™ XMS WebRTC Demo Guide* to run WebRTC demos with PowerMedia XMS.

Related Information

See the following for additional information:

- PowerMedia XMS 4.0 documentation at <http://www.dialogic.com/manuals/xms/xms4-0>.

2. PowerMedia XMS Installation

Installing PowerMedia XMS

This section provides the steps required to successfully install PowerMedia XMS.

The following instructions pertain to the PowerMedia XMS download package, labeled as *PowerMedia-4.0.xxxx-x86_64.iso* and *dialogic_xms_4.0.xxxx.tgz* where "xxxx" indicates the version number.

There are two installation methods available: [ISO Method](#) and [RPM Method](#) (used for a CentOS or RHEL installation).

System Requirements

Regardless of the installation method used, the **minimum** and **recommended** system requirements are as follows:

Item	Requirement
Hardware	Intel Architecture-based server
Operating System	64-bit variants of the following operating systems are supported: <ul style="list-style-type: none">• CentOS 7.x and 6.4 (or later)• Red Hat Enterprise Linux (RHEL) 7.x and 6.4 (or later)• Oracle Linux 6.4• Oracle Linux 7.2 with Unbreakable Enterprise Kernel (UEK) Release 4 Note: 32-bit operating systems are not supported.
Processor	Minimum: Intel Xeon E3-1220 Recommended: Intel multi-core Xeon Architecture-based server (see Reference Configurations below)
Network Adapter	Single Port 1 Gigabit Server Adapter
Memory	Minimum: 8 GB UDIMM RAM Recommended: 16-32 GB DIMM RAM for medium to large workloads (see Reference Configurations below)
Storage	Minimum: <ul style="list-style-type: none">• Capacity: 40 GB HDD• IOPS: At least 300• Throughput: At least 2 MB/s sustained random 4 KB write

Reference Configurations

The following reference configurations represent common application scenarios that utilize the PowerMedia XMS media server. These reference configurations are provided as examples of different workloads on various Intel multi-core Xeon Architecture-based server hardware.

Recommended: 120-240 GB Storage per PowerMedia XMS instance for standard applications (Storage should be scaled appropriately for application performance and storage volume requirements)

Use Case	CPU (Two Socket)	Memory (GB)	Call Rate (CPS)	Average CPU Utilization	Maximum CPU Utilization
<p>Mail Virtual Machine (16 vCPU) Voice and video mail services using the AMR container.</p> <p>Port Usage:</p> <ul style="list-style-type: none"> • 700 Basic Audio • 320 HD Voice (AMR-WB) • 320 GSMAMR Audio (AMR) • 10 Advanced Video (Up to CIF) • 10 MSRP 	E5-2665	16	22	64%	74%
<p>IVR Bare Metal VXML banking IVR and voice activated company phone directory. Intense use of ASR, TTS, and recording.</p> <p>Port Usage:</p> <ul style="list-style-type: none"> • 100 Basic Audio • 60 MRCP 	X5650	12	53	18%	31%
<p>Call Center Bare Metal MSML call center application with a high rate of slam-downs.</p> <p>Port Usage:</p> <ul style="list-style-type: none"> • 800 Basic Audio • 10 HD Voice (AMR-WB) • 30 GSMAMR (AMR-NB) • 80 LBR Audio (G.729) 	E5-2640 V3	32	73	16%	24%

Use Case	CPU (Two Socket)	Memory (GB)	Call Rate (CPS)	Average CPU Utilization	Maximum CPU Utilization
Unified Communications Bare Metal Broad mix of features and programming interfaces. Port Usage: <ul style="list-style-type: none"> • 240 Basic Audio • 10 HD Voice (Opus, EVS, AMR-WB) • 10 GSMAMR Audio (AMR-NB, GSM) • 50 LBR Audio (G.723, G.729) • 20 Advanced Video (H.264, VP8) • 20 High Resolution Video (720P) 	X5680	12	8	22%	55%

Supported Virtual Machines

The supported virtual machines (VM) are as follows:

- VMware ESXi 5.x and ESXi 6.x
- Kernel Virtual Machine (KVM)
- Oracle VM
- XenServer VM

The minimum virtual machine (VM) requirements are as follows:

- Processor: 2 vCPU
- Memory: 8 GB UDIMM RAM
- HDD: 40 GB HDD

Note: Virtualization systems chosen for PowerMedia XMS should be configured for enterprise or private virtual environments that permit customization of virtual machine (VM) settings and hypervisor performance tuning. Virtual environments running PowerMedia XMS must not over commit the CPU on the host platform to facilitate the real-time low-latency scheduling demands required for high quality media processing. Density capacity in virtual environments may vary and is generally a factor of the host platform capacity and the number of concurrent VMs running on that host.

Refer to the *Dialogic® PowerMedia™ XMS Application Note: Optimizing VMware Host Hardware and Virtual Machine to Reduce Latency* or the tuning guide for your hypervisor of choice (i.e., VMware) for more information.

Cloud Environments

The qualified cloud environments include the following:

- Amazon Web Services (AWS)

Note: Refer to the *Dialogic® PowerMedia™ XMS Application Note: Running PowerMedia XMS on Amazon Web Services* for more information.

Support for Rackspace is available as a controlled introduction for Proof of Concept (PoC), development activities, and trials. For more information, refer to the following white paper:

- *Dialogic® PowerMedia™ XMS and the Rackspace Managed Cloud* at <http://www.dialogic.com/~media/products/media-server-software/download/xms-demos/Rackspace-XMS-Verification.pdf>.

Available Application Technologies

A number of application technologies are available. The [Routing](#) page from PowerMedia XMS Admin Console illustrates how different applications like MSML, NETANN, VXML, and RESTful are engaged with PowerMedia XMS based on the content of SIP URI.

Supported Web Browsers

Browser Support for PowerMedia XMS Admin Console

The following web browsers are supported:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer
- Apple Safari

Browser Support for WebRTC

The following web browsers are supported:

- Mozilla Firefox
- Google Chrome

Note: Other release lines of Mozilla Firefox (Nightly) and Google Chrome (Canary) are subject to frequent change and may not work correctly. Any other WebRTC clients including Apple Safari and Opera may also work, but may also have some compatibility issues.

SIP Softphone

A SIP softphone should also be available for system verification of audio and video media and make SIP calls into the demo applications.

See the *Dialogic® PowerMedia™ XMS Quick Start Guide* for information about setting up PowerMedia XMS and installing suitable SIP softphones.

Note: For best results, a headset should be used on both phones and browser. If echo cancellation is available for the microphone device, it should be turned on. This can be done in the Windows sound mixer.

Bria SIP Softphone

Testing has been conducted on Bria 3. Here are the settings for testing:

- Resolution on the Bria (**Softphone > Preferences > Devices > Other Devices**) can be set to either Standard (approximately CIF) or to High resolution (approximately VGA).
- Set video codec (**Softphone > Preferences > Video Codecs**) to H.264 or VP8.
- DTMF (used for the conference demo) must be delivered as SIP INFO messages for compatibility with browser DTMF. Bria setting found under **Softphone > Preferences > Calls > DTMF**.

Linphone SIP Softphone

Linphone is a free, open source SIP softphone that works with PowerMedia XMS.

Linphone can be downloaded at <http://www.linphone.org/technical-corner/linphone.html>. For best results, you should also download and install the open source H.264 video codec at <http://www.videolan.org/developers/x264.html> rather than use the default H.263 that comes with Linphone. The Windows binary version of the codec can be found at <http://nongnu.askapache.com/linphone/plugins/win32> or <http://download.savannah.gnu.org/releases/linphone/plugins/win32>.

Once you have installed Linphone and the H.264 codec, very little configuration is necessary, as a SIP registrar will not be used for verification and initial testing. Default settings should suffice for a simple LAN-based test setup. Only audio and video codecs need to be set.

Codec configuration is accomplished as follows:

1. Click **Linphone > Preferences > Codecs > Audio codecs**.
2. Disable all audio codecs except PCMU.
3. Click **Linphone > Preferences > Codecs > Video codecs**.
4. Disable all video codecs except H264.
5. Click **Done**. The Linphone is now ready to use.

PowerMedia XMS Installation Package Policy

PowerMedia XMS is delivered in two formats: an RPM-based installation packaged as a g-zipped tar (.tgz) and an ISO install package. The RPM-based package is for installing PowerMedia XMS on an existing Linux installation, while the ISO package is a complete Linux OS installation based on CentOS that has been optimized for PowerMedia XMS. Users may use either method for installation and deployment of their PowerMedia XMS based solutions.

Dialogic makes reasonable commercial efforts to keep the ISO install package up to date with the latest applicable CentOS versions and security patches. Users who want to have individual control over the specific package versions and security updates should opt to install the RPM-based package option, which would provide them with such direct control. Alternatively, the yum update functionality provided by CentOS can be used to update a system.

Dialogic has validated PowerMedia XMS against the base CentOS version detailed in the [System Requirements](#) section.

It is recommended that users apply required updates in line with their applicable security policy/policies and to ensure that the updates are tested on a non-production PowerMedia XMS server prior to deployment. It is also recommended that a system backup and rollback procedure be put into place prior to deployment, in the event that any issues arise as a result of any updates being applied in production servers. Any issue(s) affecting the operation of PowerMedia XMS due to a security update should be reported to Dialogic.

There are certain support package versions that PowerMedia XMS uses (see the list in XMS installation log *xms_install.log* produced with *xms_install.pl -t*) where it is recommended by Dialogic to stay at those versions because moving to later versions may have undesirable effects. However, if an update to one of such support package versions is required due to a security issue, it is recommended to test all updates prior to deploying on production servers.

ISO Method

Operating System Requirement:

- Community ENTERprise Operating System (CentOS) 7.x

The ISO installation method is a complete system installation that includes the CentOS, OS optimizations, and PowerMedia XMS software. The ISO can be installed from a DVD drive to a physical or virtual machine.

Note: The ISO image is provided for ***development and trial purposes only*** and is not considered security hardened. Users who want to have individual control over the specific operating system package versions and latest security updates should opt to install the RPM-based distribution option. Only the RPM-based distribution is supported for production systems.

To perform the ISO method of installation, there are two options:

- Burn the .ISO image to a bootable DVD.
- Place the .ISO image in a virtual datastore and point the DVD drive to that location. This method is helpful for remote installations. Refer to [Appendix A: ISO Method for Remote Installation](#) for details.

Installation from the PowerMedia XMS installation DVD requires the following steps, which are described in detail after the procedure:

1. Download a single .ISO file, which contains CentOS and all required PowerMedia XMS software at <http://www.dialogic.com/products/media-server-software/xms>. Downloads can be found on the right side of your screen.

Note: You will be prompted to log in or sign up in order to download the software.

2. Use the .ISO image to create the PowerMedia XMS installation DVD.
3. Ensure the target system on which PowerMedia XMS will be installed is connected to your network.
4. Boot the target PowerMedia XMS system from the installation DVD. The DVD will install CentOS operating system and required software.

Caution: The PowerMedia XMS installation will reformat the system hard drive.

5. Perform licensing and configuration.

Getting and Burning the .ISO File

CentOS is an Enterprise-class Linux Distribution source that provides a simple method for quickly and easily setting up a PowerMedia XMS. Proceed as follows:

1. Download a single .ISO file, which contains CentOS and PowerMedia XMS packages. Go to <http://www.dialogic.com/products/media-server-software/xms> for information about downloading the .ISO file.
2. Using a DVD drive that has write capabilities, along with the appropriate DVD burning software, burn the .ISO image onto a bootable DVD.

Note: A bootable DVD must be created from the downloaded .ISO file rather than simply copying the file to the DVD.

Booting the System from the DVD

Caution: This installation will erase all data on the system and reformat your hard drive.

Once the bootable DVD is created, proceed as follows:

1. Insert the bootable DVD in the system drive on which the installation will be done and boot the system from the DVD.
2. Press **Enter** at the boot prompt.

Note: Do not use any other boot options or the automatic installation will not take place.

Setting the IP Address

The installation requires little interaction. The main task is to set up the IP characteristics for the XMS. The IP characteristics for the XMS are set at the start of the installation and are handled as follows:

- **DHCP** - The default setting is to set up an Ethernet interface to receive its addresses via DHCP. With this option, it is necessary that PowerMedia XMS be installed in an environment that provides a networked DHCP server to provide it with an IP address.

Note: If DHCP is used to assign an IP address, it should be configured to ensure that the IP address doesn't change between boots.

- **Static IP Address** - An Ethernet interface may also be given a static IP address. This option is preferable when setting up a server.

After the DVD is ready to be installed, the following console is used to set the IP address and perform the installation. If obtaining an IP address via DHCP, press **Enter** to automatically select the default **Install PowerMedia XMS with DHCP Networking**. If setting a static IP address, press **Tab** to edit the default network parameters ("ip=dhcp").

To edit the default network parameters ("ip=dhcp"), replace "dhcp" with the applicable network parameters. The CentOS 7 anaconda/dracut installer contains a comprehensive syntax to cover many network-related system boot options. The options given here are meant to simplify the process of setting up a static IP address by providing a common working example. Specify the parameters that you want to override. Parameters that are not entered will have their values automatically obtained. These are positional parameters that are "missing" from the syntax and indicated by double colons (::). When finished, press **Enter** to continue with the installation.

```
ip=<ip_addr>::<<gateway_addr>:<netmask>:<hostname>::none nameserver=<ip_addr>
```

Refer to the following guidelines:

- For parameters ending with "_addr", enter the ipv4 addresses.
- The first double colon (::), which is between "<ip_addr>" and "<gateway_addr>", defaults to no peer. Unlike other instances of double colons in the syntax, this double colon does not represent a missing (i.e., not entered) parameter.
- The second double colon (::), which is between "<hostname>" and "none", means the default Ethernet device is automatically obtained. The default Ethernet device is automatically obtained because the parameter was not entered.
- The "none" means that a static IP address is being set up.
- It is recommended to set the DNS ("nameserver=<ip_addr>") as part of the installation. The "nameserver=" parameter is separate from the "ip=" parameter.

Refer to the following example for setting up a static IP address of 192.168.1.100 with a gateway of 192.168.1.1, a netmask of 255.255.255.0, a system name of "server.xms30.com", the default Ethernet device found on the system, and a DNS of 8.8.8.8.

```
ip=192.168.1.100::192.168.1.1:255.255.255.0:server.xms30.com::none nameserver=8.8.8.8
```

For complete information on all available parameters, refer to the "Chapter 20. Boot Options" section of the Red Hat Documentation:

http://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Installation_Guide/chap-anaconda-boot-options.html#tabl-boot-options-network-formats.

Completing the Installation

Once the IP characteristics are set, the remainder of the installation is "hands off". When the CentOS install reaches the final screen, click **Reboot** to complete the installation process.

Note: Be sure to remove the installation DVD before the final reboot is done.

RPM Method

Before running the RPM installation method, the following packages, available from the OS distributor, must first be installed:

- perl-core
- perl-JSON
- openssl version 1.0.1e or higher
- httpd-2.2.15-60.el6.centos.4.x86_64 or higher

Note: If using CentOS 6.x, please ensure that the installed version (2.2.15) and release (60.el6.centos.4) of httpd is *httpd-2.2.15-60.el6.centos.4.x86_64* or higher.

Note: The WebGUI requires a minimum version of TLS 1.2. If using CentOS 6.x, please ensure that the installed version of httpd is *httpd-2.2.15-60.el6.centos.4.x86_64* or higher. If the CentOS 6.x httpd package is not updated, the XMS installation logs will indicate that "httpd may fail to start" and the WebGUI will be unresponsive.

The failure message will also appear in */var/log/messages* when trying to start httpd or reboot the system.

Note: If using VXML and CentOS/RHEL 7.x, please ensure that the installed version of js is *js-1.8.5-20.el7.x86_64* or higher.

Note: If using CentOS/RHEL 7.x, please ensure that the installed version of glibc is *glibc-2.17-260.el7.x86_64* or higher and gperftools is *gperftools-libs-2.6.1-1.el7.x86_64* or higher.

The stand-alone RPM installation method is used for installing PowerMedia XMS on existing Linux installations. Instead of an .ISO file, the RPM distribution of PowerMedia XMS uses a gzipped tar file (.tgz). The .tgz file is extracted to a directory on the machine where the PowerMedia XMS will be installed. The PowerMedia XMS installation script is run from that directory.

Note: The PowerMedia XMS Release 4.0 installation script can only upgrade systems running PowerMedia XMS Release 3.0 or higher. Users of PowerMedia XMS Release 2.x must uninstall it first before installing PowerMedia XMS Release 4.0.

The *perl-core-5.10.1-xxxxx.x86_64.rpm* package is required on the system before running the PowerMedia XMS installation script. The perl-core package is a standard package that is part of the RHEL/CentOS distribution and is normally automatically installed on virtually all systems when the operating system is installed using one or more of the RHEL/CentOS predefined package groups.

Note: However, in the case where you manually select each individual package in a RHEL/CentOS operating system installation (i.e., when using a kick start file), you must ensure that the *perl-core-5.10.1-xxxxx.x86_64.rpm* is included in the list of packages. It can be installed on an RHEL or CentOS system using "yum install perl-core".

The PowerMedia XMS installation script automatically installs any prerequisite operating system packages (other than perl-core) required by the PowerMedia XMS installation script if the yum utility is used and configured to access either the operating system installation DVD or online package repositories such as RHN.

Note: Only the standard official repositories that match the distribution and version of the operating system are supported. These supported repositories are automatically configured by the operating system during installation. Third party repositories are not supported.

If yum is not available on the system, the PowerMedia XMS installation script will print to the installation log (default: *xms_install.log*). That log contains a list of prerequisite operating system packages required to be manually installed by the user before re-running the PowerMedia XMS installation script.

Ensure that your PowerMedia XMS system firewall is configured accordingly.

Note: If using RHEL 7.x, the repository that stores the RHEL libtiff-tools package must be enabled to perform the installation. For typical installations, enable the repository using the following command:

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

Note: If using Oracle Linux 7.x, the repository that stores the libtiff-tools package must be enabled to perform the installation. For typical installations, edit the repository files using the following command:

```
sudo yum-config-manager --enable ol7_optional_latest
```

Note: If using Amazon cloud, the repository that stores the RHEL libtiff-tools package must be enabled to perform the installation. For typical installations, enable the repository using the following command:

```
sudo yum-config-manager --enable rhui-REGION-rhel-server-extras rhui-REGION-rhel-server-optional
```

Note: Reverse Path Filtering (rp_filter) should be configured so that SIP and RTP traffic is not blocked. Refer to http://www.dialogic.com/support/helpweb/helpweb.aspx/4538/incoming_ip_traffic_not_received_by_xms/PM_XMS for more information.

Reserved Ports

The default PowerMedia XMS configuration uses the following reserved ports.

Service	Port
CDR	27017 (mongo server), 28017 (mongo restful interface), 20000 (cdrserver)
Event Manager	9876
HTTP	80
HTTPS	443
Licensing	27000-27009 (licensing server, vendor daemon uses random port)
MRB	12000-12010
Perf Manager	6789 (xmserver)
RTP Audio Media Ports (RTP, RTCP)	49152-53151
RTP Video Media Ports (RTP, RTCP)	57344-61344
SIP Signaling	5060
SNMP	161, 162 (all interfaces)
SSH	22
Telnet	23
T.38 Fax	56500-56999
WebRTC (all processes)	1080
WebGUI (nodecontroller, lighttpd, httpd)	81, 10443, 9004 (lighttpd) 10080 (nodecontroller)

RPM Installation and Script Options

Note: Linux control groups (cgroups) and CPU accounting are not supported and must be disabled. Check your Linux OS documentation on how to disable these features as they prevent real-time processing required for PowerMedia XMS.

Proceed as follows to complete the RPM installation method:

1. Extract the gzipped tar file to a directory of your choice. The chosen directory will contain a subdirectory named *dialogic_xms_m.n.r-s.tgz* where *m* indicates *major version*, *n* indicates *minor version*, *r* indicates *revision*, and *s* indicates *service update #*.
2. Run *xms_install.pl* with the desired options from the subdirectory above.

These are the available options:

- [cfg-xxx Options](#)
- [Advanced Options](#)
- [Mode Options](#)
- [General Options](#)

cfg-xxx Options

These are the following platform configuration options:

```
--cfg-selinux      Disable selinux (default: ask)
--cfg-hosts        Configure /etc/hosts file (default: ask)
--cfg-prereq       Automatically install prerequisite OS packages (default: ask)
--cfg-https        Backup and replace https settings (default: ask)
```

Note: SELinux is not supported and should be disabled.

For example, to install PowerMedia XMS and automatically configure the */etc/hosts* file, use the following:

```
xms_install.pl -i --cfg-hosts
```

The *--cfg-xxx* options can be negated with *nocfg-xxxx*. For example, if the script is to ignore the */etc/hosts* file, use the following:

```
xms_install.pl -i --nocfg-hosts
```

Advanced Options

These are the following advanced configuration options:

```
--lic-check        On upgrade, when used with the -y option, force license check and
                   exit if license is incompatible. This option can also be negated
                   to skip the license check entirely (--nolic-check)
--xms-optmod NAME=yes|no  Install (or not) optional module (NAME: mongo, fax)
--xms-logdir DIR:       XMS log file directory
--xms-loglevel LVL      Default XMS log level (ERROR, WARN, NOTICE, INFO, DEBUG - default: ERROR)
```

When installing or upgrading PowerMedia XMS, additional optional modules can be selected for installation. The supported optional modules include the following:

Module	Installed by Default
fax	no
mongo	yes

To install an optional module that is not installed by default, use the following:

```
xms_install.pl --xms-optmod fax=yes
```

To negate the installation of an optional module that is installed by default, use the following:

```
xms_install.pl --xms-optmod mongo=no
```

Mode Options

These are the following mode configuration options:

-i or --install	Install XMS if no previous version exists (default)
-u or --update	Update XMS without affecting current configuration
-r or --remove	Remove XMS
-t or --test	Test system and report status without installing anything

General Options

These are the following general configuration options:

-y or --yes	Answer yes to all questions
-h or --help:	Display this message and exit
-d or --distdir DIR	Directory where the XMS distribution is located
-l or --log or --nolog	Log (or not) results to a file (default: enabled)
-f or --logfile FILE	Use FILE as the log filename (default: xms_install.log)
-v or --verbose	Print detailed progress information (-vv very verbose)
-q or --quiet	Do not write anything to standard output (implies -y)

Note: The --quiet option implies a yes answer to all questions unless --nocfg-xxxx is added to the command.

If errors occur, review the log file for error and warning information. A log file (default: *xms_install.log*) is generated automatically unless --nolog is specified.

When the installation script completes, use your browser to log in to the PowerMedia XMS Admin Console (refer to [Log In to the Console](#)).

3. PowerMedia XMS Admin Console

Using PowerMedia XMS Admin Console

The PowerMedia XMS Admin Console (also referred to herein as "Console" or "WebGUI") is a secure web-based GUI used to manage PowerMedia XMS. The [Console](#) can be reached using a web browser and the PowerMedia XMS IP address.

If DHCP is used to provide the PowerMedia XMS IP address, it will be necessary to access the system to determine the address assigned to it. Shell access to the system may be done either by the terminal used during installation or by secure shell (ssh) access. The "root" user's default password is "powermedia". If you wish to change the password, do so before proceeding.

Note: For stand-alone RPM installations, password modification is not necessary as the installation script does not change the password to "powermedia" as it does with the .ISO install.

CentOS HTTPS Setup for Console Use

Secure HTTP is used to communicate between the administrator's browser and the PowerMedia XMS Admin Console's interface. HTTPS usually requires a [security certificate](#) linked to the provider's domain and signed by a trusted third party.

With PowerMedia XMS, it is not possible to provide a certificate tied to any one domain because the PowerMedia XMS is intended to be installed in many different situations by different administrators. For this reason, a "self-signed" (non-verified) certificate is shipped with PowerMedia XMS. The procedure for creating and installing a non-verified certificate on CentOS can be found at <http://wiki.centos.org/HowTos/Https>. The web browser used to access the Console will detect the use of this self-signed certificate and flag it as a security exception.

Access the Console directly using HTTPS by adding the IP address in browser's address space. For example, `https://<ip_address_of_eth0>`.

Note: If HTTP is used the query will be redirected to HTTPS on port 443.

Accessing the Console will trigger a security exception. Handling the security exception depends on the web browser being used. Refer to the following table for instructions when using one of the four most common browsers.

Browser	Security Exception	Action	Comment
Mozilla Firefox	Connection is not trusted	Understand the Risks/Add Exception/Confirm Security Exception	Security exception remains permanently in effect
Google Chrome	Site's security certificate is not trusted	Proceed Anyway	Security exception will be seen again on starting Chrome

Browser	Security Exception	Action	Comment
Microsoft Internet Explorer	Problem with website's security certificate	Continue	Security exception will be seen again on starting new Internet Explorer window
Apple Safari	Cannot verify identity of the website	Continue	Security exception will be seen again on starting Safari

Recurring security exceptions can be overcome on Chrome, Internet Explorer, and Safari as follows:

1. Add mapping in the "hosts" file:

```
xms.localhost          <xms_ip_address>
```
2. Add the xms.localhost certificate into the Trusted Root Certification Authorities store. Hosts may be found on Linux systems under */etc* and on Windows systems under *C:\windows\system32\drivers\etc*. This differs depending on the web browser in use.
 - **Chrome** - Crossed-out lock and https symbols will be seen when the Console screen is accessed. Click **Lock Symbol > Certificate Information > Details > Copy to File** and work through the Certificate Export Wizard to save the xms.localhost certificate. It can then be imported into Chrome. Use **Tools > Options > Under the Hood > HTTPS-SSL Manage Certificates > Trusted Root Certification Authorities** to import.
 - **Internet Explorer** - A Certificate Error will be seen next to the URL entry. Install the xms.localhost certificate using **Certificate Error > View Certificates > General Tab > Install Certificate** and work through the Certificate Import Wizard. The xms.localhost certificate will end up in the Trusted Root Certification Authorities store.
 - **Safari** - A popup warning will be seen on accessing the Console. Install the xms.localhost certificate using **Show Certificate > Install Certificate** and work through the Certificate Import Wizard. The xms.localhost certificate will end up in the Trusted Root Certification Authorities store.

Note: A permanent, publicly accessible PowerMedia XMS should have a valid certificate from a signed certificate authority. Refer to the [Guidelines for Installing a Permanent Security Certificate](#) for more information.

Guidelines for Installing a Permanent Security Certificate

A permanent, publicly accessible PowerMedia XMS should use a valid certificate from a trusted certificate authority. A large number of vendors provide security certificates. Use the following guidelines when installing a certificate from your preferred vendor:

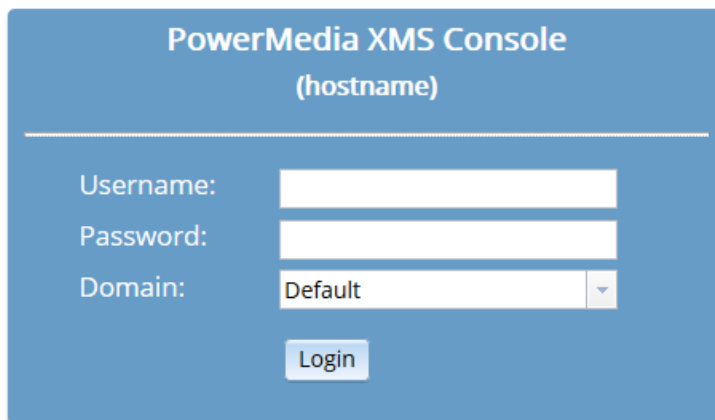
- Upon installation, the fully qualified domain name of the PowerMedia XMS is `xms.localhost`. The self-signed certificate supplied with PowerMedia XMS uses this name. Therefore, change the server name/domain.
- The web server used for the Console is Apache, version 2.2.15. There is also a `lighttpd` server on the system, but it is used for the RESTful interface to PowerMedia XMS and can be ignored.
- Secure HTTPS access is provided by `mod_ssl`, the OpenSSL interface to Apache. The OpenSSL version must be 1.0.1e or higher.
- The configuration file for the SSL Virtual Host is `/etc/httpd/conf.d/xms.conf`. Entries to modify when a purchased certificate is activated include `SSLCertificateFile`, `SSLCertificateKeyFile`, and `SSLCertificateChainFile`.

Console Login

Proceed as follows to connect to the Console:

1. Launch your web browser. In the address field, enter the IP address in URL format. For example, `https://<xms_ip_address>`.

The login page appears.



The screenshot shows a web browser window displaying the login page for the PowerMedia XMS Console. The page has a blue header with the text "PowerMedia XMS Console (hostname)". Below the header, there are three input fields: "Username:", "Password:", and "Domain:". The "Domain:" field is a dropdown menu with "Default" selected. Below the input fields is a "Login" button.

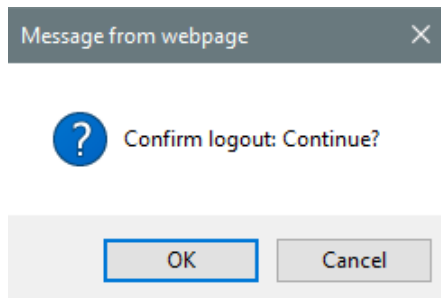
2. Choose from two login options:
 - Enter "superadmin" in the **Username** field and "admin" in the **Password** field to be granted access to all configuration functions available on the Console.
 - Enter "admin" in the **Username** field and "admin" in the **Password** field.
3. Click **Login**. After user information is authenticated, you are logged on to the initial **General** page of the **Systems** menu.

The Console is designed as follows:

- The page title at the top.
- A side-bar menu used for navigation.
- One or more tabs at the top that contain more information for each side-bar menu item.
- A display area for viewing and changing data.

The option to log out appears on each screen in the upper right-hand corner:

1. Click **logout**. Depending on your browser, a popup similar to the following appears to confirm logout.



2. Click **Cancel** to return to the Console.
3. Click **OK** to close the Console session and return to the Console's login page.

4. PowerMedia XMS Configuration

Configuring PowerMedia XMS

PowerMedia XMS configuration and operation is done through the Console. This section provides details about the Console's functionality. The side-bar menu contains the following options:

- [System](#)
- [Network](#)
- [License](#)
- [Protocol](#)
- [Codecs](#)
- [MSML](#)
- [VXML](#)
- [RESTful API](#)
- [NETANN](#)
- [Routing](#)
- [HTTP Client](#)
- [Speech](#)
- [MSRP](#)
- [Fax](#)
- [Tones](#)
- [Media](#)
- [CDR](#)
- [SNMP](#)
- [Reports](#)
- [Monitor](#)
- [Secure Storage](#)
- [Options](#)
- [Downloads](#)

Note: Whenever a port is being used, configure your firewall settings to enable each port that is selected.

System

The **System** menu provides system information about the PowerMedia XMS you have logged into. Additional options are accessible via the following tabs:

- [General](#)
- [Services](#)
- [Time](#)
- [Backup/Restore](#)
- [Upgrade](#)
- [NFS Mount Points](#)
- [Maintenance](#)
- [Account Manager](#)
- [Diagnostics](#)
- [Audit Logs](#)

General

When you log in, the **General** page of the **System** menu is displayed. On this page, PowerMedia XMS operation can be verified.

General	Services	Time	Backup/Restore	Upgrade	NFS Mount Points	Maintenance	Account Manager	Diagnostics	Audit Logs
XMS									
Release	4.0.23064 GA								
State	RUNNING								
System									
OS Release	CentOS Linux release 7.5.1804 (Core)								
Kernel Version	Linux 3.10.0-123.el7.x86_64								
Uptime	0 days 0 hours 54 minutes 6 seconds								
Cpu Load	T1=0.4 , T5=0.19 , T15=0.1								
Memory	total:3792 MB used:942 MB								
System Storage									
/dev/sda2 (/)	total: 10230 MB, used: 4524 MB								
/dev/sda5 (/var)	total: 12660 MB, used: 5790 MB								
/dev/sda1 (/boot)	total: 124 MB, used: 74 MB								
System Time									
Time	Tue Mar 12 15:00:44 2019								
Zone	America/New_York								

The following information is provided.

Item	Description
XMS	Displays release name and state of the PowerMedia XMS.
System	Displays the operating system release and version, and provides the uptime, CPU load, memory, and disk space used. Note: The T1, T5, and T15 values indicate the CPU load averages over 1, 5, and 15 minutes as reported by "top".
System Storage	Displays storage metrics, used and total KB, and names.
System Time	Displays the current time and time zone.

Services

The option to enable manual service startup mode, restart services, stop services, or perform graceful shutdown is available from the **Services** page of the **System** menu. You can also view which services are currently running.

To enable a manual service startup mode for post installation configuration, select Manual from the drop-down list in the **Startup Mode** field (Default value is Auto). When the manual service startup mode is enabled, the system allows for configuration prior to full service startup.

To restart services, click **Restart**. Verify that all services have started.

To stop services, click **Stop**. The **Overall Status** will change from RUNNING to WAITING to stop services. Services are stopped when the Status column changes from RUNNING to STOPPING.

To perform graceful shutdown, click **Graceful Shutdown**. This shuts down the media server gracefully, without intrusively terminating established calls. When activated, all active calls will remain connected for a configurable grace period length of time. Any new ingress call attempts are rejected and result in a 503 Service Unavailable response.

An additional feature is supported to allow calls initially established with a special SIP extension header (X-Call-Group) to remain active and process ingress calls containing a SIP header that references an active call group. When using this feature, new ingress calls that contain a SIP extension header referencing an active call group identifier (i.e., a party requesting to connect to a conference established with a unique X-Call-Group number) will get processed normally. All other call attempts will get rejected with a 503 Service Unavailable response. When the grace period expires, the system will forcefully terminate all sessions and shut down.

The **OS Services** section allows the user to configure optional XMS operating system service components. The adaptor service interacts with the MRB and allows the MRB to monitor the XMS. If using the MRB, enable the **On-Boot Enabled** option in order for the adaptor service to start automatically when the machine is restarted. The **Status** option reflects the current (running/stopped) status of the service, and can be used to dynamically start or stop the service independently of the **On-Boot Enabled** option.

Click **Refresh** to reload the **Services** page.

Overall Status: **RUNNING**
 Graceful Shutdown Timeout (seconds):
 Startup Mode:

[Restart](#) [Stop](#) [Graceful Shutdown](#) [Refresh](#)

Mandatory Services:

Service Name	Description	Status
hmp	Media Processing Service	RUNNING
broker	Message Routing Service	RUNNING
secstorage	Secure Storage Service	RUNNING
xmsserver	Signaling and Media Service	RUNNING
appmanager	Application Interface Service	RUNNING

Optional Services:

Service Name	Description	On Start Enabled	Status	Operations
rmtlogagent	Remote Logging Agent	<input checked="" type="checkbox"/>	RUNNING	
eventmanager	Event Manager	<input checked="" type="checkbox"/>	RUNNING	
perfmanager	Performance Manager	<input checked="" type="checkbox"/>	RUNNING	
cdrserver	CDR Service	<input checked="" type="checkbox"/>	RUNNING	
httpclient	HTTP Client	<input checked="" type="checkbox"/>	RUNNING	
mrcpclient	MRCP Client	<input checked="" type="checkbox"/>	RUNNING	
rtcweb	RTCWeb Signaling Service	<input checked="" type="checkbox"/>	RUNNING	
xmsrest	RESTful Call/Media Control Service	<input checked="" type="checkbox"/>	RUNNING	
netann	NETANN Service	<input checked="" type="checkbox"/>	RUNNING	
vxml	VXML Service	<input checked="" type="checkbox"/>	RUNNING	
msml	MSML Service	<input checked="" type="checkbox"/>	RUNNING	
msrpservice	MSRP Service	<input checked="" type="checkbox"/>	RUNNING	
faxservice	Fax Service	<input type="checkbox"/>	STOPPED	
xspeechservice	Speech Service	<input type="checkbox"/>	STOPPED	
verification	System/Application Verification Service	<input checked="" type="checkbox"/>	RUNNING	
wsapiserver	WS Api Server	<input checked="" type="checkbox"/>	RUNNING	
xmsclid	Metrics Export Service	<input type="checkbox"/>	STOPPED	

OS Services:

Service Name	Description	On Boot Enabled	Status	Operations
adaptor	MRB Adaptor Service	<input type="checkbox"/>	STOPPED	

Time

The **Time** page of the **System** menu displays the system's current date, time, and time zone, and allows an administrator to change date and time parameters.

General	Services	Time	Backup/Restore	Upgrade	NFS Mount Points	Maintenance	Account Manager	Diagnostics	Audit Logs
---------	----------	-------------	----------------	---------	------------------	-------------	-----------------	-------------	------------

Current date and time: Thu Oct 27 09:14:14 2016
NTP Daemon: ntpd

Synchronize date and time over the network

New NTP Server

Add

NTP Servers

Server Address	iburst	MAX Poll	MIN Poll	Action
0.centos.pool.ntp.org	true	10	6	Delete
1.centos.pool.ntp.org	true	10	6	Delete
2.centos.pool.ntp.org	true	10	6	Delete

Note: Double click on the cell to edit

Time Zone: America/New_York ▼

Note: Stop the XMS services to edit the Time Zone parameter

System clock uses UTC

Apply

The following information is provided.

Item	Description
Synchronize date and time over with the network	Keep the system's date and time synced using Network Time Protocol (NTP). Otherwise, allow the date/time to be manually set.
Server Address	Name or IP address of NTP server.
iburst	When the server is unreachable and at each poll interval, send a burst of eight packets instead of the usual one. This is designed to speed the initial synchronization acquisition.
MAX Poll	Maximum poll interval for NTP messages, in seconds, to the power of two.
MIN Poll	Minimum poll interval for NTP messages, in seconds, to the power of two.
Action	The option to delete an item is available.

Item	Description
System clock uses UTC	Keep the system's hardware clock in UTC/GMT or local time.

If the **Synchronize date and time over with the network** option is not selected, the date and time may be set manually to the desired value. Otherwise, it provides the option to add or delete NTP servers. NTP servers may be added, deleted, or edited. To edit the NTP servers, double-click the cell to make changes.

The system's **Time Zone** may be changed using the drop-down list, and the system's hardware clock mode (UTC/GMT or local time) may be selected.

Note: To edit the time zone, stop the XMS services.

Backup/Restore

The **Backup/Restore** page of the **System** menu provides the option to perform system backup and to restore configurations.

Note: The backup and restore process is intended to save time if reinstalling the same PowerMedia XMS release or if replicating a configuration across several PowerMedia XMS systems of the same version. It should not be used to preserve settings across PowerMedia XMS system upgrades. To perform a system upgrade, follow the upgrade process as outlined in the [Upgrade](#) section. The upgrade process automatically preserves and migrates configuration file settings in accordance with the requirements of the updated release.

General	Services	Time	Backup/Restore	Upgrade	NFS Mount Points	Maintenance	Account Manager	Diagnostics	Audit Logs
---------	----------	------	-----------------------	---------	------------------	-------------	-----------------	-------------	------------

System Backup

Upload System Restore File (*.gz)

Browse

Overwrite Existing File?

Upload

System Backup Files:

File Name	Restore	Download	Delete
xmsbackup-20161027-091616.tar.gz	<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #add8e6;">Restore</div>	<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #add8e6;">Download</div>	<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #add8e6;">Delete</div>

System Backup

Proceed as follows to create a system backup:

1. Click **System Backup** to create a system backup file.
2. Once created, the system backup file will be listed in **System Backup Files**.

Restore Backup

Proceed as follows to restore a system backup:

1. Click **Browse** from the **Upload System Restore File** section to access a system backup file that has been downloaded.
2. Once you select the system backup file, click **Upload**. After the upload completes, the system backup file will be listed in the **System Backup Files** section.
3. Locate the appropriate system backup file and click **Restore**.

Note: If there is already a system backup file listed in the **System Backup Files** section, you can click **Restore** on the appropriate system backup file.

Note: Operating system settings (such as DNS, time zone, etc.) are not saved or restored.

Upgrade

The **Upgrade** page of the **System** menu provides the option to upgrade the system by uploading a system upgrade package.

General	Services	Time	Backup/Restore	Upgrade	NFS Mount Points	Maintenance	Account Manager	Diagnostics	Audit Logs
---------	----------	------	----------------	----------------	------------------	-------------	-----------------	-------------	------------

Upload System Upgrade Package (*.tgz)

Overwrite Existing File?

System Upgrade Package:

File Name	Upgrade	Delete
dialogic_xms_trunk.14270-0.c6.tgz	<input type="button" value="Upgrade"/>	<input type="button" value="Delete"/>

Upgrade Status:

None

System Upgrade

Proceed as follows to upgrade the system:

1. Click **Browse** from the **Upload System Upgrade Package** section to access a system upgrade package file (.tgz) that has been downloaded.
2. Once you select the system upgrade package file, click **Upload**. After the upload completes, the system upgrade package file will be listed in the **System Upgrade Package** section.
3. Locate the appropriate system upgrade package file and click **Upgrade**.

Note: If there is already a system upgrade package file listed in the **System Upgrade Package** section, you can proceed to click **Upgrade** on the appropriate system upgrade package file; the web page may timeout/restart as a result.

Note: The *xms_install.log* file is placed in the */tmp* directory.

NFS Mount Points

The **NFS Mount Points** page of the **System** menu allows Network File System (NFS) version 4 file systems, offered by external servers, to be mounted on PowerMedia XMS. Resources used by PowerMedia XMS, such as media files or VXML scripts, can be kept on an external file server but may be needed for handling calls. NFS mount will allow for this.

The NFS server must be correctly configured to allow mounting of its file system on the PowerMedia XMS NFS client. This is outside the scope of this document.

General	Services	Time	Backup/Restore	Upgrade	NFS Mount Points	Maintenance	Account Manager	Diagnostics	Audit Logs
---------	----------	------	----------------	---------	-------------------------	-------------	-----------------	-------------	------------

New NFS Mount Point:	
Server Share Location	<input type="text"/>
Mount Point	<input type="text"/>
Mount Options	defaults

NFS Mount Points List				
<input type="checkbox"/>	Server Share location	Mount Point	Options	Mount
<input type="button" value="Delete"/>				<input type="button" value="Apply"/>

Adding a Mount Point

Multiple mounts may be defined. Each is individually added, and will then be displayed in the **NFS Mount Points List** section.

1. Enter the **Server Share Location**. Typically, this will consist of the IP address of the server, followed by a colon, followed by a location in the exported file system. For example, if the NFS server exports `/var/lib/media/en-US`, the **Server Share Location** `192.168.1.100:/` will mount the contents of the en-US directory at the given **Mount Point**.
2. Change the default **Mount Options** ("defaults") if desired. See the **Mount Options** section of the [nfs\(5\) Linux man page](#) for other possible settings.
3. Enter the **Mount Point**. This will be a directory in the PowerMedia XMS file system. A typical example would be `/mnt`. The **Mount Point** must already exist in the PowerMedia XMS file system or the mount operation will time out. It may be necessary to manually add mount points by logging into PowerMedia XMS using ssh.
4. Click **Add** to execute the mount operation. The mounted file system is activated.

Note: Even after removing and reinstalling PowerMedia XMS, the previously added mount points will still be listed in the **NFS Mount Points List** section.

Deleting a Mount Point

Mounted file systems are deleted by checking off the file system row in the **NFS Mount Points List** section and clicking **Delete**. The file system will be unmounted and the row will be deleted from the list.

Maintenance

The **Maintenance** page of the **System** menu provides the option to reboot or shut down the PowerMedia XMS.

General	Services	Time	Backup/Restore	Upgrade	NFS Mount Points	Maintenance	Account Manager	Diagnostics	Audit Logs
---------	----------	------	----------------	---------	------------------	--------------------	-----------------	-------------	------------

Server

Reboot
 Shutdown

WARNING:

The server shutdown and reboot will happen immediately and all current calls will be lost.

To reboot the PowerMedia XMS, click the **Reboot** radio button and then click **Apply**.

To shut down the PowerMedia XMS, click the **Shutdown** radio button and then click **Apply**.

Note: Once you click **Apply**, the reboot or shut down action occurs immediately and all current calls are lost.

Account Manager

The **Account Manager** page of the **System** menu provides options to manage accounts.

The PowerMedia XMS supports the following access levels (roles):

- **superadmin** - able to change the configuration of the PowerMedia XMS and execute administrative tasks. The role description includes read, write, and domain/user creation privileges.

Note: A "superadmin" level account can disable any account and delete "admin" and "viewer" level accounts, but cannot delete other "superadmin" level accounts without modifying their role first to "admin" and "viewer".

- **admin** - able to monitor the PowerMedia XMS, but cannot change configurations or execute administrative tasks. The role description includes read/write only privilege.
- **viewer** - able to view the PowerMedia XMS, but cannot change configurations or execute administrative tasks. The role description includes read only privilege.

Functions that are available to "superadmin", "admin", and "viewer" are noted as such. To delete an account, click **Delete**. To create a new account, click **New** and refer to [Create a New User Account](#). To edit an existing account, click **Edit**. When changing the password, the old password is required for verification prior to entering the new password. To refresh the account list, click **Refresh**. To set the password policy, click **Password Policy** and refer to [Set the Password Policy](#).

General Services Time Backup/Restore Upgrade NFS Mount Points Maintenance **Account Manager** Diagnostics Audit Logs

Accounts:

Selection	Username	Password	Role	Role Description	Status
<input type="radio"/>	superadmin	*****	superadmin	Read, Write and Domain/User Creation Privileges	<input checked="" type="checkbox"/>
<input type="radio"/>	admin	*****	admin	Read/Write Only Privilege	<input checked="" type="checkbox"/>
<input type="radio"/>	viewer	*****	viewer	Read Only Privileges	<input checked="" type="checkbox"/>

Delete New Edit Refresh Password Policy

Create a New User Account

Proceed as follows to create a new user account. Up to 20 new user accounts can be created.

Note: The account being created will have configure and provisioning permissions but will not have administrative permissions.

1. Click **New**. The **New Account Editor** dialog box will appear.

New Account Editor

Username:

New Password:

Re-enter New Password:

User Role:
 Super Admin

Apply Cancel

2. Enter a username and password in the corresponding **Username** and **Password** fields. The account being set up is a user account and not an administrative account.
3. Click **Apply** and the object and the new user will appear under the admin icon in the configuration tree or click **Cancel** to abort the operation.
4. Once the account has been created, log in to the newly created account.
5. Click **logout** in the upper right-hand corner of the page to log out of PowerMedia XMS.

Set the Password Policy

Proceed as follows to set the password policy.

1. Click **Password Policy**. The **Password Policy Settings** dialog box will appear.

Password Policy Parameters	
Min length:	5
Max length:	20
Expiration (Days):	90
Username in password:	Yes
Password Change on First Login:	No
Login Failed Max:	5
Login Failed Threshold (Minutes):	2
Lockout Duration (Minutes):	0

Password Categories	
Min categories:	1
At least one digit:	Optional
Lower case character:	Optional
Upper case character:	Optional
Non Alphanumeric:	Optional

Apply Close

Password Policy Parameters

2. In the **Min length** field, enter the minimum length of the password.
3. In the **Max length** field, enter the maximum length of the password.
4. In the **Expiration (Days)** field, enter the number of days when the password expires.
5. In the **Username in password** field, select Yes to allow username in the password or No to prohibit username in the password.
6. In the **Password Change on First Login** field, select Yes to enable password change on the first login or No to disable password change on the first login. When enabled, previously created accounts are not prompted to change their password.
7. In the **Login Failed Max** field, enter the maximum amount of failed login attempts before the account is locked out. The locked out functionality does not apply for a supradmin level account.

8. In the **Login Failed Threshold (Minutes)** field, enter the threshold (in minutes) of time in between failed login attempts.
9. In the **Lockout Duration (Minutes)** field, enter the duration (in minutes) of time that the account remains locked out before automatically becoming unlocked. If the value is set to 0, the account will remain locked until a superadmin level account unlocks it manually.

Password Categories

10. In the **Min categories** field, select the minimum number of password categories.
11. In the **At least one digit** field, select Mandatory to require at least one digit or Optional to disable.
12. In the **Lower case character** field, select Mandatory to require a lowercase character or Optional to disable.
13. In the **Upper case character** field, select Mandatory to require an uppercase character or Optional to disable.
14. In the **Non Alphanumeric** field, select Mandatory to require a non-alphanumeric character or Optional to disable.
15. Click **Apply** to save changes or click **Close** to abort the operation.

Note: The **Min Categories** defines how many password categories must be satisfied. Setting any category to Mandatory makes that category a required category to be satisfied.

If the **Min categories** is set to 3 and all the categories are set to Optional, any three of the four categories must be satisfied.

If the **Min categories** is set to 3 and one character category is set to Mandatory, three of the four categories must be satisfied, with one of the three being the category that is set to Mandatory.

Diagnostics

The **Diagnostics** page of the **System** menu provides the option to set the logging level for the PowerMedia XMS. Refer to the *Dialogic® PowerMedia™ Diagnostics Guide* for more information.

In the **Mask DTMF digits** field under **Options**, click the check box to mask DTMF digits that is normally written into the log files. Click **Apply** to save changes.

Remote Logging

PowerMedia XMS supports the ability to configure remote logging. This functionality allows users the capability to configure system diagnostics logging to a remote server with fluentd, a data collection tool. By using remote logging, users can take advantage of external logging, indexing, and search services to aid in management and troubleshooting tasks.

1. Click the **Host, IPv4, or IPv6** radio button.
2. In the **Remote Logging Daemon IP** field, enter the IP address for remote logging server.
3. In the **Remote Logging Daemon Port** field, specify the port for remote logging server.

4. Click **Apply** to save changes.

Note: The remote logging functionality is in a controlled introduction.

Service Logs

Options

Mask DTMF digits

Remote Logging Daemon IP Host IPv4 IPv6

Remote Logging Daemon Port

Apply

Click column header to change the value for all services

Service Name	Log File Size (MB)	Rotate Log Files	Logging Level
appmanager	10	100	DEBUG
broker	10	100	DEBUG
cdrserver	10	100	DEBUG
eventmanager	10	100	DEBUG
faxservice	10	100	DEBUG
httpclient	10	100	DEBUG
mrcpclient	10	100	DEBUG
msml	10	100	DEBUG
msrpservice	10	100	DEBUG
netann	10	100	DEBUG
nodecontroller	10	100	DEBUG
perfmanager	10	100	DEBUG
rtcweb	10	100	DEBUG
sysmonitor	10	100	DEBUG
verification	10	100	DEBUG
vxml	10	100	DEBUG
wsapiserver	10	100	DEBUG
xmscd	10	100	DEBUG
xmserver	10	100	DEBUG
xmserver-media	10	100	DEBUG
xmserver-signaling	10	100	DEBUG
xmsrest	10	100	DEBUG
xspeechservice	10	100	DEBUG

Download Diagnostics
Purge All Logs

Proceed as follows to configure the **Diagnostics** parameters.

Parameter	Description	Valid Values
Logging		
Service Name	The name of the internal services and protocols.	The services include xmserver, nodecontroller, appmanager, etc. The protocols include MSML, NETANN, VXML, etc.
Logging Level	When troubleshooting issues, additional information can be obtained in the logs by setting the logging level to one of five values. Refer to PowerMedia XMS Troubleshooting for additional information.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • NOTICE: Top logging level and provides references such as "System Started" type messages. • ERROR: Includes NOTICE level prints and provides known error conditions (i.e., "Engine level API FAILURES"). This is the lowest logging level. • WARNING: Includes NOTICE+ERROR prints and flags references that are not errors but could point to potential issues depending on their context. • INFO: Includes NOTICE+ERROR+WARNING prints and provides informational level logging (i.e., new call notification prints). • DEBUG: Includes NOTICE+ERROR+WARNING+INFO prints and provides lower level verbose prints that Dialogic Engineering uses to help trace a problem within the system. This is the highest logging level.
Log File Size (MB)	Sets the desired log file size in megabytes.	Range is 1 to 1000.
Rotate Log Files	Sets the number of files to keep during a service rotation.	Range is 1 to 100. To disable local file logging, enter 0.

The default PowerMedia XMS log location is */var/log/xms*.

Click **Set** and then **Apply** to save changes.

The log files can be cleared by clicking the **Purge All Logs** button.

The diagnostics can be downloaded to your system by clicking the **Download Diagnostics** button.

Download Logs x

Options

Include System Diagnostics

Archive Name	Operations
xms-diag-20161027_101152.tar.gz	

Generate ArchiveClose

Click **Generate Archive** to generate the diagnostics archive or click **Close** to abort the operation. The diagnostics archive file can be downloaded or deleted through the **Operations** column.

Audit Logs

The **Audit Logs** page of the **System** menu provides the capability to view the audit logs that capture the Console and RESTful Management changes performed by users. By default, the records of the audit logs are displayed when the user navigates to the page. The management requests are stored in an internal database and made available through the Console or retrieval commands for viewing or filtering.

The audit logs will store timestamp, IP address, username, request method, request path, and request content for management configuration functions so that administrators can audit the system configuration.

The user can provide a pattern to look for in the filter selected in the database. For example, if the user decides to view records of a particular IP address, select IP Address from the drop-down list in the **Filter** field and enter a pattern that matches the IP address in the **Pattern** field.

The pattern can simply be a substring of the pattern desired (no need for regular expression or wildcard). For example, you could enter 10.20.120 to see the exchanges from the systems on that subnet. Since the audit logs are now displayed on the page, the user would have information on what pattern to enter.

The audit logs can be exported as a csv file by clicking the **Export CSV** button.

Time Stamp	IP Address	UserName	Request Method	Request Path	Request Content Type	Request Content
2016-10-27 10:31:14.267552	10.20.120.21	superadmin	POST	/logs/archivelog	application/json	{\"downloadLogOptions\":{\"system_diagnostics\":\"yes\"}}
2016-10-27 10:31:01.925006	10.20.120.21	superadmin	DELETE	/system/upgrade/dialogic_xms_trunk.14270-0.c6.tgz		
2016-10-27 10:30:59.027019	10.20.120.21	superadmin	DELETE	/system/backup/xmsbackup-20161027-091616.tar.gz		
2016-10-27 10:30:39.531749	10.20.120.21	superadmin	PUT	/services	application/json	{\"graceful_shutdown_timeout\":120}
2016-10-27 10:25:35.439350	10.20.120.21	superadmin	DELETE	/logs/archivelog/rmDwnldArchivelog/xms-diag-20161027_101152.tar.gz		
2016-10-27 10:25:14.225539	10.20.120.21	superadmin	DELETE	/system/debug/purge/AllLog		
2016-10-27 10:23:19.416698	10.20.120.21	superadmin	PUT	/system/debug	application/json	{\"global\": {\"Name\":\"global\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"appmanager\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"broker\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"cdrserver\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"eventmanager\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"faxservice\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"httpclient\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"mrcplient\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"msmi\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"msrpservice\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":10}, {\"Name\":\"netann\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"nodecontroller\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"perfmanager\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":10}, {\"Name\":\"ftcweb\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"sysmonitor\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":10}, {\"Name\":\"verification\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":10}, {\"Name\":\"vxml\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"wsapiserver\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":10}, {\"Name\":\"xmsserver\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"xmsrest\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":100}, {\"Name\":\"xmsstats\",\"log_level\":\"DEBUG\",\"log_maxsize\":10,\"log_maxfiles\":10}}

The following information is displayed:

- TimeStamp
- IP Address
- UserName
- Request Method
- Request Path
- Request Content Type
- Request Content

The total number of audit logs is displayed. To help navigate the list of audit logs, **Next** and **Prev** buttons are available.

Click **Apply** (or press **Enter**) to display or refresh the audit logs.

Note: The **UserName** is unknown when requests come through as RESTful Management commands.

Note: The **Request Content** is not stored when uploading license files, system upgrade packages, and system backup files due to their large size.

Network

From the **Network** menu, you can view and change the [Interface Configuration](#), [DNS Configuration](#), and [NAT Configuration](#).

Note: This **Network** menu applies to system network settings, while the [Protocol](#) menu applies to PowerMedia XMS network settings.

Interface Configuration

The **Interface Configuration** page is used to configure the IPv4/IPv6 network devices. The table displays the number of network devices and their IPv4/IPv6 configurations in the system.

Interface Name	IPv4 Address	IPv6 Address	Mac Address	Status	Action
enp1s0f0				active	DISABLE
enp1s0f1				inactive	ENABLE

Changing network settings may disconnect your XMS admin session. Be prepared to log in again !!!

Click **Interface Name** to display the **Active** network device configuration dialog box.

Note: Having one adaptor with a valid IPv4/IPv6 address is required.

enp1s0f0 Configuration

Interface Name: enp1s0f0

Active
 Use DHCP

	IPv4	IPv6
Address	<input type="text"/>	<input type="text"/>
Subnet / Prefix	<input type="text"/>	<input type="text"/>
Default Gateway	<input type="text"/>	<input type="text"/>

Apply Cancel

If the **Use DHCP** check box is not checked, the static IPv4/IPv6 configurations are provided. Click **Apply** to save changes or click **Cancel** to abort the operation.

Note: The **Default Gateway** field should be the same for all interfaces since it is a system property and enables the creation of the default route. It is mandatory to set this to the same value for all interfaces.

Important Note: IPv6 Settings

Removing or disabling the IPv6 address from any of the listed interfaces can result in unexpected behavior under certain conditions. Specifically, if some services are configured to bind to IPv6 addresses, removing the IPv6 addresses from the interface may result in those services becoming unresponsive.

A proper procedure is to reconfigure all such services to not use the IPv6 networking and then disable/remove the IPv6 from the interface.

The following services can be configured to use IPv6, and therefore may be inadvertently affected if IPv6 addresses are removed from the interfaces without performing the proper procedure outlined above:

- MRCP Client
- VXML
- RESTful Interface
- MSRP
- SIP
- SNMP

DNS Configuration

The DNS Client is configured using the **DNS Configuration** page.

General	
Hostname	<input type="text"/>
DNS search path	<input type="text"/>
IPv4	
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Tertiary DNS	<input type="text"/>
IPv6	
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Tertiary DNS	<input type="text"/>

Proceed as follows to configure the **DNS Configuration** parameters in the **General** section:

1. In the **Hostname** field, enter the name of the host machine.
2. In the **DNS search path** field, enter the search path for DNS.
3. Click **Apply** to save changes.

Proceed as follows to configure the **DNS Configuration** parameters in the **IPv4** and **IPv6** sections:

1. In the **Primary DNS** field, enter the primary DNS IP address.
2. In the **Secondary DNS** field, enter the secondary DNS IP address.
3. In the **Tertiary DNS** field, enter the tertiary DNS IP address.
4. Click **Apply** to save changes.

NAT Configuration

PowerMedia XMS supports the ability to set the external IP address of the system. This is a useful feature when PowerMedia XMS is installed behind a firewall or Network Address Translation (NAT) device that is not address aware. Such is the case when installed in private networks, public or private clouds, or any network configuration in which its endpoints are not publicly accessible. The feature allows users to enter the public facing external IP address either manually (if known) or by discovery when running PowerMedia XMS in the Amazon EC2 public cloud. In the latter case, the system will query the EC2 cloud with the local IP address for the corresponding external address associated with machine image. After the external address is obtained, either entered manually or dynamically retrieved, the system will use the external address for all subsequent IP media transactions. Current support is for IPv4 addresses only.

Interface Configuration | DNS Configuration | **NAT Configuration**

Media

Direct connection to the Internet

Behind NAT (Specify gateway IP below)

Public IP address:

EC2 (public-ipv4)

Remote NAT Traversal

Signaling

Direct connection to the Internet

Behind NAT (Specify gateway IP below)

Public IP address:

EC2 (public-ipv4)

Proceed as follows to configure the **NAT Configuration** parameters:

Media

1. If the system is publicly accessible and has direct connection to the internet, click the **Direct connection to the Internet** radio button. This is the default.
2. If the system is behind a firewall or NAT device that is not address aware, click the **Behind NAT (Specify gateway IP below)** radio button and enter the public facing external IP address manually (if known) in the **Public IP address** field.
3. If the system is in the Amazon EC2 public cloud, click the **EC2 (public-ipv4)** radio button to query the EC2 cloud with the local IP address for the corresponding external address associated with machine image.
4. In the **Remote NAT Traversal** field, click the check box to specify if remote NAT traversal is enabled. When enabled, PowerMedia XMS will automatically detect if a client SIP end point is behind a NAT and update the IP address that audio and video RTP data is streamed to. This is done by comparing the negotiated remote IP address with the actual remote IP address that RTP packets are received from. If the call contains video, PowerMedia XMS will take precautions to get valid media as soon as possible. This functionality is required for SIP end points that do not support STUN/ICE negotiations.
5. Click **Apply** to save changes.

Signaling

1. If the system is publicly accessible and has direct connection to the internet, click the **Direct connection to the Internet** radio button. This is the default.
2. If the system is behind a firewall or NAT device that is not address aware, click the **Behind NAT (Specify gateway IP below)** radio button and enter the public facing external IP address manually (if known) in the **Public IP address** field.
3. If the system is in the Amazon EC2 public cloud, click the **EC2 (public-ipv4)** radio button to query the EC2 cloud with the local IP address for the corresponding external address associated with machine image.
4. Click **Apply** to save changes.

License

From the **License** menu, you can view the **License Manager** page.

License Manager

PowerMedia XMS Release 4.0 introduces cloud licensing deployment options through a revised product licensing mechanism. The new licensing mechanism provides a cloud-based network-wide licensing scheme to the PowerMedia XMS/MRB solution, in addition to a node-locked license mechanism. This product enhancement provides features entitled to a product license code that can be used among one or more instances to provide a dynamic pool of media server resources.

In this release, the PowerMedia XMS product licensing mechanism changes from the product specific node-locked (Node ID) license file to a cloud license model or a node-locked license model, enabled through a product license code. The product license code is installed on the product with product entitlements stored in the cloud. One product license code can be used to enable a single product instance or multiple product instances.

License Types

Verification License

PowerMedia XMS comes with a 1-port verification license to verify connectivity and check single port media and signaling activation. The 1-port verification license is enabled by default when no other PowerMedia XMS license is active. The verification license enables 1 Basic Audio port.

Trial License (4-port/45-day)

PowerMedia XMS software can be requested by filling out a form through the Dialogic website at <http://www.dialogic.com/xms/xms-download>.

PowerMedia XMS software comes with access to a 4-port license for a 45-day limited trial. The PowerMedia XMS trial license can be activated by clicking the **Trial License** button on the **License Manager** page through the PowerMedia XMS Admin Console. The user must fill in the form details to activate the trial license. Refer to the [Trial License](#) section for more information.

The trial license includes the following PowerMedia XMS features:

- 4 Basic Audio, 4 HD Voice (No AMR-WB), 4 Advanced Video, 4 LBR, 4 High Resolution Video, 4 MRCP Speech Server, and 4 MSRP.

Note: The trial license will allow use of all other HD Voice codecs (such as G.722, Opus, and EVS) but not AMR-WB, even though it is enabled with an HD Voice License.

This trial license is not intended to provide access to all product capability.

Note: A trial license can only be activated once per individual computer. If the individual computer was previously activated with a trial or regular license code, it does not qualify for a trial license.

Evaluation and Production Licenses

PowerMedia XMS production licenses, evaluation licenses for larger session installations or subscriptions can be obtained through your authorized Dialogic distributor or by contacting Dialogic Inside Sales (insidesales@dialogic.com).










The following licensing capabilities are supported:

- **Cloud Licensing:** PowerMedia XMS feature entitlements are stored in the cloud and the user is provided a product license code installable on each PowerMedia XMS instance. The feature resources of the cloud license can be shared among each of the PowerMedia XMS instances that are activated to that product license code.
- **License Server Licensing:** PowerMedia XMS feature entitlements are stored in the cloud and transferred to a local license server using a product license code. The local license server is enabled with its own master license code and distributes PowerMedia XMS features to share among local PowerMedia XMS instances.
- **Node-Locked Licensing:** PowerMedia XMS feature entitlements are provided through a product license code installable on the PowerMedia XMS instance.

License Features

The **Licensed Features** section of the **License Manager** page displays the licensed amounts of each feature and allows configuration of feature usage parameters.

Note: To modify or make any changes to the license, XMS services must be stopped.

Licensed Features				
Feature	Local Usage Limit	Local Maximum	License Maximum	Advanced Parameters
Basic Audio	100	100	100	
HD Voice	100	100	100	
LBR Audio	100	100	100	
GSMAMR Audio	100	100	100	
Advanced Video	100	100	100	
High Resolution Video	100	100	100	
MRCP Speech Server	100	100	100	
MSRP	100	100	100	
Fax	100	100	100	
JSR309	1	1	1	
MRB	1	1	1	

The **Licensed Features** section columns include the feature, local usage limit, local maximum, license maximum, and advanced parameters.

Feature – The name of the feature.

Local Usage Limit – The configured number of (maximum) elements that can be used by the local instance.

Local Maximum – The maximum number of elements supported on any XMS instance for configuration.

License Maximum – The maximum number of elements in the license pool.

Advanced Parameters - To configure the licensed feature, click the pencil button from column of the licensed feature you wish to modify. The following dialog box will appear.

Note: The scaling functionality is currently disabled and reserved for future use. The scaling fields and behaviors are subject to change.

Feature Configuration	
Feature:	HD Voice
Scaling Profile:	No Scaling
Local Usage Limit:	100
Minimum Allocation:	100
Block Size:	0
Next Block Threshold:	0
Idle Block Release Timer: (1 - 120 seconds)	0

1. In the **Feature** field, the name of the licensed feature is displayed.
2. In the **Scaling Profile** field, set the scaling profile. The scaling profile is a preset of license scaling parameters for a feature. The "No Scaling" displayed is the only profile available since scaling is currently disabled.
3. In the **Local Usage Limit** field, enter the local usage limit. The local usage limit is the number of elements that this XMS node is permitted to check out from the license server. When sharing a license among several XMS nodes, this parameter can be used to prevent one XMS node from consuming the entire license.

Note: The local usage limit can be modified at any time after a license has been configured. If the local usage limit is not configured, it will automatically be calculated on the next activation.
4. In the **Minimum Allocation** field, enter the minimum allocation. The minimum allocation is the initial number of feature elements to check out from the license server upon license activation. This parameter is only configurable when license scaling is enabled.
5. In the **Block Size** field, enter the block size. The block size is the number of feature elements in a block. When scaling is enabled, blocks of feature elements are checked out from the licensing server as demand increases and returned back to the licensing server after a block has remained unused for a configured period of time.
6. In the **Next Block Threshold** field, enter the next block threshold. The next block threshold is when the number of feature elements of a block become active (in use), the next block will be checked out from the licensing server in order to be available when needed. Setting this number too large may cause license starvation as the next free block will not have arrived from the license server by the time the current block is completely used. This field will be a value parameter that represents a percentage (%) of used elements in the block. For example, if block size is 50 and you choose 25 once the 25th element (50%) is used, a new block is secured.
7. In the **Idle Block Release Timer** field, enter the idle block release timer in seconds. Valid values are 1-120 (seconds). If a block of license feature elements remains unused for this amount of time, it will be returned to the license server. Setting this value too low may cause the license feature element blocks to be returned to the server prematurely and not be available on the local XMS to handle an activity spike.
8. Click **Apply** to save changes or click **Close** to abort the operation.

License Configuration

The **License Configuration** section of the **License Manager** page provides license configuration options to select the license type and set access methods. Details are described separately for [Trial License](#), [Cloud License](#), [Local Server License](#), and [Node-Locked License](#).

When XMS services are started, if the configured license is not activated, it will be automatically activated.

Note: To modify or make any changes to the license, XMS services must be stopped.

License Configuration	
License Code:	<input type="text"/>
License Type:	<input checked="" type="radio"/> Cloud <input type="radio"/> Local Server <input type="radio"/> Node Locked
Server Connection:	<input checked="" type="radio"/> Direct <input type="radio"/> Relay <input type="radio"/> Proxy
Deactivate License on Services Stop:	<input checked="" type="checkbox"/>
<input type="button" value="Test Connection"/> <input type="button" value="Apply"/>	

Trial License

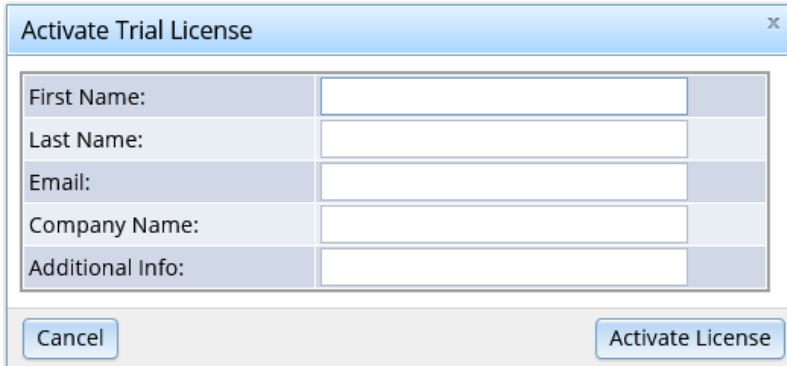
Note: A trial license can only be activated once per individual computer. If the individual computer was previously activated with a trial or regular license code, it does not qualify for a trial license.

License Configuration	
License Code:	<input type="text"/>
License Type:	<input checked="" type="radio"/> Cloud <input type="radio"/> Local Server <input type="radio"/> Node Locked
Server Connection:	<input checked="" type="radio"/> Direct <input type="radio"/> Relay <input type="radio"/> Proxy
Deactivate License on Services Stop:	<input checked="" type="checkbox"/>
<input type="button" value="Test Connection"/> <input type="button" value="Apply"/>	

License Information	
Status:	<input type="text"/>
Node Id:	<input type="text"/>
Device Id:	<input type="text"/>
Maximum Activations:	<input type="text"/>
Expiration Date:	<input type="text"/>
Maintenance Expiration Date:	<input type="text"/>
<input type="button" value="Help"/> <input type="button" value="Event Log"/> <input type="button" value="Trial License"/> <input type="button" value="Refresh"/> <input type="button" value="Activate License"/>	

Activation (Trial)

1. Click **Trial License**. The following dialog box will appear.



Activate Trial License	
First Name:	<input type="text"/>
Last Name:	<input type="text"/>
Email:	<input type="text"/>
Company Name:	<input type="text"/>
Additional Info:	<input type="text"/>
Cancel Activate License	

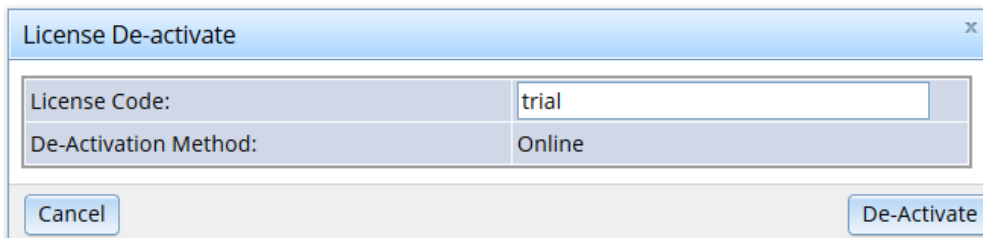
The information is used to associate customer reference information for contacting Dialogic about the trial activation. Dialogic does not identify a specific trial instance without this information.

Note: It is recommended that the user should have first created a Dialogic account. If a Dialogic account is not already registered, please contact Dialogic.

2. In the **First Name** field, enter first name (i.e., first name from Dialogic account).
3. In the **Last Name** field, enter last name (i.e., last name from Dialogic account).
4. In the **Email** field, enter email address (i.e., email address from Dialogic account).
5. In the **Company** field, enter company name (i.e., company name from Dialogic account).
6. In the **Additional Info** field, enter any additional information such as the customer reference.
7. Click **Activate License** to activate license or click **Cancel** to abort the operation. A confirmation message appears.
8. In the **Status** field under the **License Information** section, there should be "ACTIVATED" status displayed.

Deactivation (Trial)

1. Click **De-Activate**. The following dialog box will appear.



License De-activate	
License Code:	trial
De-Activation Method:	Online
Cancel De-Activate	

2. In the **License Code** field, the "trial" license code you previously activated on the system is displayed.
3. Click **De-Activate** to deactivate license or click **Cancel** to abort the operation. A confirmation message appears.
4. In the **Status** field under the **License Information** section, there should be "VERIFICATION" status displayed.

Cloud License

The cloud licensing is accessible via the internet and requires no independent configuration or management. License configuration for the cloud license is provided to facilitate network connection to the cloud licensing through direct, relay, or proxy. The cloud license can be shared between instances that use the same license code.

License Configuration	
License Code:	<input type="text"/>
License Type:	<input checked="" type="radio"/> Cloud <input type="radio"/> Local Server <input type="radio"/> Node Locked
Server Connection:	<input checked="" type="radio"/> Direct <input type="radio"/> Relay <input type="radio"/> Proxy
Deactivate License on Services Stop:	<input checked="" type="checkbox"/>

Click **Test Connection** to test the connection and verify that the cloud licensing is reachable. A confirmation message appears.

Activation (Cloud)

1. In the **License Code** field, enter the license code that you obtained from Dialogic.
2. In the **License Type** field, click the **Cloud** radio button to configure cloud license type.
3. In the **Server Connection** field, select an option from the radio buttons to configure the server connection.
 - o **Direct** - Select this option if your server has direct access to the internet.

License Configuration	
License Code:	<input type="text"/>
License Type:	<input checked="" type="radio"/> Cloud <input type="radio"/> Local Server <input type="radio"/> Node Locked
Server Connection:	<input checked="" type="radio"/> Direct <input type="radio"/> Relay <input type="radio"/> Proxy
Deactivate License on Services Stop:	<input checked="" type="checkbox"/>

- o **Relay** - Select this option if you have configured a port forwarding relay server that has access to the internet. Enter the IP address and port (Default value is 16700) of your relay server.

License Configuration	
License Code:	<input type="text"/>
License Type:	<input checked="" type="radio"/> Cloud <input type="radio"/> Local Server <input type="radio"/> Node Locked
Server Connection:	<input type="radio"/> Direct <input checked="" type="radio"/> Relay <input type="radio"/> Proxy
Ip Address:	<input type="text"/>
Port:	<input type="text" value="16700"/>
Deactivate License on Services Stop:	<input checked="" type="checkbox"/>

- **Proxy** - Select this option if you are using a proxy server to access the internet. A proxy server requires username and password authentication and provides port forwarding. Enter the IP address and port of your proxy server and choose the account name that contains the credentials for your proxy server from the drop-down list (configured through the **Account** section on **Secure Storage** page).

License Configuration	
License Code:	<input type="text"/>
License Type:	<input checked="" type="radio"/> Cloud <input type="radio"/> Local Server <input type="radio"/> Node Locked
Server Connection:	<input type="radio"/> Direct <input type="radio"/> Relay <input checked="" type="radio"/> Proxy
Ip Address:	<input type="text"/>
Port:	<input type="text"/>
Account Name:	None <input type="text"/>
Deactivate License on Services Stop:	<input checked="" type="checkbox"/>

4. In the **Deactivate License on Services Stop** field, select the check box to specify if the license should be automatically deactivated when services are stopped. If not already activated, the license is always automatically activated when services are started. If you prefer to have XMS keep the license activated when services are stopped, deselect the check box. It is recommended to leave this check box selected (default).

Note: A cloud license must always be deactivated prior to terminating the XMS instance. It is recommended to deactivate the license on services stop so a license does not remain active when not in use.

5. Click **Apply** to save changes. A confirmation message appears.
6. Click **Activate License** to activate the license. A confirmation message appears.
7. In the **Status** field under the **License Information** section, there should be "ACTIVATED" status displayed.

Deactivation (Cloud)

When a license is deactivated, resources are returned to the server.

1. Click **De-Activate**. The following dialog box will appear.

License De-activate	
License Code:	<input type="text"/>
De-Activation Method:	Online
<input type="button" value="Cancel"/> <input type="button" value="De-Activate"/>	

2. In the **License Code** field, the license code you previously activated on the system is displayed.
3. Click **De-Activate** to deactivate the license or click **Cancel** to abort the operation. A confirmation message appears.
4. In the **Status** field under the **License Information** section, there should be "CONFIGURED" status displayed.

Note: The license deactivation does not unconfigure a license. A license can be unconfigured by clearing the license code from **License Code** field and clicking **Apply**. By removing the license configuration, the XMS system returns to using the verification license.

Local Server License

Note: As a controlled introduction, customers interested in this functionality should contact their Dialogic Sales Representative or Technical Support Service Engineer for further information on usage.

Node-Locked License

The node-locked license is locked to the XMS instance. The node-locked license is activated to the instance using a certificate exchange. Once activated and locked to an instance, the node-locked license can only be moved to another instance by first deactivating the current instance and activating the license on another instance.

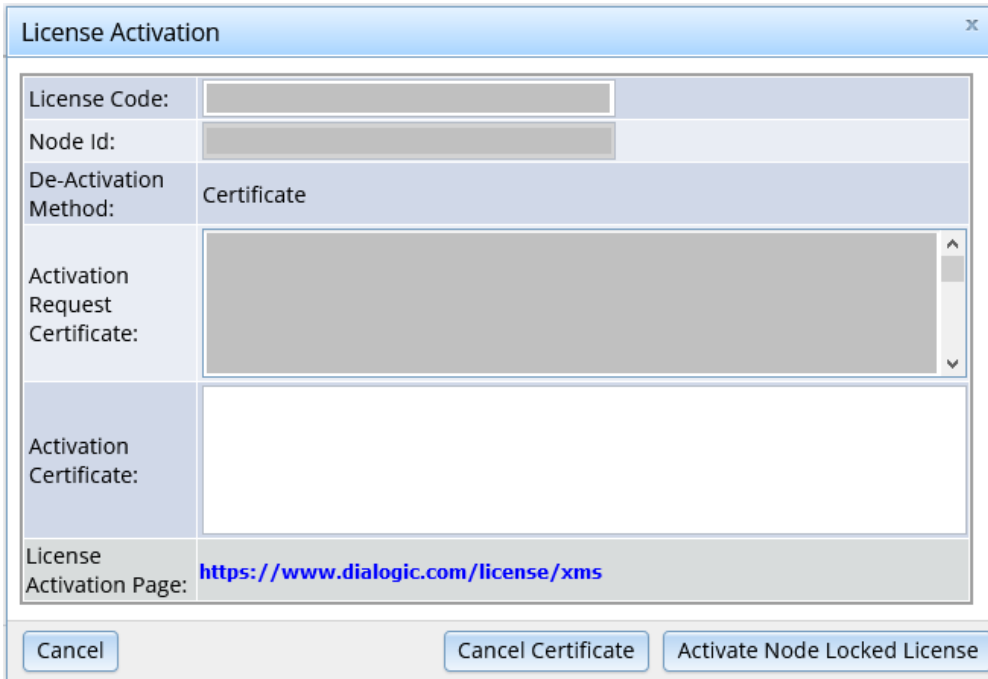
The node-locked license is activated by exchanging certificates between the PowerMedia XMS Admin Console and Dialogic Licensing Web Portal at <http://www.dialogic.com/license/xms>.

The Dialogic Licensing Web Portal can only be viewed if you are registered and logged in through the Dialogic website. If you have already registered but do not have the rights required, please contact Dialogic.

Activation (Node-Locked)

1. In the **License Code** field, enter the license code that you obtained from Dialogic.
2. In the **License Type** field, click the **Node Locked** radio button to configure node-locked license type.
3. Click **Apply** to save changes. A confirmation message appears.

- Click **Activate License**. The following dialog box will appear.



The dialog box is titled "License Activation" and contains the following fields and controls:

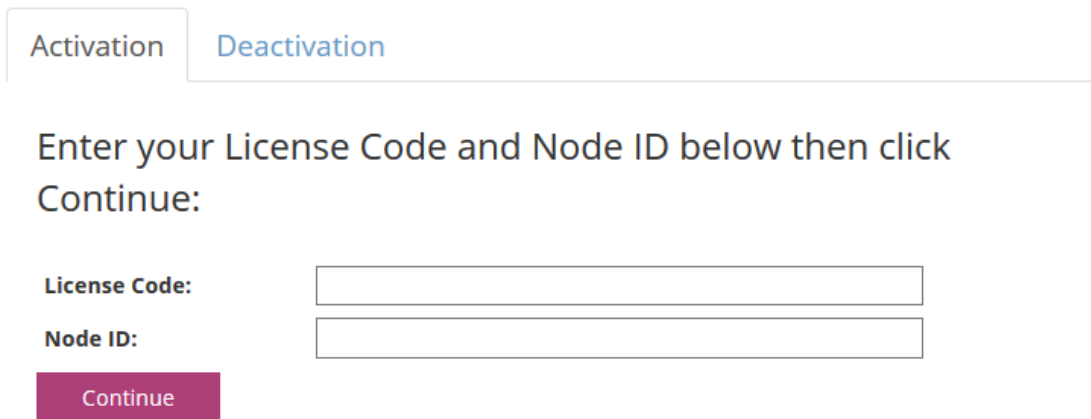
- License Code:
- Node Id:
- De-Activation Method: Certificate
- Activation Request Certificate:
- Activation Certificate:
- License Activation Page: <https://www.dialogic.com/license/xms>

Buttons at the bottom: Cancel, Cancel Certificate, Activate Node Locked License

- Copy the resulting **Activation Request Certificate** character string to a system with internet access to submit through the Dialogic Licensing Web Portal to acquire the **Activation Certificate** character string.

For example, create an activation text file, paste the **Activation Request Certificate** character string in, and save it to a removable USB memory drive.

- To get the **Activation Certificate** character string for the **Activation Certificate** field, you will need to visit <http://www.dialogic.com/license/xms> on a system with internet access. The following page will appear.



The page has two tabs: "Activation" (selected) and "Deactivation".

Enter your License Code and Node ID below then click Continue:

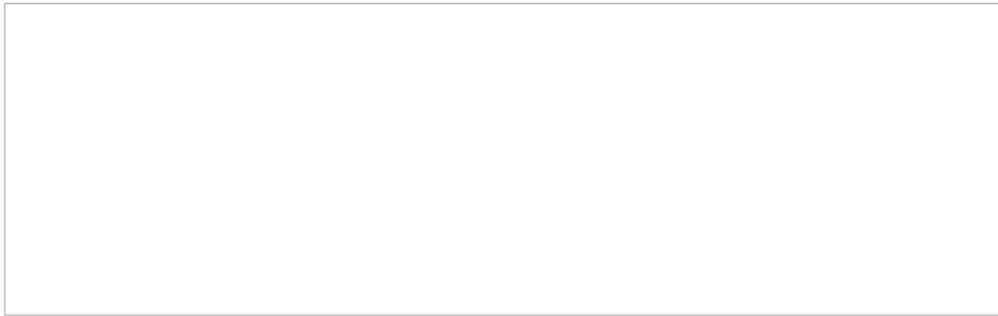
License Code:

Node ID:

- In the **License Code** field, enter the license code that you obtained from Dialogic.
- In the **Node ID** field, enter the node ID for the system to be activated. The node ID can be found under the **License Information** section through the PowerMedia XMS Admin Console.
- Click **Continue** to proceed to next page.
- In the **Activation Certificate** field, enter the **Activation Request Certificate** character string copied from the [Activation Request Certificate](#) step.

For example, access the activation text file and paste the **Activation Request Certificate** character string from the removable USB memory drive into the **Activation Certificate** field.

Activation Certificate



Activate Back



11. Click **Activate** to get the **Activation Certificate** character string or click **Back** to return to previous page. A new character string is presented. This is the **Activation Certificate** character string.
12. In the **License** field, copy the resulting **Activation Certificate** character string to be used on the **Licensing Manager** page through the PowerMedia XMS Admin Console.

For example, create a text file, paste the **Activation Certificate** character string in, and save it to a removable USB memory drive.

Note: If you cannot complete the operation immediately, save the **Activation Certificate** character string as it cannot be regenerated.

License



Copy to ClipBoard Back



- Return to the **Licensing Manager** page through the PowerMedia XMS Admin Console to complete activation.
- In the **Activation Certificate** field, paste the **Activation Certificate** character string copied from the Dialogic Licensing Web Portal.
For example, access the text file and paste the **Activation Certificate** character string from the removable USB memory drive into the **Activation Certificate** field.

- Click **Activate Node Locked License** to activate the license or click **Cancel Certificate** to cancel certificate or click **Cancel** to abort the operation. A confirmation message appears.
- In the **Status** field under the **License Information** section, there should be "ACTIVATED" status displayed.

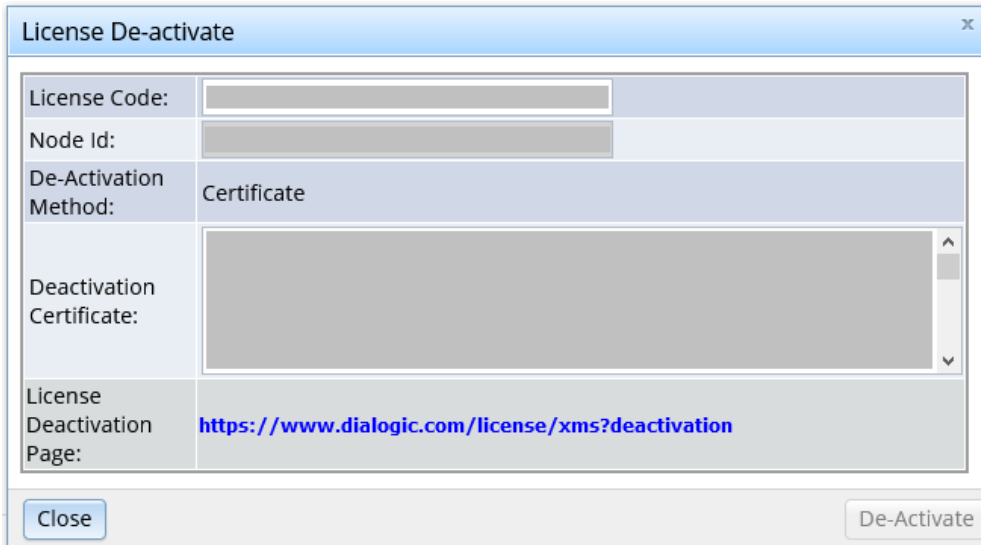
Deactivation (Node-Locked)

When a license is deactivated, resources are returned to the server.

- Click **De-Activate**. The following dialog box will appear.

- In the **License Code** field, the license code you previously activated on the system is displayed.
- In the **De-Activation Method** field, the "Certificate" activation method is displayed.
- Click **De-Activate** to create deactivation certificate or click **Cancel** to abort the operation.

5. By clicking **De-Activate**, the following dialog box will appear.



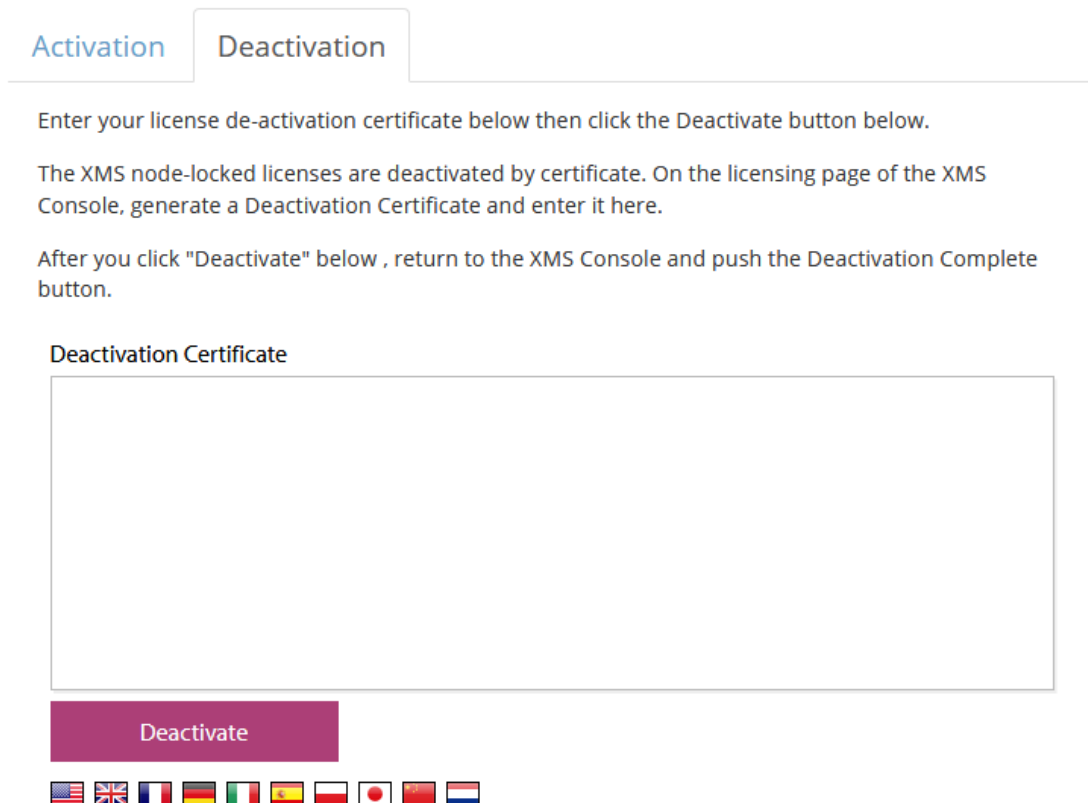
The dialog box is titled "License De-activate" and contains the following fields and controls:

- License Code:
- Node Id:
- De-Activation Method: Certificate
- Deactivation Certificate:
- License Deactivation Page: <https://www.dialogic.com/license/xms?deactivation>
- Buttons: Close, De-Activate

6. Copy the resulting **Deactivation Certificate** character string to a system with internet access to submit through the Dialogic Licensing Web Portal.

For example, create a text file, paste the **Deactivation Certificate** character string in, and save it to a removable USB memory drive.

7. To proceed with deactivating the certificate, you will need to visit <http://www.dialogic.com/license/xms> on a system with internet access. The following page will appear.



The page has two tabs: "Activation" and "Deactivation". The "Deactivation" tab is selected.


Enter your license de-activation certificate below then click the Deactivate button below.

The XMS node-locked licenses are deactivated by certificate. On the licensing page of the XMS Console, generate a Deactivation Certificate and enter it here.

After you click "Deactivate" below, return to the XMS Console and push the Deactivation Complete button.

Deactivation Certificate

Deactivate



8. In the **Deactivation Certificate** field, enter the **Deactivation Certificate** character string copied from [Deactivation Certificate](#) step.
For example, access the text file and paste the **Deactivation Certificate** character string from the removable USB memory drive into the **Deactivation Certificate** field.
9. Click **Deactivate** to deactivate the certificate.
10. Return to the **Licensing Manager** page through the PowerMedia XMS Admin Console to complete deactivation.

License Information	
License Code:	<input type="text"/>
Status:	<input type="text"/>
Node Id:	<input type="text"/>
Device Id:	<input type="text"/>
Maximum Activations:	<input type="text"/>
Expiration Date:	<input type="text"/>
Maintenance Expiration Date:	<input type="text"/>
De-activation Certificate:	<input type="text"/>

11. Click **Complete De-Activation** to deactivate the license. A confirmation message appears.
12. In the **Status** field under the **License Information** section, there should be "CONFIGURED" status displayed.

Note: The license deactivation does not unconfigure a license. A license can be unconfigured by clearing the license code from **License Code** field and clicking **Apply**. By removing the license configuration, the XMS system returns to using the verification license.

License Information

The **License Information** section of the **License Manager** page provides information on the activated license.

Click **Help** to view help information for license parameters. Click **Event Log** to view or download the licensing event log. Click **Refresh** to reload the license information. Click **De-Activate** to deactivate the license.

Note: If a license has not been activated, the **Trial License** and **Setup License** options are available.

License Information	
Status:	ACTIVATED
Node Id:	
Device Id:	
Maximum Activations:	
Expiration Date:	
Maintenance Expiration Date:	

[Help](#) [Event Log](#) [Refresh](#) [De-Activate](#)

The **License Information** section include status, node ID, device ID, maximum activations, expiration date, and maintenance expiration date.

Status – The status of the license will display whether the license is verification, trial, activated, or inactive.

Node ID – The XMS instance node ID.

Device ID – The internal XMS device ID associated with the instance.

Maximum Activations – The number of XMS instances that can activate against a license code.

Expiration Date – The expiration date of the license used for subscription or evaluation licenses.

Maintenance Expiration Date – The current expiration date for maintenance support for the product license.

Note: PowerMedia XMS will prevent software update to a release that is more current than the maintenance date.

Protocol

The **Protocol** menu contains the following tabbed pages: **SIP** and **RTP**.

Note: This **Protocol** menu applies to PowerMedia XMS network settings, while the [Network](#) menu applies to system network settings.

SIP

The **SIP** page is used to configure the SIP details.

SIP	RTP
IPv4 Address:	DEFAULT
IPv6 Address:	DISABLE
Port:	5060
Transport:	<input checked="" type="checkbox"/> Accept TCP Requests <input checked="" type="checkbox"/> Outgoing Requests Default
Session Timeout (seconds):	1800
MIME Buffer Size (KB):	12
Enable SIP Precondition:	<input type="checkbox"/>
Enable User Agent:	<input checked="" type="checkbox"/>
Send 180 Response:	<input checked="" type="checkbox"/>
<input type="checkbox"/> Enable TLS <input type="checkbox"/> Restrict Access to Specified Host	
<input type="button" value="Apply"/>	

The following information is provided.

Item	Description
IPv4 Address	<p>Specifies the SIP IPv4 address. The following values are available from the drop-down list:</p> <ul style="list-style-type: none"> • DEFAULT - This value causes xmserver to use the first non-local address reported by the OS. This will allow a new ISO installation to boot and take SIP or WebRTC calls. For further testing or production, the default should always be replaced with the explicit IP address of the desired Ethernet interface (not an Ethernet device name) on the system. • DISABLE - This value disables this parameter.
IPv6 Address	<p>Specifies the SIP IPv6 address. The following values are available from the drop-down list:</p> <ul style="list-style-type: none"> • DEFAULT - This value causes xmserver to use the first non-local address reported by the OS. This will allow a new ISO installation to boot and take SIP or WebRTC calls. For further testing or production, the default should always be replaced with the explicit IP address of the desired Ethernet interface (not an Ethernet device name) on the system. • DISABLE - This value disables this parameter.

Item	Description
Port	Specifies the SIP listening port. Default value is 5060.
Transport	Displays the transport protocol. The following protocols are available from the drop-down list: <ul style="list-style-type: none"> • UDP (User Datagram Protocol) • TCP (Transmission Control Protocol) • UDP_TCP (User Datagram Protocol - Transmission Control Protocol)
Session Timeout (seconds)	Specifies the session timeout in seconds. Valid values are 0, 90 to 86,400. A value of 0 disables the timer. Default value is 1800. An application must indicate to use the Session Timeout parameter in its initial INVITE offer.
MIME Buffer Size (KB)	Specifies the MIME buffer size in KB. Valid values are 12 to 60. Default value is 12. Note: When the MSML audit results in a large payload, that response may never be sent. Increasing the MIME buffer size may alleviate the issue. However, if the response payload is still larger than the maximum MIME buffer size, the response will still fail to be sent.
Enable SIP Precondition	Handles SIP calls in order to hold off session establishment until the SIP preconditions are met. Click the check box to enable SIP precondition.
Enable User Agent	Includes the User-Agent header in outgoing SIP messaging when selected.
Send 180 Response	Includes the 180 Ringing response to invites. When deselected, the 180 Ringing response is not sent.
Enable TLS	Handles SIP TLS when selected. Refer to Enable TLS for details.
Restrict Access to Specified Host	Restricts access to a specified host when selected. Refer to Restrict Access to Specified Host for details.

Changing the SIP IP address is necessary when you have multiple e-net interfaces and want to switch among them, or if you have manually changed the address for the single e-net interface. Refer to the [Network](#) menu for more information.

Click **Apply** to save changes.

Note: A services restart is required when any changes are made to SIP interface configurations.

Enable TLS

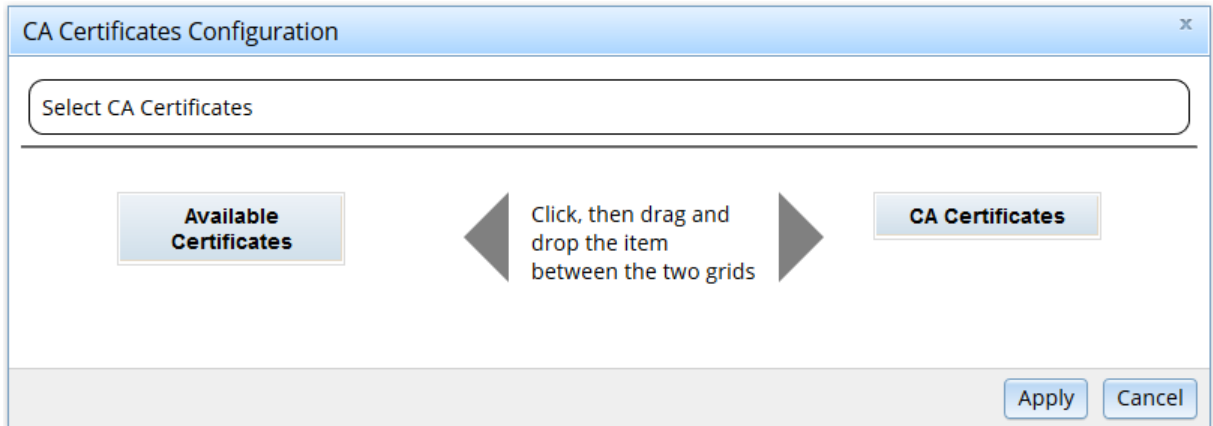
SIP Transport Layer Security (TLS) is a security mechanism for SIP call control that operates on the transport layer. SIP TLS is an added security measure that utilizes the secure storage functionality through the **Public Key Infrastructure** section on **Secure Storage** page to store certificates and provide secure signaling with trusted SIP endpoints. Prior to configuring SIP TLS, a user needs to upload certificate into the secure storage and name the certificate. The certificate would then be available as a configuration option.

SIP	RTP
IPv4 Address:	DEFAULT
IPv6 Address:	DISABLE
Port:	5060
Transport:	<input checked="" type="checkbox"/> Accept TCP Requests <input checked="" type="checkbox"/> Outgoing Requests Default
Session Timeout (seconds):	1800
MIME Buffer Size (KB):	12
Enable SIP Precondition:	<input type="checkbox"/>
Enable User Agent:	<input checked="" type="checkbox"/>
Send 180 Response:	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Enable TLS	
DSS Certificate:	None
RSA Certificate:	None
CA Certificate:	Click_To_Configure_Certificate
Chain Certificate:	Click_To_Configure_Certificate
Certificate Revocation Lists:	Click_To_Configure_Certificate
Enable Client Authentication:	<input type="checkbox"/>
Enable Session Cache:	<input type="checkbox"/>
Tls Port:	5061
<input type="checkbox"/> Restrict Access to Specified Host	
<input type="button" value="Apply"/>	

Proceed as follows to configure the **Enable TLS** parameters:

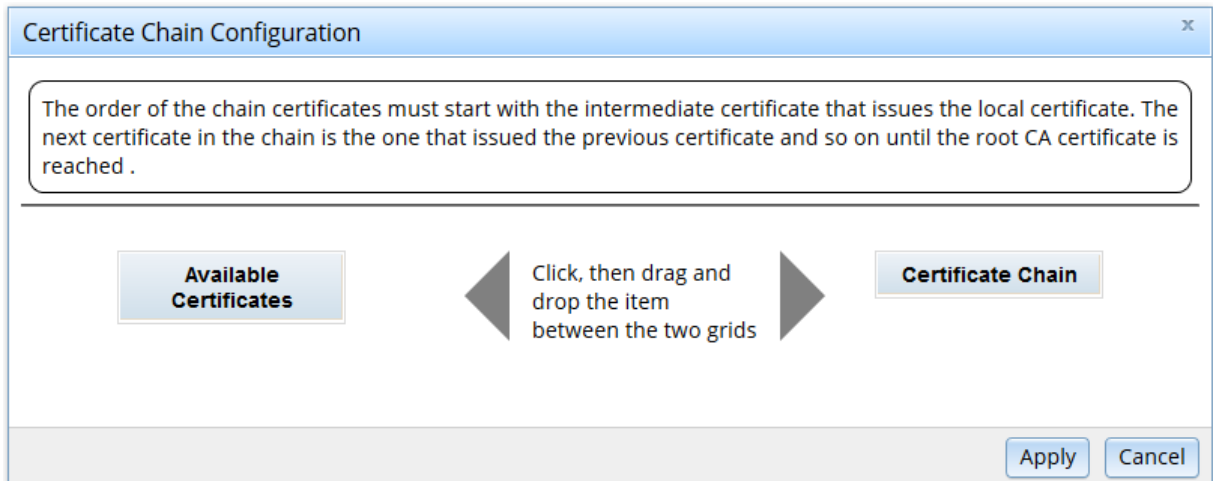
1. In the **Enable TLS** field, click the check box to specify if TLS configuration is enabled.
2. In the **DSS Certificate** field, select the DSS certificate from the drop-down list. DSS specifies the digital signature algorithm appropriate for applications requiring digital signature.

3. In the **RSA Certificate** field, select the RSA certificate from the drop-down list. RSA is a public key encryption technology.
4. In the **CA Certificate** field, click option to configure CA certificate. A certificate authority authorizes certificates by signing the contents using its private key.



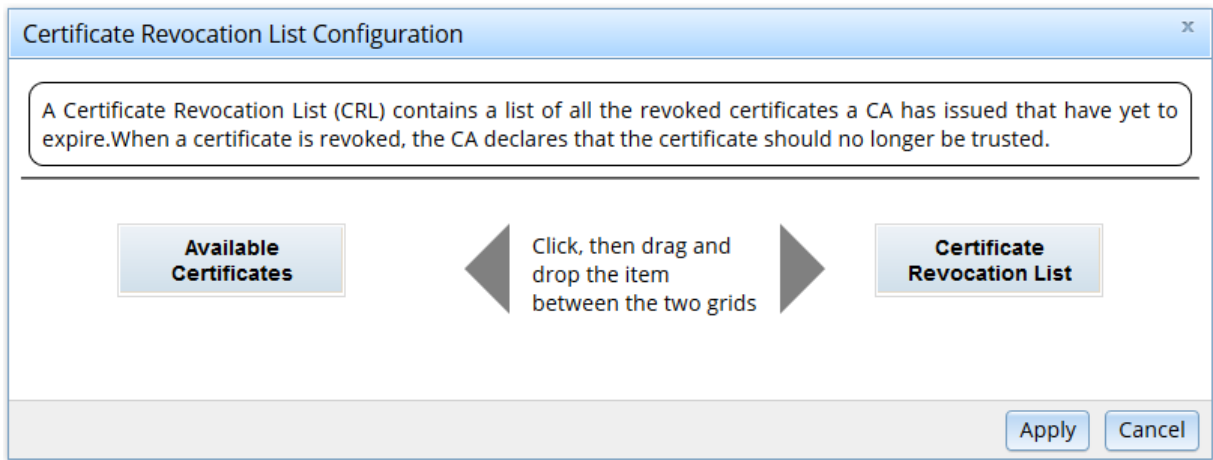
Click, then drag and drop the item between the two grids. Click **Apply** to save changes or click **Cancel** to abort the operation.

5. In the **Chain Certificate** field, click option to configure certificate chain. A certificate chain is a sequence of certificates, where each certificate in the chain is signed by the subsequent certificate. The order of the chain certificates must start with the intermediate certificate that issues the local certificate. The next certificate in the chain is the one that issued the previous certificate and so on until the root CA certificate is reached.



Click, then drag and drop the item between the two grids. Click **Apply** to save changes or click **Cancel** to abort the operation.

6. In the **Certificate Revocation Lists** field, click option to configure revocation certificate. A certificate revocation list contains a list of all the revoked certificates a CA has issued that have yet to expire. When a certificate is revoked, the CA declares that the certificate should no longer be trusted.



Click, then drag and drop the item between the two grids. Click **Apply** to save changes or click **Cancel** to abort the operation.

7. In the **Enable Client Authentication** field, click the check box to specify if client authentication is enabled.
8. In the **Enable Session Cache** field, click the check box to specify if session cache is enabled.
9. In the **Tls Port** field, enter the TLS port. Default value is 5061.
10. Click **Apply** to save changes.

Restrict Access to Specified Host

From the **Restrict Access to Specified Host** window, you can restrict access to trusted specified hosts.

The screenshot shows the configuration window for SIP settings. The 'SIP' tab is active. The 'Restrict Access to Specified Host' checkbox is checked, and the 'Host Address' field is empty. The 'Trusted Host List' is also empty. The 'Apply' button is visible at the bottom.

In the **Restrict Access to Specified Host** field, click the check box to specify if restricting access to specified host is enabled.

Enter the address you wish to add as a trusted host in the **Host Address** field and click **Add**. The address will be listed in the **Trusted Host List** section.

To delete a trusted host, click the address listed in the **Trusted Host List** section and click **Delete**.

Click **Apply** to save changes.

RTP

The **RTP** page is used to configure **Media Engine**, **RTP Timeout**, **SRTP**, and **Telephony Events** parameters.

SIP RTP

Media Engine

Interface Name	IPv4 Address	IPv6 Address	Type Of Service
eth0	234.234.234.234	None	0

Media Route Profiles

Edit New Delete

Status	Name	Match Field	Match Pattern	TOS	NIC
<					>

RTP Timeout

RTP Timeout Audio:	30000
RTCP Timeout Audio:	15000
RTP Timeout Video:	30000
RTCP Timeout Video:	15000

SRTP

Lifetime:	2147483648
Key Rotation:	1
Accept:	<input checked="" type="checkbox"/>
Enforce:	<input type="checkbox"/>
Unencrypted RTP:	<input type="checkbox"/>
Unencrypted RTCP:	<input type="checkbox"/>
Window Size Hint:	64

Telephony Events

Telephony Event:	0-15
------------------	------

Apply

Media Engine

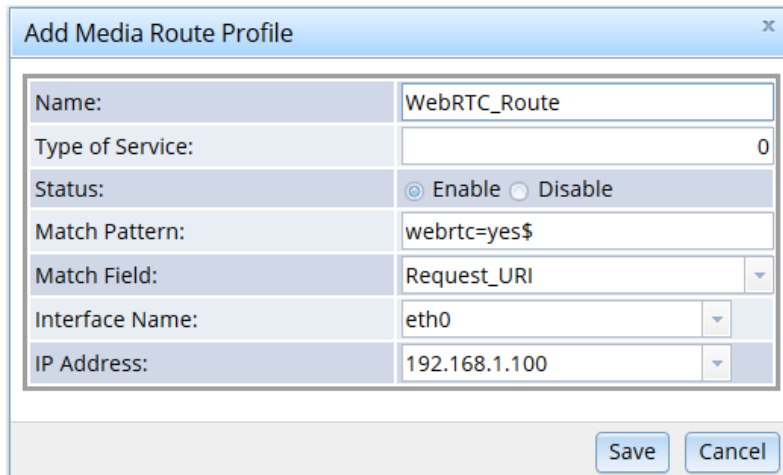
Proceed as follows to configure the **Media Engine** parameters:

1. In the **Interface Name** field, select the interface name to be used for media from the drop-down list.
2. In the **IPv4 Address** and **IPv6 Address** fields, select the default IP address to be used for media from the drop-down list.
3. In the **Type Of Service** field, enter the type of service to be specified in IPv4 headers. This can be either a 7-bit ToS (Type of Service) field or a 6-bit DSCP (Differentiated Services Code Point) field per RFC 2474. Valid values are 0 to 255. Default value is 0.
4. Add, edit, or delete media route profiles in the **Media Route Profiles** section. Refer to [Media Route Profiles](#) for details.
5. Click **Apply** to save changes.

Media Route Profiles

In the **Media Engine** section, **Media Route Profiles** allows you to partition media traffic from different networks using a designated network interface card (NIC) when connecting to the XMS. The media route profiles tell the XMS which IP address to use when establishing a media session with a remote user agent. This feature expands the functionality of the XMS for multiple network interface card (multi-NIC) support.

To add a media route profile, click **New** and configure the parameters in the **Add Media Route Profile** window. To edit a media route profile, select an existing media route profile, click **Edit**, and configure the parameters in the **Edit Media Route Profile** window. To delete a media route profile, select an existing media route profile and click **Delete**.



Add Media Route Profile	
Name:	WebRTC_Route
Type of Service:	0
Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Match Pattern:	webrtc=yes\$
Match Field:	Request_URI
Interface Name:	eth0
IP Address:	192.168.1.100

Save Cancel

The following information is provided.

Parameter	Description
Name	Name of the media route profile.
Type of Service	Apply the routing priority to transmitted packets. Valid values are 0 through 255. Default value is 0.
Status	Enable or disable the media route profile.
Match Pattern	Enter a Perl regular expression. Any valid regular expression is accepted. The system will compare the Match Field string with the regular expression. If the pattern matches, the media route profile is applied.
Match Field	Identify the field that the system will parse to determine if a media route profile is applied. Valid values are Request_URI and Connection. If using the Connection value, the XMS will parse the entire connection line (c=) in a request SDP to determine if a media route profile is applied.
Interface Name	Select the interface. The IP Address field will be populated with available addresses for the selected interface.
IP Address	Select the IP address.

In the **Add Media Route Profile** and **Edit Media Route Profile** windows, click **Save** to save changes. Click **Cancel** to abort the changes and to return to the **RTP** page. On the **RTP** page, click **Apply** to save the changes. A services restart is required.

Example

The following example has three media route profiles. Two of the media route profiles are enabled and one is disabled. The order of the media route profiles in the table determines the order that the system checks them for matches. The first enabled media route profile in the table has the first priority. In this case, WebRTC_Route is checked first, SIP_RouteIPv4 is ignored because it is disabled, and SIP_RouteIPv6 is checked second.

Because the **Request_URI** parameter was selected in the **Match Field** for the WebRTC_Route media route profile, the request URI in the call request (i.e., the start line of an ingress INVITE from the AS) is parsed. If the request URI contains "webrtc=yes" in the last field of the string, a match occurs and the system will use the IP address associated with WebRTC_Route when establishing a media connection for the call. If there are no matching strings in the request URI, the next enabled media route profile is checked (i.e., SIP_RouteIPv6). If no media route profile entry is matched, the default media address set at the top of the **Media Engine** section will be used (i.e., 234.234.234.234).

SIP

RTP

Media Engine

Interface Name	IPv4 Address	IPv6 Address	Type Of Service
eth0	234.234.234.234	None	0

Media Route Profiles

Edit
New
Delete

	Status	Name	Match Field	Match Pattern	TOS	NIC
<input type="checkbox"/>	Enabled	WebRTC_Route	Request_URI	webrtc=yes\$	0	192.168.1.100
<input type="checkbox"/>	Disabled	SIP_RouteIPv4	Connection	*\.\$+2001:db8:35a3:8d3:	0	123.123.123.123

RTP Timeout

Proceed as follows to configure the **RTP Timeout** parameters:

1. In the **RTP Timeout Audio** field, set the interval of time that audio RTP flow can be inactive before an alarm is sent. The range is 5,000ms to 120,000ms. Use 0 to disable the alarm. Default value is 30,000ms.
2. In the **RTCP Timeout Audio** field, set the interval of time that audio RTCP flow can be inactive before an alarm is sent. The range is 5,000ms to 120,000ms. Use 0 to disable the alarm. Default value is 15,000ms.
3. In the **RTP Timeout Video** field, set the interval of time that video RTP flow can be inactive before an alarm is sent. The range is 5,000ms to 120,000ms. Use 0 to disable the alarm. Default value is 30,000ms.
4. In the **RTCP Timeout Video** field, set the interval of time that video RTCP flow can be inactive before an alarm is sent. The range is 5,000ms to 120,000ms. Use 0 to disable the alarm. Default value is 15,000ms.
5. Click **Apply** to save changes.

Note: The timer resolution is 100ms. Entered values are automatically rounded down if necessary.

SRTP

Proceed as follows to configure the **SRTP** parameters (only for SDES-SRTP):

1. In the **Lifetime** field, enter the lifetime of the keys (same value for both SRTP and SRTCP). The keys are refreshed just before they expire. Valid values are 1 to 2147483648. Default value is 2147483648.
2. In the **Key Rotation** field, select the number of keys to use for key rotation from the drop-down list. Valid values are 1 to 20.
3. In the **Accept** field, click the check box to specify if accept is enabled. Accept is for incoming INVITEs with SDES. When checked, it means that incoming INVITEs with SDES are accepted. When not checked, incoming INVITEs with SDES are rejected. Default value is enabled.
4. In the **Enforce** field, click the check box to specify if enforce is enabled. Enforce is for incoming INVITEs with SDES. When checked, it means that incoming INVITEs with no SDES are rejected. When not checked, incoming INVITEs with no SDES are accepted. Default value is disabled.
5. In the **Unencrypted RTP** field, click the check box to specify if unencrypted RTP is enabled. Unencrypted RTP allows for RTP to be sent unencrypted and only RTCP will be encrypted. This parameter is negotiated with the SDPs and both sides must agree to send unencrypted RTP (both directions). Default value is disabled.
6. In the **Unencrypted RTCP** field, click the check box to specify if unencrypted RTCP is enabled. Unencrypted RTCP allows for RTCP to be sent unencrypted and only RTP will be encrypted. This parameter is negotiated with the SDPs and both sides must agree to send unencrypted RTCP (both directions). Default value is disabled.
7. In the **Window Size Hint** field, enter the window size hint. Window size hint protects against duplicate packet replay, which may be an attempt at denial of service attack. Default value is 64.
8. Click **Apply** to save changes.

Telephony Events

Proceed as follows to configure the **Telephony Events** parameters:

1. In the **Telephony Event** field, set the telephony event.
2. Click **Apply** to save changes.

Codecs

The **Codecs** menu contains the following tabbed pages: **Profiles** and **Settings**.

Profiles

The **Profiles** page is used to configure Codec Profiles, Audio Codecs, Video Codecs, and Telephone Events.

Profiles Settings

Codec Profiles

Profile:

Audio Codecs		
Name	Status	Operations
g722	<input checked="" type="checkbox"/>	
pcmu	<input checked="" type="checkbox"/>	
pcma	<input checked="" type="checkbox"/>	
opus	<input checked="" type="checkbox"/>	
EVS	<input checked="" type="checkbox"/>	
amr-wb	<input checked="" type="checkbox"/>	
amr	<input checked="" type="checkbox"/>	
g729	<input checked="" type="checkbox"/>	
gsm-efr	<input checked="" type="checkbox"/>	
gsm	<input checked="" type="checkbox"/>	
iLBC	<input checked="" type="checkbox"/>	
g723	<input checked="" type="checkbox"/>	
g726-32	<input checked="" type="checkbox"/>	

Video Codecs		
Name	Status	Operations
vp8	<input checked="" type="checkbox"/>	
vp9	<input checked="" type="checkbox"/>	
h264	<input checked="" type="checkbox"/>	
mp4v-es	<input checked="" type="checkbox"/>	
h263-2000	<input checked="" type="checkbox"/>	
h263-1998	<input checked="" type="checkbox"/>	
h263	<input checked="" type="checkbox"/>	

Telephone Events:	
Clock Rate	Operations
8000	
16000	
48000	

Codec Profiles

The **Profile** parameter specifies the name of the codec profile that will be applied when the incoming call is answered. The codec profiles are named codec configurations that enable applications to choose a specific codec configuration of their choice when answering a call.

×
Audio Codec Profile

Create Audio Codec Profile

Profile Name:

To create a codec profile, click **New** and configure the parameters in the **Audio Codec Profile** window.

1. Enter the name of the codec profile in **Profile Name**.
2. Click **Add** to create the codec profile or click **Cancel** to abort the operation.
3. Click **Save** to add the codec profile or click **Delete** to remove the codec profile.

Audio Codecs

On the **Audio Codecs** section, audio codecs are listed in priority order, with the first row having the highest priority. To change the priority, click the desired codec, and then drag and drop it within the table. In addition to changing the priority of the codecs, the codecs can be enabled and disabled.

Enable/Disable Audio Codecs

Proceed as follows to enable or disable audio codecs on the **Audio Codecs** section:

- Click the button listed in the **Status** column to toggle between enabled and disabled. The **Status** column will change to the action you selected.

Edit Audio Codec Fields

Audio Codec Parameters	
Codec Name:	amr
Mode Set: (0,1,2,...)	
Octet Align	YES
Payload Type: (96-127)	Default <input checked="" type="checkbox"/>

1. Click the pencil button from the **Operations** column of the codec you wish to modify. The parameters include **Codec Name**, **Mode Set** (amr, amr-wb), **Octet Align** (amr, amr-wb), **Payload Type** (amr, amr-wb, EVS, g726-32, gsm-efr, iLBC, opus), and **Annex B** (g729).

Note: On the **Mode Set** parameter, the default setting in the codec profile is support for all of the modes. Since this is a restrictive parameter, the user should only configure the **Mode Set** parameter if the intent is to limit the modes.

2. Click **Save** to apply changes or click **Cancel** to abort the operation.

Video Codecs

On the **Video Codecs** section, video codecs are listed in priority order, with the first row having the highest priority. To change the priority, click the desired codec, and then drag and drop it within the table. In addition to changing the priority of the codecs, the codecs can be enabled and disabled.

Enable/Disable Video Codecs

Proceed as follows to enable or disable video codecs on the **Video Codecs** section:

- Click the button listed in the **Status** column to toggle between enabled and disabled. The **Status** column will change to the action you selected.

Edit Video Codec Fields

Video Codec Parameters	
Codec Name:	h264
Packetization Mode:	0
PayLoad Type: (96-127)	Default <input checked="" type="checkbox"/>
Profile Level Id: 42001F	profile-idc: 0x42
	profile-iop: 0 item(s) selected
	level-idc: 3.1
Sprop Parameter Sets:	DEFAULT

1. Click the pencil button from the **Operations** column of the codec you wish to modify.
 - For vp8, vp9, mp4v-es, h263-2000, and h263-1998, the parameters include **Codec Name** and **Payload Type**.
 - For h264, the parameters include **Codec Name**, **Packetization Mode**, **Payload Type**, **Profile Level Id** (consists of **profile-idc**, **profile-iop**, and **level-idc**), and **Sprop Parameter Sets**.
 - For h263, there are no additional editable parameters for the codec.
2. Click **Save** to apply changes or click **Cancel** to abort the operation.

Telephone Events

The **Telephone Events** parameter sets the sample clock rate and payload type fields for RFC 2833/RFC 4733 telephony digits in the offer SDP.

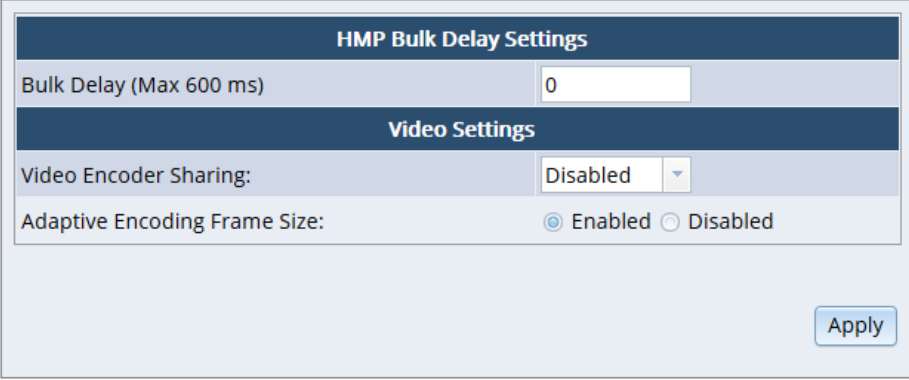
Edit Telephone Event Fields

Telephone Event Parameters	
Clock Rate:	8000
PayLoad Type: (96-127)	Default <input checked="" type="checkbox"/>

1. Click the pencil button from the **Operations** column of the clock rate you wish to modify. The parameters include **Clock Rate** and **Payload Type**.
2. Click **Save** to apply changes or click **Cancel** to abort the operation.

Settings

The **Settings** page is used to configure Bulk Delay, Video Encoder Sharing, and Adaptive Encoding Frame Size.



The screenshot shows a web interface with a navigation bar at the top containing 'Profiles' and 'Settings'. Below this is a settings panel with two sections: 'HMP Bulk Delay Settings' and 'Video Settings'. In the 'HMP Bulk Delay Settings' section, there is a label 'Bulk Delay (Max 600 ms)' followed by a text input field containing the value '0'. The 'Video Settings' section contains two items: 'Video Encoder Sharing:' with a dropdown menu set to 'Disabled', and 'Adaptive Encoding Frame Size:' with two radio buttons, 'Enabled' (which is selected) and 'Disabled'. An 'Apply' button is located at the bottom right of the settings panel.

HMP Bulk Delay Settings

On the HMP Bulk Delay Settings section, the bulk delay can be set. The **Bulk Delay** parameter sets the bulk delay for the conferencing echo canceller (EC) on all channels. The parameter is used to extend the tail length for the EC in order to cover round trip delay and reduce acoustic echo within conferences. The parameter is a global configuration that sets the amount of bulk delay time in milliseconds. The value must be a multiple of 10 and within the range of 0 to 600ms. Default value is 0.

Click **Apply** to save changes.

Video Settings

On the **Video Settings** section, the **Video Encoder Sharing** parameter can be enabled and disabled, and the **Adaptive Encoding Frame Size** can be enabled and disabled.

Video Encoder Sharing

Video encoder sharing works by reducing and optimizing the CPU resources required to perform the video encoding operation. Use the drop-down list to select one of the following valid values:

- **Disabled (default)** - None of the encoders are shared by more than one participant.
- **Static** - One encoder is shared by all participants in the same conference who have the same video size (such as VGA) and the same codec, regardless of their bandwidth. In this case, the target bitrate for the participant who has the lowest video size will be used for the shared encoder.
- **Dynamic** - One encoder is shared by participants in the same conference who have the same video size (such as VGA), the same codec, and similar target bitrates. In this mode, an encoder is dynamically assigned, added, or removed depending on the dynamically changing network environment.

Click **Apply** to save changes.

Note: This functionality is only supported for video conferencing use cases, where conference participants share the same mixed video output view.

Adaptive Encoding Frame Size

The **Adaptive Encoding Frame Size** parameter sets the video encoder to allow dynamic frame size adaptation (i.e., on-the-fly resolution changes). When enabled, the video encoder will permit video resolution changes when dynamically adapting to network bandwidth conditions. When disabled, the video encoder will not be permitted to change video resolution once the video stream has started. Disabling this item may be required for legacy devices that cannot handle dynamic frame size changes.

This parameter is only valid for H.264, VP8 and VP9 codecs. MPEG4 and H.263 codecs are restricted to fixed resolutions.

Click **Apply** to save changes.

MSML

The Media Server Markup Language (MSML) interface (RFC 5707) uses SIP INFO messages to send MSML script payloads. The **MSML** menu contains the following tabbed pages: **MSML Configuration** and **MSML Advanced Configuration**.

MSML Configuration

MSML Configuration
MSML Advanced Configuration

MSML (RFC5707) Protocol General:

Content Type:	xml	▼
Encoding:	utf-8	▼
MSML Schema Validation:	<input type="checkbox"/>	

Media Parameters:

HTTP Caching:	<input checked="" type="checkbox"/>	
Media Mode Selection:	<input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Video <input type="checkbox"/> Message <input type="checkbox"/> G.711 Fax <input type="checkbox"/> T.38 Fax	
MRCP Session Idle Timeout	End of Call	

Conferencing Parameters:

Enable AGC By Default:	<input type="checkbox"/>	
------------------------	--------------------------	--

Apply

Proceed as follows to configure the **MSML Configuration** parameters:

Parameter	Description	Valid Values
MSML (RFC5707) Protocol General		
Content Type	Specifies the SIP INFO Content-Type header that will be used in SIP INFO responses.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> xml (default) msml+xml

Parameter	Description	Valid Values
Encoding	Specifies XML encoding.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> utf-8 (default) us-ascii
MSML Schema Validation	Controls activation of the XML validation of the media control message body. Validation is performed based on the <i>msml.xsd</i> XML schema definition file. Note: This parameter is MIPS intensive and is recommended during application development and troubleshooting, and not for normal operation.	Click the check box to enable or disable. MSML Schema Validation is disabled by default. Note: Due to a limitation in the Xerces schema validation library included in the supported Linux distributions, the schema for MSML speech and namespace extensions (xml:lang) remain disabled as they require fetching of external (http://) files. To avoid validation failures, ensure that the schema validation is disabled.
Media Parameters		
HTTP Caching	Controls a caching mechanism to improve performance when servicing network and remote file operations.	Click the check box to enable or disable. HTTP Caching is disabled by default (does not perform caching; all network requests result in remote access).

Parameter	Description	Valid Values
Media Mode Selection	Specifies the MSML media mode.	<p>Click one or more check boxes to enable or disable each valid media value:</p> <ul style="list-style-type: none"> • Audio • Video • Message • G.711 Fax • T.38 Fax <p>Note: The interaction between the license, codec, and media mode parameter combinations are shown in the Media Mode Combinations table.</p>
MRCP Session Idle Timeout	Sets the default value of the MRCP session idle timeout property.	<p>Use the drop-down list to select Disabled, End of Call, or a number between 1 - 300s.</p> <p>Default value is End of Call.</p>
Conferencing Parameters		
Enable AGC By Default	Enables automatic gain control (AGC).	<p>Click the check box to enable or disable AGC by default.</p> <p>This is disabled by default.</p>

Click **Apply** to save changes.

Note: The system services must be restarted for the changes to take effect.

Media Mode Combinations

The following table shows the interaction between the license, codec, and media mode parameter combinations.

License	Codecs	Media Mode	Delayed Offer Call Result
A	A	A	Pass
A	A	A/V	Fail - 503 Service Unavailable.
A	A/V	A	N/A - Not possible to be configured, since video codecs are removed when license is audio only.

License	Codecs	Media Mode	Delayed Offer Call Result
A	A/V	A/V	N/A - Not possible to be configured, since video codecs are removed when license is audio only.
A/V	A	A	Pass
A/V	A	A/V	Fail - 503 Service Unavailable.
A/V	A/V	A	Pass
A/V	A/V	A/V	Pass
A/V	A/V	V	Pass
A/V	A	V	Fail - 503 Service Unavailable.
A/V	V	V	Pass - Call initiated with video only.
A	A	V	Fail - 503 Service Unavailable.
A	AV	V	N/A - Not possible to be configured, since video codecs are removed when license is audio only.
A	V	V	N/A - Not possible to be configured, since video codecs are removed when license is audio only.
V	V	V	Fail - 590 Destination Unreachable (Port Unreachable) ICMP message. The Destination port is 5060.
V	A	V	N/A - Not possible to be configured, since audio codecs are removed when license is video only.
V	A/V	V	N/A - Not possible to be configured, since audio codecs are removed when license is video only.

MSML Advanced Configuration

MSML Configuration		MSML Advanced Configuration	
Special Modes:			
Clear Digit Buffer (cleardb):		Default True	▼
DTMF Start Timer:		<input type="checkbox"/>	
DTMF Mode:		RFC2833	▼
DTMF Reception Modes:		Default	▼
MOML Events:		RFC-5707	▼
Alarms:			
Audio RTP Timeout:		<input type="checkbox"/>	
Audio RTCP Timeout:		<input type="checkbox"/>	
Video RTP Timeout:		<input type="checkbox"/>	
Video RTCP Timeout:		<input type="checkbox"/>	

Apply

Proceed as follows to configure the **MSML Advanced Configuration** parameters in the **Special Modes** section:

1. In the **Clear Digit Buffer (cleardb)** field, use the drop-down list to select a value. The following values are provided.

Clear Digit Buffer (cleardb) Values	Description
RFC 5707	Default option. For <play>, cleardb defaults to false if not specified in the request, and for <dtmf/collect >, cleardb defaults to true.
Default True	When cleardb is not specified in the request, it defaults to true for both <play> and <dtmf/collect>.
Default False	When cleardb is not specified in the request, it defaults to false for both <play> and <dtmf/collect>.
Force True	Regardless of what is specified in the request, cleardb will always be treated as true for both <play> and <dtmf/collect>.
Force False	Regardless of what is specified in the request, cleardb will always be treated as false for both <play> and <dtmf/collect>.

2. To enable **DTMF Start Timer**, click the check box.
3. In the **DTMF Mode** field, use the drop-down list to select the value. Valid values are "RFC2833", "IN-BAND", or "SIP INFO".
4. In the **DTMF Reception Modes** field, use the drop-down list to select the value(s). Valid values are "Default", "RFC2833", "IN-BAND", or "SIP INFO".

The **DTMF Reception Modes** parameter indicates the mode(s) of the DTMF digits that the application server wishes to receive.

The "Default" option selects the appropriate reception mode based on the **DTMF Mode** parameter. Most users should leave the **DTMF Reception Modes** parameter at its "Default" option as this automatically selects the matching mode. The users wishing to receive digits from a mode in addition to the mode determined by the SDP negotiation can enable it in the **DTMF Reception Modes** parameter.

For example, if the **DTMF Mode** parameter is set to "RFC2833" and was negotiated in the SDP exchange, and the application server also wishes to receive any digits that may have arrived "IN-BAND", the **DTMF Reception Modes** parameter should be set with both "RFC2833" and "IN-BAND" options enabled. Only digits that have arrived over the selected modes will be forwarded to the application server.

Note that if the **DTMF Mode** parameter is set to "IN-BAND", the "RFC2833" option of the **DTMF Reception Modes** parameter is unavailable as the required RTP payload type for "RFC2833" will not have been determined by the SDP negotiation.

5. In the **MOML Events** field, use the drop-down list to select the value. Valid values are "RFC-5707" or "Disable". This option controls the behavior of moml events when <exit> or <disconnect> elements are executed. When set to "Disable", MSML will not send moml.exit and moml.disconnect events. Default value is "RFC5707".
6. Click **Apply** to save changes.

Proceed as follows to configure the **MSML Advanced Configuration** parameters in the **Alarms** section:

1. To enable **Audio RTP Timeout**, **Audio RTCP Timeout**, **Video RTP Timeout**, and **Video RTCP Timeout**, click the associated check boxes.
2. Click **Apply** to save changes.

Note: The system services must be restarted for the changes to take effect.

VXML

Voice Extensible Markup Language (VoiceXML or VXML) is an integral part of PowerMedia XMS. VXML is designed for creating dialogs that feature synthesized speech, digitized audio, speech recognition and DTMF key input, speech recording, telephony, and mixed initiative conversations.

VXML Interpreter Configuration

The **VXML Interpreter Configuration** page is used to configure **General Settings** and **Web Server Settings** for the VXML Interpreter.

Vxml Interpreter Configuration		VXML Application Configuration
General Settings:		
Allow Call Transfer	<input checked="" type="checkbox"/>	
Initial URI	file:///var/lib/xms/vxml/www/vxml/index.vxml	
DTMF Mode	RFC2833	
Default Input Mode	dtmf voice	
Max Channels	2000	
VXML App Logs Enabled	<input type="checkbox"/>	
XSI Schema Validation Disabled	<input checked="" type="checkbox"/>	
Call Establishment Error Handling	Default	
Default Timeout Settings (seconds):		
ASR Complete Timeout	0.8	
ASR Incomplete Timeout	1	
Max Speech Timeout	15	
Inter-digit Timeout	3	
No Input Timeout	3.4	
MRCP Session Idle Timeout	End of Call	
Default Locale Settings:		
Grammar Locale	en-US	
Prompt Locale	en-US	
Record Locale	en-US	
Builtin Locale	en-US	
Web Server Settings:		
Static Content Directory	/var/lib/xms/vxml/www	
IP Address(es)	127.0.0.1	
Port	9002	
User Name		
Password		
Call Placer Settings:		
Call Placer Encoded	<input type="checkbox"/>	
<input type="button" value="Apply"/>		

General Settings

Proceed as follows to configure the **General Settings** parameters.

Parameter	Description	Valid Values
Allow Call Transfer	Specifies whether call transfers are allowed.	Click the check box to enable or disable.

Parameter	Description	Valid Values
Initial URI	URI of the initial page to execute when receiving or making a call. The value must be a full URI because relative URIs are not allowed. Both HTTP and local file URIs are supported. In the latter case, the file:// protocol specifier must precede the path.	Enter the initial URI. Default value is <i>file:///var/lib/xms/vxml/www/vxml/index.vxml.</i>
DTMF Mode	Sets the DTMF mode.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • RFC2833 • SIP INFO • InBand
Default Input Mode	Sets the default input mode.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • dtmf voice • dtmf • voice

Parameter	Description	Valid Values
Max Channels	<p>Maximum number of VXML Interpreter channels to be used simultaneously. Each channel runs as a separate thread within the VXML Interpreter executable.</p> <p>Actual resources increase only according to the real needs.</p> <p>Note: The resources used for a channel may not be available immediately after a call is disconnected because the VXML Interpreter can continue processing dialogs on behalf of a call. To avoid call rejection due to busy resources, it is generally recommended to add twenty percent (20%) more channels than the total concurrent number of calls PowerMedia XMS is expected to handle.</p>	1 - 1024 (depending on machine capabilities)
VXML App Logs Enabled	Specifies whether to enable VXML application logging.	Click the check box to enable or disable.
XSI Schema Validation Disabled	Specifies whether to disable XSI schema validation.	Click the check box to enable or disable.
Call Establishment Error Handling	Specifies whether to handle errors encountered during call establishment.	<p>Use the drop-down list to select one of the following valid values:</p> <ul style="list-style-type: none"> • Default • RFC5552

Default Timeout Settings (seconds)

Proceed as follows to configure the **Default Timeout Settings (seconds)** parameters.

Parameter	Description	Valid Values
ASR Complete Timeout	Sets the default value of the VXML complete timeout property in seconds.	0.2sec - 10s Default value is 0.8s.
ASR Incomplete Timeout	Sets the default value of the VXML incomplete timeout property in seconds.	0.2s - 10s Default value is 1s.
Max Speech Timeout	Sets the maximum default value of the VXML timeout property in seconds.	Default value is 15s.
Inter-digit Timeout	Sets the default value of the VXML interdigit timeout property in seconds.	0 - 600s Default value is 3s.
No Input Timeout	Sets the default value of the VXML timeout property in seconds.	0.05s - 20000s Default value is 3.4s.
MRCP Session Idle Timeout	Sets the default value of the MRCP session idle timeout property.	Use the drop-down list to select Disabled, End of Call, or a number between 1 - 300s. Default value is End of Call.

Default Locale Settings

Proceed as follows to configure the **Default Locale Settings** parameters.

Parameter	Description	Valid Values
Grammar Locale	Sets the default RFC 3066 language identifier to use for grammar.	Default language is en-US.
Prompt Locale	Default system language. The value should be a language-identifier as per RFC 3066. It can have a particular voice name appended. For example, en-US-Crystal.	Default language is en-US.

Parameter	Description	Valid Values
Record Locale	Affects the default storage location of the recordings in the PowerMedia XMS media directories.	Default language is en-US.
Built-in Locale	Controls the locale of the built-in generic audio prompts.	Default language is en-US.

Web Server Settings

The web server is used to fetch local VXML documents using *http://protocol* instead of *absolute file://* and to receive the application server requests, if any.

Proceed as follows to configure the local **Web Server Settings** parameters:

1. In the **Static Content Directory** field, enter the location where the VXML pages are stored.
2. In the **IP Address(es)** field, enter the local IP address to use or LOCALHOST with 127.0.0.1. Also, entering ANY can be used to allow access with any IP address although not recommended.
3. In the **Port** field, enter the port number. Default value is 9002.
4. In the **User Name** field, enter the username to log in, if any.
5. In the **Password** field, enter the password to log in, if any.
6. Click **Apply** to save changes.

Call Placer Settings

In the **Call Placer Encoded** field, click the check box to enable VXML outbound SIP calls. Refer to the *Dialogic® PowerMedia™ XMS VoiceXML Reference Guide* for more information.

VXML Application Configuration

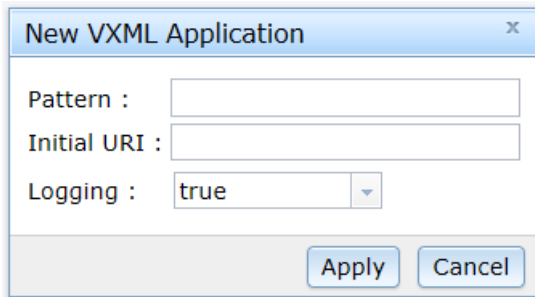
The **VXML Application Configuration** page is used to configure the VXML application.

Vxml Interpreter Configuration **VXML Application Configuration**

Pattern	Initial URI	Logging
<input type="button" value="Delete"/> <input type="button" value="Add"/> <input type="button" value="Apply"/>		

To add a new VXML application to the **VXML Application Configuration** page, click **Add**.

The following dialog box will appear.



The dialog box titled "New VXML Application" has a close button (x) in the top right corner. It contains three input fields: "Pattern :", "Initial URI :", and "Logging :". The "Logging" field is a dropdown menu with "true" selected. At the bottom, there are two buttons: "Apply" and "Cancel".

Proceed as follows to configure the **VXML Application Configuration** parameters:

1. In the **Pattern** field, enter the regular expression that will be compared to the user part of the call request URI. Do not include sip: or rtc: in the pattern. For example, if the incoming call URI is sip:test123@example.com, the regular expression pattern ^test.* will be a match and the configured initial URI will be executed.
2. In the **Initial URI** field, enter the initial URI for this VXML application.
3. In the **Logging** field, select true or false from the drop-down list to enable the logging for this VXML application.
4. Click **Apply** to save changes.

Note: When a new VXML application is added, it is automatically added to the bottom of the routing rules table on the **Routing > Routes** page. The routing rules are matched against an incoming call request URI in the order shown on the **Routes** page. The routing rules should be ordered from most specific to least specific. Check the **Routes** page to verify and adjust the order of the new VXML application rule so that it is ordered higher than any existing routing rule that might also match the incoming call. Otherwise, VXML calls to the desired VXML application may not get routed as expected. Refer to the [Routing](#) section for details.

RESTful API

The **RESTful API** menu opens to the **RESTful API Configuration** page, which is used to configure several aspects of the RESTful call control and media API.

RESTful Media API

Web Server HTTP Port:

Enable Web Server HTTP Port:

Web Server HTTPS Port:

Enable Web Server HTTPS Port:

Enable IPv6:

New Application ID

Add

Trusted Application IDs

App Id	Status	Action
app	enable	Disable Delete

Apply

RESTful API Credentials

Management API:

Media API:

Apply

RESTful Media API

Proceed as follows to configure the **RESTful Media API** parameters. The port number is used by the lighttpd web server, which services the RESTful API.

1. In the **Web Server HTTP Port** field, enter the HTTP port number for web server. Default value is 81.
2. In the **Enable Web Server HTTP Port** field, click the check box to specify if HTTP port is enabled for web server.
3. In the **Web Server HTTPS Port** field, enter the HTTPS port number for web server. Default value is 444.
4. In the **Enable Web Server HTTPS Port** field, click the check box to specify if HTTPS port is enabled for web server.

5. In the **Enable IPv6** field, click the check box to specify if IPv6 is enabled for web server. This enables RESTful services to bind to an IPv6 address, provided that IPv6 is enabled on the operating system.
6. Click **Apply** to save changes.

Application ID

Application IDs are used in the **Routes** page to map a SIP URL to a specific application. The enabled Application IDs are available from the **Application** drop-down list on the **Routes** page.

To add an Application ID to the **Trusted Application IDs** section, enter the name in the **New Application ID** field. Click the **Add** button. The ID will be added to the **Trusted Application IDs** section. The ID will be enabled by default.

It may be disabled but kept in the list by clicking **Disable**. It can be re-enabled by clicking **Enable**. The entry can be entirely removed from the list by clicking **Delete**.

Click **Apply** to save changes.

Note: The system services must be restarted for the changes to take effect.

RESTful API Credentials

Proceed as follows to configure the **RESTful API Credentials** parameters.

Management API

In the **Management API** field, select the account to be used (configured through the **Account** section on **Secure Storage** page) from the drop-down list. Click **Apply** to save changes.

Media API

In the **Media API** field, select the account to be used (configured through the **Account** section on **Secure Storage** page) from the drop-down list. Click **Apply** to save changes.

NETANN

Network Announcement (NETANN) is an announcement server that can be directed to play media files and put callers into a conference by adding directives to the SIP URL used to contact PowerMedia XMS. The **NETANN** menu opens to the **NETANN Configuration** page, which is used to configure NETANN media and conference settings.

The screenshot shows the 'NETANN Configuration' page. It has a header 'NETANN Configuration' and a dark grey bar below it. The page is divided into two main sections: 'Global Settings:' and 'Conference Settings:'. Under 'Global Settings:', there is a 'Media Type' field with a dropdown menu set to 'Audio and Video'. Under 'Conference Settings:', there are several input fields: 'Max Conference Parties' (500), 'Max Active Talkers' (3), 'Max Audio Conferences' (1000), 'Max Video Conferences' (100), and 'Video Conference Regions' (Automatic). There is also a 'Clamp DTMF Digits' checkbox which is checked. At the bottom left, there is an 'Apply' button.

Proceed as follows to configure the **NETANN Configuration** parameters:

1. In the **Media Type** field, select the media type to configure from the drop-down list. When the NETANN service answers incoming SIP calls, it will use this media type in the SDP negotiation. Valid values are Audio and Video or Audio.
2. In the **Max Conference Parties** field, enter the maximum number of parties in the conference.
3. In the **Max Active Talkers** field, enter the maximum number of active talkers in the audio mix.
4. In the **Max Audio Conferences** field, enter the maximum number of audio conferences.
5. In the **Max Video Conferences** field, enter the maximum number of video conferences.
6. In the **Video Conference Regions** field, select the number of regions in the video conference from the drop-down list. Valid values are 1 to 9 or Automatic.
7. In the **Clamp DTMF Digits** field, click the check box to enable or disable. When enabled (default), DTMF digits generated by a conference party are clamped at the conference input and not transmitted to the other parties. When disabled, DTMF digits generated by a conference party are transmitted to all the other parties.
8. Click **Apply** to save changes.

Routing

The **Routing** menu opens to the **Routes** page, which illustrates how different applications like MSML, NETANN, VXML, and RESTful are engaged with PowerMedia XMS based on the content of SIP URI (User Request Indicator).

Routes

New Route

Pattern Application

	Pattern	Application
<input type="checkbox"/>	^(sip sips rtc):annc.*	NETANN
<input type="checkbox"/>	^(sip sips rtc):conf=.*	NETANN
<input type="checkbox"/>	^(sip sips rtc):dialog.*momi=.*	MSML
<input type="checkbox"/>	^(sip sips rtc):dialog.*	VXML
<input type="checkbox"/>	^(sip sips rtc):msml.*	MSML
<input type="checkbox"/>	^(sip sips rtc):play_demo.*	verification
<input type="checkbox"/>	^(sip sips rtc):conf_demo.*	verification
<input type="checkbox"/>	^(sip sips rtc):join_demo.*	verification
<input type="checkbox"/>	^(sip sips rtc):demo.*	verification
<input type="checkbox"/>	^rtc:sip:.*	verification
<input type="checkbox"/>	^(sip sips rtc):.*	app

There are two editable fields as part of the **New Route** section on the **Routes** page: **Application** and **Pattern**. The **Pattern** field is a regular expression that is matched against the incoming call URI. Proceed as follows to enter a new route:

1. To enter a new route, enter a pattern in the **Pattern** field and then select an Application ID from the **Application** drop-down list. Valid values are NETANN, VXML, MSML, verification, or app.
2. Click the **Add** button.
3. Click **Apply** to save changes.

The new route will now be listed on the **Routes** page. Routes can be deleted by clicking in the appropriate check box and clicking the **Delete** button. The default route for all calls is the Application ID "app".

Note: A route can be moved up or down by clicking it and then dragging and dropping it within the table. The more specific routes (less inclusive) should be placed higher than the less specific routes (more inclusive) to avoid the less specific routes from servicing the call.

Application ID

Application IDs are used to map a SIP URL to a specific application. Application IDs are available from the **Application** drop-down list as mentioned above.

To add an Application ID, refer to the **Application ID** section of the **RESTful API** page.

HTTP Client

The **HTTP Client** menu opens to the **HTTP Client Configuration** page, which is used to configure cache on the HTTP Client.

HTTP Client Configuration	
Max Age (seconds)	60
Max Stale (seconds)	0
Http Cache	YES
Http Cache Size	1000
Low Speed Threshold (bytes per second)	1
Low Speed Timeout (seconds)	20
Connection Timeout (seconds)	10
DNS Cache Timeout (seconds)	60 (-1: entries never expire , 0: disabled)
Client Certificate:	Default



Apply

Proceed as follows to configure the **HTTP Client Configuration** parameters:

1. In the **MAX AGE (seconds)** field, enter the maximum amount of time in seconds that a file will be cached.
2. In the **MAX STALE (seconds)** field, enter the maximum amount of time in seconds that is allowed before a cached file becomes stale.
3. In the **HTTP CACHE** field, select YES to enable cache or NO to disable cache from the drop-down list.
4. In the **HTTP CACHE SIZE** field, enter the cache size limit (MB) when **HTTP CACHE** is enabled.
5. In the **Low Speed Threshold (bytes per second)** field, enter the transfer speed threshold in bytes per second. A value of 0 disables this parameter and implies 0 in the **Low Speed Timeout** parameter. Default value is 1.
6. In the **Low Speed Timeout (seconds)** field, enter the number of seconds the transfer speed must stay below the **Low Speed Threshold** parameter for a timeout event to be triggered. A value of 0 disables this parameter and implies 0 in the **Low Speed Threshold** parameter. Default value is 20.
7. In the **Connection Timeout (seconds)** field, enter the connection timeout in seconds. Default value is 10 seconds. The connection timeout is the amount of time in seconds that the XMS HTTP Client will wait for a connection to be established to an external web server before timing out.
8. In the **DNS Cache Timeout (seconds)** field, enter the DNS cache timeout in seconds. If 0 is entered, the DNS cache timeout is disabled. If -1 is entered, the DNS cache entries never expire.
9. In the **Client Certificate** field, select Default or client certificate (configured through the **Public Key Infrastructure** section on **Secure Storage** page) from the drop-down list.
10. Click **Apply** to save changes.

Speech

The **Speech** menu contains the following tabbed pages: **Providers** and **Profiles**.

Name	Description	Status	Action
mrCP	MRCP	<input type="checkbox"/>	
aws	AWS	<input type="checkbox"/>	

Providers

MRCP Provider

The Media Resource Control Protocol (MRCP) is used by PowerMedia XMS as an interface to Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) systems. MRCP provides an easy way to build voice user interfaces, allowing a grammar to be built for speech input and providing a way to easily translate text into voice prompts without reading and recording them.

The **MRCP Provider** section is used to configure the MRCP Provider.

MRCP Provider x

Global Configuration:

MRCP Client IP Address(es)	146.152.124.67
Connection Retry Interval (seconds)	10
Connection Retry Count	3
Server Recovery Delay (minutes)	5
Maximum Sessions Count	100
UDP Retransmit Timer (msecs)	100
UDP Retransmit Count	2

Speech Server Id	Status	Role	Action
sample	Enable	primary	Delete

Proceed as follows to configure the **MRCP Provider** parameters:

1. In the **MRCP Client IP Address(es)** field, enter the local IP address to be used for the MRCP Client. The IP address can be IPv4.
2. In the **Connection Retry Interval (seconds)** field, enter the keep alive interval for connection with speech server.

3. In the **Connection Retry Count** field, enter the keep alive count for connection with the speech server.
4. In the **Server Recovery Delay (minutes)** field, enter the delay in minutes before a failed speech server is attempted again.
5. In the **Maximum Sessions Count** field, enter the maximum number of MRCP sessions supported.

Note: The **Maximum Sessions Count** field should be set to the number of desired active sessions. Each active session supports both ASR and TTS. The number of active sessions should not exceed the number of MRCP licenses.

6. In the **UDP Retransmit Timer (msecs)** field, enter the amount of time (in milliseconds) between retransmissions when using UDP for the transport of the MRCP signaling.
7. In the **UDP Retransmit Count** field, enter the maximum number of retransmissions before a request is considered failed when using UDP for the transport of the MRCP signaling.
8. Click **Save** to apply changes or click **Cancel** to abort the operation.

Speech Server Configuration

Proceed as follows to add a speech server and to configure its parameters:

1. Click **Add**. The following dialog box will appear.

Speech Server Id	new_server
Speech Server IP Address(es)	0.0.0.0
Speech Server Port	5060
Protocol Version	MRCP/2.0
Transport	TCP
ASR	true
TTS	true
Enabled	false
Role	primary

Note: Split addressing is not supported for speech server signaling and media.

2. In the **Speech Server Id** field, enter the speech server identification for MRCP.
3. In the **Speech Server IP Address(es)** field, enter the IP address of the MRCP server to connect to. The IP address can be IPv4/IPv6.
4. In the **Speech Server Port** field, enter the IP port of the MRCP server to connect to.
5. In the **Protocol Version** field, select MRCP/1.0 or MRCP/2.0 from the drop-down list to indicate the protocol version.

6. In the **Transport** field, select UDP or TCP from the drop-down list to indicate the SIP transport protocol.

Note: For SIP usage only. Once the session is established, MRCP uses TCP.

7. In the **ASR** field, select true or false from the drop-down list to enable Automatic Speech Recognition for this speech server.
8. In the **TTS** field, select true or false from the drop-down list to enable Text-to-Speech usage for this speech server.
9. In the **Enabled** field, select true or false from the drop-down list to enable this speech server.

Note: Mixing V1 and V2 speech servers is not supported. V1 and V2 servers can appear in the configuration concurrently, however, only servers of one or the other version can be enabled concurrently. For example, if enabling V2 servers, all V1 servers must first be disabled.

10. In the **Role** field, select primary or backup from the drop-down list to indicate the role to use.
11. When executing MRCP operations, PowerMedia XMS will load balance requests to primary speech servers (round robin). If all primary speech servers are unavailable, configured backup speech servers will be used. Attempts will be made to recover primary speech servers according to the **Server Recovery Delay (minutes)** field from **Global Configuration** parameters.

Note: When no primary server is enabled and an attempt is made to enable a backup server, the backup server state is reverted to disabled. At least one primary server must be enabled before a backup server is enabled.

12. Click **Apply** to save changes or click **Cancel** to abort the operation.

PowerMedia XMS supports load balancing and failover as follows:

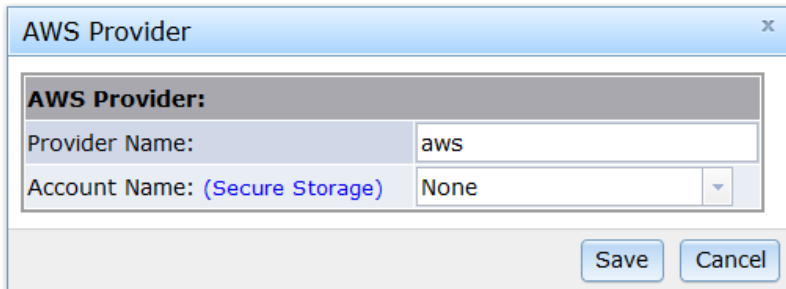
- If more than one primary speech server is configured, each primary server will be automatically load balanced by the MRCP Client. The MRCP Client accesses each primary server in a round robin fashion thereby ensuring an even distribution of requests among all primary servers.
- If a primary server fails to respond to a given request, the request will be attempted on the next configured primary server.
- If all primary servers configured fail to respond to a given request, the request will be attempted on each backup server configured until a successful transaction is achieved.
- When a backup server is being used, recovery of primary servers will be attempted in accordance to the configured primary server recovery timer.

AWS Provider

Amazon Polly is an Amazon Web Service (AWS) used by PowerMedia XMS for Text-to-Speech (TTS) that turns text into lifelike speech to build speech enabled products using dozens of languages and voices. PowerMedia XMS leverages the languages and voices supported by Amazon Polly to be used to build speech enabled prompts and telephony applications with existing PowerMedia XMS APIs.

Note: AWS limits the number of Amazon Polly transactions per second. Verify the limits imposed by AWS at <http://docs.aws.amazon.com/polly/latest/dg/limits.html>.

The **AWS Provider** section is used to configure the AWS Provider.



AWS Provider

AWS Provider:

Provider Name: aws

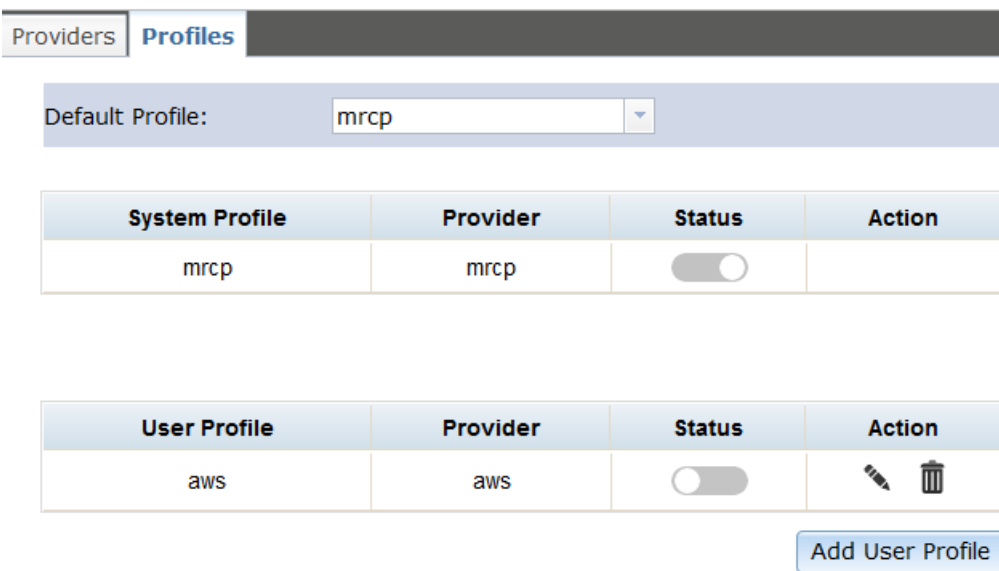
Account Name: (Secure Storage) None

Save Cancel

Proceed as follows to configure the **AWS Provider** parameters:

1. In the **Provider Name** field, enter the name of the provider.
2. In the **Account Name (Secure Storage)** field, select the account that should be used from the drop-down list (configured through the **Account** section on **Secure Storage** page).
3. Click **Save** to apply changes or click **Cancel** to abort the operation.



Profiles



Providers Profiles

Default Profile: mrpc

System Profile	Provider	Status	Action
mrpc	mrpc	<input checked="" type="checkbox"/>	

User Profile	Provider	Status	Action
aws	aws	<input type="checkbox"/>	 

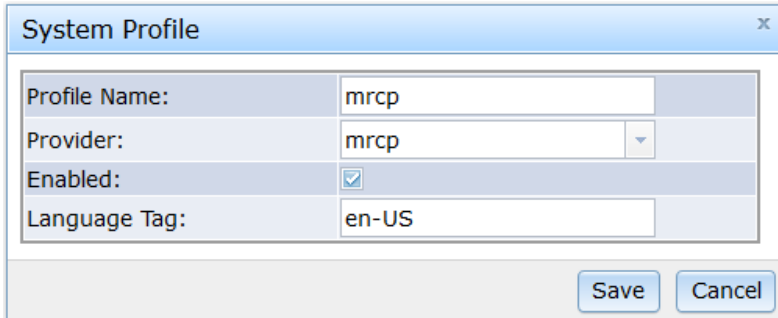
Add User Profile

MRCP System Profile

The **MRCP System Profile** section is used to configure the MRCP System Profile.

Proceed as follows to configure the **System Profile** parameters:

1. In the **System Profile** section, click the pencil button from **Action** column of the profile you wish to modify. The following dialog box will appear.



The screenshot shows a dialog box titled "System Profile" with a close button (x) in the top right corner. The dialog contains four rows of input fields:

Profile Name:	mrcp
Provider:	mrcp
Enabled:	<input checked="" type="checkbox"/>
Language Tag:	en-US

At the bottom right of the dialog are two buttons: "Save" and "Cancel".

2. In the **Profile Name** field, enter the name of the profile.
3. In the **Provider** field, select the provider that should be used from the drop-down list.
4. In the **Enabled** field, click the check box to specify if the profile is enabled.
5. In the **Language Tag** field, enter the language tag that should be used.
6. Click **Save** to apply changes or click **Cancel** to abort the operation.

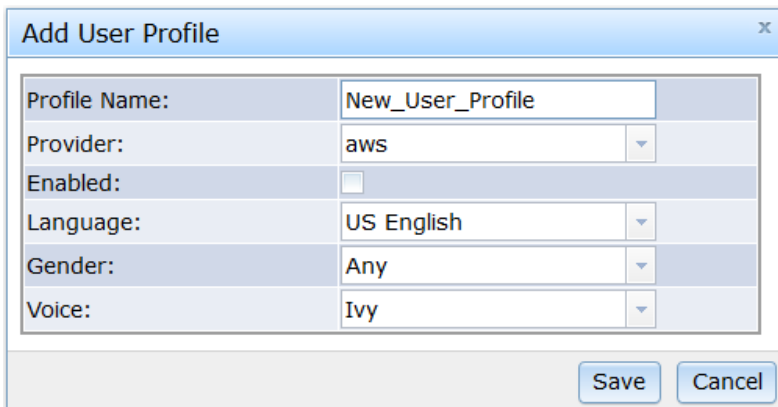
AWS User Profile

Amazon Polly is an Amazon Web Service (AWS) used by PowerMedia XMS for dynamic selection of Text-To-Speech (TTS) voices. An application can dynamically select the voice and provider source that it would like to use for TTS on a call-by-call basis.

The **AWS User Profile** section is used to configure the AWS User Profile.

Proceed as follows to configure the **Add User Profile** parameters:

1. In the **User Profile** section, click **Add User Profile** to add a new user profile or click the pencil button from **Action** column of the profile you wish to modify. The following dialog box will appear.



The screenshot shows a dialog box titled "Add User Profile" with a close button (x) in the top right corner. The dialog contains six rows of input fields:

Profile Name:	New_User_Profile
Provider:	aws
Enabled:	<input type="checkbox"/>
Language:	US English
Gender:	Any
Voice:	Ivy

At the bottom right of the dialog are two buttons: "Save" and "Cancel".

2. In the **Profile Name** field, enter the name of the profile.
3. In the **Provider** field, select the provider that should be used from the drop-down list.
4. In the **Enabled** field, click the check box to specify if the profile is enabled.
5. In the **Language** field, select the language that should be used from the drop-down list.
6. In the **Gender** field, select the gender that should be used from the drop-down list.
7. In the **Voice** field, select the voice that should be used from the drop-down list.
8. Click **Save** to apply changes or click **Cancel** to abort the operation.

MSRP

The Message Session Relay Protocol (MSRP) is a session-oriented instant message transport protocol. These sessions are used to provide peer-to-peer file or text transfer, photo sharing, or chat services. The **MSRP** menu opens to the **MSRP Configuration** page. The **MSRP Configuration** page is used to configure the MSRP service.

MSRP Configuration	
Global Settings:	
MSRP Address(es)	<input type="text" value="0.0.0.0"/>
MSRP Port	<input type="text" value="2855"/>
Transport	TLS <input type="checkbox"/> Accept Unencrypted Connections <input type="checkbox"/>
Max Payload Size	<input type="text" value="2048"/>
Response delay	<input type="text" value="30"/>
Connection Timeout	<input type="text" value="30"/>
Success Report	<input checked="" type="checkbox"/>
Failure Report	<input type="text" value="yes"/>
File Path	<input type="text" value="/var/lib/xms/media/en-US"/>
Allow Absolute Paths	<input type="checkbox"/>
<input type="button" value="Apply"/>	

Proceed as follows to configure the **MSRP Configuration** parameters:

1. In the **MSRP Address(es)** field, enter the local address(es) to be used for MSRP.

Note: IPv4 or IPv6 addresses are allowed. Only one address must be configured. If more than one address is entered, use a comma, semi-colon, or space to separate each address.
2. In the **MSRP Port** field, enter the MSRP port number. Default value is 2855. Range is 1-65535.
3. In the **Transport** field, click the check box to specify if **TLS** is enabled and if **Accept Unencrypted Connections** is enabled.
4. In the **Max Payload Size** field, enter the maximum size of MSRP payloads supported in bytes. Default value is 2048 bytes. Must be greater than 0.

5. In the **Response delay** field, enter the response delay time in seconds. Default value is 30 seconds. Must be greater than 0.
6. In the **Connection Timeout** field, enter the connection timeout in seconds. Default value is 30 seconds. Must be greater than 0. The connection timeout is the amount of time in seconds that the MSRP transport connection will be left open while in an idle state.
7. In the **Success Report** field, click the check box to indicate if there is a success report. A success report is an end-to-end report that is sent by the receiver to indicate if a successful MSRP message (SEND) exchange has occurred.
8. In the **Failure Report** field, select yes, no, or partial from the drop-down list to indicate if there is a failure report. A failure report is a hop-to-hop report that notifies the user app when a SEND failure has occurred. Default value is yes.
9. In the **File Path** field, enter the file path for media files. Default value is */var/lib/xms/media/en-US*.
10. In the **Allow Absolute Paths** field, click the check box to specify if absolute paths are enabled.
11. Click **Apply** to save changes.

Fax

The **Fax** menu opens to the **Fax Configuration** page.

Fax Configuration	
General	
IP Address:	0.0.0.0
Error Correction Mode:	TRUE
Local ID:	PowerMedia XMS Fax
T.38 re-INVITE Delay (inbound):	1,000
T.38 re-INVITE Timeout (outbound):	4,000
Reception Page Quality Thresholds	
Page Length: (0 - 255 units of 10 lines)	0
Error %:	5
Consecutive Bad Lines:	3
FAX page will be considered failed when one or more of these thresholds are breached	
<input type="button" value="Apply"/>	

Refer to the following table to configure fax. When complete, click **Apply** to save the changes.

Fax Configuration	Description
General	
IP Address	Select the IP address from the drop-down list or enter it manually. Note: To use the fax service, an IP address must be entered.
Error Correction Mode	Enable or disable the error connection mode.
Local ID	Enter the local ID. The local ID can have 0 to 20 characters.
T.38 re-INVITE Delay (inbound)	Enter the inbound T.38 re-INVITE delay value in milliseconds. Default value is 4,000.
T.38 re-INVITE Timeout (outbound)	Enter the outbound T.38 re-INVITE timeout value in milliseconds. Default value is 10,000.
Reception Page Quality Thresholds	
Page Length	Enter the page length. The range is 0 to 255 units of 10 lines. Default value is 0.
Error %	Enter the error percentage. Default value is 5.
Consecutive Bad Lines	Enter the consecutive bad lines. The range is 0 to 20. Default value is 3.
Note: Fax page will be considered failed when one or more of these thresholds are breached.	

Tones

The **Tones** menu contains the following tabbed pages: **Basic Tone Definitions**, **CPA Tone Definitions**, and **CPA Profiles**.

Note: A services restart is required after adding, modifying, or deleting a tone.

Basic Tone Definitions

The Basic Tone Definitions page is used to add, modify, and delete tones.

Note: A maximum of 20 tones may be defined.

The screenshot shows the 'Basic Tone Definitions' page with three tabs: 'Basic Tone Definitions' (active), 'CPA Tone Definitions', and 'CPA Profiles'. Below the tabs is a table with columns for 'Name', 'Type', and 'Cadence'. There are 'Delete' and 'Add' buttons below the table.

The following information is provided.

Item	Description
Name	Name of the tone.
Type	Specifies whether the tone is a single or dual tone.
Cadence	Specifies cadence. Valid values are as follows: <ul style="list-style-type: none">• Yes - Cadence tone• No - Continuous tone

Add a Tone

Proceed as follows to add a tone:

1. On the **Basic Tone Definitions** page, click **Add**. The **New Tone Definition** dialog box appears.

The 'New Tone Definition' dialog box contains the following fields:

- Tone Name:** Text input field with 'New' entered.
- Tone 1:**
 - Frequency (Hz): Spin box with '0' selected.
 - Tolerance (Hz): Text input field with '0'.
- Tone 2:**
 - Frequency (Hz): Text input field with '0'.
 - Tolerance (Hz): Text input field with '0'.
- Cadence:**
 - On Time (ms): Text input field with '0'.
 - Tolerance (ms): Text input field with '0'.
 - Off Time (ms): Text input field with '0'.
 - Tolerance (ms): Text input field with '0'.
 - repetitions : Text input field with '0'.

Buttons: 'Apply' and 'Cancel'.

2. Enter the name of the new tone in the **Tone Name** field.
3. In the mandatory **Tone 1** section, enter the frequency in hertz in the **Frequency (Hz)** field. Frequency range is between 300 Hz to 3.5 kHz.
4. Complete the **Tolerance (Hz)** field to specify the deviation in hertz.

Note: The **Tone 2** field is optional. If only **Tone 1** is defined, then the tone is a single tone. If both **Tone 1** and **Tone 2** are defined, then the tone is a dual tone.

Note: Dual tones with frequency components closer than approximately 63 Hz cannot be detected. In this case, use a single tone definition.

5. In the **Cadence** section, enter the following information in the fields provided:
 - **On Time (ms)** field - Tone-on time in milliseconds (minimum 40 ms). Set to 0 to define a continuous tone.
 - **Tolerance (ms)** field - Tone-on time deviation in milliseconds. Cadence only.
 - **Off Time (ms)** field - Tone-off time in milliseconds (minimum 40 ms). Cadence only.
 - **Tolerance (ms)** field - Tone-off time deviation in milliseconds. Cadence only.
 - **repetitions** field - Amount of repetitions.
6. Click **Apply** to save changes.

Modify a Tone

Proceed as follows to modify a tone:

1. On the **Basic Tone Definitions** page, click the check box to the left of the tone you wish to modify.
2. Click the tone name.
3. Change the desired fields in accordance with steps 3 through 7 as listed in the procedure to add a tone.

Delete a Tone

On the **Basic Tone Definitions** page, delete a tone by selecting the check box to the left of the tone you wish to delete and clicking **Delete**.

CPA Tone Definitions

The **CPA Tone Definitions** page is used to display and modify the CPA tone definitions.

Basic Tone Definitions	CPA Tone Definitions	CPA Profiles
------------------------	-----------------------------	--------------

Id	State
busy1	Enabled
busy2	Enabled
dialtone_international	Enabled
dialtone_local	Enabled
fax1	Enabled
fax2	Enabled
ringback1	Enabled
ringback2:seg1	Enabled
ringback2:seg2	
sit_no_circuit:seg1	Enabled
sit_no_circuit:seg2	
sit_no_circuit:seg3	
sit_operator_intercept:seg1	Enabled
sit_operator_intercept:seg2	
sit_operator_intercept:seg3	
sit_reorder:seg1	Enabled
sit_reorder:seg2	
sit_reorder:seg3	
sit_vacant_circuit:seg1	Enabled
sit_vacant_circuit:seg2	
sit_vacant_circuit:seg3	

The following information is provided.

Item	Description
Id	Name of the profile.
State	State of the profile.

Modify a Tone

Proceed as follows to modify a tone:

1. On the **CPA Tone Definitions** page, click the tone you wish to modify.
2. Change the desired fields.

busy1 - Tone Definition

CPA Tone State: Enabled

Label: busy1

Tone 1

Frequency (Hz): 480

Tolerance (Hz): 30

Tone 2

Frequency (Hz): 620

Tolerance (Hz): 30

Twin Frequency

Frequency (Hz): 0

Tolerance (Hz): 0

Cadence

On Time (ms): 500

Tolerance (ms): 150

Off Time (ms): 500

Tolerance (ms): 150

repetitions : 2

Apply Cancel

3. Click **Apply** to save changes.



CPA Profiles

The CPA Profiles page is used to add, modify, and delete profiles.

Note: A maximum of 4 profiles may be defined.

Basic Tone Definitions CPA Tone Definitions **CPA Profiles**

CPA Profiles

Profile Id	State	Continuous No Signal	PAMD Fail Time	No Answer	Operations
voip	Enabled	40000	30000	4000	 

[Add](#)

The following information is provided.

Item	Description
Profile Id	Name of the profile.
State	State of the profile.
Continuous No Signal	Maximum time in milliseconds of silence (no signal) allowed immediately after cadence detection begins. Default value is 40000.
PAMD Fail Time	Maximum time in milliseconds to wait for positive answering machine detection or positive voice detection after a cadence break. Default value is 30000.
No Answer	Length of time in milliseconds to wait after first ringback before deciding that the call is not answered. Default value is 4000.
Operations	Option to modify (pencil button) or delete (trash button) the profile.

Add a Profile

Proceed as follows to add a profile:

- On the **CPA Profiles** page, click **Add**. The **Create CPA Profile** dialog box appears.

Main Parameters	
Profile Id:	New_Profile_Id
CPA Profile State:	Enabled
Duration Of No Signal Time Out Delay:	40000
Wait For PAMD/PVD After Cadence Break:	30000
Time Before No Answer After 1st Ring:	4000

Advanced Parameters	
PVD	Edit
PAMD	Edit

Apply Cancel

Main Parameters

- Enter the name of the new profile in the **Profile Id** field.
- Select Enabled or Disabled from the **CPA Profile State** drop-down list.
- Set the maximum time in milliseconds of silence (no signal) allowed immediately after cadence detection begins in the **Duration Of No Signal Time Out Delay** field. Default value is 40000.
- Set the maximum time in milliseconds to wait for positive answering machine detection or positive voice detection after a cadence break in the **Wait for PAMD/PVD After Cadence Break** field. Default value is 30000.
- Set the length of time in milliseconds to wait after first ringback before deciding that the call is not answered in the **Time Before No Answer After 1st Ring** field. Default value is 4000.
- Click **Apply** to save changes.

Advanced Parameters

Note: The PVD and PAMD Qualification parameters are optimally set and normally do not require modification. Improper modification will result in PVD and PAMD failures. Please contact Dialogic Technical Services and Support for further information on usage.

CPA PVD Parameters

CPA PVD Parameters		x
PVD		
Min Allowable SNR:	50	
Max Allowable SNR:	600	
Max Num Peaks For Voice:	2	
Max Num Frames For Ringback Not Voice:	5	
Signal To Noise Ratio For Ringback:	10000	
Num Frames In a Window Sample:	8	
Minimum Energy For Voice:	5000	
Lower Freq of Ringback:	380	
Upper Freq of Ringback:	510	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

CPA PAMD Parameters

CPA PAMD Parameters		x
PAMD		
Minimum allowable Ring Duration:	190	
Mask:	1	
Maximum Answer Duration:	159	
Maximum Answer Duration #2:	159	
Maximum Answer Duration #3:	159	
Low Hiss (noise) Range:	22	
High Hiss (noise) Range:	16	
Noise Below Hiss Ratio:	5	
Cv. Threshold #1:	80	
Cv. Threshold #2:	165	
Maximum Cv. Threshold:	390	
Maximum Broad Band Energy - Noise:	2	
Maximum Total Energy - Noise:	65	
Maximum Silence:	40	
Voice Threshold:	25	
Silence Threshold:	5000	
Freq Band Filter - Lower Limit in Hz:	0	
Freq Band Filter - Upper Limit in Hz:	0	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Modify a Profile

Proceed as follows to modify a profile:

1. On the **CPA Profiles** page, click the pencil button from **Operations** column of the profile you wish to modify.
2. Click the profile name.
3. Change the desired fields as listed in accordance with steps 2 through 6 in the procedure to add a profile.

Delete a Profile

On the **CPA Profiles** page, delete a profile by clicking the trash button from **Operations** column of the tone you wish to delete and clicking **Delete**.

Media

The **Media** menu contains the following tabbed pages: **Media Configuration** and **Media Management**.

Media Configuration

The **Media Configuration** page is used to configure PowerMedia XMS media, transient recordings, and audio recording fidelity.

Media Configuration	
Media Configuration	
Media File Path:	<input type="text" value="/var/lib/xms/media"/>
Locale:	<input type="text" value="en-US"/>
Allow Absolute Paths:	<input type="checkbox"/>
Transient Recordings Configuration:	
Enabled:	<input checked="" type="checkbox"/>
Record Location:	<input type="text" value="transient"/>
File Linger Time (0-120 seconds):	<input type="text" value="15"/>
Advanced Parameters	<input type="checkbox"/>
Default Audio Recording Fidelity (wav):	
Sample Rate:	<input type="text" value="16000"/>
Sample Size:	<input type="text" value="16"/>
<input type="button" value="Manage Undelivered Recordings"/>	
<input type="button" value="Apply"/>	

Proceed as follows to configure the **Media Configuration** parameters:

Media Configuration

1. In the **Media File Path** field, enter the file path for media files.
2. In the **Locale** field, select the locale from the drop-down list.
3. In the **Allow Absolute Paths** field, click the check box to specify if absolute paths for media is allowed.

If the **Allow Absolute Paths** field is deselected (disabled), a media file can only be found by concatenating the **Locale** onto the **Media File Path** and looking for the specified media file there. If the **Allow Absolute Paths** field is selected (enabled), the full file specification for the media can be used in the application. The application may also use the **Media File Path** and **Locale** combination.

For absolute path, the file URI would look something like the following:

```
<audio uri=file:///var/lib/xms/media/en-US/verification/main_menu.wav
```

For relative path, the file URI would look something like the following:

```
<audio uri=file://./verification/main_menu.wav
```

Transient Recordings Configuration

4. In the **Enabled** field, click the check box to specify if transient recordings configuration is enabled.
5. In the **Record Location** field, enter the location of the record.
6. In the **File Linger Time (0-120 seconds)** field, enter the time of how long the file lingers in seconds. Valid values are 0-120.
7. In the **Advanced Parameters** field, click the check box to show **Play Location** field and enter the play location. By default, the play location is empty. An empty play location indicates that the play location is the same as the record location. In most cases, this field should be left at its default value (empty). If a comma separated list of paths is entered, PowerMedia XMS will attempt to play transient recordings from each of the paths until the transient recording is found.

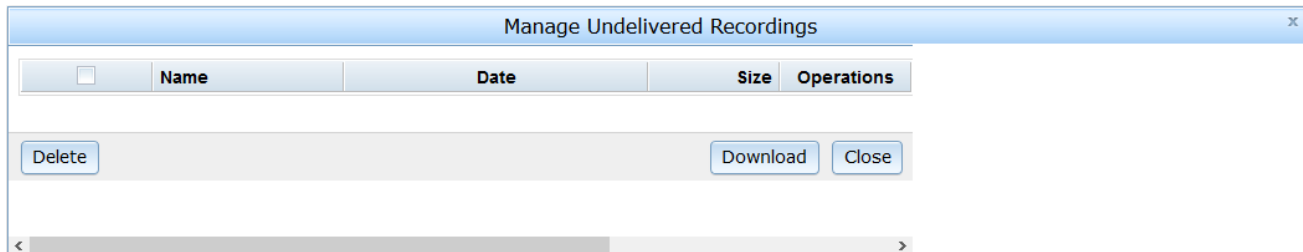
Default Audio Recording Fidelity (wav)

8. In the **Sample Rate** field, select the sample rate from the drop-down list. Valid values are 8000 or 16000.
9. In the **Sample Size** field, select the sample size from the drop-down list. Valid values are 8 or 16.
10. Click **Apply** to save changes.

Manage Undelivered Recordings

When recording to http:// destination, PowerMedia XMS records to a temporary file and subsequently transfers the recording to the requested http:// URI. In the event that a recording cannot be transferred to the supplied http:// URI after two attempts (i.e., a server problem), the recording will be saved so that it may be recovered if necessary.

From the **Media Configuration** page, click **Manage Undelivered Recordings**. The **Manage Undelivered Recordings** dialog box will appear.



Proceed as follows to manage the undelivered recordings.

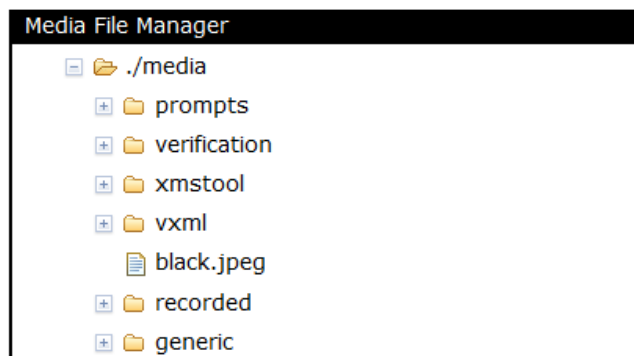
1. To download an undelivered recording, select a recording and click **Download**.
2. To delete an undelivered recording, select a recording and click **Delete**.
3. To abort the operation, click **Close**.

The check box on the top left can be used to select all the recordings listed in the **Manage Undelivered Recordings** dialog box. It will select every recording in the media directory, and the **Download/Delete** function can be used to apply to all.

Media Management

The **Media Management** page is used to view and manage the PowerMedia XMS media files. Functionality includes the following:

- [Uploading a Media File](#)
- [Deleting a Media File](#)
- [Creating a Media File Directory](#)
- [Deleting a Media File Directory](#)

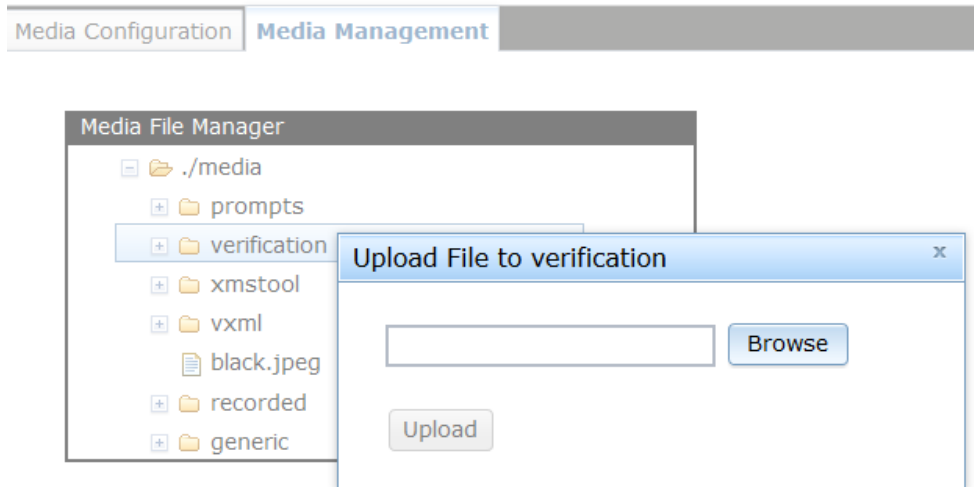


The *./media* directory shown in **Media File Manager** is a virtual directory. The virtual directory is rooted at the configured path and locale from the **Media Configuration** page. For example, when the path is configured as */tmp/files* and the locale is kept as the default *en-US*, the virtual directory will show media files from */tmp/files/en-US*.

Uploading a Media File

Proceed as follows to upload a media file:

1. Select the directory where the downloaded file will reside. For a new directory, see the [Creating a Media File Directory](#) section.
2. Right-click the directory and select **Upload Media File**. The upload dialog box appears.



3. Click **Browse** to access the desired media file. The appearance of the file explorer is tied to the operating system of the web browser used.
4. Select a media file that has been downloaded to the system on which your web browser is running.
Note: The field in which the media file appears is read-only and cannot be edited. To change the file, you must click the **Browse** button again and repeat the steps 3 and 4.
5. Click **Upload** to start the upload process. After a successful upload, the file will appear under the selected directory.

Deleting a Media File

Proceed as follows to delete a media file:

1. Select the file to delete.
2. Right-click and select **Delete**. A delete media file notification dialog will confirm whether to delete media file.
3. Click **OK** to delete the file or click **Cancel** to abort the operation. Upon successful delete completion, the file is removed from the Console's list display.

Creating a Media File Directory

Proceed as follows to create a media file directory:

1. Select the parent directory that will contain the new directory.
2. Right-click and select **Create Directory**. The **Enter Directory Name** dialog appears. Enter the name of the directory. To cancel the operation, click **x** in the right top corner of the dialog box.
3. To execute the directory creation after typing the name, press **Enter**. A dialog box is displayed indicating if PowerMedia XMS created the directory.
4. Click **OK**. The new directory will show on the list.

Deleting a Media File Directory

Proceed as follows to delete a media file directory:

1. Select the directory to delete.
Note: The root directory (*./media*) cannot be deleted.
2. Right-click and select **Delete**. A delete directory notification dialog will confirm whether to delete the directory and all its contents.
3. Click **OK** to delete the file or click **Cancel** to abort the operation. Upon successful delete completion, the directory is removed from the Console's list display.

CDR

The Call Detail Record (CDR) stores information about the details of a call. On PowerMedia XMS, a CDR is a stored data set record for each signaling and/or media transaction on the system.

The **CDR** menu contains the **CDR Query** page and the **CDR Configuration** page.

CDR Query

The **CDR Query** page is used to view, search for, and filter CDR logs. The CDRs can only be queried through this page when CDR generation is enabled in PowerMedia XMS. Enable CDR from the **System > Services** page.

The **CDR Query** page provides preset queries and user-created queries to filter CDR logs. The preset queries have filters that are already configured. The preset queries and their filters cannot be edited, renamed, or deleted. For custom queries, user queries can be created and saved.

CDR Queries

--- Preset Query ---

Select	Filter	Parameters	Operations
--------	--------	------------	------------

CDR Result

|<< << >> >>|

Select	Called Uri	Caller Uri	Call StartTime	SIP Call Id	call Dir	Protocol	Call State
--------	------------	------------	----------------	-------------	----------	----------	------------

|<< << >> >>|

Run a Query

To run a CDR query, select the query from the dropdown list and click **Run**. If there are no relevant CDR logs, a "No match found for the requested filter" message appears in the **CDR Result** field.

Add a User Query

To add a user query, click **New** and enter a name for the query in the **Add User Query Name** popup window. When finished, click **Submit**. User queries with no filters have an asterisk added to the name once the user query is added to the **CDR Queries** dropdown list.

Add a Filter

Proceed as follows to add a filter to a CDR user query:

1. Select the user query from the **CDR Queries** field. If a user query has not been created, refer to [Add a User Query](#). Preset queries cannot be edited.
2. Click **Add Filter** to display the **Add Filter** popup window.

- Click the **Filter Type** drop-down list, select the desired filter type, adjust the parameters as necessary, and click **OK** when finished. Refer to the following table for details on the filters and parameters.

Filter Type	Description
TIME	Filter CDR logs by start and end dates and by start and end times.
CALL STATE	Filter CDR logs by call states. To select multiple call states, hold down the Shift key while clicking each one.
CALL DIRECTION	Filter CDR logs by the direction of the call: inbound or outbound.
REL CODE	Filter CDR logs by release codes. To select multiple release codes, hold down the Shift key while clicking each one.
PROTOCOL	Filter CDR logs by SIP or RTCWeb protocol.
CALLING URI	Filter CDR logs by a specified calling URI string. For example, if the calling URI parameter is "9901*", any From header that contains the 9901 string will be included in the query result.
CALLED URI	Filter CDR logs by a specified called URI string. For example, if the called URI parameter is "9901*", any To header that contains the 9901 string will be included in the query result.
CALL DURATION	Filter CDR logs by call duration. Enter minimum, maximum, or minimum and maximum call duration parameters. Call duration is in seconds. Note: This filter only applies to completed calls.
CDR COUNT PER PAGE	Show 10, 20, 50, or 100 CDR logs per page.
JITTER (QoS)	Filter CDR logs by jitter. Enter minimum, maximum, or minimum and maximum jitter parameters. Jitter is in milliseconds.
PACKET LOSS (QoS)	Filter CDR logs by packet loss. Enter minimum, maximum, or minimum and maximum packet loss parameters. Packet loss is in percent.

- Click **Save** to save the new filter to the user query. User queries that have not been saved have an asterisk added to the query name.

Edit a Filter

Proceed as follows to edit an existing filter that is part of a user query:

1. Select the user query from the **CDR Queries** field.
2. In the filter's **Operations** section, click the edit icon.
3. In the **Add Filter (Edit)** popup window, adjust the filter and parameters as necessary and then click **OK**.
4. Click **Save** to save the filter changes and update the user query. User queries that have not been saved have an asterisk added to the query name.

Delete a Filter

Proceed as follows to delete an existing filter that is part of a user query:

1. Select the user query from the **CDR Queries** field.
2. In the filter's **Operations** section, click the delete icon.
3. Click **Save** to save the filter changes. User queries that have not been saved have an asterisk added to the query name.

Rename a User Query

To rename a user query, select the user query in the **CDR Queries** field and enter a new user query name in the **Edit User Query Name** popup window. When finished, click **Submit**.

Delete a User Query

To delete a user query, select the user query in the **CDR Queries** field and then click **Delete**.

Enable or Disable Automatic CDR Log Updates

Click the **Enable Auto Refresh** button to automatically update CDR logs every 3 seconds. If **Enable Auto Refresh** enabled, the **Disable Auto Refresh** button appears instead of the **Enable Auto Refresh** button. Click the **Disable Auto Refresh** button to not automatically update CDR logs.

Manage Columns

Click the **Manage Columns** button to configure the CDR result columns.

Manage CDR Result Columns x

CDR Result Columns					
Call AnswerTime	<input type="checkbox"/>	Call EndTime	<input type="checkbox"/>	release Dir	<input type="checkbox"/>
rel Reason	<input type="checkbox"/>	Req Uri	<input type="checkbox"/>	Rel Code	<input type="checkbox"/>
Answer SDP	<input type="checkbox"/>	Call Duration	<input type="checkbox"/>	Audio BitRate	<input type="checkbox"/>
Audio ClockRate	<input type="checkbox"/>	Audio Coder FrameSz	<input type="checkbox"/>	Audio Dir	<input type="checkbox"/>
Audio Encoding	<input type="checkbox"/>	Audio FramesPerPkt	<input type="checkbox"/>	Audio LocalIp	<input type="checkbox"/>
Audio LocalPort	<input type="checkbox"/>	Audio PayloadType	<input type="checkbox"/>	Audio RemoteIp	<input type="checkbox"/>
Audio RemotePort	<input type="checkbox"/>	Audio VAD Enabled	<input type="checkbox"/>	DTMF Mode	<input type="checkbox"/>
RTP StartTime	<input type="checkbox"/>	RTP EndTime	<input type="checkbox"/>	video BitRate	<input type="checkbox"/>
Video MaxBitRate	<input type="checkbox"/>	Video SamplingRate	<input type="checkbox"/>	Video ImgWidth	<input type="checkbox"/>
Video ImgHeight	<input type="checkbox"/>	Video Dir	<input type="checkbox"/>	Video Encoding	<input type="checkbox"/>
Video PayloadType	<input type="checkbox"/>	Video LocalIp	<input type="checkbox"/>	Video LocalPort	<input type="checkbox"/>
Video RemoteIp	<input type="checkbox"/>	Video RemotePort	<input type="checkbox"/>	Stream Id	<input type="checkbox"/>
QOS LocalTimeStamp	<input type="checkbox"/>	QOS LostPkts	<input type="checkbox"/>	QOS Jitter	<input type="checkbox"/>
QOS RTLatency	<input type="checkbox"/>	QOS LocalTxPkts	<input type="checkbox"/>	QOS LocalTxOcts	<input type="checkbox"/>
QOS LocalCumuLost	<input type="checkbox"/>	QOS RemoteTxPkts	<input type="checkbox"/>	QOS RemoteTxOcts	<input type="checkbox"/>
QOS RemoteCumuLost	<input type="checkbox"/>	QOS LocalSeqNum	<input type="checkbox"/>	QOS RemoteTimeStamp	<input type="checkbox"/>
QOS RemoteSeqNum	<input type="checkbox"/>				

Click **Apply** to save changes.

CDR Configuration

The **CDR Configuration** page is used to configure the CDR related parameters.

CDR Query **CDR Configuration**

CDR File Duration (in Hours)	<input type="text" value="1"/>
Active CDR Age (in Hours)	<input type="text" value="1"/>
Maximum Disk Space (in MB)	<input type="text" value="4096"/>
Database Type:	<input type="text" value="local"/>

Proceed as follows to configure the **CDR Configuration** parameters:

1. In the **CDR File Duration (in Hours)** field, select the duration (in hours) of time in which CDR are kept in a single CDR file from the drop-down list. Possible values are restricted to a factor of 24 (1, 2, 3, 4, 6, 8, 12, 24) so that any CDR file contains CDR of only a particular date.
2. In the **Active CDR Age (in Hours)** field, enter the duration (in hours) of time in which CDR files will be kept in the database. After the expiration of this duration, the CDR files are moved to the flat CDR files and removed from the database. Range is 1 to 72.
3. In the **Maximum Disk Space (in MB)** field, enter the maximum disk space (in megabytes) allocated for CDR files on disk. As soon as the total size of CDR files on disk exceeds this maximum size threshold, a configurable percentage of this space (as configured in the CDR configuration file `/etc/xms/cdrserver/config/cdrconfig.json`, `cdrPurgeSizeInPercent` parameter) will be recovered by the system by permanently removing one or more, oldest CDR files from the disk. If the maximum disk space is changed, the SNMP threshold for disk usage percentage will become invalid and need to be configured again. Range is 64 to 40960 (40 GB).
4. In the **Database Type** field, select the type of database from the drop-down list. Valid values are local, Mongo (Remote), and Postgres (Remote).

Mongo (Remote) and Postgres (Remote) are remote database options and can be configured for separate CDR storage from the default PowerMedia XMS local storage normally used for CDR storage. A remote database can also be beneficial for database replication, redundancy, and high data availability to provide a level of fault tolerance against the loss of a single database server.

Note: The remote database functionality is in a controlled introduction.

5. Click **Set Configuration** to save changes.
6. Click **Purge CDR Database** to clear the CDR database.

Note: The system services must be restarted for the changes in CDR configuration to take effect.

The CDR files are generated and can be found in the following location on the PowerMedia XMS installation:

```
/var/local/xms/cdr
```

For more details about the CDR fields and the call data logged, refer to the [Appendix C: CDR](#).

Remote Database (Mongo)

The **Mongo (Remote)** section of the **CDR Configuration** page is used to configure the CDR related parameters with the Mongo database.

CDR File Duration (in Hours)	<input type="text" value="1"/>		
Active CDR Age (in Hours)	<input type="text" value="1"/>		
Maximum Disk Space (in MB)	<input type="text" value="4096"/>		
Database Type:	<input type="text" value="Mongo (Remote)"/>		
Database Account:	<input type="text"/>		
<input type="checkbox"/> Replication	Replica Set Name: <input type="text" value="cdr"/>		
<input type="button" value="Add DB Host"/>			
Host ID	Port	Description	Operations

Proceed as follows to configure the **Mongo (Remote)** parameters:

1. In the **Database Account** field, select the account to be used with Mongo database (configured through the **Account** section on **Secure Storage** page) from the drop-down list.
2. Click the check box for **Replication** to enable replication and enter the name of replica set.
3. Click **Add DB Host** to add a database host. This action results in the following popup window.

Add CDR DB Profile x

Port:	<input type="text"/>
<input type="radio"/> Host <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	<input type="text"/>
Description:	<input type="text"/>

Proceed as follows to configure the **Add CDR DB Profile** parameters:

- In the **Port** field, specify the port for CDR remote database.
 - Click the **Host**, **IPv4**, or **IPv6** radio button and enter the IP address for CDR remote database.
 - In the **Description** field, enter a description for CDR remote database.
 - Click **Save** to add a CDR remote database.
4. Click **Set Configuration** to save changes.

Remote Database (Postgres)

The **Postgres (Remote)** section of the **CDR Configuration** page is used to configure the CDR related parameters with the Postgres database.

The Postgres schema file is available on the **Downloads** page so users can configure their remote Postgres database.

CDR Query	CDR Configuration
CDR File Duration (in Hours)	<input type="text" value="1"/>
Active CDR Age (in Hours)	<input type="text" value="1"/>
Maximum Disk Space (in MB)	<input type="text" value="4096"/>
Database Type:	<input type="text" value="Postgres (Remote)"/>
Database Account:	<input type="text"/>
<input type="radio"/> Host <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	<input type="text" value="127.0.0.1"/>
Port:	<input type="text" value="5432"/>

Set Configuration

Purge CDR Database

Proceed as follows to configure the **Postgres (Remote)** parameters:

1. In the **Database Account** field, select the account to be used with Postgres database (configured through the **Account** section on **Secure Storage** page) from the drop-down list.
2. Click the **Host**, **IPv4**, or **IPv6** radio button and enter the IP address for CDR remote database.
3. In the **Port** field, specify the port for CDR remote database.
4. Click **Set Configuration** to save changes.

Access to CDR Files

To provide user access to the CDR files, the PowerMedia XMS system administrator will need to create a login for the user who wants to access CDR files on the system. The following set of commands needs to be run by the system administrator as root user:

```
useradd -d /var/local/xms/cdr <username>
passwd <username>
Changing password for user <username>.
New password: *****
Retype new password: *****
chown <username> /var/local/xms/cdr
chgrp <username> /var/local/xms/cdr
chmod 544 /var/local/xms/cdr
```

SNMP

Simple Network Management Protocol (SNMP) is a standard-based IP network management mechanism for exchanging information between SNMP agents that typically reside on a managed device and SNMP management systems. The **SNMP** menu opens to the **Configuration** page, which allows the display and configuration of the SNMP parameters required for PowerMedia XMS.

For more information about SNMP, refer to the [Appendix B: SNMP](#).

SNMPD Services for IPv6

Trap Destinations

Select	Protocol	Destination Host	Port	Version
--------	----------	------------------	------	---------

V2c Communities

Select	Community	Access
--------	-----------	--------

V3 Users

Select	User Name	Security Level	Access
<input type="checkbox"/>	XMSUser	AuthPriv	RO

Configuration

The **Configuration** page allows the display and configuration of the SNMP parameters required for PowerMedia XMS.

SNMPD Services for IPv6

If the PowerMedia XMS is configured for IPv6, it is possible to configure the SNMP services to leverage IPv6 networking. The **Enable** button enables the SNMP to use IPv6 networking, provided IPv6 is enabled. The **Disable** button disables the use of IPv6 services.

Trap Destinations

The **Trap Destinations** section of the **Configuration** page enables you to configure the recipients of the SNMP traps generated by the PowerMedia XMS installation.

Adding a New Trap Destination

Click the **Add** button to add a new trap destination. This action results in the following popup window.

Trap destination	
Protocol	TCP
Destination Host	10.40.2.21
Port	162
Version	V2c

V2c Community	
Community String	public

Save Cancel

In the **Trap Destination** section, enter the following information:

- **Protocol** - the IP transport protocol for the SNMP traps (TCP, UDP, TCP6, or UDP6).
- **Destination Host** - the destination of the host, which will receive the SNMP traps.
- **Port** - the IP port number of the recipient.
- **Version** - the SNMP version supported by the recipient (V2c or V3).

Note: The only versions supported by the current implementation are SNMP V2c and V3.

If the **Version** field in the **Trap Destination** section has V2c selected, enter the **Community String** in the **V2c Community** section for SNMP version V2c and click **Save**.

Trap destination	
Protocol	TCP
Destination Host	10.40.2.21
Port	162
Version	V3

V3 User	
Security Name	myuser
Authentication Protocol	MD5
Privacy Protocol	DES
Authentication Key	myauthpass
Privacy Key	myauthpass
Security	noAuthnoPriv
Engine ID	10.1.2.34567890123456789012345678901234

Save Cancel

If the **Version** field in the **Trap Destination** section has V3 selected, follow these steps in the **V3 User** section:

1. In the **Security Name** field, enter the security name.
2. In the **Authentication Protocol** field, select MD5 or SHA from the drop-down list.
3. In the **Privacy Protocol** field, select AES or DES from the drop-down list.
4. In the **Authentication Key** field, enter the authentication key name.
5. In the **Privacy Key** field, enter the privacy key name.
6. In the **Security** field, select noAuthnoPriv, AuthNoPriv, or AuthPriv from the drop-down list.
7. In the **Engine ID** field, enter the engine ID number.
8. Click **Save**.

The new SNMP trap destination will be added to the list of destinations.

Editing a Trap Destination

Click the **Edit** button to edit a trap destination.

In the **Trap Destination** section, select the trap destination to be edited (using the check box on the left) and click **Edit**. A popup similar to the one described in the previous section will open. All the fields in this popup will be populated by the values of the chosen destination. Edit the values and click **Save**. The popup will disappear and the trap destination will be modified.

Deleting a Trap Destination

Click the **Delete** button to delete a trap destination.

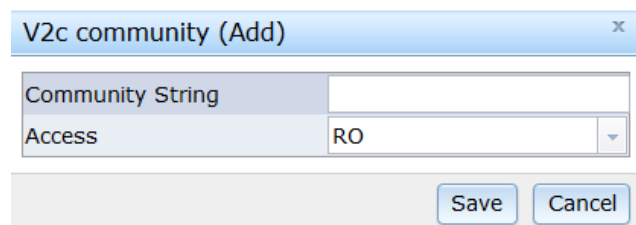
In the **Trap Destination** section, select the trap destination to be deleted (using the check box on the left) and click **Delete**. The selected destination will be deleted.

SNMP V2c Communities

The SNMP V2c communities can be added or modified from the **V2c Communities** section on the **Configuration** page. This section displays a table showing the **Community String** and its **Access** rights.

Adding a V2c User

In the **V2c Communities** section, click the **Add** button. The following popup appears.



The screenshot shows a popup window titled "V2c community (Add)". It contains two input fields: "Community String" and "Access". The "Access" field is a dropdown menu currently showing "RO". At the bottom of the popup are two buttons: "Save" and "Cancel".

Proceed as follows to add a V2c User:

1. In the **Community String** field, enter the community string name.
2. In the **Access** field, select RO or RW from the drop-down list.
3. Click **Save**.

The new community string with the chosen access rights will be added.

Editing a V2c Community

In the **V2c Communities** section, select the V2C community to be edited (using the check box on the left) and click **Edit**. A popup similar to the one shown in the previous section will appear. Edit the values and click **Save**. The updated values of the SNMP v2c community will be saved.

Deleting a V2c User

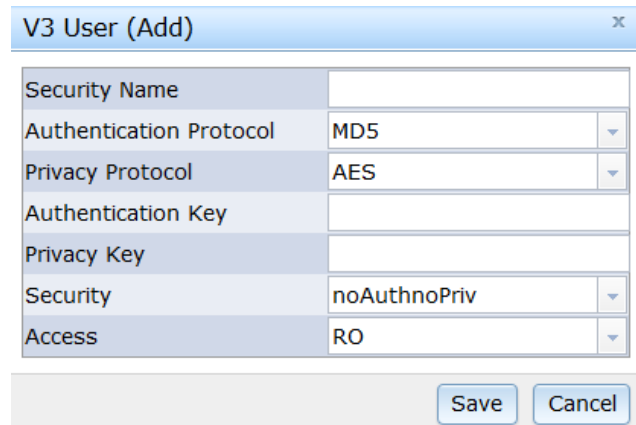
In the **V2c Communities** section, select the V2C community to be deleted (using the check box on the left) and click **Delete**. The selected community will be deleted.

SNMP V3 Users

The SNMP V3 users can be added or modified from the **V3 Users** section on the **Configuration** page. This section displays a table showing the various users and their properties.

Adding a V3 User

In the **V3 Users** section, click the **Add** button. The following popup appears.



V3 User (Add)	
Security Name	<input type="text"/>
Authentication Protocol	MD5
Privacy Protocol	AES
Authentication Key	<input type="text"/>
Privacy Key	<input type="text"/>
Security	noAuthnoPriv
Access	RO

Save Cancel

Proceed as follows to add a V3 User:

1. In the **Security Name** field, enter the security name.
2. In the **Authentication Protocol** field, select MD5 or SHA from the drop-down list.
3. In the **Privacy Protocol** field, select AES or DES from the drop-down list.
4. In the **Authentication Key** field, enter the authentication key.
5. In the **Privacy Key** field, enter the privacy key.
6. In the **Security** field, select noAuthnoPriv, AuthNoPriv, or AuthPriv from the drop-down list to indicate which type of security is being used.
7. In the **Access** field, select RO or RW from the drop-down list.
8. Click **Save**.

The new V3 user will be created and added to the list of existing V3 users.

Editing a V3 User

In the **V3 Users** section, select the V3 user to be edited (using the check box on the left) and click **Edit**. A popup similar to the one shown in the previous section will appear. Edit the values and click **Save**. The updated values of the SNMP V3 user will be saved.

Deleting a V3 User

In the **V3 Users** section, select the V3 user to be deleted (using the check box on the left) and click **Delete**. The selected user will be deleted.

High Threshold Configuration

The **High Threshold Configuration** page enables the user to set the High Threshold values for various meters in the PowerMedia XMS subsystem. An SNMP trap is triggered if the configured threshold value for any meter is breached. To avoid an SNMP trap storm (due to meters hunting around the threshold value), the PowerMedia XMS system clears the trap condition if the meter value becomes less than or equal to the 90% mark of the configured threshold (in the downward direction).

The trap severity trigger values are percentages (0-100) of the maximum value for a given number. A value of 0 disables the trap for given severity category.

Configuration		High Threshold Configuration			
License Features					
Name	Warning	Minor	Major	Critical	
Basic Audio	0	0	0	0	
HD Voice	0	0	0	0	
GSM/AMR Audio	0	0	0	0	
LBR Audio	0	0	0	0	
MRCP Speech Server	0	0	0	0	
Advanced Video	0	0	0	0	
High Resolution Video	0	0	0	0	
Fax Calls High	0	0	0	0	
License Expirations					
Name	Warning	Minor	Major	Critical	
License Expiry (Days)	60	45	30	10	
Maintenance Plan Expiry (Days)	60	45	30	10	
License Server Unreachable (% Grace Period)	0	25	50	75	
Resources					
Name	Warning	Minor	Major	Critical	
ASR/TTS Sessions	0	0	0	0	
Conf. Call Parties	0	0	0	0	
Conf. Media Parties	0	0	0	0	
Conf. Rooms	0	0	0	0	
Fax Sessions	0	0	0	0	
Media Transactions	0	0	0	0	
RTP Sessions	0	0	0	0	
Signaling Sessions	0	0	0	0	
CDR Disk Usage	0	0	0	0	

Trap severity trigger values are percentages (0-100) of the maximum value for a given counter except as noted. A value of 0 disables the trap for given severity category.

Apply

For the purpose of trap generation, the PowerMedia XMS system enables the user to set percentage values for the following meters in **Warning**, **Minor**, **Major**, and **Critical** severity categories:

License Features

- **Basic Audio** license usage (percentage value range: 0 to maximum licensed capacity)
- **HD Voice** license usage (percentage value range: 0 to maximum licensed capacity)
- **GSM/AMR Audio** license usage (percentage value range: 0 to maximum licensed capacity)
- **LBR Audio** license usage (percentage value range: 0 to maximum licensed capacity)
- **MRCP Speech Server** license usage (percentage value range: 0 to maximum licensed capacity)
- **Advanced Video** license usage (percentage value range: 0 to maximum licensed capacity)
- **High Resolution Video** license usage (percentage value range: 0 to maximum licensed capacity)
- **Fax Calls High** license usage (percentage value range: 0 to maximum licensed capacity)

License Expirations

- **License Expiry (Days)**
- **Maintenance Plan Expiry (Days)**
- **License Server Unreachable (% Grace Period)**

Resources

- **ASR/TTS Sessions** (percentage value range: 0 to 100 percent of available sessions)
- **Conf. Call Parties** (percentage value range: 0 to 100 percent of available conference call parties)
- **Conf. Media Parties** (percentage value range: 0 to 100 percent of available conference media parties)
- **Conf. Rooms** (percentage value range: 0 to 100 percent of available conference rooms)
- **Fax Sessions** (percentage value range: 0 to 100 percent of available fax sessions)
- **Media Transactions** (percentage value range: 0 to 100 percent of available media transactions)
- **RTP Sessions** (percentage value range: 0 to 100 percent of available RTP sessions)
- **Signaling Sessions** (percentage value range: 0 to 100 percent of available signaling sessions)
- **CDR Disk Usage** (percentage value range: 0 to 100 percent of configured maximum CDR disk capacity)

Enter a percentage value within the percentage value range for each meter and click **Apply** to commit the percentage values to the PowerMedia XMS system. If a percentage value is entered that exceeds the meter’s maximum licensed capacity, an error message appears when **Apply** is clicked and the invalid values are reset to the original values. If a percentage value is entered that exceeds the **CDR Disk Usage** meter’s maximum disk capacity, the percentage value cell turns red and an exclamation mark appears next to it. Adjust the maximum disk capacity in the **Maximum Disk Space (in MB)** field on the **CDR > CDR Configuration** page if necessary.

For more information about SNMP, refer to the [Appendix B: SNMP](#).

Reports

The **Reports** menu opens to the **Metrics Export** page, which is used to configure **Parameters** and **Rotation Policy** for exporting reports on metrics.

Note: The functionality on the **Metrics Export** page is in a controlled introduction. The metrics contained in the exported file may change in future PowerMedia XMS releases.

Note: The Export Metrics Service must be enabled for reports to be generated.

Metrics Export

Parameters:

File Format	CSV
Sampling Rate (minutes)	1
File Duration	30min
File Name Prefix	xms
Storage Location	Local Default

Rotation Policy:

Size on Disk (MB)	100
Maximum Age (Days)	1

*The Export Metrics Service must be enabled for reports to be generated.

Download
Purge Local Files
Configure Meters
Apply

Parameters

Proceed as follows to configure the **Parameters**.

Parameter	Description	Valid Values
File Format	Specifies the format type of the exported file.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> CSV (default) JSON XML

Parameter	Description	Valid Values
Sampling Rate (minutes)	Specifies the sampling rate.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • 1 (default) • 5 • 10 • 15 • 30 • 60
File Duration	Specifies the duration of the file.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • 15min • 30min • 1hr • 2hr • 3hr • 4hr • 6hr • 8hr • 12hr • 24hr
File Name Prefix	Specifies the prefix of the file name.	Enter the name of the prefix. 1 - 64 character alphanumeric with no spaces.
Storage Location	Specifies the storage location of the file.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • Local Default • (NFS -- mounted)

Rotation Policy

Proceed as follows to configure the **Rotation Policy**.

Parameter	Description	Valid Values
Size on Disk (MB)	Specifies the maximum size on disk.	0 - 4096 (0 is disabled)
Maximum Age (Days)	Specifies the maximum age.	0 - 31 (0 is disabled)

Click **Apply** to save changes.

Download

The metrics report archive can be downloaded to your system by clicking the **Download** button.

Generated Report Archives		
Archive Name	Size	Operations
xms-metrics-20171010_134911.tar.gz	77	

Click **Generate Archive** to generate the metrics report archive. The metrics report archive file can be downloaded or deleted through the **Operations** column.

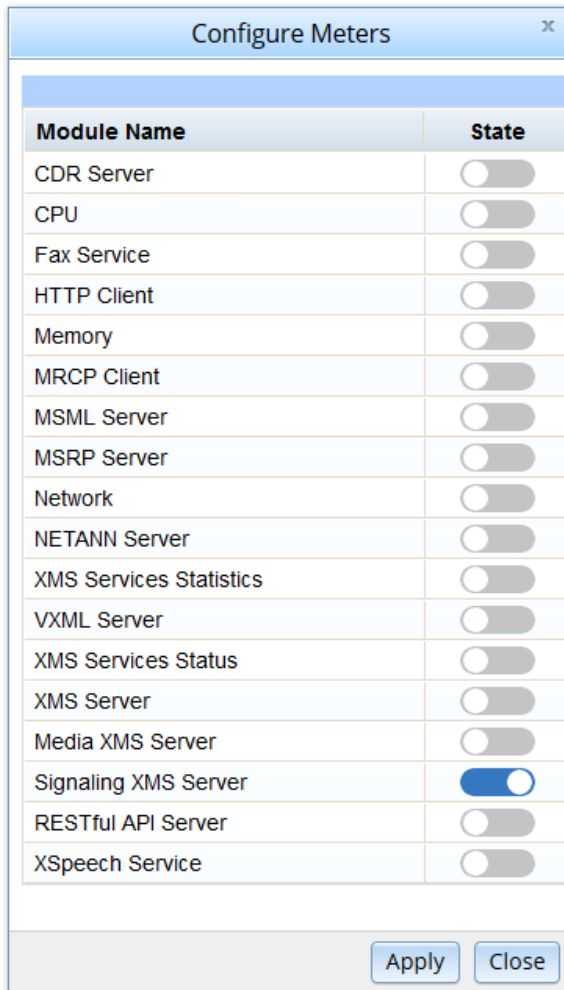
Purge Local Files

The local files can be purged by clicking the **Purge Local Files** button. Click **OK** to purge all reports or click **Cancel** to abort the operation.

Configure Meters

Proceed as follows to configure the meters to export.

1. Click **Configure Meters**. The **Configure Meters** dialog box will appear.



Module Name	State
CDR Server	<input type="checkbox"/>
CPU	<input type="checkbox"/>
Fax Service	<input type="checkbox"/>
HTTP Client	<input type="checkbox"/>
Memory	<input type="checkbox"/>
MRCP Client	<input type="checkbox"/>
MSML Server	<input type="checkbox"/>
MSRP Server	<input type="checkbox"/>
Network	<input type="checkbox"/>
NETANN Server	<input type="checkbox"/>
XMS Services Statistics	<input type="checkbox"/>
VXML Server	<input type="checkbox"/>
XMS Services Status	<input type="checkbox"/>
XMS Server	<input type="checkbox"/>
Media XMS Server	<input type="checkbox"/>
Signaling XMS Server	<input checked="" type="checkbox"/>
RESTful API Server	<input type="checkbox"/>
XSpeech Service	<input type="checkbox"/>

2. Click the button listed in the **State** column to toggle between enabled and disabled for the modules to include in the meters export. The **State** column will change to the action you selected.
3. Click **Apply** to save changes or click **Close** to abort the operation.

Monitor

The **Monitor** menu contains the following tabbed pages: **Dashboard**, **Call Groups**, **Graph**, and **Options**.

Dashboard

The **Dashboard** page displays the real-time active counts of resources and licenses being used by PowerMedia XMS. Applications can use this data to monitor the system call, code, conferencing status, and usage.

Dashboard	Call Groups	Graph	Options
------------------	-------------	-------	---------

Licenses	Available	Used	Free	% Used
Basic Audio	200	0	200	0.0
HD Voice	200	0	200	0.0
GSMAMR Audio	200	0	200	0.0
LBR Audio	200	0	200	0.0
MRCP Speech Server	200	0	200	0.0
MSRP	0
Advanced Video	200	0	200	0.0
High Resolution Video	200	0	200	0.0
Fax	1	0	1	0.0

Resources	Active
Media Transactions	0
Conference Rooms	0
Conference Parties	0
Conference Media Parties	0
Signaling Sessions	0
RTP Sessions	0
ASR / TTS Sessions	0
Fax Sessions	0

Refresh

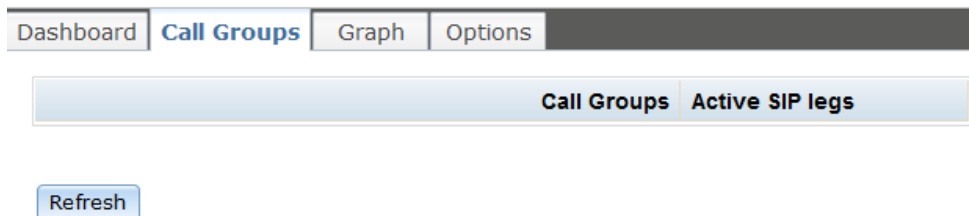
The **Dashboard** page shows a snapshot of counters for the following parameters:

- Licenses and Usage
 - Basic Audio
 - HD Voice
 - GSMAMR Audio
 - LBR Audio
 - MRCP Speech Server
 - MSRP
 - Advanced Video
 - High Resolution Video
 - Fax
- Active Resources
 - Media Transactions
 - Conference Rooms
 - Conference Parties
 - Conference Media Parties
 - Signaling Sessions
 - RTP Sessions
 - ASR/TTS Sessions
 - Fax Sessions

Click **Refresh** to reload the **Dashboard** page.

Call Groups

The **Call Groups** page displays the call groups and active SIP legs.



Click **Refresh** to reload the **Call Groups** page.

Graph

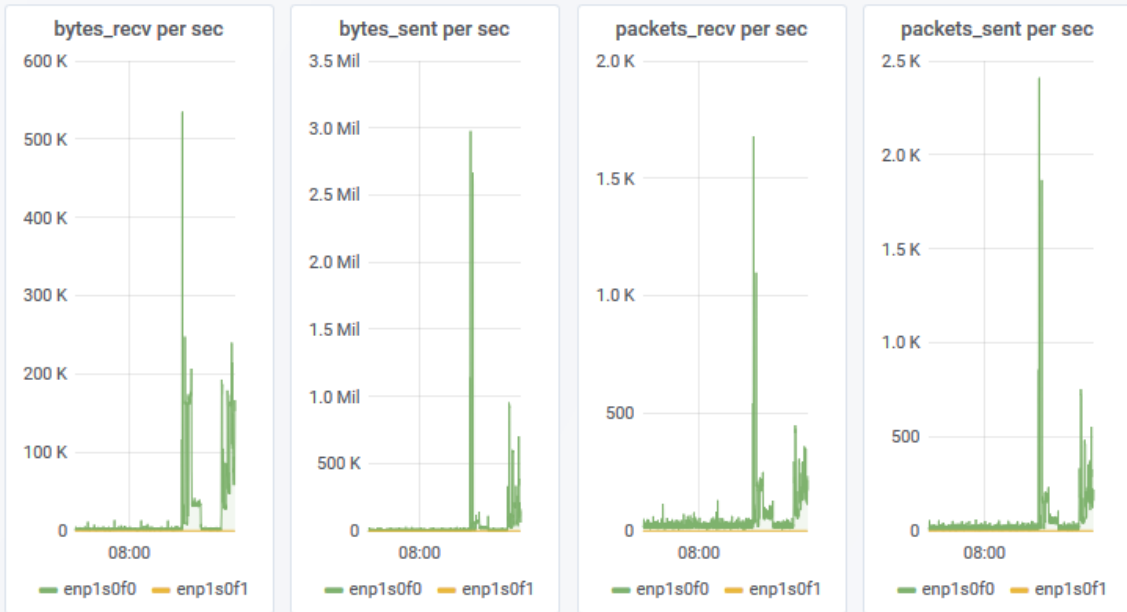
The **Graph** page displays, collects, and stores Key Performance Indicator (KPI) metrics in the resource dashboards. The dashboards cover real-time and report-driven KPI metrics gathered at desired collection intervals and provide a KPI subsystem to monitor system metrics and insight into media application usage of media resources.

Network Performance ▾

Last 3 hours Refresh every 5s

Interface All ▾ Type All ▾

Basic Performance



Advanced Performance



Top Header

The top header displays the following:

- Dashboard: This drop-down list shows which dashboard is currently being viewed and allows switching to another dashboard.
- Share Dashboard: This button provides options to create direct link to a dashboard, share a dashboard, and export a dashboard.
- Time Picker: This button provides access to relative time range options, auto refresh options, and custom absolute time range options.
- Refresh: This button refreshes all the panels (fetch new data).

Dashboards

For more information and a list of KPI subsystem counters, refer to the [Appendix F: Dashboard Counters](#).

Application Resources

- Appmanager
- Broker
- HMP
- MSML
- Mrcp
- Msrp
- Netann
- Nodecontroller
- Rtcweb
- Vxml
- Xmserver

CDR Resources

- Query Performance
- General
- Export
- Server Performance

FAX Resources

- Basic Performance
- Advanced Performance

HTTP Client Resources

- get
- put
- post
- delete

MRCP Resources

- Session
- Request
- Completion Cause
- Stop

Note: The dashboard reports "Unknown" server status until at least one MRCP session establishment is attempted to that server.

MSML Resources

- call
- conference
- conferenceparty
- media
- play
- speech
- record
- cpa
- faxrcv
- faxsend
- collect
- dtmfgen
- faxdetect
- fileop
- transfer

MSRP Resources

- Message
- Session
- Txrn General
- Txrn File
- Txrn Message

NETANN Resources

- Media
- Conference
- Conference Party

Network Performance

- Basic Performance
- Advanced Performance

RESTful Resources

- Call
- Conference
- MRCP

Speech Service

- Session
- TTS

Summary

- Service Status
- License Status
- XMS Resources
- System Resources

System Resources

- CPU Usage
- Memory
- Disk
- Disk IO
- Network Performance
- Processes Status

VXML Resources

- Voice
- Record
- Transfer
- DTMF
- Prompt Speech
- Prompt Play
- Sayas
- Connection

XMS Licenses

- Advanced Video
- Basic Audio
- FAX
- GSM-AMR
- HD Voice
- High Resolution Video
- LBR Audio

- MRCP
- MSRP

XMS Metrics

- appmanager
- cdr
- cpu
- disk
- diskio
- faxservice
- httpclient
- kernel
- mem
- mrcp
- msml
- msrp
- net
- netann
- processes
- procstat
- swap
- system
- vxml
- xmsGeneric
- xmsSystem
- xmserver
- xmsrest

XMS Resources

- Session
- Resource
- RTP

Note: MRCP SIP traffic will not be included in any SIP counters.

Options

The **Options** page is used to configure the retention policy for metrics.

Dashboard | Call Groups | Graph | **Options**

Retention Policies

Metrics retention policy (days):

Apply

In the **Metrics retention policy (days)** field, enter the number of days for metrics retention. Click **Apply** to save changes.

Secure Storage

The **Secure Storage** menu opens to the **Secure Storage** page, which is used to configure secure storage options for **Public Key Infrastructure** and **Account**.

Secure Storage

Add

Certificate Secure Storage		
Name	Type	Operations

Credential Secure Storage		
Name	Account Type	Operations

Public Key Infrastructure

Public Key Infrastructure (PKI) is the network security architecture of an organization. It includes software, encryption technologies, and services that enable secure transactions on the internet, intranets, and extranets.

Certificate Authority

Upload PKI File

Secure Storage Name:

PKI:

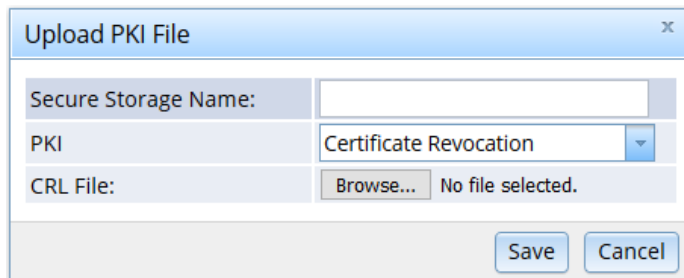
Certificate File: No file selected.

Save Cancel

Proceed as follows to configure the **Upload PKI File** parameters for Certificate Authority:

1. In the **Secure Storage Name** field, enter the name of secure storage.
2. In the **PKI** field, select Certificate Authority from the drop-down list to indicate which public key infrastructure should be used.
3. In the **Certificate File** field, browse to and select the certificate that should be used.
4. Click **Save** to apply changes or click **Cancel** to abort the operation.

Certificate Revocation



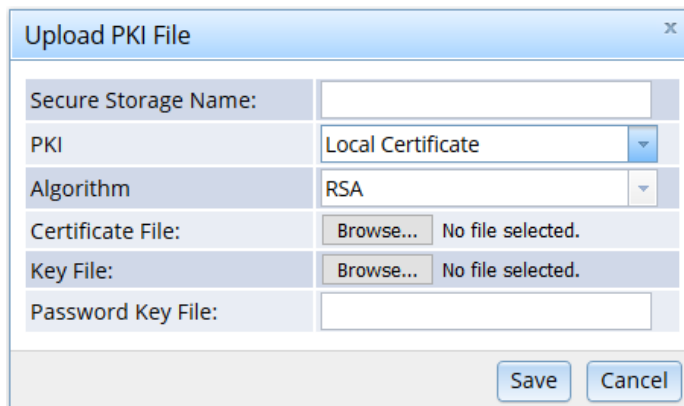
The screenshot shows a dialog box titled "Upload PKI File" with a close button (X) in the top right corner. It contains the following fields and controls:

- Secure Storage Name:** An empty text input field.
- PKI:** A dropdown menu with "Certificate Revocation" selected.
- CRL File:** A "Browse..." button followed by the text "No file selected."
- At the bottom right, there are "Save" and "Cancel" buttons.

Proceed as follows to configure the **Upload PKI File** parameters for Certificate Revocation:

1. In the **Secure Storage Name** field, enter the name of secure storage.
2. In the **PKI** field, select Certificate Revocation from the drop-down list to indicate which public key infrastructure should be used.
3. In the **CRL File** field, browse to and select the certificate revocation list that should be used.
4. Click **Save** to apply changes or click **Cancel** to abort the operation.

Local Certificate



The screenshot shows a dialog box titled "Upload PKI File" with a close button (X) in the top right corner. It contains the following fields and controls:

- Secure Storage Name:** An empty text input field.
- PKI:** A dropdown menu with "Local Certificate" selected.
- Algorithm:** A dropdown menu with "RSA" selected.
- Certificate File:** A "Browse..." button followed by the text "No file selected."
- Key File:** A "Browse..." button followed by the text "No file selected."
- Password Key File:** An empty text input field.
- At the bottom right, there are "Save" and "Cancel" buttons.

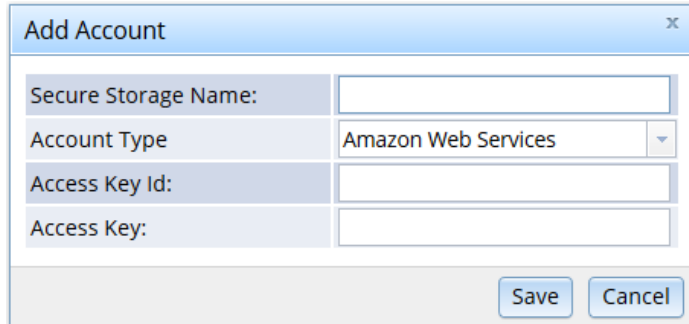
Proceed as follows to configure the **Upload PKI File** parameters for Local Certificate:

1. In the **Secure Storage Name** field, enter the name of secure storage.
2. In the **PKI** field, select Local Certificate from the drop-down list to indicate which public key infrastructure should be used.
3. In the **Algorithm** field, select RSA or DSA from the drop-down list to indicate which algorithm should be used. RSA is a public key encryption technology. DSA is used for creating and verifying digital signature.
4. In the **Certificate File** field, browse to and select the certificate that should be used.
5. In the **Key File** field, browse to and select the key that should be used.

6. In the **Password Key File** field, enter the name of password key file.
7. Click **Save** to apply changes or click **Cancel** to abort the operation.

Account

Amazon Web Services



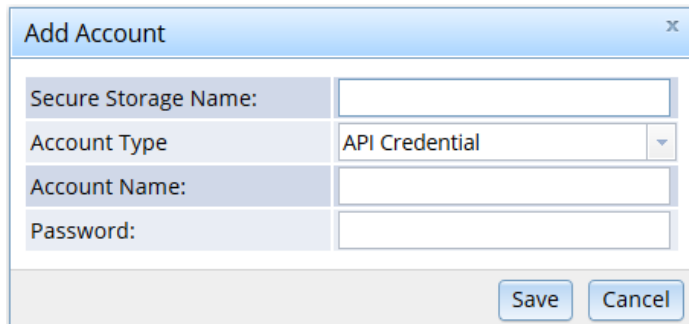
Proceed as follows to configure the **Add Account** parameters for Amazon Web Services:

1. In the **Secure Storage Name** field, enter the name of secure storage.
2. In the **Account Type** field, select Amazon Web Services from the drop-down list to indicate which account type should be used.
3. In the **Access Key Id** field for Amazon Web Services, enter the access key identification.
4. In the **Access Key** field for Amazon Web Services, enter the access key.
5. Click **Save** to apply changes or click **Cancel** to abort the operation.

Note: If you do not have an existing Amazon Web Services developer account and need to register, refer to the Amazon Marketplace Web Service documentation:

http://docs.developer.amazonservices.com/en_US/dev_guide/DG_Registering.html

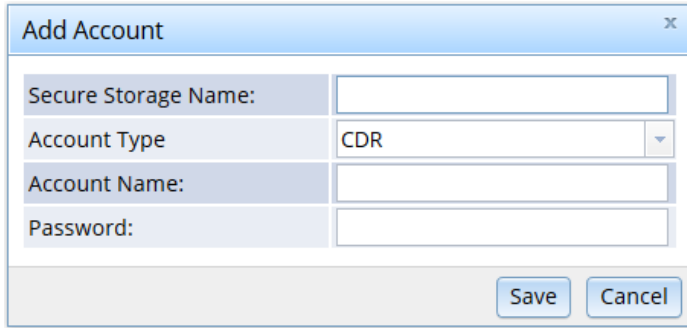
API Credential



Proceed as follows to configure the **Add Account** parameters for API Credential:

1. In the **Secure Storage Name** field, enter the name of secure storage.
2. In the **Account Type** field, select API Credential from the drop-down list to indicate which account type should be used.
3. In the **Account Name** field for API Credential, enter the account name.
4. In the **Password** field for API Credential, enter the password.
5. Click **Save** to apply changes or click **Cancel** to abort the operation.

CDR

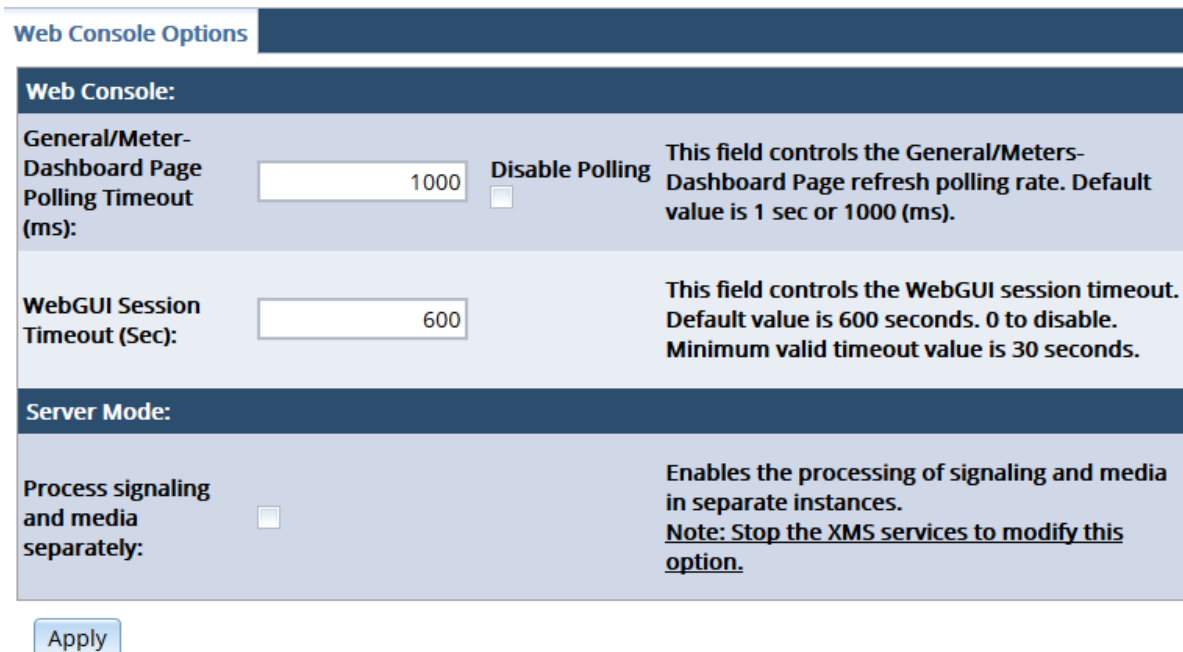


Proceed as follows to configure the **Add Account** parameters for CDR:

1. In the **Secure Storage Name** field, enter the name of secure storage.
2. In the **Account Type** field, select CDR from the drop-down list to indicate which account type should be used.
3. In the **Account Name** field for CDR, enter the account name.
4. In the **Password** field for CDR, enter the password.
5. Click **Save** to apply changes or click **Cancel** to abort the operation.

Options

The **Options** menu opens to the **Web Console Options** page, which is used to configure or disable the Console timeout options.



Proceed as follows to configure the **Web Console Options** parameters.

Web Console

General/Meter-Dashboard Page Polling Timeout (ms)

This parameter controls the refresh polling rate. Default value is 1 second or 1000 ms. Enter the desired value in the space provided and click **Apply**.

To disable polling timeout, click the check box for **Disable Polling** and then click **Apply**.

WebGUI Session Timeout (sec)

This parameter controls the WebGUI session timeout. Default value is 600 seconds. The minimum valid timeout value is 30 seconds. Enter the desired value in the space provided and click **Apply**.

To disable session timeout, enter the value of 0 and then click **Apply**.

Server Mode

Process Signaling and Media Separately

This parameter controls the processing of signaling and media in separate instances. To enable, click the check box for **Process signaling and media separately** and then click **Apply**.

Note: To modify the option, stop the XMS services.

Downloads

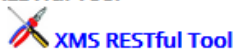
The **Downloads** menu opens to the **Tools** page, which will be updated periodically as additional demos and tools become available.

Tools

XMS RESTful Verification Demo



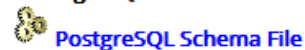
XMS RESTful Tool



Remote Logging Server Sample Configuration



Remote PostgreSQL CDR Database Schema



The **Tools** page contains the following applications to download:

- **XMS RESTful Verification Demo** unzips the XMS Verification Demo to your local directory. Refer to the *Dialogic® PowerMedia™ XMS Quick Start Guide* for more information.
- **XMS RESTful Tool** unzips the XMSTool RESTful Utility to your local directory. Refer to the [XMSTool RESTful Utility](#) section for more information.
- **Remote Logging Server Sample Configuration** unzips the sample configuration file to your local directory. Refer to the [Remote Logging](#) section for more information.
- **Remote PostgreSQL CDR Database Schema** unzips the PostgreSQL schema file to your local directory. Refer to the [Remote Database \(Postgres\)](#) section for more information.

To download a file, click the file name and follow the instructions.

Note: Files are downloaded to the local directory you specify.

5. PowerMedia XMS Troubleshooting

This section provides information about the installation log files and Linux RTC device verification available to enhance the user experience. It contains the following topics:

- [PowerMedia XMS Log Files](#)
- [Linux RTC Device Verification](#)

PowerMedia XMS Log Files

The default PowerMedia XMS log location is `/var/log/xms`. Consult these log files when troubleshooting specific PowerMedia XMS problems.

Note: Multiple log files are created and capped at 2 MB each.

Retrieving PowerMedia XMS Logs

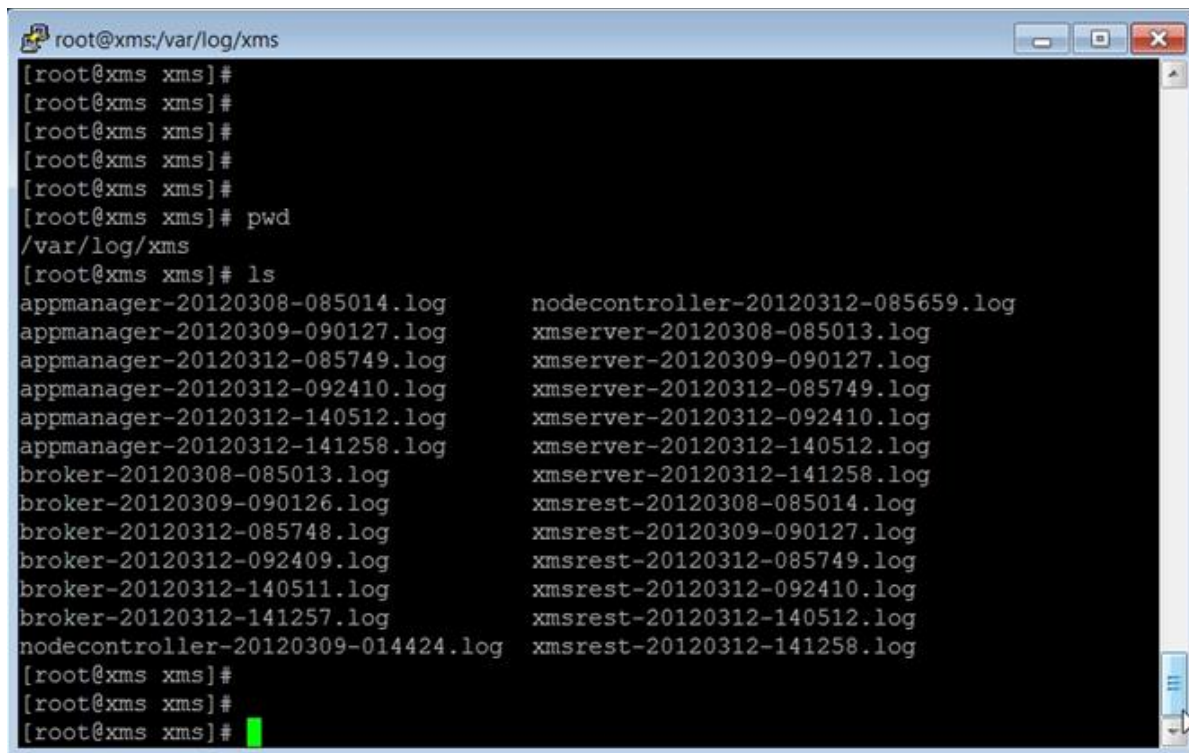
Most of the PowerMedia XMS logs are not accessible through the Console.

To retrieve the logs, it is necessary to access the PowerMedia XMS using secure shell (ssh).

The "root" user's default password is "powermedia". If you wish to change the password, do so before proceeding.

Note: For stand-alone RPM installations, password modification is not necessary because the installation script does not change the password to "powermedia" as it does with the .ISO install.

Access the files from `/var/log/xms` and copy the logs to the desired location. See the example below.



```
root@xms:/var/log/xms
[root@xms xms]#
[root@xms xms]#
[root@xms xms]#
[root@xms xms]#
[root@xms xms]#
[root@xms xms]# pwd
/var/log/xms
[root@xms xms]# ls
appmanager-20120308-085014.log      nodecontroller-20120312-085659.log
appmanager-20120309-090127.log     xmserver-20120308-085013.log
appmanager-20120312-085749.log     xmserver-20120309-090127.log
appmanager-20120312-092410.log     xmserver-20120312-085749.log
appmanager-20120312-140512.log     xmserver-20120312-092410.log
appmanager-20120312-141258.log     xmserver-20120312-140512.log
broker-20120308-085013.log         xmserver-20120312-141258.log
broker-20120309-090126.log         xmsrest-20120308-085014.log
broker-20120312-085748.log         xmsrest-20120309-090127.log
broker-20120312-092409.log         xmsrest-20120312-085749.log
broker-20120312-140511.log         xmsrest-20120312-092410.log
broker-20120312-141257.log         xmsrest-20120312-140512.log
nodecontroller-20120309-014424.log  xmsrest-20120312-141258.log
[root@xms xms]#
[root@xms xms]#
[root@xms xms]#
```

Linux RTC Device Verification

On physical hardware systems, PowerMedia XMS derives its system clocking from the Linux `/dev/rtc` device. The Linux kernel uses the RTC or HPET hardware on the system motherboard to provide the clock for the `/dev/rtc` device. It has been observed on some earlier system platforms that the HPET hardware can cause erratic timing performance.

If media processing performance is continuously irregular on your system, examine the `/var/log/messages` file for a regular and frequent occurrence of messages such as "lost 22 rtc interrupts" (the number will vary). An occasional occurrence of this message is considered normal and does not adversely affect system performance.

In cases where a consistent issue with lost rtc interrupts is observed, the default kernel clock source and timer mode must be changed in the grub boot loader configuration. The user must disable the use of the HPET timer using the kernel boot parameters.

To override the default options, proceed as follows to change the grub bootfile:

1. Carefully edit `/boot/grub/menu.lst` and append the `nohpet` parameter at the end of the kernel entry that will boot by default. If your file has more than one kernel entry, make sure to edit the kernel boot line that corresponds to the `default= <value>` field in the file. For example, if the file contains `default=0`, edit the first kernel entry.
2. Reboot the system.
3. Verify that the HPET has been disabled by running the following command:

```
dmesg | grep nohpet
```

The kernel line is displayed with the option set.

Virtual Memory Increase between Application Restarts

In testing scenarios, cache memory has been observed to grow between application restarts on HMP/XMS regression systems until the cache memory consumes all available memory, which causes swapping to occur. When swapping begins to occur, the kernel swaps instead of automatically reclaiming cache memory. To force the kernel to reclaim cache memory in favor of swapping, it is recommended to set the `swappiness` to 10 if the system has enough RAM.

Contacting Dialogic Technical Services and Support

When reporting an issue to Dialogic Technical Services and Support, be prepared to provide the following information:

- Full description of the issue.
- Version and trunk number of the PowerMedia XMS software you are using.
- PowerMedia XMS log files.
- Whether the issue is reproducible; the steps that you took.

Note: The latest software update and release notes are available through the Dialogic website at <http://www.dialogic.com/products/media-server-software/xms>. Downloads can be found on the right side of your screen. You will be prompted to log in or sign up in order to download the software.

6. XMSTool RESTful Utility

XMSTool RESTful Utility

This section provides details about the XMSTool RESTful Utility (also referred to herein as "XMSTool" or "Utility"). XMSTool is used for developing, debugging, and supporting applications for the PowerMedia XMS using the HTTP RESTful API.

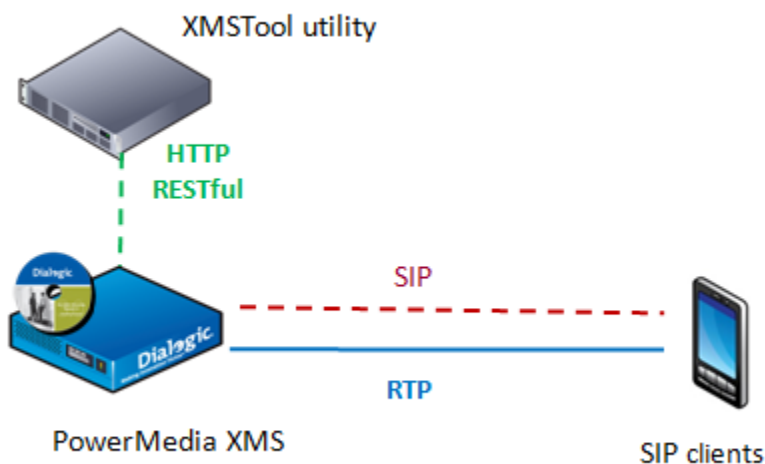
XMSTool is a Java-based test application for passing and receiving RESTful API messages to and from the PowerMedia XMS. Supported for both 1PCC and 3PCC (see the [Call Control Models](#)), it can be used to build and parse individual RESTful messages and can drive and record simple applications. The utility provides the following:

- Ability to manually enter and execute the RESTful API commands and observe the results
- Pre-recorded Macros available for commonly used call scenarios
- Method to record Macros for automated execution of command sequences (**Demo mode**), enabling users to create simple Demos and debug their applications
- Logging capabilities

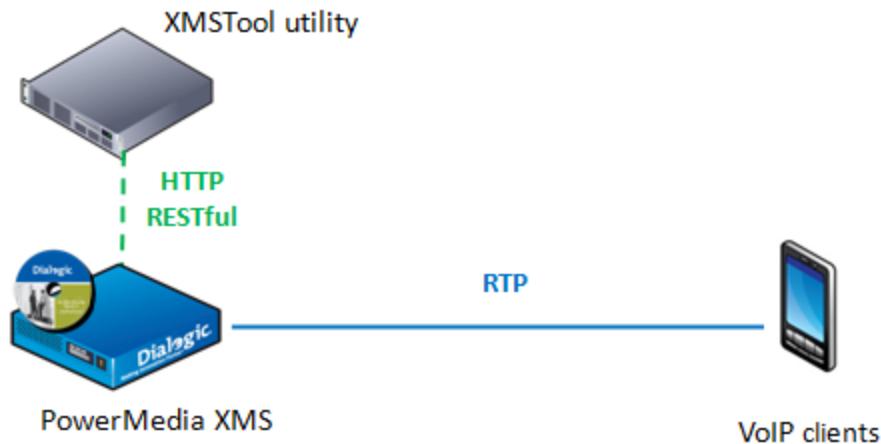
Call Control Models

XMSTool can establish media connections on both 1PCC and 3PCC models.

With the 1PCC model, as shown in the following illustration, the PowerMedia XMS handles inbound and outbound SIP calls, taking advantage of its built-in SIP call control functionality. XMSTool controls all aspects of the PowerMedia XMS operation, including SIP call control.



With the 3PCC model, as shown in the following illustration, the XMSTool only directs the PowerMedia XMS to establish and manipulate the RTP-based media sessions. This model is commonly used in VoIP network environments such as IMS, where SIP call control is performed by an application server. This model permits using signaling protocols other than SIP and allows application architects the flexibility of choosing the signaling protocol.



Prerequisites

Prior to using XMSTool, the user is expected to do the following:

- Understand the functionality and operation of the PowerMedia XMS.
- Be familiar with the HTTP RESTful control interface of the PowerMedia XMS in order to use the tool in **Demo** mode.
- Understand the HTTP RESTful interface of the PowerMedia XMS and have a working knowledge of XML and related topics (data structures, XSD, etc.) in order to use the tool at the individual command level (**Advanced** mode).
- Understand the key concepts of a service-oriented architecture and HTTP RESTful interface.
- Have a working knowledge of Java programming.

Starting XMSTool

XMSTool is written in Java, making it operating system independent. The PowerMedia XMS on which it runs requires a Java Runtime Environment (JRE). The version of Java Standard Edition (JSE) used for the tests described in this document is Version 7, Update 2, build 1.7.0_02-b13.

A SIP softphone should be available. See the *Dialogic® PowerMedia™ XMS Quick Start Guide* for information about setting up PowerMedia XMS and installing suitable SIP softphones.

To use the XMSTool utility, access the **Downloads > Tools** page from the Console and click the **XMS RESTful Tool** (*XMSTool.zip*) to download and install the file. Unzip the downloaded distribution and then go to the top level directory where you will see the */dist* and */testing* directories. From the top level directory, run the tools as follows:

```
> java -jar dist/XMSTool.jar -g -m <xms_ip_address>
```

Note: XMSTool can be run to expose its graphical user interface (GUI) or as a command line interface. Using the GUI provides access to both modes: **Demo/Simple** and **Advanced**. Running from the CLI only allows **Demo/Simple** mode.

XMSTool Utility Modes

XMSTool can be run in two different modes:

- **Demo/Simple Mode** uses predefined XML scripts; short application scenarios can be executed to demonstrate most of the PowerMedia XMS RESTful functionality. Session logging is available to examine the message interchange. Only sessions using inbound SIP calls are currently available in this mode.
- **Advanced Mode** allows individual RESTful commands to be manually entered for full PowerMedia XMS control. This mode is intended to be used by developers who are looking to become familiar with the RESTful API messages used to control PowerMedia XMS. It also allows the individual commands that make up a macro/demo to be recorded for replay or to provide an accurate way to reproduce a problem in PowerMedia XMS.

Demo/Simple Mode

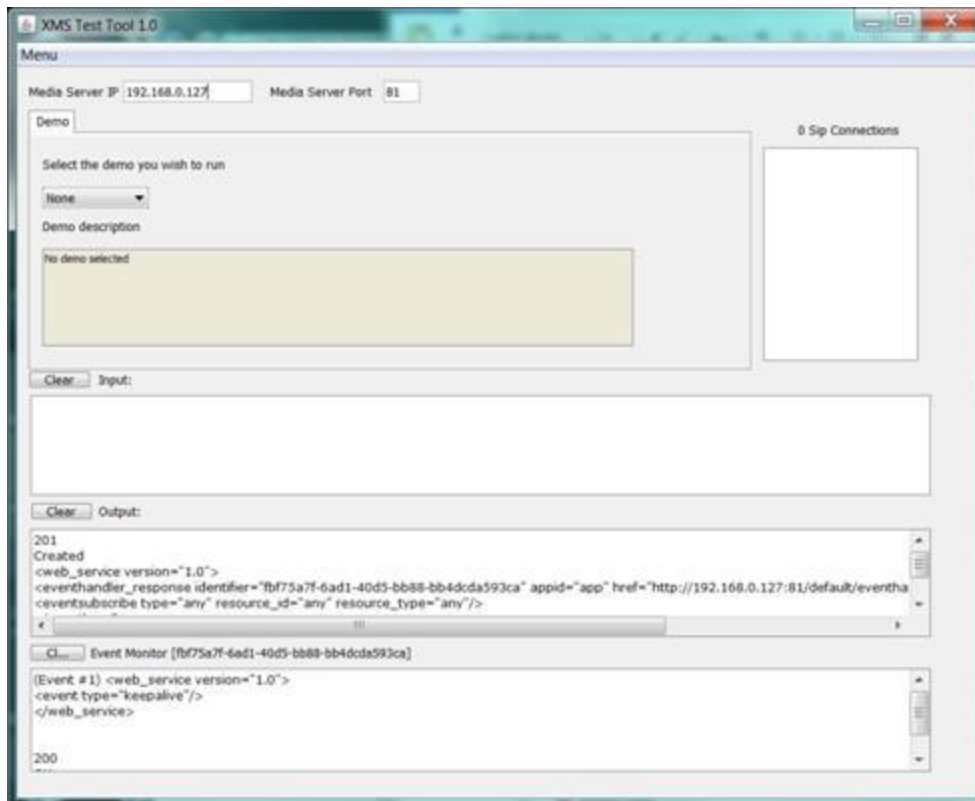
In this mode, XMSTool is used to execute predefined demos or macros that string together a series of RESTful request and response messages to make up a simple application, such as answering a call and playing a file or putting a caller into a video conference.

The **Demo** screen provides access to the demos listed below.

Note: All demos are multimedia—both audio and video.

- **Play** answers an inbound call and plays a file.
- **Collect** answers an inbound call (audio only) and collects four (4) digits. When the 4th digit is entered, the digit collection event is seen in the event handler window. The call will be automatically disconnected several seconds after the digit event is returned.
- **Join** connects two inbound callers into a conference. The callers remain connected for ten (10) seconds, and then the conference is torn down.
- **Conference** joins a single inbound caller into a conference. The caller remains connected for eight (8) seconds, and then the conference is torn down.
- **Confplay** joins two inbound callers into a conference and a file is played. After the play terminates, the conference is torn down.
- **Record** begins the recording. An inbound caller is prompted by a file. After the prompt is played, **Record** mode is entered. The recording can be terminated with # or ends by itself after ten (10) seconds.

Note: Inbound calls are only supported via SIP, but support is provided for outbound calls to/from WebRTC.



Proceed as follows to run a demo:

1. Select a demo from the drop-down list.
2. Place an inbound call from a SIP softphone. Any SIP username (or extension) may be used with XMSTool because the scenario selection is done through the drop-down list.
3. Make a call to the IP address of the PowerMedia XMS. The call will be answered by PowerMedia XMS and XMSTool, and the appropriate scenario will be played.

Note: Several scenarios will use two callers.

Details about the application's call flow may be found in the XMSTool's session log, which is located in the testing directory and named *xmstool.log*. The logger overwrites the log file each time XMSTool starts.

Note: All demo scenarios start when an inbound call is received. Currently, outbound calls cannot be used.

Accessing XMSTool using CLI

Demos are also accessed through the command line interpreter (CLI) when a windowing system on the host computer is not available.

Proceed as follows to use the CLI interface:

1. Start the tool from the operating system command prompt:

```
> java -jar dist/XMSTool.jar -r -m <xms_ip_address>
```

2. Upon successful connection to PowerMedia XMS, all available test scenarios for inbound calls are displayed:

```
XMSTool Application
-----
Demos
-----

[collect]
Description: Play and collect demo

[conference]
Description: 2 party 10 second conference demo

[confplay]
Description: 2 party conference play demo

[join]
Description: Join 2 calls for 10 seconds demo

[play]
Description: Play demo

[record]
Description: Record demo

Waiting for incoming calls ...

XMSTool>
```

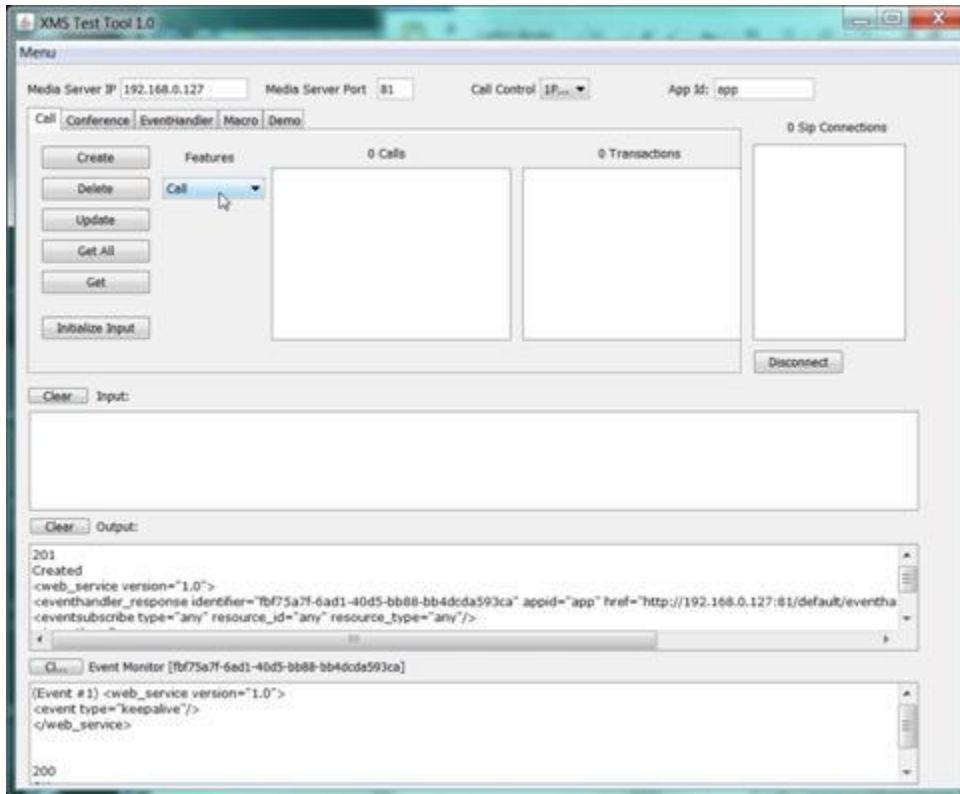
3. Access a scenario by placing a SIP video call to the IP address of PowerMedia XMS using the test name as the SIP username. For example, entering `Sip:play@192.168.1.100` will connect to the PowerMedia XMS at IP address 192.168.1.100 and execute the multimedia file "play" test scenario.
4. Stop XMSTool using the exit command at the CLI prompt.

Advanced Mode

Advanced users and RESTful application developers may choose to enter individual commands to closely examine the RESTful messages used. This method is useful when designing and coding one's own RESTful applications.

To accomplish this, select Advanced Mode from the **Menu** drop-down list.

The following window appears.



The following existing connection and operation parameters are displayed:

- **PowerMedia XMS IP** - Display only, set with XMSTool command line startup -m option.
- **PowerMedia XMS Port** - Display only, set with XMSTool command line startup -p option.
- **Call Control** - Specifies protocol used.
- **App Id** - Specifies the PowerMedia XMS application to connect to. Corresponds to an application set on the **Routing > Routes** page from the Console. Defaults to "app".

The **Call**, **Conference**, **EventHandler**, **Macro**, and **Demo** tabs pertain to the different modes and messages used by XMSTool, while the **Create**, **Delete**, **Update**, **Get All**, and **Get** buttons determine the HTTP methods (GET, POST, PUT, DELETE) used to send the RESTful messages.

The **Features** drop-down list is used to select the media and call actions that make up the application flow. The **Calls**, **Transactions**, and **SIP Connections** areas list the IDs of all active calls, media transactions, and SIP connections.

The three large horizontal text windows are used for building the XML input to PowerMedia XMS, for displaying responses from PowerMedia XMS to RESTful messages that have been sent, and for displaying events sent from the event handler in PowerMedia XMS.

When XMSTool starts, the event handler is created to relay unsolicited events to the XMSTool Client. An Event Monitor ID is seen on the top of the lowest window. All content is cleared using the **Clear** button.

Individual commands, such as **Create**, are sent in a specific sequence for successful operation. The following table explains the sequences.

Sequence	Tasks
Create	<ol style="list-style-type: none"> 1. Select either the Call feature from the Call tab or the Conference Feature from the Conference tab. 2. Click Initialize Input to initialize the command and clear any existing content. 3. Edit, if necessary, the default command. For example, <code>max_parties</code> for a conference defaults to 2 and may need to be increased, or the destination URI for an outbound SIP call may need to be adjusted. 4. Click Create to generate an HTTP POST containing the RESTful command issued. <p>Responses to commands are displayed in the Output window.</p>
Update	<ol style="list-style-type: none"> 1. Select the entity (call, conference, or transaction) ID. For example, issuing a Stop command on a Play operation only requires selecting the Play transaction ID. Adding a party to a conference requires two ID selections: Call ID and Conference ID. 2. Click Initialize Input to clear any existing input and update with the default XML used with the command. 3. Edit the RESTful commands as desired. For example, change the file to play in a Play operation. 4. Click Update to generate an HTTP PUT that contains the new RESTful command. <p>Responses to commands are displayed in the Output window.</p>
Get All and Get	<ol style="list-style-type: none"> 1. Select either the Call tab or Conference tab to access existing calls or existing conferences. 2. Click Get All to generate an HTTP GET, which returns information on all calls or all conferences depending on the tab selected. 3. For specific call or conference information, click Get to generate an HTTP GET. <p>Information returned is displayed in the Output window.</p>

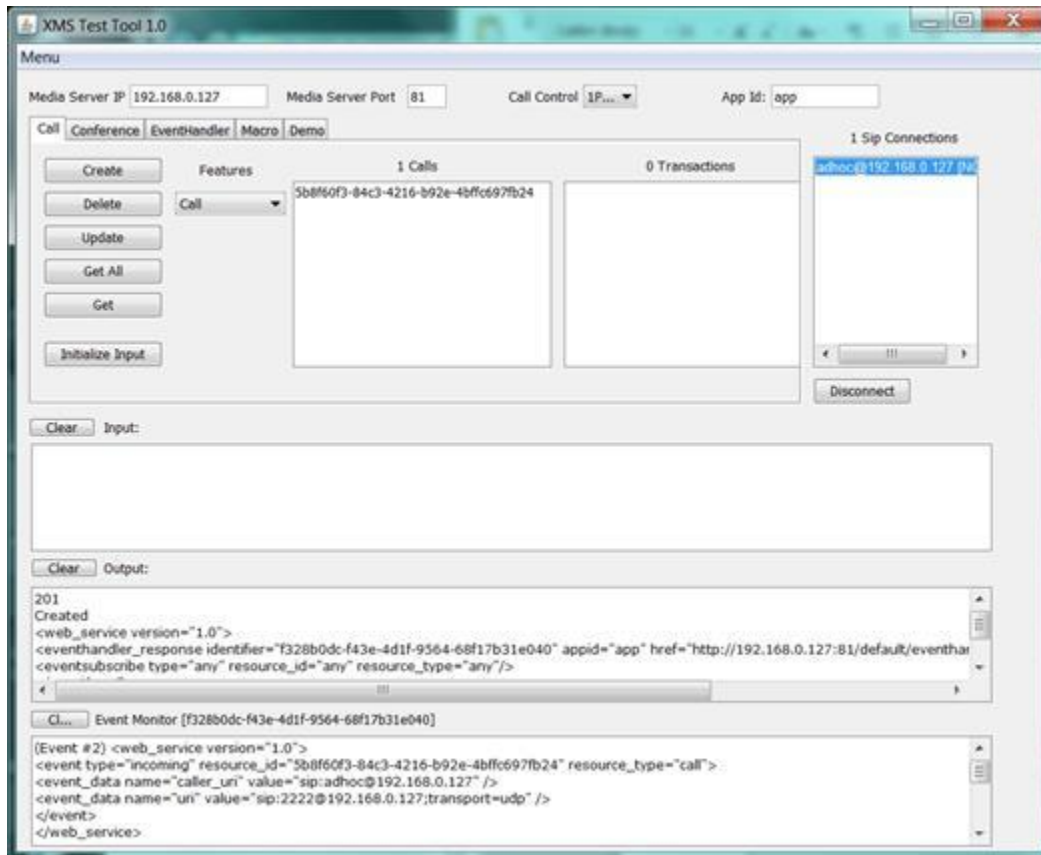
Sequence	Tasks
Delete	<ol style="list-style-type: none"> 1. Select the ID of the call or conference. 2. Click Delete to generate an HTTP DELETE for the selected entity. <p>A 200-series OK reply with no content will be displayed in the Output window.</p>

Basic Operation and Commands

The following sections provide examples of basic commands.

Receiving an Inbound Call

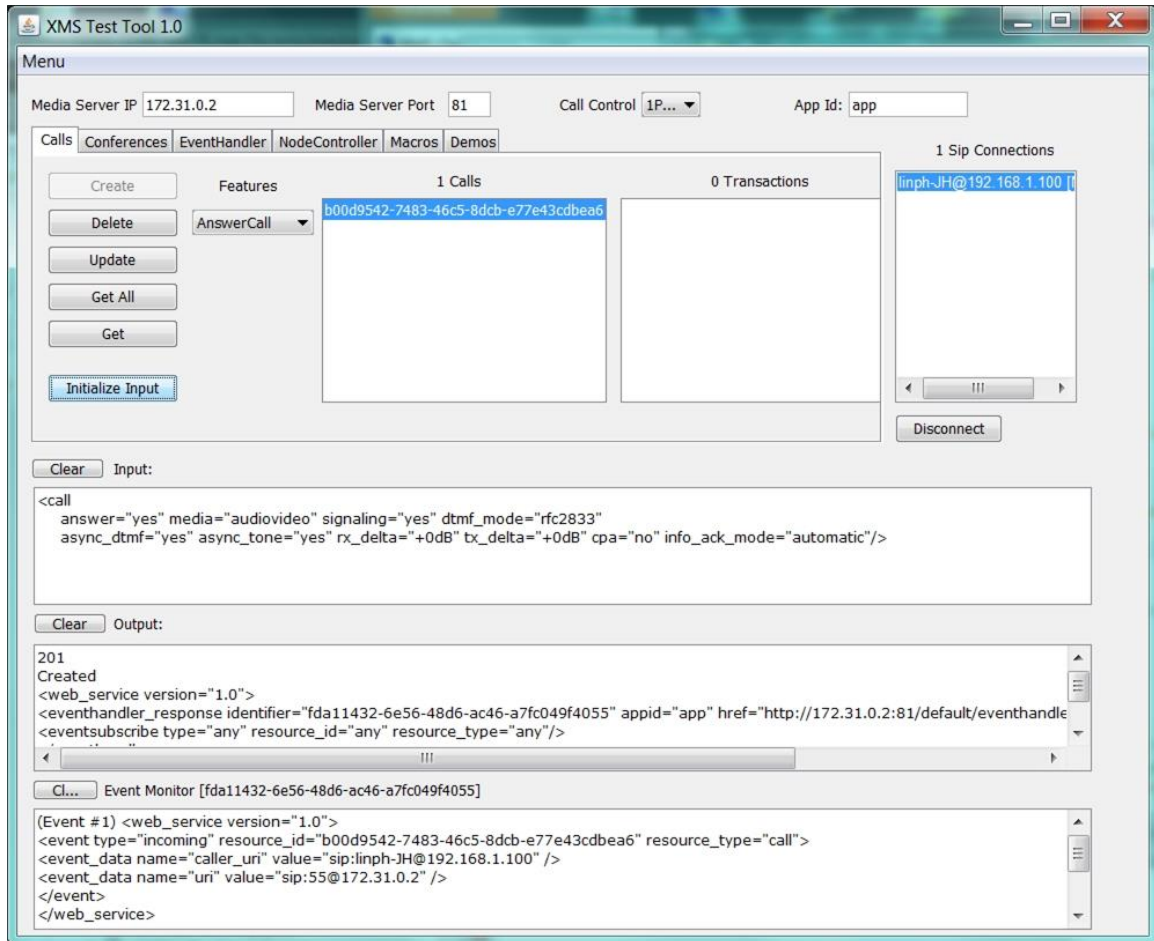
The **Call** tab is used to handle setup and teardown of a call. Inbound calls require a SIP softphone to initiate the call using any SIP username (or extension). When a call is made to the IP address of the PowerMedia XMS, notification of the call is sent to XMSTool and displayed in the Input window as shown below.



The call offered event ("incoming") can be observed in the Event Monitor window. Proceed as follows to reply to the event:

1. In the **Call** tab, select the ID of the received call.
2. Select AnswerCall from the **Features** drop-down list. Alternately, AcceptCall could be selected. For example, if early media were desired. This would allow a file to be played to the caller before the call is answered.

- Click **Initialize Input** to create a reply to the call offered event. The answer message will be automatically generated. Note that the default values set in the message may be edited if desired.



- Click **Update** to send the answer message. The connection to the SIP softphone is now established.

Making an Outbound Call

The **Call** tab is used to handle outbound call setup and teardown. The SIP softphone being called should be set in a mode where it can detect incoming calls and either ring or automatically answer them. Proceed as follows to make an outbound call:

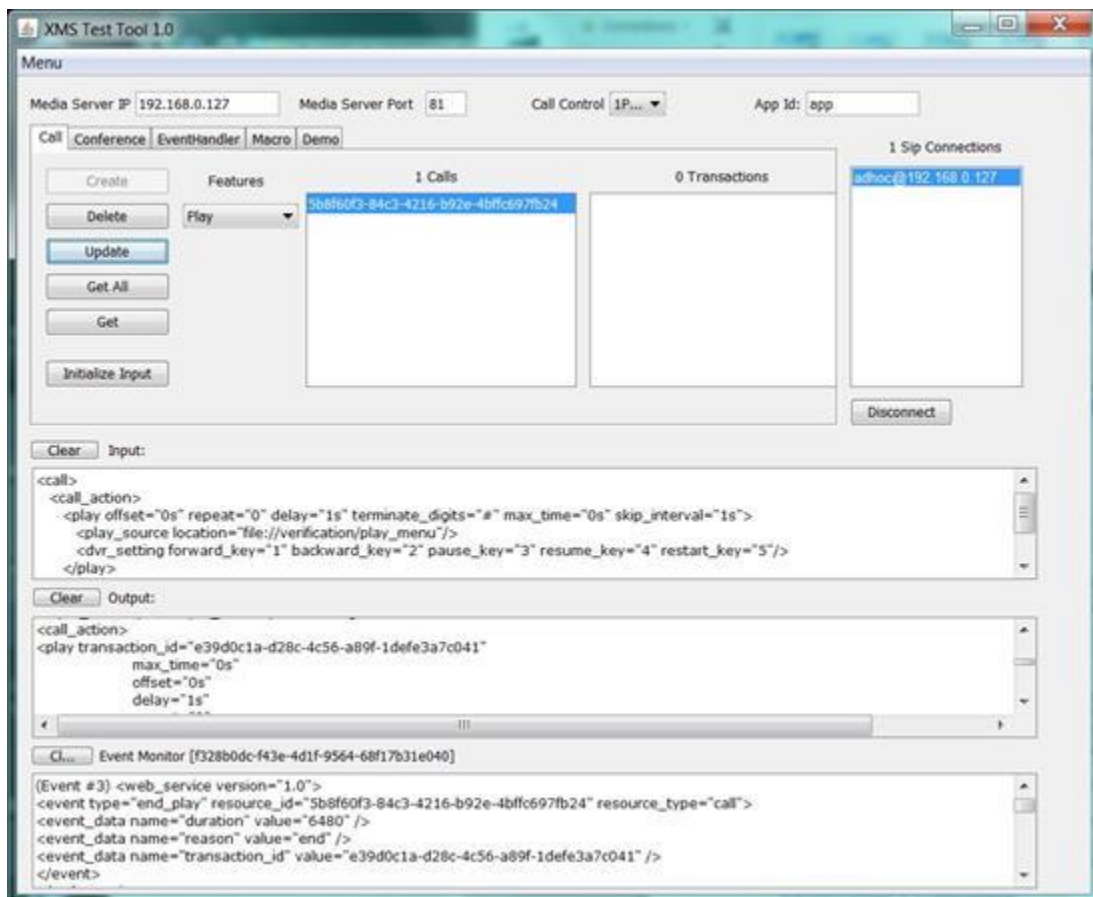
- Click **Initialize Input** to generate a RESTful call command.
- Edit the default command. For example, the `destination_uri` and `source_uri` should reflect the SIP address of the SIP softphone being called and the PowerMedia XMS, respectively. Other default values may be adjusted if desired.
- Click **Create** to launch the call. The SIP softphone will ring and the call is connected when answered.

Playing a File into a Call

Once a call is connected, media commands may be issued. In the following example, a multimedia file is played.

- Select the call ID.

2. Select Play from the **Features** drop-down list.
3. Click **Initialize Input** to provide a call action command to play a file. Although a default file and default parameters are provided, these may be edited before being sent.
4. Click **Update** to send the message. If successful, the audio/video is heard/seen on the SIP softphone. The response to the play command is displayed in the Output window when the play is initiated, and a play termination event is seen in the Event Monitor window once the play is complete.

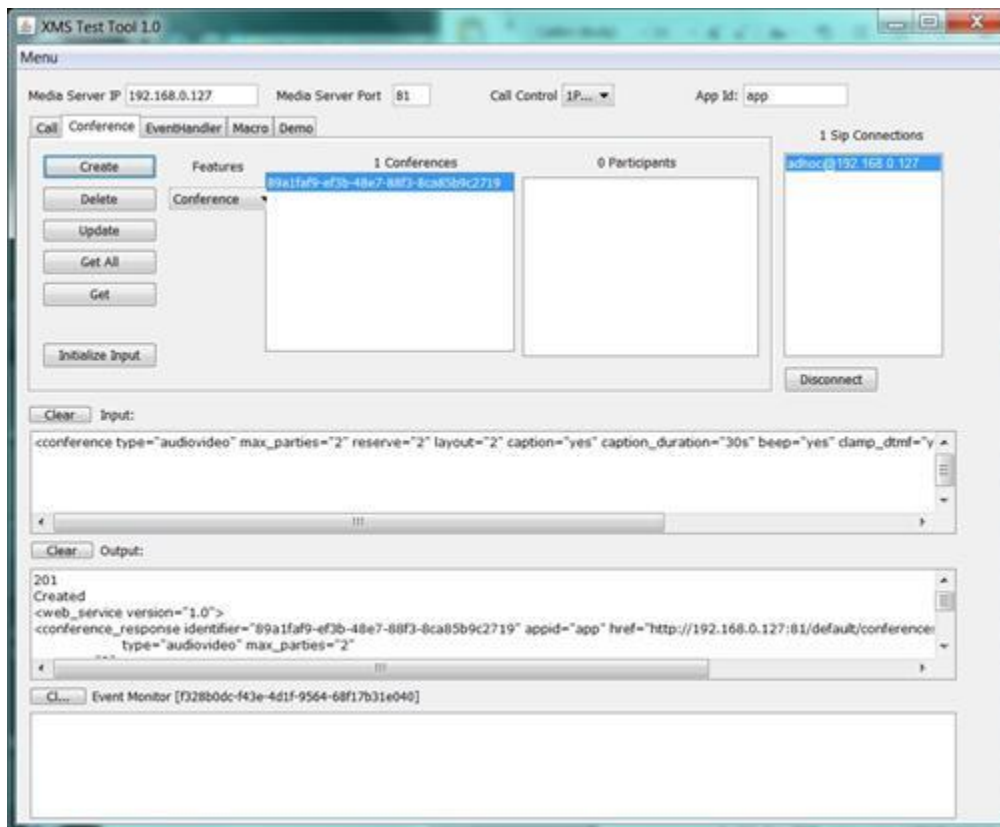


Establishing a Conference

Once a call is established and idle, a video conference may be started. First, create a conference in which to add the call:

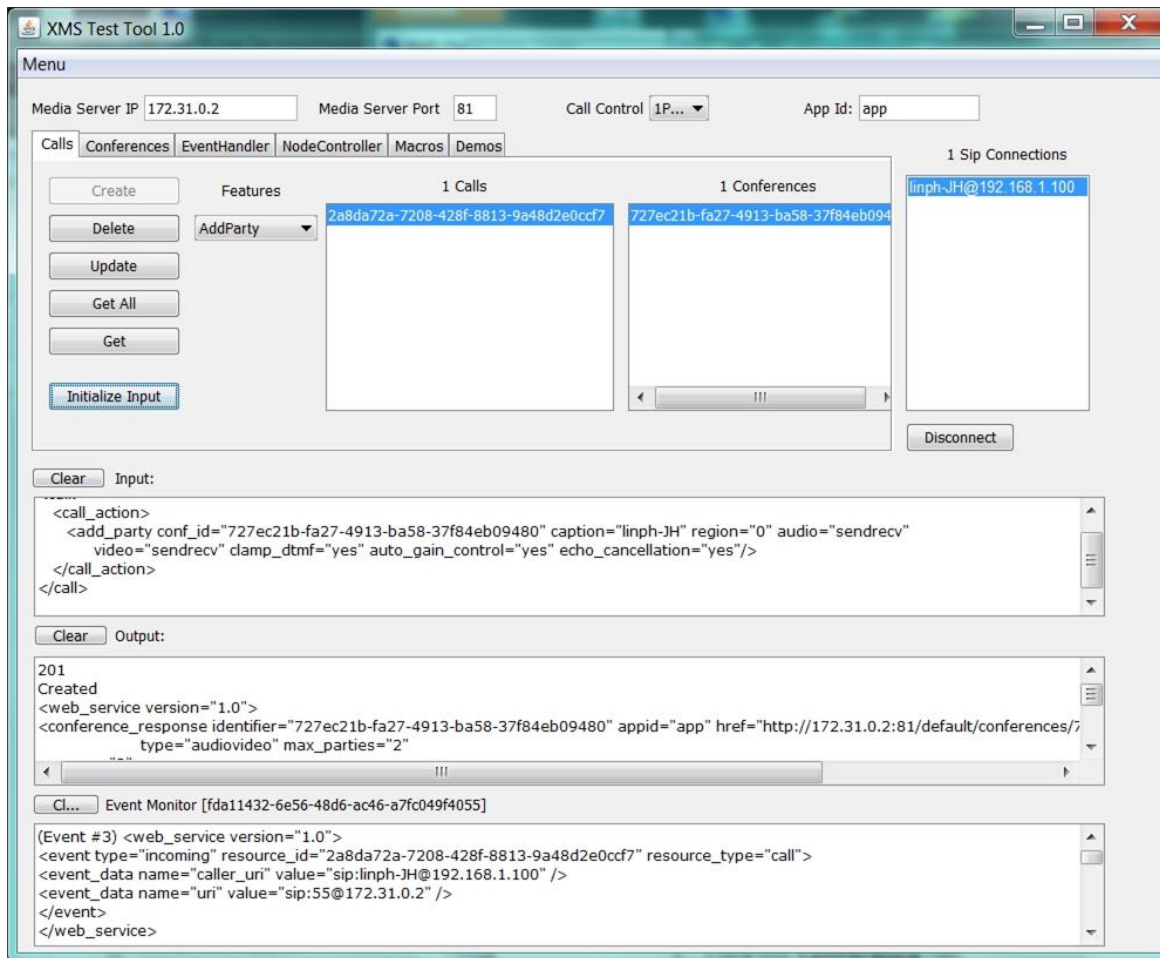
1. Click the **Conference** tab. Verify that Conference has been selected from the **Features** drop-down list.
2. Click **Initialize Input** to get the default conference creation parameters. Edit them if desired.

3. Click **Create** to establish the conference and generate a conference ID.



4. Click the **Call** tab.
5. Select the call ID and the ID of the conference just created.
6. Select AddParty from the **Features** drop-down list.
7. Click **Initialize Input** to build the XML message, which may be edited as desired.
8. Click **Update** to add the caller to the conference. The SIP caller will be in a single-person conference.

For a multi-party conference, make additional calls and add each to the conference using the above procedure.



Proceed as follows to tear down and clean up a conference:

1. Click the **Calls** tab.
2. Select the call ID from the **Participants** field and select RemoveParty from the **Features** drop-down list. Repeat for each party in the conference.
3. Select the **Initialize Input** button to build the XML message, which may be edited as desired.
4. Select **Update to remove the party from the conference**.
5. Select the call ID from the **Calls** field and click **Disconnect** for each party in the conference.
6. Select the conference ID from the **Conferences** field and click **Delete**.

Additional XMSTool Commands

Many additional XMS RESTful commands can be run using XMSTool. For the complete list of commands and their parameters, refer to the *Dialogic® PowerMedia™ XMS RESTful API User's Guide*.

The following call actions are available from the **Features** drop-down list in the **Call** tab. In most cases default values can be used, but it is good practice to check the parameters before applying them. For all commands, the call ID must be selected before clicking **Initialize Input**.

Command	Description
accept	Accept an offered call, but do not answer it yet. This command is desirable for early media or to redirect a call elsewhere.
answer	Answer an offered call.
playcollect	Play a multimedia file and collect DTMF digits during the play. The default message is set to collect four (4) digits. The result of the digit collect operation will be displayed in the Event Monitor window.
playrecord	Play an introductory multimedia file and then record it. Default recording termination is either the # key or a maximum time (10 seconds). The resulting file, "recorded_file", is played back using the Play command and setting play_source location=file://recorded_file.
overlay	Display an image overlay on the active call.
join/unjoin	Bridge or un-bridge two active calls.
add_party/ update_party/ remove_party	Add, modify, or remove a call from an existing conference. It may be necessary to change the default add and update options for this command. Note: A conference must be created before adding a party.
send_dtmf	Send the specified DTMF tones to the connected call.
send_info	Send a SIP INFO message to the caller.
send_info_ack	Manually acknowledge a SIP INFO message received from the caller.
transfer	Transfer (attended or unattended) the caller to the specified SIP URI.
redirect	Redirect an accepted but unanswered call to the specified SIP URI.
hangup	Send a SIP BYE message with the specified content to hang up the call. This is the equivalent of hanging up using the HTTP DELETE method, but allows a message to be sent along with the BYE.

The following call actions affecting an ongoing conference are available from the **Features** drop-down list on the **Conference** tab. For all commands, the call ID must be selected before clicking **Initialize Input**.

Command	Description
play	Play a file in an ongoing conference. The video will appear as an overlay to the entire conference.
update_play	Change the play characteristics of the ongoing play file in the conference.
stop	Stop playing a file in an ongoing conference and return the conference to the participants.

Note: The **Disconnect** button under the SIP Connections window sends a DELETE to the proper call ID to hang up the call, making it easier for the user to know which call they disconnected. This feature specifies which call ID corresponds to which incoming SIP call.

Using XMSTool to Record Macros/Demos

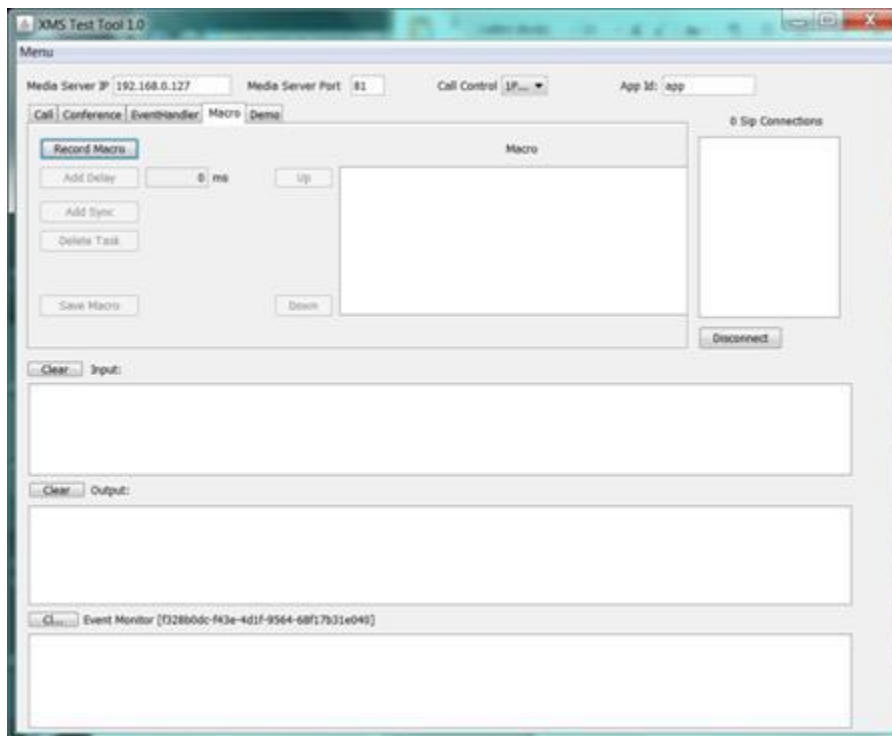
XMSTool has the ability to record a sequence of commands for an application scenario for later use. The recording can be saved and will appear in the installation's Demo directory.

Note: Macros are saved in XML format in the */testing* directory under *macro_name.xml* file.

Prior to recording a Macro, be sure that XMSTool is completely idle and that no Demos are running. To see Demo status, click the **Demo** tab and verify that none are listed in the Demo box.

To start a recording, click the **Macro** tab and click **Record Macro**.

The following window appears.



Note: Macro recording begins when an inbound call is received. Currently, outbound calls cannot be used with **Record Macro**, either at the start of the macro or within it.

When an inbound call arrives, individual commands may be accomplished until the application scenario is complete. Since all manual commands, even erroneous ones, are logged, it is suggested that a scenario be run several times with no error responses before clicking **Record Macro**. To stop recording, click **Stop Macro**.

The **Add Delay** button is provided for timing an indeterminate command, such as a conference for a given number of seconds, before moving on to the next command. Add a delay by clicking **Add Delay** and setting a value in milliseconds.

Note: Many RESTful commands have a time parameter.

The **Add Sync** button is provided to sync the actions of all participants involved in either the same conference or joined call. This option verifies that all inbound calls have arrived before continuing with a macro. Callers are grouped together using their SIP "From" username. For example, if six callers all have the same SIP From username and the executing macro has a <Sync> command, that macro waits until all other callers in that group are at that point before continuing.

The **Delete Task** button is used when an erroneous command is identified. The line containing the command may be deleted by selecting the entire line and clicking **Delete Task**. Tasks can be ordered differently using the **Up** and **Down** buttons next to the Macro window.

When satisfied with the recording, name the file and click **Save Macro**. The file is now written into an XML file in the */testing* directory and will be available in the **Demo** list for replay.

Note: The name of the recording must be manually added to the */testing* directory under *xmstool.cfg* file if the macro is desired when XMSTool is restarted.

7. Third Party ASR and TTS Engine Notes

There are additional steps to enable third party ASR and TTS engines to operate correctly within PowerMedia XMS.

In many cases, the information is specific to the current version of the third party engine in question. For example, it may refer to an issue in the current version and describe a workaround for the issue.

Note: This information might change as third party engines are upgraded in future releases of PowerMedia XMS.

Nuance

Some versions of the Nuance Speech Server return the results of speech recognition in the XML result as a set of keys: SWI_meaning, SWI_literal, and SWI_grammarName. The presence of these keys in the result affects the syntax that the VXML code uses to extract the results of speech recognition.

The following example shows how VXML code needs to use the syntax of **input_word.SWI_literal** instead of **input_word** to extract the results of the speech recognition:

```
<?xml version="1.0" encoding="UTF-8"?>
<vxml xmlns="http://www.w3.org/2001/vxml" xmlns:conf="http://www.w3.org/2002/vxml-conformance"
version="2.0">
  <form>
    <field name="input_word" modal="true">
      <grammar root="toprule" mode="voice" type="application/srgs+xml">
        <rule id="toprule">
          <one-of>
            <item> apple </item>
            <item> orange </item>
            <item> pizza </item>
          </one-of>
        </rule>
      </grammar>
      <prompt>
        Please say a word
      </prompt>
      <filled>
        <prompt>
          You said the word <value expr="input_word.SWI_literal"/>
        </prompt>
      </filled>
    </field>
  </form>
</vxml>
```

To resolve this issue, the Nuance configuration *Baseline.xml* file needs to be modified to command the Nuance Speech Server to not insert the SWI_literal, SWI_meaning, and SWI_grammarName keys in the XML result.

The **swirec_extra_nbest_keys** parameter in the file needs to be changed from:

```
<!-- Add a ScanSoft grammar key to the XML result. -->
param name="swirec_extra_nbest_keys">
<value>SWI_meaning</value>
<value>SWI_literal</value>
<value>SWI_grammarName</value>
</param>
```

to:

```
<!-- Add a ScanSoft grammar key to the XML result. -->
param name="swirec_extra_nbest_keys">
<value></value>
</param>
```

The Nuance Speech Server must be restarted after changing the *Baseline.xml* file.

After the change, the VXML code can use the following syntax to extract the results of speech recognition:

```
<prompt>
  You said the word <value expr="input_word"/>
</prompt>
```

This issue is also documented in the following link:

http://docwiki.cisco.com/wiki/Audio:_SpeechWorks_Does_Not_Work_with_Unified_CVP

8. Appendix A: ISO Method for Remote Installation

VMware ESXi

To perform the ISO method of installation using VMware ESXi, there are two options:

- Burn the .ISO image to a bootable DVD. For more information on this method, refer to the [ISO Method](#) section of this document.
- Place the .ISO image in the VMware ESXi datastore and point the DVD drive to that location.

This section covers the second option, which is helpful for remote installations. This procedure contains references to VMware ESXi documentation, which is located at <http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html>. Verify that you are using the correct VMware release. Proceed as follows to perform the installation:

1. Download the PowerMedia XMS .ISO image to your desktop.
2. Place the .ISO image in the VMware datastore.
3. Create a virtual machine or replace an existing virtual machine in preparation for the installation. Refer to the VMware document *vSphere Virtual Machine Administration* for details.

Note: When entering the information for the virtual machine, refer to the [System Requirements](#) section of this document.

4. Point the DVD drive to the .ISO image following the "Configure a Datastore ISO file for the CD/DVD Drive in the vSphere Client" section of the VMware document *vSphere Virtual Machine Administration*.

Note: Connect At Power On is required.

5. Make the BIOS setup screen available on boot up and delay the boot sequence following the "Delay the Boot Sequence in the vSphere Web Client" section of the VMware document *vSphere Virtual Machine Administration*.

Note: Force BIOS setup is required.

6. Power on the virtual machine.
7. Click the **Console** tab.
8. In the **Boot** section of the BIOS setup screen, move **CD-ROM** so that it is listed first and therefore scanned first when booting.
9. Set the IP address. Refer to the [Setting the IP Address](#) section in this document for details. Once the IP address is set, the installation begins automatically and does not require any user interaction.

Note: When the installation is complete, do not click **Reboot** yet. Doing so will restart the entire installation process.

10. Right-click the virtual machine and click **Edit Settings**.
11. Expand **CD/DVD Drive**, select **Client Device**, and click **OK**.
12. Click **Reboot**. When prompted to disconnect and override the CD-ROM door lock, select **Yes** and click **OK**.

To test the success of the installation, enter the IP address of the virtual machine in a web browser and sign in to the WebGUI with the username "superadmin" and the password "admin". On the **System > General** page, verify that the correct release is running on the correct operating system.

9. Appendix B: SNMP

The PowerMedia XMS SNMP implementation supports SNMPv2c and SNMPv3. This implies that it supports the V2c communities as well the advanced security features of V3.

The PowerMedia XMS SNMP enterprise MIB begins at OID = .1.3.6.1.4.1.3028.6.3.101. The enterprise MIB provides for (read-only) variables and traps and can be found in the following location on a PowerMedia XMS installation:

```
/usr/share/snmp/mibs/
```

The PowerMedia XMS installation includes the following MIBs:

- DLGC-GLOBAL-REG.mib
- ITU-ALARM-TC.mib
- XMS-NOTIFICATIONS.mib
- XMS-PERFORMANCE.mib
- XMS-PERFORMANCE-METERS.mib
- XMS-ROOT.mib

The implementation also supports some standard MIBs.

List of Standard MIBs

The following table lists the supported standard MIBs:

MIB	Description
EtherLike-MIB	Defines generic objects for Ethernet like network interfaces (RFC 3635)
HOST-RESOURCES-MIB	Management of host systems (RFC - many)
IF-MIB	Defines generic objects for network interface sub-layers (RFC 2863)
IP-MIB	Management of IP and ICMP implementation (RFC 4293)
IPV6-MIB	Management of IPv6 implementation
TCP-MIB	Management of TCP implementation (RFC 4022)
UDP-MIB	Management of UDP implementation (RFC 4113)
RFC1213-MIB	Defines MIB-II (RFC 1213)

List of Standard Traps

The following table lists the traps raised by PowerMedia XMS installation as a result of the incorporation of the standard MIBs:

Trap Name	Description
coldStart	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is re-initializing itself and that its configuration may have been altered.

Trap Name	Description
linkUp	<p>A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.</p> <p>Objects (ifIndex, ifAdminStatus, ifOperStatus)</p> <ul style="list-style-type: none"> • ifIndex: index of the interface • ifAdminStatus: (up, down, testing) • ifOperStatus: (up, down, testing, unknown, dormant, notPresent, lowerLayerDown)
linkDown	<p>A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of the ifOperStatus.</p> <p>Objects (ifIndex, ifAdminStatus, ifOperStatus)</p>

Enterprise (Proprietary) MIB

The PowerMedia XMS enterprise MIB contains traps and (currently read-only) performance related variables. The following sections detail the traps and variables.

Enterprise (Proprietary) Traps

The following table lists the enterprise traps raised by PowerMedia XMS:

Trap Name	Associated Variables	Type	Description
xmsLicenseHighThreshMet	xmsTrapSeverity	ItuPerceivedSeverity <ul style="list-style-type: none"> • Major:4 = Threshold breach • Cleared:1 = Threshold cleared 	Trap is generated when a threshold defined for a license resource is met during periodic collection of license meters.
	xmsAffectedLicenseResource	INTEGER representing license type below: <ul style="list-style-type: none"> • AMR AUDIO = 1 • BASIC AUDIO = 2 • HD AUDIO = 3 • LBR AUDIO = 4 • MRCP SPEECH = 5 • BASIC VIDEO = 6 • HIRES VIDEO = 7 • FAX = 8 • MSRP = 9 	
	xmsBreachValue	Integer32	

Trap Name	Associated Variables	Type	Description
	xmsConfiguredValue	Integer32	
xmsLicenseServerUnreachable	xmsTrapSeverity	ItuPerceivedSeverity <ul style="list-style-type: none"> • Critical:3 = Server can't be reached • Cleared:1 = Server is reachable 	Trap is generated when licensing server cannot be reached. When using a license server and the licensing subsystem encounters an unrecoverable error, this trap will be sent after the xmsLicensingSubsytemError trap is sent due to the licensing server becoming unreachable.
	xmsDescription	DisplayString	
xmsLicensingSubsystemError	xmsTrapSeverity	ItuPerceivedSeverity <ul style="list-style-type: none"> • Critical:3 = Licensing subsystem is unavailable or mal-functioning • Cleared:1 = Licensing server is operational 	Trap is generated when licensing subsystem is unavailable or mal-functioning.
	xmsDescription	DisplayString	
xmsLicenseExpiry	xmsTrapSeverity	ItuPerceivedSeverity <ul style="list-style-type: none"> • Major:4 = Threshold breach • Cleared:1 = Threshold cleared 	Trap is generated when threshold defined for license expiration is met during periodic collection of license meters.
	xmsDescription	DisplayString	

Trap Name	Associated Variables	Type	Description
xmsMaintenanceExpiry	xmsTrapSeverity	ItuPerceivedSeverity <ul style="list-style-type: none"> • Major:4 = Threshold breach • Cleared:1 = Threshold cleared 	Trap is generated when threshold defined for maintenance expiration is met during periodic collection of maintenance meters.
	xmsDescription	DisplayString	
xmsIncorrectLoginAttempt	xmsTrapSeverity	ItuPerceivedSeverity <ul style="list-style-type: none"> • Warning = For failed login attempts • Cleared = When the password is entered correctly after a failed login attempt 	Trap is generated when login attempt fails due to any reason in WebGUI.
	xmsWebUIUserName	DisplayString	
	xmsDescription	DisplayString	
xmsWebUserProfileChanged	xmsTrapSeverity	ItuPerceivedSeverity <ul style="list-style-type: none"> • Warning = For changes in the web user's profile 	Trap is generated if user's profile is changed in WebGUI.
	xmsWebUIUserName	DisplayString	
	xmsUserProfileChangeType	DisplayString	
	xmsDescription	DisplayString	
xmsServiceStatusChanged	xmsTrapSeverity	ItuPerceivedSeverity <ul style="list-style-type: none"> • Warning:6 = For status (STOPPED, STARTING, STOPPING, UNRESPONSIVE, OUTFSERVICE) • Cleared:1 = For RUNNING status 	Trap is sent when status of a monitored service changes.

Trap Name	Associated Variables	Type	Description
	xmsServiceIdentifier	DisplayString <ul style="list-style-type: none"> • hmp • broker • xmserver • appmanager • perfmanager • httpclient-xmserver • mrcpclient • rtcweb • xmsrest • netann • vxml • msml • msrpservice • faxservice • cdrserver 	
	xmsServicePreviousState	xmsServiceStatusEnum <ul style="list-style-type: none"> • STOPPED = 1 • STARTING = 2 • RUNNING = 3 • STOPPING = 4 • UNRESPONSIVE = 5 • OUTFSERVICE = 6 	
	xmsServiceCurrentState	xmsServiceStatusEnum	
	xmsDescription	DisplayString describing the cause of the trap (i.e., broker status change from STOPPED to STARTING)	
xmsCdrDeleted	xmsTrapSeverity	ItuPerceivedSeverity	Trap is generated when one or more CDR files are deleted by the CDR subsystem.
	xmsCdrLastTimeStamp	DateAndTime	
	xmsDescription	DisplayString	
xmsCdrCreationFailed	xmsTrapSeverity	ItuPerceivedSeverity	

Trap Name	Associated Variables	Type	Description
	xmsDescription	DisplayString	Trap is generated when the CDR subsystem fails to create new CDR files.
xmsCdrSizeHighThresMet	xmsTrapSeverity	ItuPerceivedSeverity	Trap is generated when a threshold defined for a total CDR file size is met.
	xmsBreachValue	Integer32	
	xmsConfiguredValue	Integer32	

Enterprise (Proprietary) Variables

The following table lists the enterprise variables supported by PowerMedia XMS:

Variable Name	Type	Description
xmsSignalingSessions	Gauge32	Count of currently active signaling sessions.
xmsRtpSessions	Gauge32	Count of currently active RTP sessions.
xmsMediaTransactions	Gauge32	Count of currently active media transactions.
xmsConferenceRooms	Gauge32	Count of currently active conference rooms.
xmsConferenceCallParties	Gauge32	Count of currently active conference call parties.
xmsConferenceMediaParties	Gauge32	Count of currently active conference media parties.
xmsASRTTSessions	Gauge32	Count of currently active ASR/TTS sessions.
xmsCallGroupTable	SEQUENCE of xmsCallGroupEntry	Table containing a list of currently active call-groups.
xmsCallGroupEntry	SEQUENCE	<pre>SEQUENCE { xmsCallGroupIndex xmsCallGroupName xmsCallGroupActiveCalls }</pre> <p>Information of a single call-group (call-group name and active calls in the call-group).</p>
xmsCallGroupIndex	Integer32	Auxiliary variable used for identifying instances of the column objects in the xmsCallGroupTable table.
xmsCallGroupName	DisplayString	Name of the call-group.

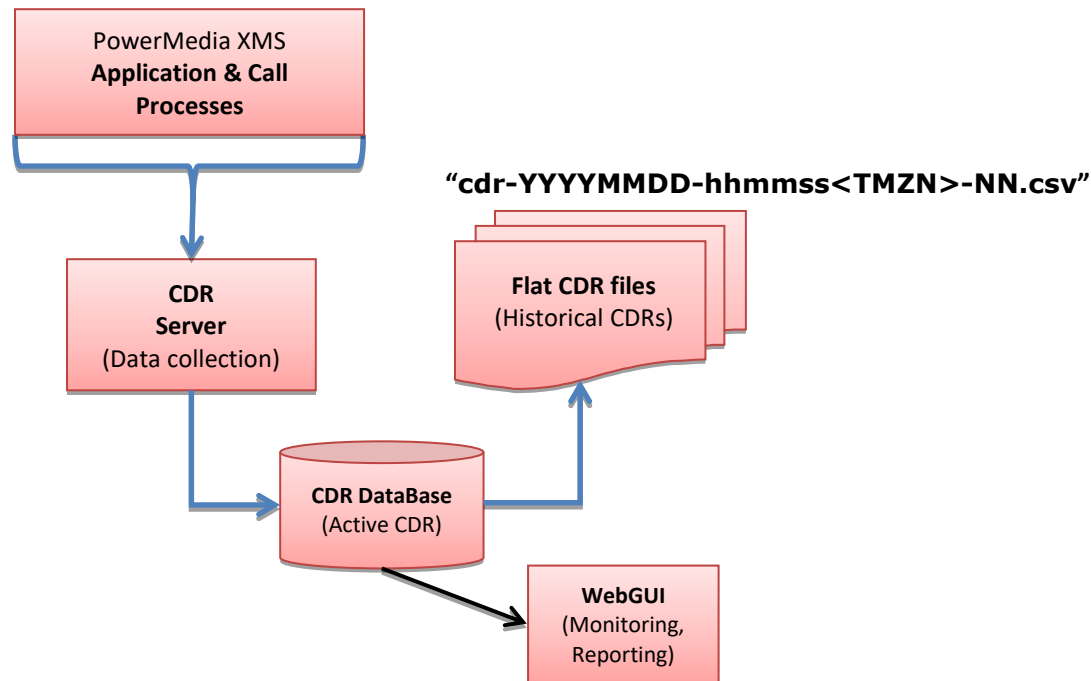
Variable Name	Type	Description
xmsCallGroupActiveCalls	Gauge32	Count of active calls in the call-group.
xmsLicenseUsageTable	SEQUENCE of xmsLicenseUsageTableEntry	Conceptual table that contains the list of current license usage of type xmsLicenseUsageTableEntry.
xmsLicenseUsageTableEntry	SEQUENCE	SEQUENCE { xmsLicenseName xmsLicenseUsage } Information of a particular license usage.
xmsLicenseName	INTEGER (enumerated)	{ amraudio(1), basicaudio(2), hdaudio(3), lbraudio(4), mrcpspeech(5), basicvideo(6), hiresvideo(7) } Name of the license type.
xmsLicenseUsage	Gauge32	Count of licenses of a particular type currently being used.
xmsServiceUpTime	TimeTicks	Time since the services were last re-initialized.
xmsServiceLastReset	DateAndTime	Date/Time of the last reset on the media server.
xmsServiceOverallStatus	xmsServiceStatusEnum	Overall status of services in native mode.
xmsServiceIndex	Integer32	Integer index for the table.
xmsServiceName	DisplayString	Unique identifiable string representing service name.
xmsServiceType	INTEGER	Mandatory or optional service.
xmsServiceStatus	xmsServiceStatusEnum	Status of service in the row.
xmsServiceDescription	DisplayString	Brief description of the service.
xmsServiceStatusTable	SEQUENCE of xmsServiceStatusTableEntry	Table row that shows status of a single service.

Refer to the MIBs for more details.

10. Appendix C: CDR

The PowerMedia XMS CDR implementation supports stored data set record for each signaling and media transaction on the system.

The following figure shows internal flow of CDR data.



The CDR data is collected by the CDR Service and first recorded to an internal CDR Database table. The CDR data stored in the database is moved periodically to flat disk files. This is done to avoid any performance hit on the database insertions due to huge database collection (table) size.

The flat disk CDR files will contain in each row one CDR for each call, in which the fields will be "#" delimited. In order to make CDR files accessible in Microsoft Excel on a Windows operating system, the CDR files are given an extension .csv, and to save disk space, these are compressed using the gzip utility. Therefore, the final CDR files on hard disk will have the extension .csv.gz.

The CDR files are generated and can be found in the following location on the PowerMedia XMS installation:

```
/var/local/xms/cdr
```

List of CDR Fields

The following table lists the call data logged in the CDR files for PowerMedia XMS:

CDR Component	Field Name	Field Type	Field Description	Example Value/Range
Signaling	Called URI	character string	URI in To header of initial INVITE request	<sip:msml@10.40.2.183:5060>;tag=f226f8b0
	Caller URI	character string	URI in From header of initial INVITE request	<sip:sipp@10.40.2.162:5060>;tag=6237SIPpTag001
	Call StartTime	ISO Date	Call start time in GMT time zone	2015-01-29T05:51:23.387Z
	Call AnswerTime	ISO Date	Call answer time in GMT time zone	2015-01-29T05:51:23.549Z
	Call EndTime	ISO Date	Call end time in GMT time zone	2015-01-29T05:51:23.552Z
	SIP Call Id	character string	SIP Call-ID header for this call	1-6237@10.40.2.162
	call Dir	character string	Direction of call with respect to XMS	"INBOUND" for incoming call and "OUTBOUND" for outgoing call
	release Dir	character string	Call terminating end point	"XMS" or "network"
	Protocol	character string	Protocol	"SIP" or "RTCWEB"
	rel Reason	character string	SIP release reason phrase	800 Bye/ 408 Request Time Out, etc.
	Req Uri	character string	Request URI in initial INVITE request	sip:msml@10.40.2.183:5060
	Rel Code	integer	SIP release code in final SIP response	SIP 3xx, 4xx, 5xx, 6xx response or 800 for normal call termination
	Call State	character string	State of call signaling during the call	idle, offering, accepting, accepted, answering, answered, dialing, proceeding, ringing, connected, transferring, clearing, cleared, message

CDR Component	Field Name	Field Type	Field Description	Example Value/Range
	Call Duration	integer	Duration of the call	Duration of the call (included only when the call is successfully answered and connected)
RTP Stream	DTMF Mode	character string	DTMF mode	inband, outofband, rfc2833
	RTP StartTime	ISO Date	RTP stream start time	2015-01-29T05:51:23.544Z
	RTP EndTime	ISO Date	RTP stream end time	2015-01-29T05:51:23.553Z
RTP Stream (Audio Codec)	Audio BitRate	integer	Bitrate of audio codec used in the call	64000
	Audio ClockRate	integer	Clock rate of audio codec used in the call	8000
	Audio Coder FrameSz	integer	Coder frame size for audio codec used in the call	20
	Audio Dir	character string	Direction for audio RTP stream	sendrecv, sendonly, recvonly, inactive
	Audio Encoding	character string	Encoding selected for audio RTP	pcmu, pcma, etc.
	Audio FramesPerPkt	integer	Frames per packet for audio encoding	1
	Audio LocalIp	character string	Local IP for audio stream	10.40.2.183
	Audio LocalPort	integer	Local port for audio stream	49158
	Audio PayloadType	integer	Audio payload type in SDP	0
	Audio RemoteIp	character string	Remote IP for audio stream	10.40.2.162
	Audio RemotePort	integer	Remote port for audio stream	6000

CDR Component	Field Name	Field Type	Field Description	Example Value/Range
	Audio VAD Enabled	integer	VAD (voice activity detection) is enabled for the call	0 or 1 (for disabled or enabled respectively)
RTP Stream (Video Codec)	video BitRate	integer	Bitrate of video codec	768000
	Video MaxBitRate	integer	Maximum bitrate	0
	Video SamplingRate	integer	Sampling rate of codec	1
	Video ImgWidth	integer	Image width in video	640
	Video ImgHeight	integer	Image height in video	480
	Video Dir	character string	Direction of video RTP stream	sendrecv, sendonly, recvonly, inactive
	Video Encoding	character string	Encoding selected for video RTP	vp8
	Video PayloadType	integer	Payload type for video media	120
	Video LocalIp	character string	Local IP for video stream	10.40.2.183
	Video LocalPort	integer	Local port for video stream	49158
	Video RemoteIp	character string	Remote IP for video stream	10.40.2.162
	Video RemotePort	integer	Remote port for video stream	6000
RTP Stream (QoS)	QOS Jitter	integer	Average jitter since the beginning of the call (in msec)	14
	QOS LostPkts	integer	Percent of lost packets since the beginning of the call	0
	QOS LocalTxPkts	integer	Number of packets sent by the local sender	3871

CDR Component	Field Name	Field Type	Field Description	Example Value/Range
	QOS LocalTxOcts	integer	Number of bytes sent by the local sender	597120
	QOS RemoteCumLost	integer	Number of packets lost, as computed by the remote receiver	0
	QOS RemoteTxPkts	integer	Number of packets sent by the remote sender	3606
	QOS RemoteTxOcts	integer	Number of bytes sent by the remote sender	576960
	QOS LocalCumLost	integer	Number of packets lost, as computed by the local receiver	0
	QOS LocalTimeStamp	integer	Local time stamp	1052560549
	QOS LocalSeqNum	integer	Local sequence number	249
	QOS RemoteTimeStamp	integer	Remote time stamp	63920
	QOS RemoteSeqNum	integer	Remote sequence number	363

CDR Management

This section explains how the CDR data is maintained internally to avoid disk space overrun by the CDR database and CDR files.

The amount of time that the data is kept in the CDR database and the amount of data contained in the CDR files on hard disk is controlled by following two configuration parameters:

1. Active CDR Age (in hours) - Time that CDRs remain in the CDR database.
2. CDR File Duration (in hours) - Time windows that CDRs are grouped into. When the CDR File Duration time window ends, the group of CDRs in that time window are exported to hard disk.

Note: CDRs can only be viewed in the WebGUI that are in the CDR database. The CDRs will remain in the CDR database for at least the time period set for "Active CDR Age". CDR data moved to CDR files are considered Historical CDRs and can be retrieved by the user for offline data analysis.

Logic of CDR File Creation and CDR Removal from the CDR Database

The Active CDR Age in combination with CDR File Duration dictates how long CDRs will remain in the database after their insertion. The CDRs will be removed from the database only when they fulfill the following two conditions:

1. The CDRs have completed the "Active CDR Age" time in the database.
2. The CDRs have completed the "CDR File Duration" time and have been exported to hard disk.

The CDR database is checked to see if conditions have been met in the last hour (i.e., 12:00AM, 1:00AM, and so on) at every hour past 5 minutes (i.e., 12:05AM, 01:05AM, and so on). If the CDR File Duration condition has been met, the applicable CDRs are exported to hard disk. If the CDRs that have been exported to hard disk also meet the Active CDR Age condition, the CDRs are removed from the database.

Example 1

In this example, the PowerMedia XMS system starts receiving calls at 1:30AM. The Active CDR Age is 3, so the CDR database will always contain the last 3 hours of CDRs. The CDR File Duration is 4, so the CDRs will be grouped in 4-hour time windows: 12:00AM to 4:00AM, 4:00AM to 8:00AM, and so on—the last time window of a day being 8:00PM to 12:00AM. When the CDR database is checked to see if conditions have been met every hour past 5 minutes, there are no results until 4:05AM.

At 4:05AM, the CDR database is checked to see if any conditions were met between 3:00AM and 4:00AM. The CDRs from the 4-hour time window of 12:00AM to 4:00AM are exported as a single file to hard disk because they now meet the 4-hour CDR File Duration condition. No CDRs meet the 3-hour Active CDR Age condition yet because the XMS node did not receive calls until 1:30AM, which makes the oldest CDR in the database a maximum of 2.5 hours old.

At 5:05AM, the CDR database is checked to see if any conditions were met between 4:00AM and 5:00AM. CDRs from 1:30AM to 2:00AM now meet the 3-hour Active CDR Age condition because they have been on the database for more than 3 hours. The CDRs from 1:30AM to 2:00AM already met the 4-hour CDR File Duration condition at 4:05AM. Because the CDRs from 1:30AM to 2:00AM now meet both conditions, they are removed from the database.

The next time CDRs are removed from the database is at 6:05AM. The CDRs that will be removed are those in the database from 2:00AM to 3:00AM.

The next export to hard disk will happen at 8:05AM. The file will contain CDRs from 4:00AM to 08:00AM.

Example 2

In this example, the PowerMedia XMS system starts receiving calls at 5:00PM on July 1. The Active CDR Age is 72 hours, so the database will always contain the last 72 hours of CDRs. The CDR File Duration is 24 hours, so the CDRs will be grouped in 24-hour time windows from 12:00AM to 11:59PM (one day). These are the maximum configurable values for these parameters.

On July 2 at 12:05AM, the CDRs from the 24-hour time window of 12:00AM to 11:59PM for July 1 are exported as a single file to hard disk because they now meet the 24-hour CDR File Duration condition. No CDRs meet the 72-hour Active CDR Age condition yet because the oldest CDR in the database is a maximum of 7 hours old.

On July 3 at 12:05AM, the CDRs from the 24-hour time window of 12:00AM to 11:59PM for July 2 are exported as a single file to hard disk because they now meet the 24-hour CDR File Duration condition. No CDRs meet the 72-hour Active CDR Age condition yet because the oldest CDR in the database is a maximum of 31 hours old.

On July 4 at 12:05AM, the CDRs from the 24-hour time window of 12:00AM to 11:59PM for July 2 are exported as a single file to hard disk because they now meet the 24-hour CDR File Duration condition. No CDRs meet the 72-hour Active CDR Age condition yet because the oldest CDR in the database is a maximum of 55 hours old.

On July 4 at 6:05PM, the CDRs from 5:00PM to 6:00PM on July 1 meet the 72-hour Active CDR Age condition because they have been on the database for more than 72 hours. The CDRs from 5:00PM to 6:00PM on July 1 already met the 24-hour CDR File Duration condition and were exported to hard disk on July 2 at 12:05AM. Because the CDRs from 5:00PM to 6:00PM on July 1 meet the Active CDR Age condition and have been exported to hard disk, they now meet both conditions and are removed from the database.

CDR File Rotation

The CDR files created will be kept on the hard disk of the PowerMedia XMS system for a limited period of time. This is controlled by two parameters:

1. Maximum Disk Space (in MB) - This is configurable from the WebGUI.
2. cdrPurgeSizeInPercent (in percent)- This is not configurable from the WebGUI but can be configured in the CDR configuration file (/etc/xms/cdrserver/config/cdrconfig.json).

Once the cumulative size of all CDR files on hard disk crosses the Maximum Disk Space threshold, the older CDR files will be removed to recover a fraction of Maximum Disk Space size. This fraction is configured in the parameter cdrPurgeSizeInPercent as a percentage value. For example, if Maximum Disk Space is configured to 4096 MB and cdrPurgeSizeInPercent is configured to 25%, then when cumulative size of all CDR files crosses 4096 MB, the oldest CDR files are deleted to recover 25% of 4096 MB (i.e., 1024 MB) of disk space.

Retrieval of Historical CDR Files

A CDR file written to the disk is considered a Historical CDR file. Only those CDRs that are currently in the CDR database can be queried (and viewed) from the WebGUI. CDRs that have been moved to the hard disk as Historical CDRs cannot be fetched via the WebGUI. As such, Historical CDRs will only be available in the form of files and can be downloaded via secure copy (SCP) by the authorized users.

The XMS administrator can create a user account that has access to the CDR files so that the CDR files can be downloaded before they are removed from the PowerMedia XMS system due to reaching the cumulative Maximum Disk Space size limit.

Refer to [Access to CDR Files](#) for information on creating a user account that has access to CDR files.

Note: When the cumulative size of CDR files crosses the configured high threshold value "CDR Disk Usage" (default=75%), then an SNMP trap is raised by the system (xmsCdrFileHighThresMet). This trap is an indication to the CDR user that the CDR files should be downloaded to a machine or backed up to a separate server before they hit the 100% threshold and are removed automatically from the XMS machine.

Naming Convention of CDR Files

The CDR files are created by exporting data from the CDR database to the hard disk with the following a naming convention:

cdr-YYYYMMDD-hhmmss<TMZN>-NN.csv

YYYY, MM, and DD correspond to year, month and date of file creation and hh, mm, and ss correspond to hour, minute, and second of file creation time. The TMZN is the time zone of the PowerMedia XMS system and contains five characters representing the numerical UTC time zone offset. For example, -0500 or +0530 for EST or IST time zones, respectively. The NN component is the number of hours contained in the CDR file, which equals the CDR File Duration parameter as configured from the WebGUI.

Example

A CDR file generated on July 6, 2015 at 3:00AM in the UTC-0400 time zone with a CDR File Duration of 1 hour results in the following file name: *cdr-20150706-030000-0400-01.csv*.

Format of CDR files

The CDR files will be in .csv formats, but in order to save the disk space, cdrserver gzips these files so the CDR files will have extension .csv.gz.

The CDR file will contain first line `sep=#` (the # is used as a separator here so that a field containing a semicolon (;), which is generally used as field separator for csv files, is not misinterpreted as a field separator. A CDR field will not usually contain # character.

Following is a sample CDR generated for a video call.

```
sep=#
callId#calledUri#callerUri#callStartTime#callAnswerTime#callEndTime#SIPCallId#callDir#releaseDir#
protocol#relReason#reqUri#relCode#callState#callDuration#audioBitRate#audioClockRate#audioCoderFr
ameSz#audioDir#audioEncoding#audioFramesPerPkt#audioLocalIp#audioLocalPort#audioPayloadType#audio
RemoteIp#audioRemotePort#audioVADEnabled#dtmfMode#rtpStartTime#rtpEndTime#videoBitRate#videoMaxBi
tRate#videoSamplingRate#videoImgWidth#videoImgHeight#videoDir#videoEncoding#videoPayloadType#vide
oLocalIp#videoLocalPort#videoRemoteIp#videoRemotePort#qosLostPkts#qosJitter#qosRTLatency#qosLocal
TxPkts#qosLocalTxOcts#qosLocalCumulativeLost#qosRemoteTxPkts#qosRemoteTxOcts#qosRemoteCumulativeLost#qosLocal
TimeStamp#qosLocalSeqNum#qosRemoteTimeStamp#qosRemoteSeqNum#
e3fb0ecb-a414-4367-b1fc-b57d9a1f50ec#<sip:mssl@10.40.2.212>;tag=f7288b50-d402280a-13c4-65014-15e-
25cffc45-15e#<sip:2422@14.96.218.81>;tag=FpW-zD1f1#2015-08-21T15:10:31-0400#2015-08-21T15:10:31-
0400#2015-08-21T15:10:53-0400#LhBt6Ynz0i#INBOUND#network#SIP#800
Bye#sip:mssl@10.40.2.212#800#cleared#22#64000#8000#20#sendrecv#pcmu#1#10.40.2.212#49152#0#192.168
.250.138#7078#0#rfc2833#2015-08-21T15:10:31-0400#2015-08-21T15:10:53-
0400#384000#0#1#352#288#sendrecv#h263-
1998#96#10.40.2.212#57344#192.168.250.138#9078#0#0##1085#167040#0#600#96000#0#3910533713#629#1063
20##
```

Note:

1. The first line of each CDR file will be `sep=#` so that when the user opens this on Windows platform by double clicking the file, it is opened in Microsoft Excel as a csv file.
2. The second line of each CDR file will contain the field names separated by # character.
3. After the second line, each line will contain the CDR for a call.

CDR-Related SNMP Traps and Their Meaning

For the CDR subsystem, the following SNMP traps have been defined:

- **xmsCdrDeleted** - This SNMP trap is raised by the PowerMedia XMS system when the CDR subsystem deletes one or more oldest CDR files on the hard disk because the cumulative size of CDR files on the disk have exceeded their maximum size threshold.
- **xmsCdrCreationFailed** - This SNMP trap is raised by the PowerMedia XMS system when the CDR subsystem fails to export CDR files to hard disk. The CDR file export might fail due to one of the following reasons:
 - a. Insufficient disk space.
 - b. An internal error due to the inability of a CDR service to communicate with CDR database.
 - c. An internal API error.
- **xmsCdrSizeHighThresMet** - This SNMP trap is raised by the PowerMedia XMS system when the cumulative size of CDR files on hard disk reaches the configured high threshold value "CDR Disk Usage" (default=75%) of total configured Maximum Disk Space. This trap serves as an indication to the CDR user that the oldest CDR files will soon be deleted once they hit their 100% size threshold. The user should download the CDR files to the system to preserve Historical CDR data.

11. Appendix D: Sample Use Cases

PowerMedia XMS includes a set of scripts to provide access of management commands through the Command Line Interface (CLI). PowerMedia XMS CLI scripts use the RESTful Management API to provide repeatable management functionality through CLI that can be used by remote script processes for PowerMedia XMS management purposes. The set of CLI scripts provide an example that can be expanded by system administrators to cover a variety of PowerMedia XMS management functions.

The following describes the command scripts covered by the CLI:

- [Start/Stop Service and Application](#)
- [Check Status of Service](#)
- [Check/Install License](#)
- [MSML Configuration](#)
- [Tone Configuration](#)
- [Codec Configuration](#)

Note: PowerMedia XMS CLI does not cover all the configuration options of the Console.

Script Location

The CLI is implemented via scripts located in the following directories:

```
/sbin  
/usr/sbin
```

For the scripts to work, these directories must be in the path of the administrator login.

Start/Stop Service and Application

To start/stop/restart the services, run the following command:

```
service nodecontroller stop|start|restart
```

The following shows the sample output of the command:

```
[root@xms ~]# service nodecontroller restart  
Stopping: nodecontroller ..... [ OK ] .....  
Starting: nodecontroller ..... [ OK ] .....
```

Check Status of Service

To get the status of all services, run the following command:

```
xmstatus-python
```

The following shows the sample output of the command:

```
[root@xms ~]# xmstatus-python  
[<service id="hmp" state="RUNNING" description="Media processing services." optional="no"  
onStart="yes" />]  
[<service id="broker" state="RUNNING" description="Message routing services." optional="no"  
onStart="yes" />]  
[<service id="xmserver" state="RUNNING" description="Signalling and Media services."  
optional="no" onStart="yes" />]  
[<service id="httpclient" state="RUNNING" description="HTTP Client." optional="yes"  
onStart="yes" />]  
[<service id="mrcpclient" state="RUNNING" description="MRCP Client." optional="yes"  
onStart="yes" />]  
[<service id="rtcweb" state="RUNNING" description="RtcWeb Signalling Server." optional="yes"  
onStart="yes" />]
```



```

['<service id="appmanager" state="RUNNING" description="Application interface." optional="no"
onStart="yes" />']
['<service id="xmsrest" state="RUNNING" description="RESTful API for call control and media
control." optional="yes" onStart="yes" />']
['<service id="netann" state="RUNNING" description="NETANN Process." optional="yes" onStart="yes"
/>']
['<service id="vxml" state="RUNNING" description="VXML Process." optional="yes" onStart="yes"
/>']
['<service id="msml" state="RUNNING" description="MSML Server" optional="yes" onStart="yes" />']
['<service id="msrpservice" state="RUNNING" description="MSRP Service." optional="yes"
onStart="yes" />']
['<service id="verification" state="RUNNING" description="System/Application Verification Server"
optional="yes" onStart="yes" />']
['<service id="xmssysstats" state="RUNNING" description="Application to provide system stats to
Performance Manager" optional="yes" onStart="yes" />']
['<service id="perfmanager" state="RUNNING" description="Performance Manager" optional="yes"
onStart="yes" />']
['<service id="eventmanager" state="RUNNING" description="Event Manager" optional="yes"
onStart="yes" />']

```

Check/Install License

To get the details regarding the currently installed licenses, run the following command:

```
checklicense-python
```

The following shows the sample output of the command:

```

[root@xms ~]# checklicense-python
XMS2x__host_pur_000C2909F9F6.lic :
verification.lic :
('Advanced Video', '0')
('Basic Audio', '2000')
('GSMAMR Audio', '0')
('HD Voice', '0')
('High Resolution Video', '0')
('LBR Audio', '0')
('MRB', '0')
('MRCP Speech Server', '0')
('MSRP', '0')

```

To install a license, run the following command:

```
activatelicence-python <license-file>
```

Note: The <license-file> must reside in the current directory and it must be specified as a pure file name (as opposed to path).

For example, specifying `"/XMS2x__host_pur_000C299A815E.lic"` would be incorrect. The new installed licenses take effect only after a PowerMedia XMS service restart.

The following shows the sample output of the command:

```

[root@xms tmp]# activatelicence-python XMS2x__host_pur_000C299A815E.lic
COPYING XMS2x__host_pur_000C299A815E.lic to /etc/xms/license
ACTIVATING XMS2x__host_pur_000C299A815E.lic
SERVER RESPONSE:
<?xml version='1.0'?>
<web_service version="1.0">
  <response>
    <license id="XMS2x__host_pur_000C299A815E.lic" type="Purchased"
expires="permanent" status="active" >
      <feature id="advanced_video" display_name="Advanced Video" value="300" />
      <feature id="basic_audio" display_name="Basic Audio" value="200" />
      <feature id="gsmamr_audio" display_name="GSMAMR Audio" value="100" />
      <feature id="hd_voice" display_name="HD Voice" value="200" />
      <feature id="high_res_video" display_name="High Resolution Video"
value="40" />
      <feature id="lbr_audio" display_name="LBR Audio" value="100" />
      <feature id="mrb" display_name="MRB" value="0" />
      <feature id="mrcp_speech_server" display_name="MRCP Speech Server"
value="150" />

```

```

        <feature id="msrp" display_name="MSRP" value="250" />
    </license>
</response>
</web_service>
#####
Service Restart is Required!!
#####

```

MSML Configuration

To get the current MSML configuration, run the following command:

```
showmsmlparams-python
```

The following shows the sample output of the command:

```

[root@xms ~]# showmsmlparams-python
{
  "version" : "1.1",
  "http_caching" : "yes",
  "http_connect_timeout" : "30",
  "schema_validation" : "no",
  "adaptor_port" : "",
  "storage_directory" : "",
  "content_type" : "xml",
  "encoding" : "utf_8",
  "clear_db" : "no",
  "dtmf_start_time" : "no",
  "adv_digit_pattern" : "no",
  "video_fast_update" : "",
  "video_bandwidth" : "512",
  "conf_agc_default" : "no",
  "default_amr_alignment" : "BANDWIDTH_EFFICIENT",
  "dtmf_detect_mode" : "RFC-2833",
  "dns_cache_timeout" : "0",
  "cert_verify_peer" : "no",
  "cert_verify_host" : "no",
  "cpa" : []
}

```

To set a specific parameter in the MSML configuration, run the following command:

```
setmsmlparams-python <msml-params-file-name>
```

The <msml-params-file-name> is the path to the file, which contains the MSML parameters in JSON format. A good way to modify any parameter would be to generate this file using the "showmsmlparams-python" command, modify the value of the specific parameter in the file, and supply this file as an argument to the "setmsmlparams-python". See the *Dialogic® PowerMedia™ XMS RESTful Management API User's Guide (/msml section)* for detailed information about these parameters.

The following sequence of commands illustrates the procedure:

```

[root@xms ~]# setmsmlparams-python msml
Request url =http://127.0.0.1:10080/msml
SERVER RESPONSE:
{
  "version" : "1.1",
  "http_caching" : "yes",
  "http_connect_timeout" : "45",
  "schema_validation" : "yes",
  "adaptor_port" : "",
  "storage_directory" : "hello",
  "content_type" : "msml_xml",
  "encoding" : "utf_ascii",
  "clear_db" : "yes",
  "dtmf_start_time" : "yes",
  "adv_digit_pattern" : "yes",
  "video_fast_update" : "INFO",
  "video_bandwidth" : "256",
  "conf_agc_default" : "yes",

```

```

    "default_amr_alignment" : "OCTET-ALIGNED",
    "dtmf_detect_mode" : "IN-BAND",
    "dns_cache_timeout" : "100",
    "cert_verify_peer" : "yes",
    "cert_verify_host" : "yes",
    "cpa" : []
}
#####
Service Restart is Required!!
#####

```

Tone Configuration

To get a listing of the current tones, run the following command:

```
showtones-python
```

The following shows the sample output of the command:

```

[root@xms ~]# showtones-python
{
  "tones" : [
    {
      "New" : {
        "freq1" : 300,
        "fq1dev" : 0,
        "freq2" : 400,
        "fq2dev" : 0,
        "ontime" : 40,
        "ontdev" : 1,
        "offtime" : 40,
        "offtdev" : 1,
        "repcnt" : 0
      }
    }
  ]
}

```

To set a custom tone, run the following command:

```
settones-python <tones-file-name>
```

The <tones-file-name> is the path to the file, which contains the JSON formatted tone information (usually the output of "showtones-python"). A good way to modify any parameter would be to generate this file using the "showtones-python" command, modify the value of the specific parameter in the file, and supply this file as an argument to the "settones-python".

The following sequence of commands illustrates the procedure:

```

[root@xms ~]# showtones-python > tones.txt
<modify the values in the "tones.txt" using any editor>
[root@xms ~]# settones-python tones.txt
Request url =http://127.0.0.1:10080/tones
SERVER RESPONSE:
{
  "tones" : [
    {
      "New" : {
        "freq1" : 350,
        "fq1dev" : 2,
        "freq2" : 450,
        "fq2dev" : 4,
        "ontime" : 45,
        "ontdev" : 1,
        "offtime" : 50,
        "offtdev" : 1,
        "repcnt" : 0
      }
    }
  ]
}

```

```
}  
#####  
Service Restart is Required!!  
#####
```

Codec Configuration

To get a listing of the current codecs and their parameters, run the following command:

```
savecodecs-python
```

The following shows the sample output of the command:

```
[root@xms ~]# savecodecs-python  
{  
  "audio_codecs" : [  
    {  
      "g722" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "pcmu" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "pcma" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "g726-32" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "amr" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "g723" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "g729" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "amr-wb" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "iLBC" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "opus" : {  
        "enabled" : "yes"  
      }  
    },  
    {  
      "gsm" : {  
        "enabled" : "yes"  
      }  
    }  
  ],  
}
```

```

        {
            "gsm-efr" : {
                "enabled" : "yes"
            }
        }
    ],
    "video_codecs" : [
        {
            "h264" : {
                "enabled" : "yes"
            }
        },
        {
            "mp4v-es" : {
                "enabled" : "yes"
            }
        },
        {
            "h263" : {
                "enabled" : "yes"
            }
        },
        {
            "h263-1998" : {
                "enabled" : "yes"
            }
        },
        {
            "h263-2000" : {
                "enabled" : "yes"
            }
        },
        {
            "vp8" : {
                "enabled" : "yes"
            }
        }
    ],
    "video_encoder_sharing" : "Disabled"
}

```

To set a custom tone, run the following command:

```
setcodecs-python <codecs-file-name>
```

The <codecs-file-name> is the path to the file, which contains the JSON formatted codec information (usually the output of "savecodecs-python"). A good way to modify any parameter would be to generate this file using the "setcodecs-python" command, modify the value of the specific parameter in the file, and supply this file as an argument to the "savecodecs-python".

The following sequence of commands illustrates the procedure:

```

[root@xms ~]# savecodecs-python > codecs.txt
<modify the values in the "codecs.txt" using any editor>
[root@xms ~]# setcodecs-python codecs.txt
{
    "audio_codecs" : [
        {
            "pcmu" : {
                "enabled" : "yes"
            }
        },
        {
            "pcma" : {
                "enabled" : "yes"
            }
        },
        {
            "g726-32" : {
                "enabled" : "yes"
            }
        }
    ]
}

```

```

    },
    {
      "amr" : {
        "enabled" : "yes"
      }
    },
    {
      "g723" : {
        "enabled" : "yes"
      }
    },
    {
      "g729" : {
        "enabled" : "yes"
      }
    },
    {
      "amr-wb" : {
        "enabled" : "yes"
      }
    },
    {
      "iLBC" : {
        "enabled" : "yes"
      }
    },
    {
      "opus" : {
        "enabled" : "yes"
      }
    },
    {
      "gsm" : {
        "enabled" : "yes"
      }
    },
    {
      "gsm-efr" : {
        "enabled" : "yes"
      }
    },
    {
      "g722" : {
        "enabled" : "no"
      }
    }
  ],
  "video_codecs" : [
    {
      "h264" : {
        "enabled" : "yes"
      }
    },
    {
      "mp4v-es" : {
        "enabled" : "yes"
      }
    },
    {
      "h263" : {
        "enabled" : "yes"
      }
    },
    {
      "h263-1998" : {
        "enabled" : "yes"
      }
    },
    {
      "h263-2000" : {

```

```
        "enabled" : "yes"
    },
    {
        "vp8" : {
            "enabled" : "yes"
        }
    }
],
"video_encoder_sharing" : "Disabled"
```

12. Appendix E: SIP OPTIONS Ping Processing

The SIP OPTIONS ping responses are coordinated between the PowerMedia XMS and PowerMedia MRB to provide consistent responses that take into consideration the system status and resource availability at each network element. The SIP OPTIONS ping response also considers the status of the XMS-monitored subservices and licenses.

For the XMS to respond to a SIP OPTIONS ping with a 200 OK, all XMS services must be operational and there must be one available signaling license to accept a new call. When the XMS services are operational but there are no available signaling licenses, XMS responds with 486 Busy. When an XMS service is not operational, XMS responds with 503 Service Unavailable. Refer to the following table.

Services/Conditions	Operational Status	Response
XMS Services	Active (All services are operational and there is an available signaling license.)	200 OK
	Failed (All services are not operational.)	503 Service Unavailable
Signaling Licenses	Available (All services are operational and there is an available signaling license.)	200 OK
	Unavailable (All services are operational but all signaling licenses are in use.)	486 Busy

Note: Services that are administratively disabled at system startup or stopped are excluded when the XMS checks the operational status of the services.

Note: Every SIP OPTIONS ping processed by the XMS consumes a signaling license for the duration of the transaction. Typical use of this feature may require pinging up to five services concurrently (msml, vxml, xmsrest, and netann) resulting in the periodic use of five licenses. Because this feature allows for up to 256 concurrent pings, up to 256 licenses can be consumed.

13. Appendix F: Dashboard Counters

CDR Server

The following table lists the counters used for CDR Server:

Name	Description
CDR Server Database Size	The size of the uncompressed data in the database (bytes).
CDR Server Number of Records	The number of records in the database.
CDR Server Index Size	The size of all indexes in the database (bytes).
CDR Server Resident Memory	The resident memory.
CDR Server Virtual Memory	The virtual memory used by the database (bytes).
CDR Server Bulk Op Duration	Bulk operation duration (ms).
CDR Server Bulk Op Size	The number of requests (insert/update) in a bulk operation.
CDR Server Errors Per Minute	Database operation errors per minute.
CDR Server Query Attempts	Database query attempts.
CDR Server Update Attempts	Database update attempts.
CDR Server Update Failures	Database update failures.
CDR Server Storage Size	The amount of disk storage used by the database (bytes).
CDR Server Export Duration	The duration of database export operations.
CDR Server Export Records	The number of records in an export operation.
CDR Server Op Queue Size	The number of database operations waiting to be executed.
CDR Server Export Storage	The amount of storage occupied by the export archive files (bytes).

Fax Service

The following table lists the counters used for Fax Service:

Name	Description
Fax Service FAX Session Attempts	The fax session attempts.
Fax Service FAX Session Failures	The fax session failures.
Fax Service FAX Session Failure Training	The fax session training failures.
Fax Service FAX Session Failure Not Auth	The fax session not authorized failures.
Fax Service FAX Session TA Attempt	The fax session turnaround attempts.
Fax Service FAX Session TA Failure	The fax session turnaround failures.
Fax Service FAX Send Failures	The fax send failures.
Fax Service FAX Rcv Failures	The fax receive failures.
Fax Service FAX Session Active	Active fax sessions.
Fax Service FAX Rcv Active	Active fax receive operations.
Fax Service FAX Send Active	Active fax send operations.
Fax Service FAX Session Active T30	Active T.30 fax sessions.
Fax Service FAX Session Active T38	Active T.38 fax sessions.
Fax Service FAX Page Send Attempts	The fax page send attempts.
Fax Service FAX Page Send Failures	The fax page send failures.
Fax Service FAX Page Rcv Attempts	The fax page receive attempts.
Fax Service FAX Page Rcv Failure	The fax page receive failures.
Fax Service FAX Cvt tiff2pdf Attempts	TIFF to PDF fax conversion attempts.
Fax Service FAX Cvt tiff2pdf Failures	TIFF to PDF fax conversion failures.
Fax Service FAX Cvt tiff2pdf Active	Active TIFF to PDF fax conversions.
Fax Service FAX Cvt pdf2tiff Attempts	PDF to TIFF fax conversion attempts.
Fax Service FAX Cvt pdf2tiff Failures	PDF to TIFF fax conversion failures.
Fax Service FAX Cvt pdf2tiff Active	Active PDF to TIFF fax conversions.
Fax Service FAX HTTP GET Attempts	The fax HTTP GET attempts.
Fax Service FAX HTTP GET Failures	The fax HTTP GET failures.

Name	Description
Fax Service FAX HTTP GET Active	Active fax HTTP GET operations.
Fax Service FAX HTTP PUT Attempts	The fax HTTP PUT attempts.
Fax Service FAX HTTP PUT Failures	The fax HTTP PUT failures.
Fax Service FAX HTTP PUT Active	Active fax HTTP PUT operations.

HTTP Client

The following table lists the counters used for HTTP Client:

Name	Description
HTTP Client Cache Hits	The number of GET requests satisfied from the cache.
HTTP Client Cache Size	The amount of storage occupied by the cache (bytes).
HTTP Client DELETE Active	The number of active DELETE requests.
HTTP Client DELETE Attempts	The number of DELETE attempts.
HTTP Client DELETE Failures	The number DELETE failures.
HTTP Client GET Active	The number of active GET requests.
HTTP Client GET Attempts	The number of GET attempts.
HTTP Client GET Failures	The number of GET failures.
HTTP Client POST Active	The number of active POST requests.
HTTP Client POST Attempt	The number of POST attempts.
HTTP Client POST Failure	The number of POST failures.
HTTP Client PUT Active	The number of active PUT requests.
HTTP Client PUT Attempts	The number of PUT attempts.
HTTP Client PUT Failure	The number of PUT failures.
HTTP Client HTTP DELETE Success	Successful HTTP DELETE operations.
HTTP Client HTTP GET Success	Successful HTTP GET operations.
HTTP Client HTTP PUT Success	Successful HTTP PUT operations.
HTTP Client HTTP POST Success	Successful HTTP POST operations.

MRCP Client

The following table lists the counters used for MRCP Client:

Name	Description
MRCP Client Recognize Active	The number of active ASR operations.
MRCP Client Recognize Attempts	The number of ASR attempts.
MRCP Client Recognize Cmpltd Cause 000	The number of ASR operations with complete cause 000.
MRCP Client Recognize Cmpltd Cause 001	The number of ASR operations with complete cause 001.
MRCP Client Recognize Cmpltd Cause 002	The number of ASR operations with complete cause 002.
MRCP Client Recognize Cmpltd Cause 003	The number of ASR operations with complete cause 003.
MRCP Client Recognize Cmpltd Cause 004	The number of ASR operations with complete cause 004.
MRCP Client Recognize Cmpltd Cause 005	The number of ASR operations with complete cause 005.
MRCP Client Recognize Cmpltd Cause 006	The number of ASR operations with complete cause 006.
MRCP Client Recognize Cmpltd Cause 007	The number of ASR operations with complete cause 007.
MRCP Client Recognize Cmpltd Cause 008	The number of ASR operations with complete cause 008.
MRCP Client Recognize Cmpltd Cause 009	The number of ASR operations with complete cause 009.
MRCP Client Recognize Cmpltd Cause 010	The number of ASR operations with complete cause 010.
MRCP Client Recognize Cmpltd Cause 011	The number of ASR operations with complete cause 011.
MRCP Client Recognize Cmpltd Cause 012	The number of ASR operations with complete cause 012.
MRCP Client Recognize Cmpltd Cause 013	The number of ASR operations with complete cause 013.
MRCP Client Recognize Cmpltd Cause 014	The number of ASR operations with complete cause 014.
MRCP Client Recognize Cmpltd Cause 015	The number of ASR operations with complete cause 015.
MRCP Client Recognize Cmpltd Cause 016	The number of ASR operations with complete cause 016.
MRCP Client Recognize Failure	The number of ASR operation failures.
MRCP Client Server State (ASR)	MRCP ASR server state.
MRCP Client Server State (TTS)	MRCP TTS server state.
MRCP Client Sessions Active	The number of active MRCP sessions.
MRCP Client Session Attempts	The number of MRCP session attempts.
MRCP Client Session Connection Failure	The number of MRCP session connection failures.

Name	Description
MRCP Client Session Signalling Failure	The number of MRCP session signaling failures.
MRCP Client Speak Active	The number of active TTS operations.
MRCP Client Speak Attempts	The number of TTS operation attempts.
MRCP Client Speak Cmpltd Cause 000	The number of TTS operations with complete cause 000.
MRCP Client Speak Cmpltd Cause 001	The number of TTS operations with complete cause 001.
MRCP Client Speak Cmpltd Cause 002	The number of TTS operations with complete cause 002.
MRCP Client Speak Cmpltd Cause 003	The number of TTS operations with complete cause 003.
MRCP Client Speak Cmpltd Cause 004	The number of TTS operations with complete cause 004.
MRCP Client Speak Cmpltd Cause 005	The number of TTS operations with complete cause 005.
MRCP Client Speak Cmpltd Cause 006	The number of TTS operations with complete cause 006.
MRCP Client Speak Cmpltd Cause 007	The number of TTS operations with complete cause 007.
MRCP Client Speak Failure	The number of TTS operation failures.
MRCP Client Stop Active	The number of active stop operations.
MRCP Client Stop Attempts	The number of stop attempts.
MRCP Client Stop Failure	The number of stop failures.
MRCP Client Update Session Active	The number of active update session operations.
MRCP Client Update Session Attempts	The number of update session attempts.
MRCP Client Update Session Failure	The number of update session failures.
MRCP Client MRCP SIP Session Attempts	The number of MRCP SIP session establishment attempts.
MRCP Client MRCP SIP Session Failures	The number of MRCP SIP session establishment failures.
MRCP Client MRCP Active SIP Sessions	The number of active MRCP SIP sessions.
MRCP Client MRCP SIP Sent INVITE	The number of transmitted MRCP INVITE requests.
MRCP Client MRCP SIP Rcv Resp INVITE 2xx	The number of received 2xx responses to MRCP INVITE requests.
MRCP Client MRCP SIP Sent Responses	The number of transmitted MRCP SIP responses.
MRCP Client MRCP SIP Rcv Responses	The number of received MRCP SIP responses.
MRCP Client MRCP SIP Sent BYE	The number of transmitted MRCP SIP BYE requests.

Name	Description
MRCP Client MRCP SIP Rcv BYE	The number of received MRCP SIP BYE requests.
MRCP Client Recognize Success	Successful MRCP recognize operations.
MRCP Client Speak Success	Successful MRCP speak operations.
MRCP Client Stop Success	Successful MRCP stop operations
MRCP Client MRCP Session Success	Successful MRCP sessions.

MSML Server

The following table lists the counters used for MSML Server:

Name	Description
MSML Server Calls Active	Active MSML calls.
MSML Server Media Active	Active MSML media operations.
MSML Server Collect Active	Active collect/dtmf operations.
MSML Server Collect Attempts	The collect/dtmf attempts.
MSML Server Collect Failures	The collect/dtmf failures.
MSML Server CPA Active	Active CPA operations.
MSML Server CPA Attempts	CPA attempts.
MSML Server CPA Failures	CPA failures.
MSML Server Dtmfgen Active	Active dtmfgen operations.
MSML Server Dtmfgen Attempts	The dtmfgen attempts.
MSML Server Dtmfgen Failures	The dtmfgen failures.
MSML Server Faxdetect Active	Active faxdetect operations.
MSML Server Faxdetect Attempts	The faxdetect attempts.
MSML Server Faxdetect Failures	The faxdetect failures.
MSML Server Faxrcv Active	Active faxrcv operations.
MSML Server Faxrcv Attempts	The faxrcv attempts.
MSML Server Faxrcv Failures	The faxrcv failures.
MSML Server Faxsend Active	Active faxsend operations.

Name	Description
MSML Server Faxsend Attempts	The faxsend attempts.
MSML Server Faxsend Failures	The faxsend failures.
MSML Server Fileop Active	Active fileop operations.
MSML Server Fileop Attempts	The fileop attempts.
MSML Server Fileop Failures	The fileop failures.
MSML Server Play Active	Active play operations.
MSML Server Play Attempts	The play attempts.
MSML Server Play Failures	The play failures.
MSML Server Record Active	Active record operations.
MSML Server Record Attempts	The record attempts.
MSML Server Record Failures	The record failures.
MSML Server Speech Actives	Active speech operations.
MSML Server Speech Attempts	The speech attempts.
MSML Server Speech Failures	The speech failures.
MSML Server Transfer Active	Active transfer operations.
MSML Server Transfer Attempts	The transfer attempts.
MSML Server Transfer Failures	The transfer failures.
MSML Server Vad Active	Active vad operations.
MSML Server Vad Attempts	The vad attempts.
MSML Server Vad Failures	The vad failures.
MSML Server Conference Active	Active conferences.
MSML Server Conference Attempts	The conference creation attempts.
MSML Server Conference Failures	The conference creation failures.
MSML Server Conference Party Active	Active conference parties.
MSML Server Conference Party Attempts	The conference party creation attempts.
MSML Server Conference Party Failures	The conference party creation failures.

Name	Description
MSML Server Connections Active	Active network connections.
MSML Server Connection Attempts	The network connection attempts.
MSML Server Connection Failures	The network connection failures.
MSML Server Dialog Active	Active dialogs.
MSML Server Dialog Attempts	The dialog execution attempts.
MSML Server Dialog Failures	The dialog execution failures.
MSML Server Transactions Active	Active MSML transactions.
MSML Server Transaction Attempts	MSML transaction attempts.
MSML Server Transaction Failures	MSML transaction failures.

MSRP Server

The following table lists the counters used for MSRP Server:

Name	Description
MSRP Server Messages Active	Active MSRP messages.
MSRP Server Message Attempts	The message tx/rx attempts.
MSRP Server Message Failures	The message tx/rx failures.
MSRP Server Sessions Active	Active sessions.
MSRP Server Session Attempts	The session attempts.
MSRP Server Session Failures	The session failures.
MSRP Server File Rcv Active	Active file receive operations.
MSRP Server File Rcv Attempts	The file receive attempts.
MSRP Server File Rcv Failures	The file receive failures.
MSRP Server File Send Active	Active file send operations.
MSRP Server File Send Attempts	The file send attempts.
MSRP Server File Send failures	The file send failures.
MSRP Server Msg Rcv Active	Active message receive operations.
MSRP Server Msg Rcv Attempts	The message receive attempts.

Name	Description
MSRP Server Msg Rcv Failure	The message receive failures.
MSRP Server Msg Send Active	Active message send operations.
MSRP Server Msg Send Attempts	The message send attempts.
MSRP Server Msg Send Failure	The message send failures.

NETANN Server

The following table lists the counters used for NETANN Server:

Name	Description
NETANN Server Play Active	
NETANN Server Play Attempts	
NETANN Server Play Failures	
NETANN Server Conference Active	
NETANN Server Conference Attempts	
NETANN Server Conference Failures	
NETANN Server Conference Party Active	
NETANN Server Conference Party Attempts	
NETANN Server Conference Party Failures	
NETANN Server Connection Active	
NETANN Server Connection Attempts	
NETANN Server Connection Failures	

RESTful API Server

The following table lists the counters used for RESTful API Server:

Name	Description
RESTful API Server Call Active	
RESTful API Server Call Attempts	
RESTful API Server Call Failure	
RESTful API Server Conference Active	
RESTful API Server Conference Attempt	

Name	Description
RESTful API Server Conference Failure	
RESTful API Server MRCP Active	
RESTful API Server MRCP Attempts	
RESTful API Server MRCP Failures	

VXML Server

The following table lists the counters used for VXML Server:

Name	Description
VXML Server Field DTMF Active	
VXML Server Field DTMF Attempts	
VXML Server Field DTMF Failures	
VXML Server Field Voice Active	
VXML Server Field Voice Attempts	
VXML Server Field Voice Failures	
VXML Server Prompt Play Active	
VXML Server Prompt Play Attempts	
VXML Server Prompt Play Failures	
VXML Server Prompt Speech Active	
VXML Server Prompt Speech Attempts	
VXML Server Prompt Speech Failures	
VXML Server Record Active	
VXML Server Record Attempts	
VXML Server Record Failures	
VXML Server Say-as Active	
VXML Server Say-as Attempts	
VXML Server Say-as Failures	
VXML Server Transfer Active	

Name	Description
VXML Server Transfer Attempts	
VXML Server Transfer Failures	
VXML Server Connections Active	
VXML Server Connections Allocated	
VXML Server Connection Incoming Attempts	
VXML Server Connection Incoming Failures	
VXML Server Connection Outgoing Attempts	
VXML Server Connection Outgoing Failures	

XMS Server

The following table lists the counters used for XMS Server:

Name	Description
XMS Server Codec AMR Active	Active AMR codec instances.
XMS Server Codec AMR-WB Active	Active AMR-WB codec instances.
XMS Server Codec EVS Active	Active EVS codec instances.
XMS Server Codec G.722 Active	Active G.722 codec instances.
XMS Server Codec G.723 Active	Active G.723 codec instances.
XMS Server Codec G.729 Active	Active G.729 codec instances.
XMS Server Codec G.726 Active	Active G.726 codec instances.
XMS Server Codec GSM Active	Active GSM codec instances.
XMS Server Codec GSM-EFR Active	Active GSM-EFR codec instances.
XMS Server Codec iLBC Active	Active iLBC codec instances.
XMS Server Codec Opus Active	Active Opus codec instances.
XMS Server Codec PCMA Active	Active PCMA codec instances.
XMS Server Codec PCMU Active	Active PCMU codec instances.
XMS Server Codec H.263 Active	Active H.263 codec instances.
XMS Server Codec H.263-1998 Active	Active H.263-1998 codec instances.

Name	Description
XMS Server Codec H.263-2000 Active	Active H.263-2000 codec instances.
XMS Server Codec H.264 Active	Active H.264 codec instances.
XMS Server Codec MP4-ES Active	Active MP4-ES codec instances.
XMS Server Codec VP8 Active	Active VP8 codec instances.
XMS Server Codec VP9 Active	Active VP9 codec instances.
XMS Server Lic BA Active	Active Basic Audio licenses.
XMS Server Lic BA Max	Maximum Basic Audio licenses.
XMS Server Lic GSM-AMR Active	Active GSM-AMR licenses.
XMS Server Lic GSM-AMR Max	Maximum GSM-AMR licenses.
XMS Server Lic HD-Voice Active	Active HD-Voice licenses.
XMS Server Lic HD-Voice Max	Maximum HD-Voice licenses.
XMS Server Lic LBR Active	Active LBR licenses.
XMS Server Lic LBR Max	Maximum LBR licenses.
XMS Server Lic FAX Active	Active Fax licenses.
XMS Server Lic FAX Max	Maximum Fax licenses.
XMS Server Lic MRCP Active	Active MRCP licenses.
XMS Server Lic MRCP Max	Maximum MRCP licenses.
XMS Server Lic MSRP Active	Active MSRP licenses.
XMS Server Lic MSRP Max	Maximum MSRP licenses.
XMS Server Lic Adv-Video Active	Active Adv-Video licenses.
XMS Server Lic Adv-Video Max	Maximum Adv-Video licenses.
XMS Server Lic HR-Video Active	Active HR-Video licenses.
XMS Server Lic HR-Video Max	Maximum HR-Video licenses.
XMS Server SIP Rcv BYE	Received SIP BYE requests.
XMS Server SIP Rcv INVITE	Received SIP INVITE requests.
XMS Server SIP Sent BYE	Sent SIP BYE requests.

Name	Description
XMS Server SIP Sent INVITE	Sent SIP INVITE requests.
XMS Server SIP Rcv Responses	Received SIP responses.
XMS Server SIP Rcv Resp INVITE 2xx	Received INVITE response 2xx.
XMS Server SIP Sent Responses	Sent SIP responses.
XMS Server SIP Sent Resp INVITE 2xx	Sent INVITE response 2xx.
XMS Server SIP Sent Resp INVITE 486	Sent INVITE response 486.
XMS Server SIP Sent Resp INVITE 503	Sent INVITE response 503.
XMS Server Conference Active	Active conference resources.
XMS Server Conference MCU Active	Active MCU conference resources.
XMS Server Conference MCU Attempts	MCU conference creation attempts.
XMS Server Conference MCU Failures	MCU conference creation failures.
XMS Server Conference SFU Active	Active SFU conference resources.
XMS Server Conference SFU Attempts	SFU conference creation attempts.
XMS Server Conference SFU Failures	SFU conference creation failures.
XMS Server Conference Party Active	Active conference parties.
XMS Server Conference Party Media Active	Active media operations on a conference.
XMS Server Media Active	Active media operations.
XMS Server Play Active	Active media play operations.
XMS Server Play Attempts	The media play attempts.
XMS Server Play Failures	The media play failures.
XMS Server Record Active	Active media record operations.
XMS Server Record Attempts	The media record attempts.
XMS Server Record Failures	The media record failures.
XMS Server FAX Session Active	Active fax sessions.
XMS Server FAX Session Attempts	The fax session attempts.
XMS Server FAX Session Failures	The fax session failures.

Name	Description
XMS Server MRCP Session Active	Active MRCP sessions.
XMS Server MRCP Session Attempts	MRCP session attempts.
XMS Server MRCP Session Failures	MRCP session failures.
XMS Server RTP Session Active	Active RTP sessions.
XMS Server RTP Session Attempts	RTP session attempts.
XMS Server RTP Session Failures	RTP session failures.
XMS Server SIP Session Active	Active SIP sessions.
XMS Server SIP Session (in) Attempts	Incoming SIP session attempts.
XMS Server SIP Session (in) Failures	Incoming SIP session failures.
XMS Server SIP Session (out) Attempts	Outgoing SIP session attempts.
XMS Server SIP Session (out) Failures	Outgoing SIP session failures.
XMS Server WebRTC Session Active	Active WebRTC sessions.
XMS Server WebRTC Session (in) Attempts	Incoming WebRTC session attempts.
XMS Server WebRTC Session (in) Failures	Incoming WebRTC session failures.
XMS Server WebRTC Session (out) Attempts	Outgoing WebRTC session attempts.
XMS Server WebRTC Session (out) Failures	Outgoing WebRTC session failures.
XMS Server Callgroup Calls Active	Active callgroups.

XMS System

The following table lists the counters used for XMS System:

Name	Description
XMS System SIP Session Active	Active SIP sessions.
XMS System SIP Session (in) Attempts	Incoming SIP session attempts.
XMS System SIP Session (in) Failures	Incoming SIP session failures.
XMS System SIP Session (out) Attempts	Outgoing SIP session attempts.
XMS System SIP Session (out) Failures	Outgoing SIP session failures.
XMS System SIP Rcv BYE	Received SIP BYE requests.

Name	Description
XMS System SIP Rcv INVITE	Received SIP INVITE requests.
XMS System SIP Sent BYE	Sent SIP BYE requests.
XMS System SIP Sent INVITE	Sent SIP INVITE requests.
XMS System SIP Rcv Responses	Received SIP responses.
XMS System SIP Rcv Resp INVITE 2xx	Received SIP INVITE responses 2xx.
XMS System SIP Sent Responses	Sent SIP responses.
XMS System SIP Sent Resp INVITE 2xx	Sent SIP INVITE responses 2xx.
XMS System SIP Sent Resp INVITE 486	Sent SIP INVITE responses 486.
XMS System SIP Sent Resp INVITE 503	Sent SIP INVITE responses 503.