



Dialogic® PowerMedia™ XMS

Installation and Configuration Guide

Copyright and Legal Notice

Copyright © 2012-2016 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 6700 Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. **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, Dialogic Blue, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, PowerVille, PowerNova, MSaaS, ControlSwitch, I-Gate, Mobile Experience Matters, Network Fuel, Video is the New Voice, Making Innovation Thrive, Diastar, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, NaturalAccess and Shiva, 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 6700 Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. 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	11
Related Information	11
2. PowerMedia XMS Installation	12
Installing PowerMedia XMS	12
System Requirements	12
Supported Virtual Machines.....	13
Available Application Technologies	13
Supported Web Browsers.....	13
SIP Softphone	13
PowerMedia XMS Installation Package Policy	14
ISO Method	15
Getting and Preparing the .ISO File.....	16
Installing the Operating System from the DVD	16
RPM Method.....	16
Reserved Ports	17
RPM Installation and Script Options.....	18
3. PowerMedia XMS Admin Console	20
Using PowerMedia XMS Admin Console.....	20
CentOS HTTPS Setup for Console Use	20
Guidelines for Installing a Permanent Security Certificate	21
Console Login	22
4. PowerMedia XMS Configuration	23
Configuring PowerMedia XMS	23
System	24
General	24
Services	25
Mode.....	26
Time	27
Backup/Restore	28
Upgrade	29
NFS Mount Points	30
Maintenance	30
Account Manager	31
Diagnostics	32
Audit Logs	33
Network	34
Interface Configuration.....	34
DNS Configuration	36
NAT Configuration	36
Proxy Configuration	37
License	38
Add a License.....	39
Delete a License	39
MSML.....	39
MSML Configuration	39
MSML Advanced Configuration.....	43
MRCP Client.....	44
Global Configuration	44
Speech Server Configuration.....	45

HTTP Client.....	47
NETANN	48
VXML	48
VXML Interpreter Configuration	49
VXML Application Configuration	53
RESTful API	54
Port	54
RESTful Services for IPv6	55
Application ID	55
MSRP.....	55
Protocol	56
SIP	56
RTP.....	59
Codecs.....	60
Enable/Disable Audio Codecs	60
Enable/Disable Video Codecs.....	61
Routing	62
Application ID	63
Tones	63
Add a Tone	64
Modify a Tone	65
Delete a Tone.....	65
Media.....	65
Media Configuration	65
Media Management.....	66
Monitor	68
Dashboard	68
Call Groups.....	69
Graphs	70
Configuration	74
SNMP.....	75
SNMPD Services for IPv6	75
Trap Destinations	75
SNMP V2c Communities.....	77
SNMP V3 Users.....	78
High Threshold Configuration	79
CDR.....	80
Access to CDR Files.....	81
Options	82
General/Meter-Dashboard Page Polling Timeout (ms).....	82
Header Polling Timeout (ms).....	82
WebGUI Session Timeout (sec)	82
Downloads.....	83
5. PowerMedia XMS Troubleshooting	84
RemoteRtfTool	84
Rtf Configuration Manager	86
PowerMedia XMS Log Files.....	89
Linux RTC Device Verification.....	90
Contacting Dialogic Technical Services and Support	91
6. XMSTool RESTful Utility.....	92
XMSTool RESTful Utility.....	92
Call Control Models	92

Prerequisites	93
Starting XMSTool.....	93
XMSTool Utility Modes	94
Demo/Simple Mode	94
Accessing XMSTool using CLI	95
Advanced Mode.....	96
Basic Operation and Commands	99
Receiving an Inbound Call	99
Making an Outbound Call.....	100
Playing a File into a Call	100
Establishing a Conference	101
Additional XMSTool Commands	103
Using XMSTool to Record Macros/Demos	105
7. CLI Command Scripts	107
Script Location	107
Mode	107
Start/Stop Service and Application	107
Check Status of Service	107
Check/Install License	108
MSML Configuration	109
Tone Configuration	110
Codec Configuration.....	111
8. Third Party ASR and TTS Engine Notes.....	115
Nuance	115

Revision History

Revision	Release Date	Notes
05-2704-012 (Updated)	May 2016	Appendix A: SNMP : Updated the Enterprise (proprietary) Traps section.
05-2704-012 (Updated)	April 2016	Removed WebRTC support.
05-2704-012 (Updated)	October 2015	VXML : Updated the default value of the initial URI in the VXML Interpreter Configuration section, updated the procedure to configure the VXML Application Configuration parameters, and added a note to the VXML Application Configuration section.
05-2704-012 (Updated)	September 2015	PowerMedia XMS Installation : Updated Reserved Ports . PowerMedia XMS Admin Console : Updated Guidelines for Installing a Permanent Security Certificate .
05-2704-012 (Updated)	June 2015	System : Added details for filter pattern to Audit Logs page. Network : Added details for Remote NAT Traversal parameter to NAT Configuration page. Protocol : Added Key Rotation parameter to RTP page.
05-2704-012	February 2015	Updates to support PowerMedia XMS Release 2.4. Installing PowerMedia XMS : Updated list of supported processors. System : Added viewer option to Account Manager page. Added new Audit Logs page. Network : Added new Proxy Configuration page. License : Updated to include MRB in the licensed features. HTTP Client : Added Low Speed Threshold and Low Speed Timeout parameters to HTTP Client Configuration page. MSRP : Removed Max Sessions parameter from MSRP Configuration page. Protocol : Added Enable SIP Precondition parameter to SIP page. Added SRTP parameters to RTP page. Codecs : Added Video Encoder Sharing parameter to Video page. Monitor : Updated Graphs page with different views for

Revision	Release Date	Notes
		<p>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 A: SNMP: Added new traps to Enterprise (proprietary) Traps table. Added new variables to Enterprise (proprietary) Variables table.</p> <p>Appendix B: CDR: Added new section.</p>
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>

Revision	Release Date	Notes
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 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 A: 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> <p>MRCP Client: Updated note about MRCP sessions.</p> <p>Third Party ASR and TTS Engine Notes: Added new section.</p>

Revision	Release Date	Notes
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>

Revision	Release Date	Notes
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 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.</p>
05-2704-003	August 2012	<p>RPM Method: Added information about the perl-core package.</p> <p>XMSTool RESTful Utility: Updated the Starting XMSTool and Demo/Simple Mode sections.</p>
05-2704-002	July 2012	<p>Updates to support PowerMedia XMS Release 1.1. This is a 64-bit only release.</p> <p>RPM Method: Added new section.</p> <p>Configuring PowerMedia XMS: Added new Time and Backup/Restore pages to Systems menu. Added new Network menu. Renamed the Interface menu to Protocol.</p> <p>XMSTool RESTful Utility: Added new section.</p>
05-2704-001	March 2012	Initial release of this document.
Last modified: May 2016		

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").

Related Information

See the following for additional information:

- PowerMedia XMS 2.4 documentation at <http://www.dialogic.com/manuals/xms/xms2.4.aspx>.

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-2.4.xxxx-x86_64.iso* and *dialogic_xms_2.4.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).

Note: WebRTC functionality is no longer supported on XMS 2.4 due to fundamental changes in the newer versions of Chrome and Firefox. For any further WebRTC work, use XMS 3.0 or later.

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	Note: 32-bit operating systems are not supported. Community ENTerprise Operating System (CentOS) 6.4 (provided with the ISO Method installation) Red Hat Enterprise Linux (RHEL) 6.4 Oracle Enterprise Linux (OEL) 6.4 Note: The <i>perl-core-5.10.1-xxxxx.x86_64.rpm</i> is required if using the RPM Method installation.
Processor	Minimum: Intel Xeon E5-1620 Quad-Core (3.60 GHz, 1600 MHz, 10 MB Cache), Intel QPI (0 GT/s) for low end solutions Recommended: Intel Xeon E5-2665 Dual Octal-Core (2.40 GHz, 1333 MHz, 20 MB Cache), 2 Intel QPI (8 GT/s) or better for performance systems
Ethernet	Single or Dual NIC 1000Base-TX (RJ-45)
Memory	Minimum: 8 GB RAM Recommended: 16 GB RAM or higher
Storage	Minimum: 250 GB HDD Recommended: 2 TB HDD for advanced logging

Item	Requirement
<p>Note: The recommended server configuration is applicable for higher density audio solutions of 1500 or greater sessions, video transcoding solutions, or solutions utilizing virtualization.</p>	

Supported Virtual Machines

The supported virtual machines (VM) are as follows:

- VMWare ESXi 5.x
- Kernel Virtual Machine (KVM)
- Oracle VM
- XenServer VM

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 also restrict the number of VMs hosted on a single platform to facilitate the real-time low-latency scheduling demands required for high quality media processing. Density capacity in virtual environments may vary and are generally a factor of the host platform capacity and the number of VMs running PowerMedia XMS. Generally, the aggregate density of all VMs running PowerMedia XMS will be less than the bare metal capacity of the platform. Testing has shown hypervisor overhead to reduce density by 15-20 percent. Additionally, running more VMs requires extra overhead for hypervisor scheduling of resources between real-time systems. It is highly recommended to limit to 1-2 VMs per physical system as there is a higher processing overhead associated with more than 2 VMs per physical server system due to hypervisor switching or packet scheduling.

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

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 core package versions that PowerMedia XMS uses (see list below) where it is recommended by Dialogic to stay at those versions, as moving to later versions may have undesirable effects. However, if an update to one of such core package versions is required due to a security issue, it is recommended to test all updates prior to deploying on production servers.

These are the following core packages:

- zeromq.i386
- xerces-c.i686
- fcgi.i686
- lighttpd lighttpd-fastcgi spawn-fcgi js.i686
- libwebsockets.i386
- ImageMagick.i686
- ImageMagick-c++ .i686
- ilbc opus
- libmongodb.i686
- mongodb-org-server
- mongodb-org-shell
- mongodb-org-tools

ISO Method

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.

This installation 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 Preparing 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.

Installing the Operating 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.

The installation requires little interaction. The main task is setting up the IP characteristics for the PowerMedia XMS. The IP characteristics are set at the start of the installation using a text-based setup tool and are handled as follows:

- The default setting is to set up an Ethernet interface (eth0) 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.
- Eth0 may also be given a static IP address. This option is preferable when setting up a server. Set the IP address, Netmask and Gateway, as well as the DNS server address if desired.

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.

Once the IP characteristics are complete, the remainder of the installation is "hands off". Once 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

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.

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 (for example, 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. 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.

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	10000-10010
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

Service	Port
T.38 Fax	56500-56999
WebUI (nodecontroller, lighttpd, httpd)	81, 10443, 9004 (lighttpd) 10080 (nodecontroller)

RPM Installation and Script Options

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](#)
- [Mode Options](#)
- [General Options](#)

cfg-xxx Options

These are platform configuration options. They include the following:

```
--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
```

Mode 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

```
-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 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") 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.

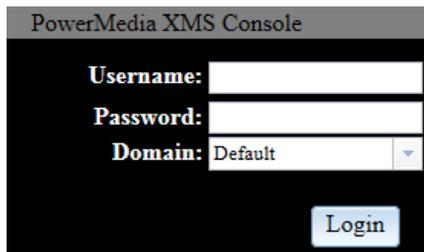
- Secure HTTPS access is provided by mod_ssl, the OpenSSL interface to Apache. The OpenSSL version must be 1.0.1e or higher.
- The configuration file for the SSL Virtual Host is `/etc/httpd/conf.d/ssl.conf`. Entries to modify when a purchased certificate is activated include `SSLCertificateFile`, `SSLCertificateKeyFile`, 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.



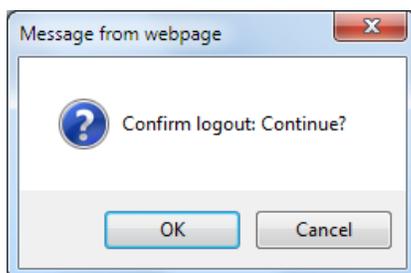
2. Choose from two login options:
 - Enter "superadmin" in the **Username** field and "admin" in the **Password** field to be granted access to all configuration functions available on the Console.
 - Enter "admin" in the **Username** field and "admin" in the **Password** field.
3. Click **Login**. After 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](#)
- [MSML](#)
- [MRCP Client](#)
- [HTTP Client](#)
- [NETANN](#)
- [VXML](#)
- [RESTful API](#)
- [MSRP](#)
- [Protocol](#)
- [Codecs](#)
- [Routing](#)
- [Tones](#)
- [Media](#)
- [Monitor](#)
- [SNMP](#)
- [CDR](#)
- [Options](#)
- [Downloads](#)

Note: The functionality displayed on the side-bar menu will differ between the two operation modes: **Native** (Default) and **MSML** (Legacy).

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](#)
- [Mode](#) (visible only to superadmin)
- [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	Mode	Time	Backup/Restore	Upgrade	NFS Mount Points	Maintenance	Account Manager	Diagnostics	Audit Logs
XMS										
release	svn-trunk									
mode	native									
state	RUNNING									
System										
os release	CentOS release 6.4 (Final)									
os version	Linux 2.6.32-358.el6.x86_64									
uptime	22 days 10 hours 20 minutes 3 seconds									
cpu load	T1=1.09 , T5=1.19 ,T15=1.28									
memory	total:3924772 KB used:741356 KB									
license mac	00:0c:29:d5:95:2c									
System Storage										
/dev/sda2 (/)	total: 8256952 KB, used: 7233448 KB									
/dev/sda1 (/boot)	total: 126931 KB, used: 28183 KB									
/dev/sda5 (/var)	total: 15350776 KB, used: 4239116 KB									
System Time										
time	Wed Feb 18 09:46:04 2015									
zone	America/New_York									

The following information is provided.

Item	Description
XMS	Displays release name, mode, 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. It also displays the MAC address used for licensing. 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 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.

Note: Upon starting up, the Overall Status of the services indicates RUNNING (in green) once the services are initialized successfully. However, it may take up to a minute or longer for PowerMedia XMS to be ready to make/receive calls. Call attempts made during this period may result in a 486 Busy Here response.

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 STOPPED.

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 (e.g., 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.

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

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

Overall Status: **RUNNING**

Graceful Shutdown Timeout (seconds):

Mandatory Services:

Service Name	Description	Status
hmp	Media processing services.	RUNNING
broker	Message routing services.	RUNNING
xmsserver	Signalling and Media services.	RUNNING
appmanager	Application interface.	RUNNING

Optional Services:

Service Name	Description	On Start Enabled	Status
httpclient	HTTP Client.	yes	RUNNING
mrcpclient	MRCP Client.	yes	RUNNING
rtcweb	RtcWeb Signalling Server.	yes	RUNNING
xmsrest	RESTful API for call control and media control.	yes	RUNNING
netann	NETANN Process.	yes	RUNNING
vxml	VXML Process.	yes	RUNNING
msml	MSML Server	yes	RUNNING
msrpservice	MSRP Service.	yes	RUNNING
verification	System/Application Verification Server	yes	RUNNING
perfmanger	Performance Manager	yes	RUNNING
eventmanager	Event Manager	yes	RUNNING
cdrserver	CDR Server	yes	RUNNING

Restart Stop Graceful Shutdown Refresh

Mode

The **Mode** page of the **System** menu displays the operation mode of the PowerMedia XMS, which defaults to **Native** mode.

Note: The **Mode** page is present only when logged in as superadmin.

There are two operational modes:

- **Native** mode is the default and recommended mode used for media control using interfaces such as MSML, NETANN, VXML, RESTful, etc.
- **MSML** mode is a legacy mode provided for users that have not yet migrated from legacy MSML to native MSML.

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

Media Server Operation Mode

Native
 MSML

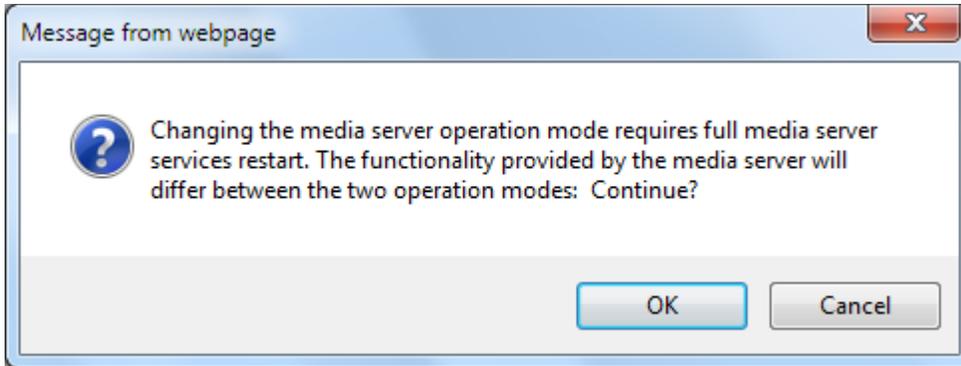
IMPORTANT:

Changing the media server operation mode requires full media server services restart. The functionality provided by the media server will differ between the two operation modes.

Apply

Proceed as follows to switch between modes:

1. Select the **Mode** page.
2. Click the desired radio button: **Native** (Default) or **MSML** (Legacy).
3. Click **Apply**. The following popup appears.



4. Click **OK** to continue or **Cancel** to return to the **Mode** page.

Note: Once **OK** is clicked, PowerMedia XMS will stop and restart automatically.

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

Current date and time: Wed Feb 18 09:52:25 2015

Synchronize date and time over the network

New NTP Server

NTP Servers

Server Address	iburst	MAX Poll	MIN Poll	Action
0.centos.pool.ntp.org	false	10	6	<input type="button" value="Delete"/>
1.centos.pool.ntp.org	false	10	6	<input type="button" value="Delete"/>
2.centos.pool.ntp.org	false	10	6	<input type="button" value="Delete"/>

Note: Double click on the cell to edit

Time Zone: America/New_York

System clock uses UTC

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.
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: System services must be stopped before any changes made on this screen are applied.

Backup/Restore

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

General
Services
Mode
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

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 the **System Backup Files** section.

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.

Upgrade

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

The screenshot shows a web interface with a navigation menu at the top containing: General, Services, Mode, Time, Backup/Restore, Upgrade, NFS Mount Points, Maintenance, Account Manager, Diagnostics, and Audit Logs. The 'Upgrade' tab is selected. Below the menu is a form titled 'Upload System Upgrade Package (*.tgz)'. This form contains a text input field, a 'Browse' button, an 'Overwrite Existing File?' checkbox, and an 'Upload' button. Below this form is a section titled 'System Upgrade Package:' which contains a table with columns for 'File Name', 'Upgrade', and 'Delete'. Underneath the table is an 'Upgrade Status:' label and a text input field containing the word '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.

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.

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

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

Adding a Mount Point

Multiple mounts may be defined. Each is individually added and then displayed in the **NFS Mount Points List** section. Proceed as follows to add a mount point:

1. Complete the **Server Share Location** field. 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. Complete the **Mount Point** field. 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.

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 Mode 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.

Apply

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.
- **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.

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

Accounts:

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

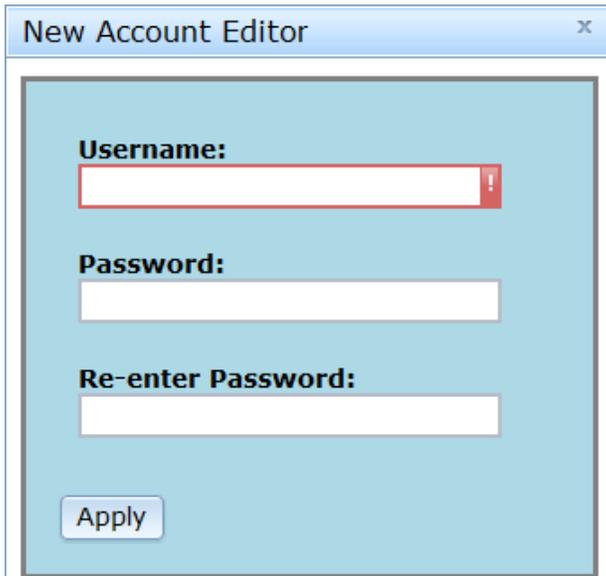
Delete New Edit Refresh

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.

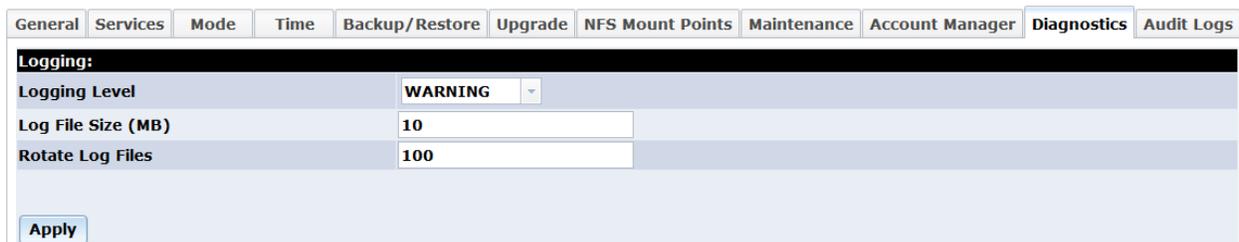


The screenshot shows a dialog box titled "New Account Editor" with a close button (x) in the top right corner. The dialog has a light blue background and contains three input fields: "Username:" with a red exclamation mark icon, "Password:", and "Re-enter Password:". An "Apply" button is located at the bottom left of the dialog.

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.
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.

Diagnostics

The **Diagnostics** page of the **System** menu provides the option to set the logging level for the PowerMedia XMS.



The screenshot shows the "Diagnostics" page in the PowerMedia XMS interface. The page has a navigation bar with tabs: General, Services, Mode, Time, Backup/Restore, Upgrade, NFS Mount Points, Maintenance, Account Manager, Diagnostics, and Audit Logs. The "Diagnostics" tab is active. Below the navigation bar, there is a "Logging:" section with three rows: "Logging Level" set to "WARNING", "Log File Size (MB)" set to "10", and "Rotate Log Files" set to "100". An "Apply" button is at the bottom left.

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

Parameter	Description	Valid Values
Logging		
Logging Level	When troubleshooting issues, additional information can be obtained in the logs by setting the logging level to one of five values.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • ERROR • WARNING • NOTICE • INFO • DEBUG
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.

Click **Apply** to save changes.

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.

Time Stamp	IP Address	UserName	Request Method	Request Path	Request Content Type	Request Content
2015-05-19 07:15:52.792189	10.20.120.4	superadmin	PUT	/services	application/json	{"graceful_shutdown_timeout":120}

1 - 1 of 1

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](#), [NAT Configuration](#), and [Proxy 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
eth0				active	DISABLE

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 adapter with a valid IPv4/IPv6 address is required.

The screenshot shows a configuration window titled "eth0 Configuration". It includes a text field for "Interface Name" with the value "eth0". There are two checkboxes: "Active" (checked) and "Use DHCP" (unchecked). Below these are two columns, "IPv4" and "IPv6", each containing three text input fields for "Address", "Subnet / Prefix", and "Default Gateway". At the bottom right, there are "Apply" and "Cancel" buttons.

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

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.

Interface Configuration		DNS Configuration		NAT Configuration		Proxy Configuration	
General							
Hostname							
DNS search path							
IPv4							
Primary DNS							
Secondary DNS							
Tertiary DNS							
IPv6							
Primary DNS							
Secondary DNS							
Tertiary DNS							
<input type="button" value="Apply"/>							

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	Proxy Configuration
-------------------------	-------------------	--------------------------	---------------------

Direct connection to the Internet
 Behind NAT (Specify gateway IP below)
Public IP address:
 EC2 (public-ipv4)

Remote NAT Traversal

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

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.

Proxy Configuration

The proxy address is configured using the **Proxy Configuration** page.

Interface Configuration	DNS Configuration	NAT Configuration	Proxy Configuration
-------------------------	-------------------	-------------------	----------------------------

Proxy Address:
Proxy Port:

Note: Default value for proxy port is 5060

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

1. In the **Proxy Address** field, enter the address to use as the proxy. Acceptable proxy addresses include IPv4, IPv6, or hostname.
2. In the **Proxy Port** field, enter the port to use for the proxy. Default value is 5060.
3. Click **Apply** to save changes.

License

From the **License** menu, you can view the **License Manager** page. The **License Manager** page provides the options to view available licenses, browse for new licenses, and add, activate, or delete licenses. The primary method of activation is interactive through use of the Console. To activate your license, you must have access to the license file from the License Certificate or via an email from Dialogic.

PowerMedia XMS comes with a 4-port verification license to get started. The name of the license file is *verification.lic*. When another license is enabled, the Verification License automatically becomes inactive.

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

The **License Features** section of the **License Manager** page provides a view of license features and the number of active licenses in use. The **Licenses** section provides a list of licenses available on PowerMedia XMS. To toggle between disabling and enabling the license, click the check box to the left of the license name to select a license, and then click **ENABLE** or **DISABLE** in the **Action** column.

Note: Mixing verification, trial, and permanent licenses are not allowed, however, multiple purchased licenses can be active at the same time. This is known as additive licensing.

License Manager

Licensed Features:

Feature	Active Licenses
Advanced Video	10
Basic Audio	20
FAX	10
GSMAMR Audio	10
HD Voice	10
High Resolution Video	10
LBR Audio	10
MRB	0
MRCP Speech Server	10
MSRP	10

Add License (*.lic)

Overwrite Existing File?

Licenses:

Selection	License Name	Type	Expires	Status	Action
<input type="checkbox"/>	<u>XMS2x_host_pur_5254006F56F4.lic</u>	Purchased	permanent	active	<input type="button" value="DISABLE"/>
<input type="checkbox"/>	<u>verification.lic</u>	Verification	permanent	inactive	<input type="button" value="ENABLE"/>

Add a License

Proceed as follows to add a license in the **Add License** section:

1. Click **Browse** to access available licenses that have been downloaded to the PowerMedia XMS on which your web browser is running.
2. Once you select the license, click **Upload**.
3. Restart services using the **System > Services** page to apply changes to the licensing.

Delete a License

Proceed as follows to delete a license in the **Licenses** section:

1. Click in the check box to the left of the license you wish to delete.
2. Once you select the license, click **Delete**.
3. Restart services using the **System > Services** page to apply changes to the licensing.

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:			
MSML Version:	1.1		
Content Type:	xml		
Encoding:	utf-8		
Schema Validation:	<input type="checkbox"/>		
Media Parameters:			
HTTP Caching:	<input type="checkbox"/>		
Media Mode Selection:	<input checked="" type="checkbox"/> Audio	<input checked="" type="checkbox"/> Video	<input type="checkbox"/> Message
Conferencing Parameters:			
Enable AGC By Default:	<input type="checkbox"/>		

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

Parameter	Description	Valid Values
MSML (RFC5707) Protocol General		
MSML Version	Specifies the MSML version used by the media server.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • 1.0 • 1.1 (default)
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
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
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. 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.	Click one or more check boxes to enable or disable each valid media value: <ul style="list-style-type: none"> • Audio • Video • Message Note: The interaction between the license, codec, and media mode parameter combinations are shown in the Media Mode Combinations table.
Conferencing Parameters		
Enable AGC By Default	Enables automatic gain control.	Click the check box to enable or disable AGC by default. This is disabled by default.

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.
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.

License	Codecs	Media Mode	Delayed Offer Call Result
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):	RFC 5707 <input type="button" value="v"/>
DTMF Start Timer:	<input type="checkbox"/>
DTMF Detection Mode:	RFC2833 <input type="button" value="v"/>

Alarms:

RTP Timeout:	<input type="checkbox"/>
RTCP Timeout:	<input type="checkbox"/>

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 Detection Mode** field, use the drop-down list to select the value. Valid values are RFC2833, IN-BAND, or SIP INFO.
4. Click **Apply** to save changes.

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

1. To enable **RTP Timeout**, click the check box.
2. To enable **RTCP Timeout**, click the check box.
3. Click **Apply** to save changes.

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

MRCP Client

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 Client** menu from the Console is used to configure the PowerMedia XMS client side of the MRCP server.

Global Configuration

The **Global Configuration** page is used to configure the MRCP Client.

Global Configuration	
MRCP Client IP Address(es)	0.0.0.0
Connection Retry Interval (seconds)	10000
Connection Retry Count	3
Server Recovery Delay (minutes)	5
Maximum Sessions Count	100
UDP Retransmit Timer (msecs)	100
UDP Retransmit Count	2

Apply

Proceed as follows to configure the **Global Configuration** 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.

- 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.
- 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.
 - 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.
 - Click **Apply** to save changes.

Speech Server Configuration

The **Speech Server Configuration** page is used to configure the speech server.

The screenshot shows the 'Speech Server Configuration' page. At the top, there are two tabs: 'Global Configuration' and 'Speech Server Configuration'. Below the tabs is a table with the following data:

Speech Server Id	Status	Role	Action
undefined	Disable	...	Delete
sample	Disable	primary	Delete

Below the table, there is an 'Add' button.

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

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

The screenshot shows a dialog box titled 'new_server'. It contains the following fields and values:

- 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

At the bottom of the dialog box, there are 'Apply' and 'Cancel' buttons.

- In the **Speech Server Id** field, enter the speech server identification for MRCP.
- 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.

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.

11. Click **Apply** to save changes.

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.

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
Low Speed Threshold (bytes per second)	1
Low Speed Timeout (seconds)	20

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 **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.
5. 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.
6. 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.

NETANN Configuration	
Global Settings:	
Media Type	Audio and Video
Conference Settings:	
Max Conference Parties	500
Max Active Talkers	3
Max Audio Conferences	1000
Max Video Conferences	100
Video Conference Regions	Automatic
<input type="button" value="Apply"/>	

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. Click **Apply** to save changes.

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 type="checkbox"/>	true
Initial URI	<input type="text" value="/var/lib/xms/vxml/www/vxml/index.vxml"/>	
DTMF Mode	<input type="checkbox"/>	RFC2833
Default Input Mode	<input type="checkbox"/>	dtmf voice
Max Channels	<input type="text" value="2000"/>	
VXML App Logs Enabled	<input type="checkbox"/>	false
XSI Schema Validation Disabled	<input type="checkbox"/>	false
Default Timeout Settings (seconds):		
ASR Complete Timeout	<input type="text" value="0.8"/>	
ASR Incomplete Timeout	<input type="text" value="1"/>	
Max Speech Timeout	<input type="text" value="15"/>	
Inter-digit Timeout	<input type="text" value="3"/>	
No Input Timeout	<input type="text" value="3.4"/>	
Default Locale Settings:		
Grammar Locale	<input type="text" value="en-US"/>	
Prompt Locale	<input type="text" value="en-US"/>	
Record Locale	<input type="text" value="en-US"/>	
Builtin Locale	<input type="text" value="en-US"/>	
Web Server Settings:		
Static Content Directory	<input type="text" value="/var/lib/xms/vxml/www"/>	
IP Address(es)	<input type="text" value="127.0.0.1"/>	
Port	<input type="text" value="9002"/>	
User Name	<input type="text"/>	
Password	<input type="text"/>	
<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.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • true • false
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
Max Channels	Maximum number of VXML Interpreter channels to be used simultaneously. Each channel runs as a separate thread within the VXML Interpreter executable. Actual resources increase only according to the real needs.	1 - 1024 (depending on machine capabilities)

Parameter	Description	Valid Values
	<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>	
VXML App Logs Enabled	Specifies whether to enable VXML application logging.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • true • false
XSI Schema Validation Disabled	Specifies whether to disable XSI schema validation.	Use the drop-down list to select one of the following valid values: <ul style="list-style-type: none"> • true • false

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.

Parameter	Description	Valid Values
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.

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.
Record Locale	Affects the default storage location of the recordings in the PowerMedia XMS media directories.	Default language is en-US.
Builtin 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.

VXML Application Configuration

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

The screenshot shows a web interface with two tabs: "Vxml Interpreter Configuration" and "VXML Application Configuration". The "VXML Application Configuration" tab is selected. Below the tabs is a table with three columns: "Pattern", "Initial URI", and "Logging". Below the table are three buttons: "Delete", "Add", and "Apply".

To add a new VXML application to the **VXML Application Configuration** page, click **Add**. The following dialog box will appear.

The screenshot shows a dialog box titled "New VXML Application". It has a title bar with a close button (x). The dialog contains three fields: "Pattern" with an empty text box, "Initial URI" with an empty text box, and "Logging" with a dropdown menu showing "true". At the bottom are "Apply" and "Cancel" buttons.

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@examplexms.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 API Configuration

XMS RESTful Web Server Port:

Enable RESTful Services for IPv6

New Application ID

Trusted Application IDs

App Id	Status	Action
app	enable	<input type="button" value="Disable"/> <input type="button" value="Delete"/>

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

Port

The port number is used by the lighttpd web server, which services the RESTful API.

If the service needs to be run on a port other than the default port 81, this may be configured in the **XMS RESTful Web Server Port** field. Enter the new port and click **Apply**.

RESTful Services for IPv6

Click the **Enable RESTful Services for IPv6** check box. This enables RESTful services to bind to an IPv6 address, provided that IPv6 is enabled on the operating system.

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.

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)	0.0.0.0
MSRP Port	2855
TCP Enabled	<input checked="" type="checkbox"/>
TLS Enabled	<input type="checkbox"/>
Max Payload Size	2048
Response delay	30
Connection Timeout	30
Success Report	<input checked="" type="checkbox"/>
Failure Report	yes
File Path	/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 **TCP Enabled** field, click the check box to specify if TCP is enabled.
4. In the **TLS Enabled** field, click the check box to specify if TLS is enabled.
5. 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.
6. In the **Response delay** field, enter the response delay time in seconds. Default value is 30 seconds. Must be greater than 0.
7. In the **Connection Timeout** field, enter the connection timeout in seconds. Default value is 30 seconds. Must be greater than 0.
8. 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.
9. 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.
10. In the **File Path** field, enter the file path for media files. Default value is */var/lib/xms/media/en-US*.
11. In the **Allow Absolute Paths** field, click the check box to specify if absolute paths are enabled.
12. Click **Apply** to save changes.

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 **IPv4 Address**, **IPv6 Address**, **Port**, **Transport**, **Session Timeout (seconds)**, and **Restrict Access to Specified Host** information.

SIP
RTP

IPv4 Address:	DEFAULT
IPv6 Address:	DISABLE
Port:	5060
Transport:	UDP
Session Timeout (seconds):	1800
Enable SIP Precondition	<input type="checkbox"/>
<input type="checkbox"/> Restrict Access to Specified Host	

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 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 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.
Port	<p>Specifies the SIP listening port. Default value is 5060.</p>
Transport	<p>Displays the transport protocol. The following protocols are available from the drop-down list:</p> <ul style="list-style-type: none"> UDP (User Datagram Protocol) TCP (Transmission Control Protocol) UDP_TCP (User Datagram Protocol - Transmission Control Protocol)

Item	Description
Session Timeout (seconds)	Specifies the session timeout in seconds. Default value is 1800.
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.
Restrict Access to Specified Host	Click the check box to restrict access to a specified host.

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.

Restrict Access to Specified Host

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

The screenshot shows a configuration window with two tabs: 'SIP' (selected) and 'RTP'. The 'SIP' tab contains several fields: 'IPv4 Address:' set to 'DEFAULT', 'IPv6 Address:' set to 'DISABLE', 'Port:' set to '5060', 'Transport:' set to 'UDP', and 'Session Timeout (seconds):' set to '1800'. The 'Enable SIP Precondition' checkbox is unchecked. The 'Restrict Access to Specified Host' checkbox is checked. Below this, there is a 'Host Address' field with an 'Add' button. A 'Trusted Host List' section contains an empty list box and a 'Delete' button. At the bottom left, there is an 'Apply' button.

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** and **SRTP** parameters.

SIP	RTP		
Media Engine			
Type Of Service :	<input type="text" value="0"/>		
Interface Name:	<input type="text" value="eth0"/>		
IPv4 Address:	<input type="text"/>	IPv6 Address:	<input type="text"/>
SRTP			
Lifetime:	<input type="text" value="2147483648"/>		
Key Rotation:	<input type="text" value="1"/>		
Accept:	<input checked="" type="checkbox"/>		
Enforce:	<input type="checkbox"/>		
Unencrypted RTP:	<input type="checkbox"/>		
Unencrypted RTCP:	<input type="checkbox"/>		
Window Size Hint:	<input type="text" value="64"/>		
<input type="button" value="Apply"/>			

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

1. 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.
2. In the **IPv4 Address** and **IPv6 Address** fields, select the appropriate IP address from the drop-down list.
3. Click **Apply** to save changes.

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.

Codecs

The **Codecs** menu contains the following tabbed pages: **Audio** and **Video**. On each page, 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.

Audio Video

Name	Status	Action
g722	Enabled	Disable
pcmu	Enabled	Disable
pcma	Enabled	Disable
g726-32	Enabled	Disable
amr	Enabled	Disable
g723	Enabled	Disable
g729	Enabled	Disable
amr-wb	Enabled	Disable
iLBC	Enabled	Disable
opus	Enabled	Disable
gsm	Enabled	Disable
gsm-efr	Enabled	Disable

Apply

Enable/Disable Audio Codecs

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

1. Click the button listed in the **Action** column to toggle between **Disable** and **Enable**.
2. Click **Apply** to save changes. The **Status** column will change to the action you selected.

Audio Video

Name	Status	Action
h264	Enabled	Disable
mp4v-es	Enabled	Disable
h263	Enabled	Disable
h263-1998	Enabled	Disable
h263-2000	Enabled	Disable
vp8	Enabled	Disable

Video Encoder Sharing: Disabled

Apply

Enable/Disable Video Codecs

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

1. Click the button listed in the **Action** column to toggle between **Disable** and **Enable**.
2. Click **Apply** to save changes. The **Status** column will change to the Action you selected.

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.

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

Add

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

Delete **Apply**

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.

Tones

The **Tones** menu opens to the **Basic Tone Definitions** page, which is used to add, modify, and delete tones.

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

Basic Tone Definitions

	Name	Type	Cadence
<input type="button" value="Delete"/>			<input type="button" value="Add"/>

Note: A maximum of 20 tones may be defined.

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 screenshot shows a dialog box titled "New Tone Definition" with a close button (x) in the top right corner. The dialog is divided into several sections:

- Tone Name:** A text input field containing the word "New".
- Tone 1:** A section with two input fields: "Frequency (Hz): 0" and "Tolerance (Hz): 0".
- Tone 2:** A section with two input fields: "Frequency (Hz): 0" and "Tolerance (Hz): 0".
- Cadence:** A section with five input fields: "On Time (ms): 0", "Tolerance (ms): 0", "Off Time (ms): 0", "Tolerance (ms): 0", and "repetitions : 0".

At the bottom of the dialog, there are two buttons: "Apply" and "Cancel".

2. Enter the name of 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

Proceed as follows to delete a tone:

1. On the **Basic Tone Definitions** page, click the check box to the left of the tone you wish to delete.
2. Click **Delete**.

Media

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

Media Configuration

The Media Configuration page is used to configure PowerMedia XMS media file paths.

The screenshot shows a web interface with two tabs: "Media Configuration" (active) and "Media Management". Below the tabs are three configuration fields:

Media File Path:	<input type="text" value="/var/lib/xms/media"/>
Locale:	<input type="text" value="en-US"/>
Allow Absolute Paths:	<input type="text" value="NO"/>

At the bottom left of the configuration area is an "Apply" button.

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

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. Valid values are zh-CN, en-US, or sp-SP.
3. In the **Allow Absolute Paths** field, select **NO** to disable absolute paths or **YES** to enable absolute paths from the drop-down list.

If the **Allow Absolute Paths** field is set to **NO**, 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 set to **YES**, 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:

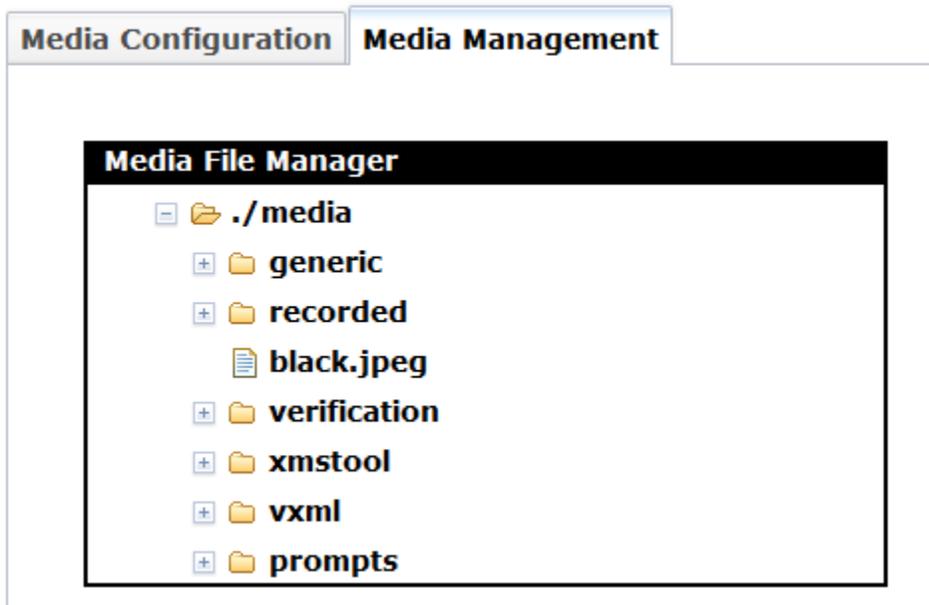
```
<audio uri=file://./verification/main_menu.wav
```

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

Media Management

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

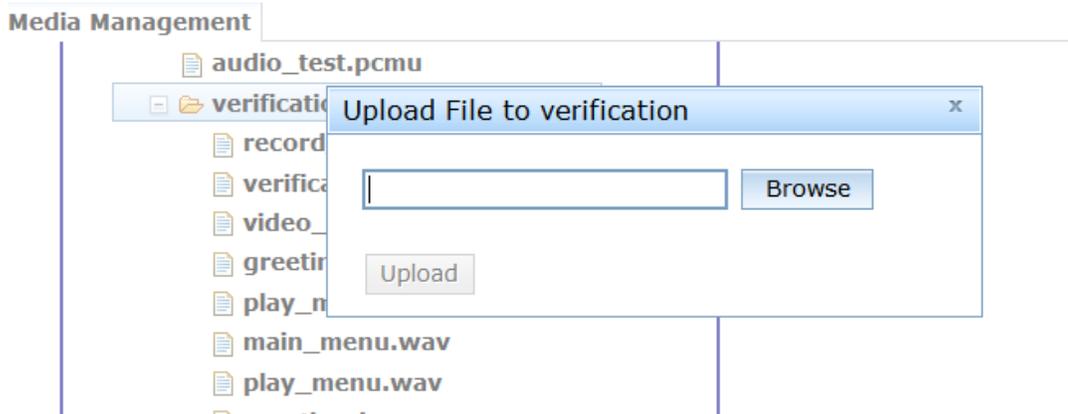
- [Uploading a Media File](#)
- [Deleting a Media File](#)
- [Creating a Media File Directory](#)
- [Deleting a Media File Directory](#)



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.

Monitor

The **Monitor** menu contains the following tabbed pages: [Dashboard](#), [Call Groups](#), [Graphs](#), and [Configuration](#).

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 Graphs Configuration

Licenses	Available	Used	Free	% Used
Basic Audio	250	134	116	53.6
HD Voice	0	0	0	--
GSMAMR Audio	250	96	154	38.4
LBR Audio	0	0	0	--
MRCP Speech Server	0	0	0	--
MSRP	250	1	249	0.4
Advanced Video	30	24	6	80.0
High Resolution Video	0	0	0	--

Resources	Active
Signaling Sessions	210
RTP Sessions	210
Media Transactions	125
Conference Rooms	0
Conference Parties	0
Conference Media Parties	0
ASR / TTS 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
- Active Resources
 - Signaling Sessions
 - RTP Sessions
 - Media Transactions
 - Conference Rooms
 - Conference Parties
 - Conference Media Parties
 - ASR/TTS Sessions

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

Call Groups

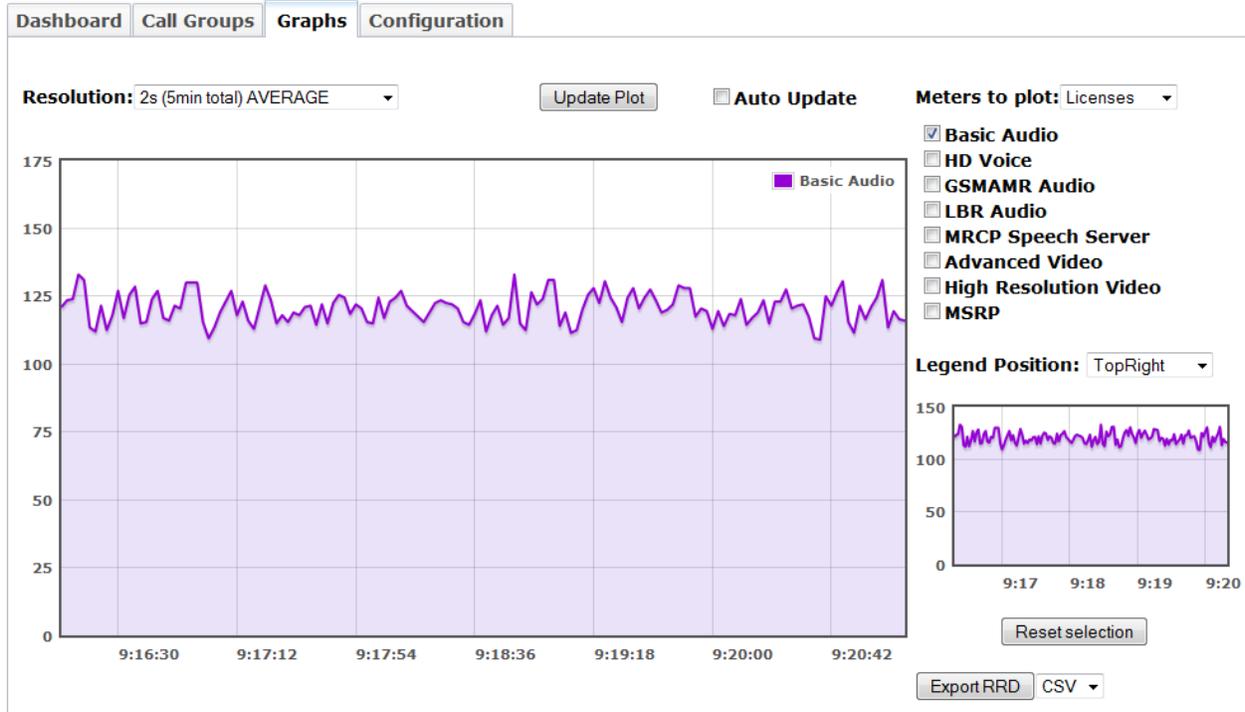
The **Call Groups** page displays the call groups and active SIP legs.



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

Graphs

The **Graphs** page displays and stores previous values of meters, enabling you to view the history of various parameters over a particular period of time (in seconds, minutes, hours, or days).



Meters

Licenses

When **Licenses** is selected in the **Meters to plot** field, the following meters can be displayed on the graph by clicking in the appropriate check box and then clicking on the **Update Plot** button:

- Basic Audio
- HD Voice
- GSMAMR Audio
- LBR Audio
- MRCP Speech Server
- Advanced Video
- High Resolution Video
- MSRP

Resources

When **Resources** is selected in the **Meters to plot** field, the following meters can be displayed on the graph by clicking in the appropriate check box and then clicking on the **Update Plot** button:

- Signaling Sessions
- RTP Sessions
- Media Transactions
- Conference Rooms
- Conference Parties
- Conference Media Parties
- ASR/TTS Sessions

Memory

When **Memory** is selected in the **Meters to plot** field, the following meter can be displayed on the graph by clicking in the appropriate check box and then clicking on the **Update Plot** button: Memory Used (in KBytes).

CPU

When **CPU** is selected in the **Meters to plot** field, the following meters can be displayed on the graph by clicking in the appropriate check box and then clicking on the **Update Plot** button:

- CPU 1 Minute Load Average
- CPU 5 Minute Load Average
- CPU 15 Minute Load Average

Note: The load average graphs are scaled (multiplied) by 100 to show values in integers.

Network

When **Network** is selected in the **Meters to plot** field, the following meters can be displayed on the graph by clicking in the appropriate check box and then clicking on the **Update Plot** button:

- Eth0 Received
- Eth0 Transmitted

Under the Network selection, all available physical Ethernet interfaces are listed. For each of these interfaces, the received and transmitted bytes can be plotted.

Legend

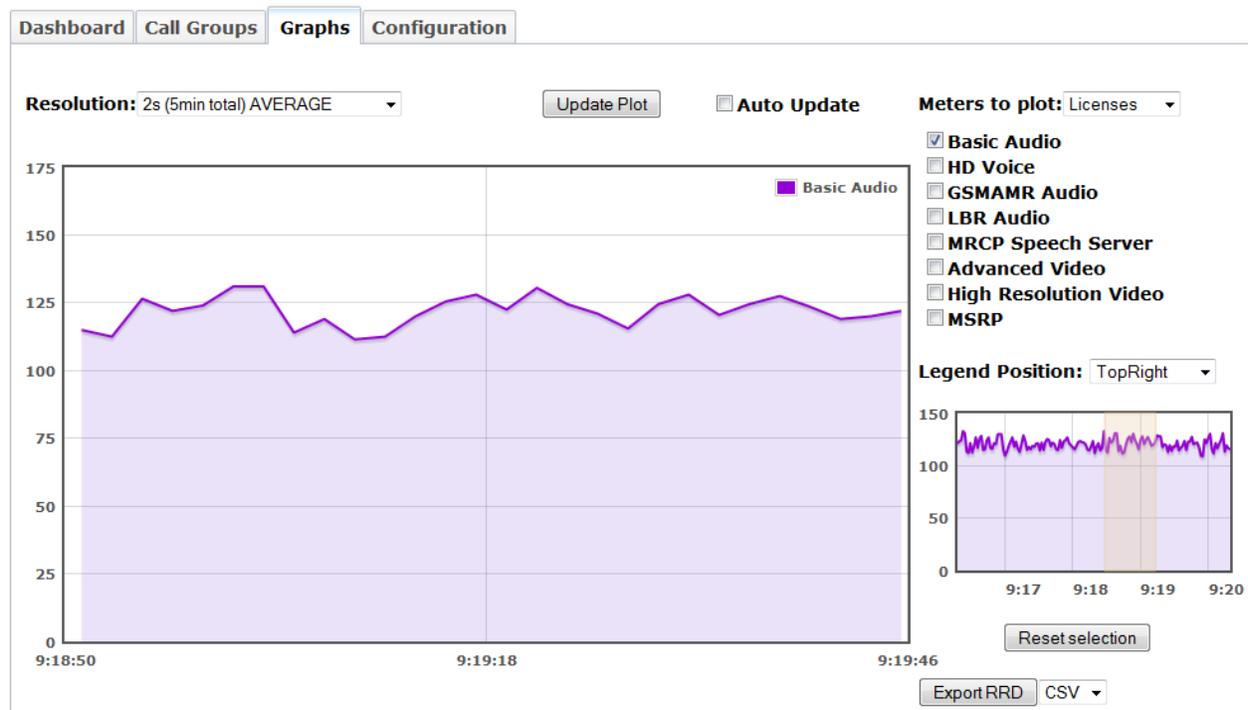
The meters that are checked will appear on the graph. Each meter is represented by a different color as shown in the color key on the graph. The **Legend Position** drop-down list enables you to relocate the color key to different areas of the graph: Top, Bottom, TopRight, BottomRight, or None.

Resolution

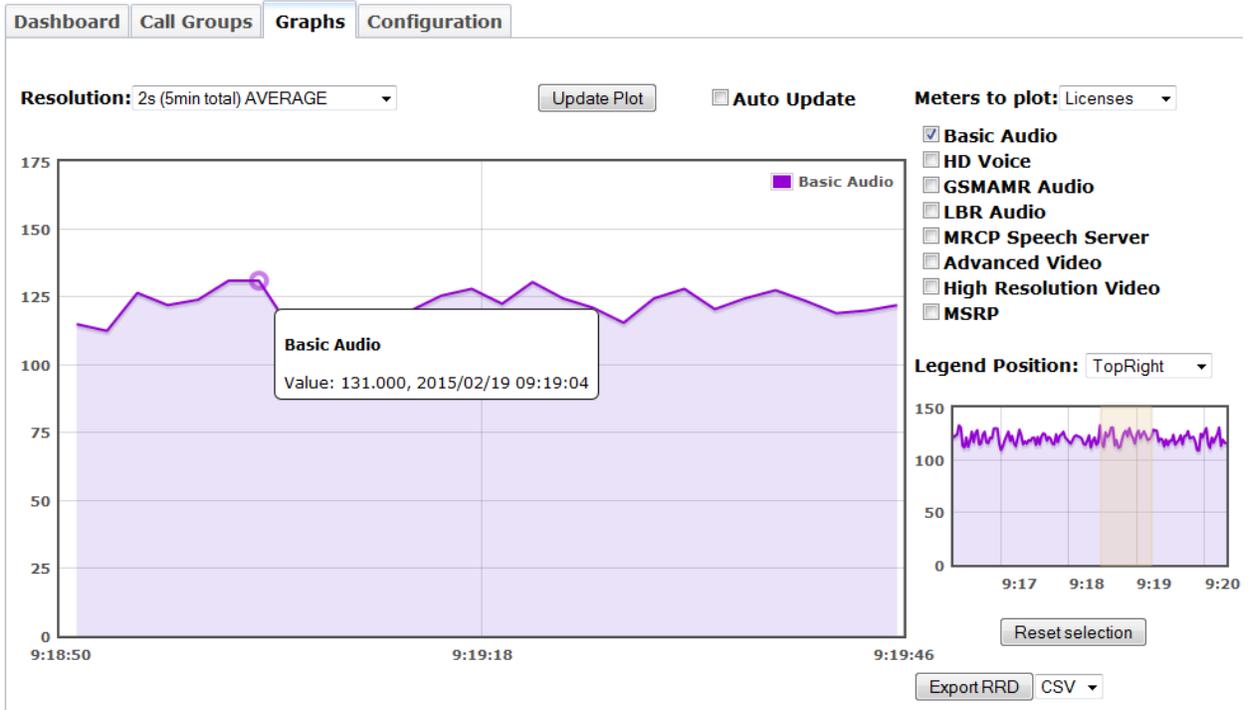
To view the different resolution variables, click the **Resolution** drop-down list and select a resolution. It is possible to view and store data with the following resolutions and durations.

Resolutions	Duration
2 seconds	5 minutes total AVERAGE
60 seconds	60 minutes total AVERAGE
5 minutes	24 hours total AVERAGE
60 minutes	7 days total AVERAGE
2 seconds	5 minutes total MAX
60 seconds	60 minutes total MAX
5 minutes	24 hours total MAX
60 minutes	7 days total MAX

Once a resolution is selected, the values lining the graph's horizontal axis will change based upon your selection. Likewise, the meters plotted on the graph itself will shift accordingly. Click and drag your cursor on the graph to highlight and view a desired selected area. Refer to the example that follows.



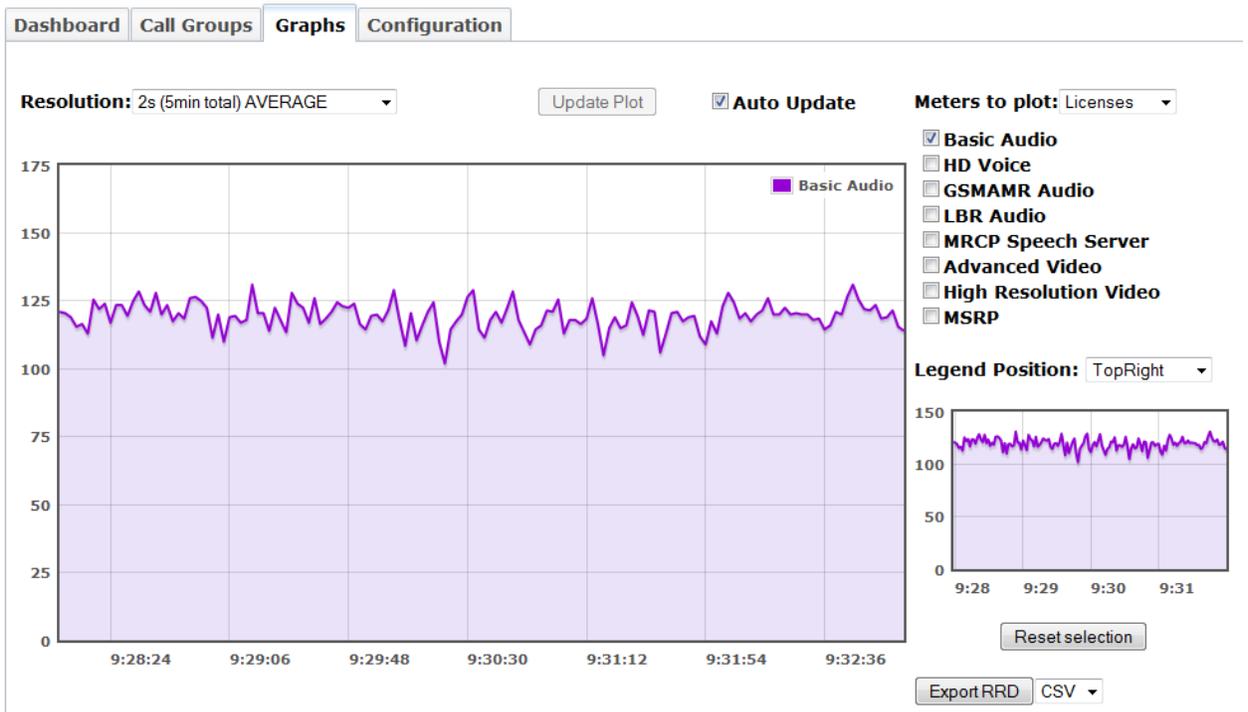
A thumbnail view of the graph is shown to the right of your screen. When you zoom-in on the graph, the thumbnail view will always show the complete graph highlighting the selected area, as shown below. This enables you to know which areas you zoomed into on the graph.



Move the pointer of your mouse over the dominant meter shown on the graph and a box will appear indicating that specific meter's number value.

Click the **Update Plot** button at any time to load the latest meter data onto the graph. Click the **Reset selection** button to reset the entire **Graphs** page back to its original settings.

Auto Update



The **Auto Update** check box can be utilized in the following ways:

- If left unchecked, the graph will be stationary and all the features will work as described above.
- If checked, the graph will be affected in the following ways:
 - The graph will refresh once every 4 seconds.
 - All other features will be usable except for the **Update Plot** button, which will become disabled.
 - If a user makes a selection or zooms in on the graph, the **Auto Update** will stop and the check box will become unchecked. As a result, the graph will stop displaying the zoomed in area.
- If unchecked and a user has selected/zoomed in on an area of the graph, the graph will be affected as follows: If a user clicks on the **Auto Update** check box in this instance, a dialog box will appear asking the user to reset the selection because the **Auto Update** feature can only be used when the graph is not zoomed in on.

Configuration

The **Configuration** page displays the meters that can be enabled. Each check box enables or disables RRD file generation for the corresponding meters. The RRD files are used to generate graphs in the **Graphs** page. If a meter is not checked, its graph will not display in the **Graphs** page.

Dashboard Call Groups Graphs **Configuration**

Select the meters to enable:

XMS Licenses					
Basic Audio	<input checked="" type="checkbox"/>	HD Voice	<input checked="" type="checkbox"/>	GSMAMR Audio	<input checked="" type="checkbox"/>
LBR Audio	<input checked="" type="checkbox"/>	MRCP Speech Server	<input checked="" type="checkbox"/>	Advanced Video	<input checked="" type="checkbox"/>
High Resolution Video	<input checked="" type="checkbox"/>	MSRP	<input checked="" type="checkbox"/>		

XMS Resources					
Signaling Sessions	<input checked="" type="checkbox"/>	RTP Sessions	<input checked="" type="checkbox"/>	Media Transactions	<input checked="" type="checkbox"/>
Conference Rooms	<input checked="" type="checkbox"/>	Conference Parties	<input checked="" type="checkbox"/>	Conference Media Parties	<input checked="" type="checkbox"/>
ASR/TTS Sessions	<input checked="" type="checkbox"/>				

XMS System Stats					
Memory Used	<input checked="" type="checkbox"/>	CPU 1 Minute Load Average	<input checked="" type="checkbox"/>	CPU 5 Minute Load Average	<input checked="" type="checkbox"/>
CPU 15 Minute Load Average	<input checked="" type="checkbox"/>	Eth0 Received	<input checked="" type="checkbox"/>	Eth0 Transmitted	<input checked="" type="checkbox"/>
Io Transmitted	<input type="checkbox"/>	Io Received	<input type="checkbox"/>		

*Changes will require services to be restarted.

Click **Apply** to save changes.

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 A: SNMP](#).

Configuration High Threshold Configuration

SNMPD Services for IPv6

Trap Destinations

Select	Protocol	Destination Host	Port	Version
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		

V2c Communities

Select	Community	Access
<input type="checkbox"/>	Craftsperson	RO
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

V3 Users

Select	User Name	Security Level	Access
<input type="checkbox"/>	Craftsperson	AuthPriv	RO
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	

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 popup window as shown below:

Trap destination	
Protocol	TCP
Destination Host	10.40.2.31
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	10.40.2.31
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	10.1.1.1:162:162:162:162:162:162:162

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.

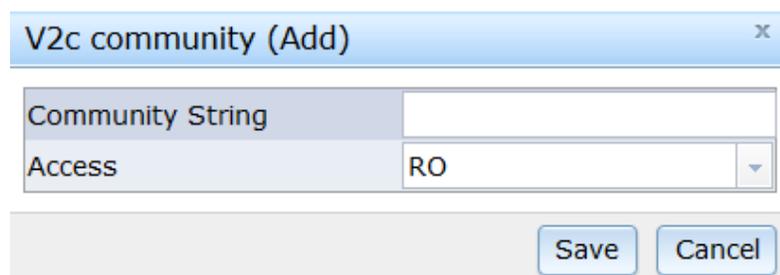
In the **Trap Destination** section, select the trap destination to be deleted (using the check box on the left) and click **Delete**. The selected destination will be deleted.

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.



V2c community (Add) x	
Community String	<input type="text"/>
Access	RO ▼
<input type="button" value="Save"/> <input type="button" value="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) x	
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 ▼

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 sub-system. 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).

High Threshold Configuration	
High Threshold (Percentage Value)	
Basic Audio	75
HD Voice	75
GSM/AMR Audio	75
LBR Audio	75
MRCP Speech Server	75
Advanced Video	75
High Resolution Video	75
CDR Disk Usage	75

Apply

For the purpose of trap generation, the PowerMedia XMS system enables the user to set thresholds in the **High Threshold (Percentage Value)** section for the following meters:

- **Basic Audio** license usage
- **HD Voice** license usage
- **GSM/AMR Audio** license usage
- **LBR Audio** license usage
- **MRCP Speech Server** license usage
- **Advanced Audio** license usage
- **High Resolution Video** license usage
- **CDR Disk Usage** license usage

Enter values (in percentage) for the various meters and click **Apply**. The configured values are committed to the PowerMedia XMS system.

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

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 opens to the **CDR Configuration** page. The **CDR Configuration** page is used to configure the CDR related parameters. This menu is available only when PowerMedia XMS is running in **Native** mode.

CDR Configuration	
Enable CDR	<input checked="" type="checkbox"/>
CDR File Duration (in Hours)	1
Active CDR Age (in Hours)	1
Maximum Disk Space (in MB)	4096

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

1. In the **Enable CDR** field, click the check box to enable generation of CDR.
2. 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.
3. 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.
4. 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).
5. Click **Apply** to save changes.

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 B: CDR](#).

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 need 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
```

Options

The **Options** menu opens to the **Web Console Options** page, which is used to configure or disable the Console's polling timeouts.

Web Console Options

General/Meter-Dashboard Page Polling Timeout (ms):	<input type="text" value="1000"/>	Disable Polling <input type="checkbox"/>	This field controls the General/Meters-Dashboard Page refresh polling rate. Default value is 1 sec or 1000 (ms).
Header Polling Timeout (ms):	<input type="text" value="3000"/>	Disable Polling <input type="checkbox"/>	This field controls the Header refresh polling rate. Default value is 3 sec or 3000 (ms).
WebGUI Session Timeout (Sec):	<input type="text" value="0"/>		This field controls the WebGUI session timeout. Default value is 600 seconds. 0 to disable. Minimum valid timeout value is 30 seconds.

Proceed as follows to configure the **Web Console Options** parameters.

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 to the right of **Disable Polling** and then click **Apply**.

Header Polling Timeout (ms)

This parameter controls the header refresh polling rate. Default value is 3 seconds or 3000 ms. Enter the desired value in the space provided and click **Apply**.

To disable polling timeout, click the check box to the right of **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**.

Downloads

The **Downloads** menu opens to the **Tools** page, which will be updated periodically as additional demos and tools become available.



The **Tools** page contains the following applications to download:

- **Window Logger Manager Tool** unzips the RemoteRtfTool to your local directory. Refer to the [RemoteRtfTool](#) section for more information.
- **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. Refer to the [XMSTool RESTful Utility](#) 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 RemoteRtfTool utility and installation log files available to enhance the user experience. It contains the following topics:

- [RemoteRtfTool](#)
- [PowerMedia XMS Log Files](#)
- [Linux RTC Device Verification](#)

RemoteRtfTool

PowerMedia XMS logs are accessed through the RemoteRtfTool utility.

To use the RemoteRtfTool utility, access the **Downloads > Tools** page from the Console and perform the following procedure:

1. Click the **Window Logger Manager Tool** (*RemoteRtfToolInstaller.msi*) to download and install the file.



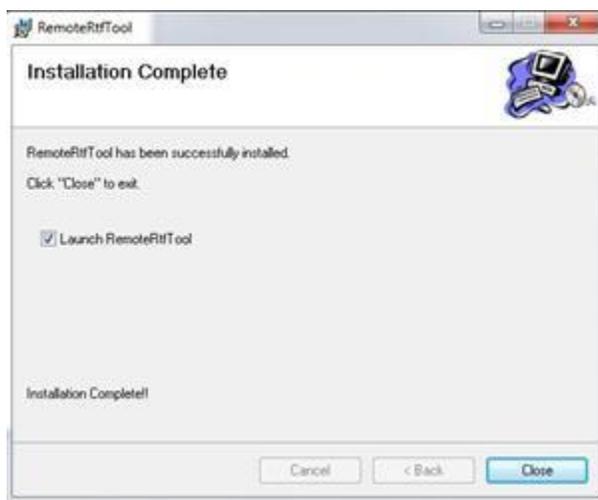
2. Run *RemoteRtfToolInstaller.msi* to start the setup wizard.



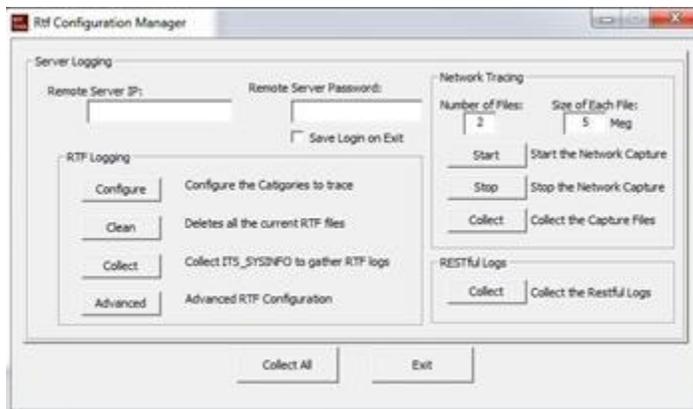
3. Click **Next**.



4. Browse to the folder indicated in the screen capture above and click **Next** to start the installation. When the installation is complete, the following screen appears.



The RemoteRtftool launches and displays the Rtf Configuration Manager window.



Rtf Configuration Manager

The Rtf Configuration Manager contains four sections:

- [Server Logging](#)
- [RTF Logging](#)
- [Network Tracing](#)
- [RESTful Logs](#)

Clicking **Collect All** collects all log files in accordance with the default settings of the PowerMedia XMS. Proceed below to change the default settings.

Server Logging

Proceed as follows to configure the server log:

1. Enter the IP address on which to perform the trace in the **Remote Server IP** field.
2. Enter a valid password in the **Remote Server Password** field.

Note: The password is not the Console password, but rather the combination used for Username: root and Password: powermedia. 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.

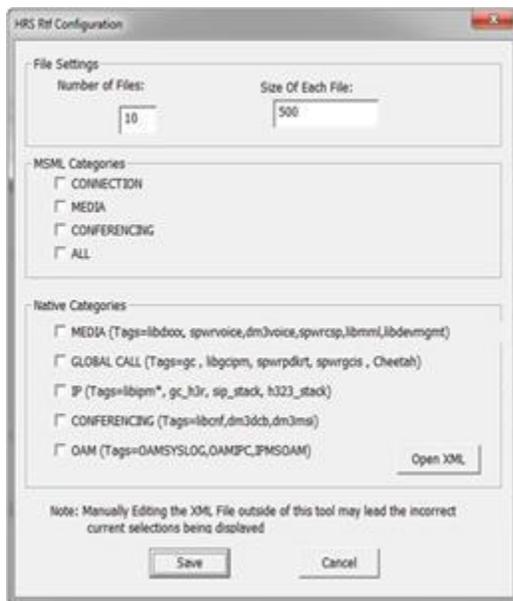
3. Click the check box if you wish to save the login upon exiting the Rtf Configuration Manager.

RTF Logging

The buttons in the RTF Logging section are described below.

Configure

Click **Configure** to configure the categories to trace for both **Native** and **MSML** modes. The following popup appears.



1. In **File Settings** field, enter the number of files to trace and the maximum size of each file.
2. In **MSML Categories** section, click the check box for each MSML Category you wish to trace.
3. In **Native Categories** section, click the check box for each media engine category you wish to trace.
4. Click **Save** to save configuration settings.

Clean

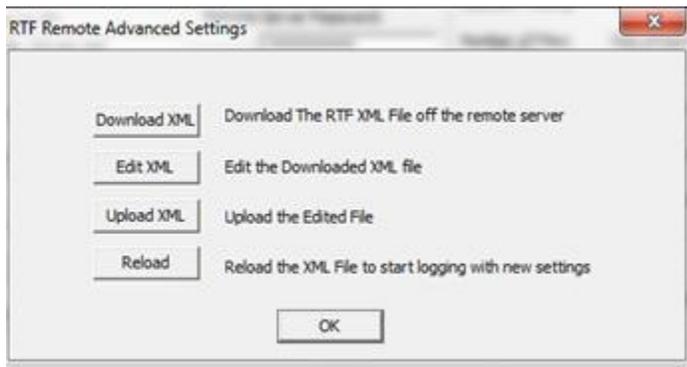
Click **Clean** to delete the currently stored RTF log files.

Collect

Click **Collect** to run **ItsSysinfo** used to gather RTF log files.

Advanced

Click **Advanced** to provide the advanced RTF configuration settings.



- **Download XML** downloads the *RtfConfigLinux.xml* file.
- **Edit XML** navigates to the *RtfConfigLinux.xml* file and opens it for editing.
- **Upload XML** uploads the edited file to PowerMedia XMS.
- **Reload** causes the RTF service to reread and restart RTF logging according to the new settings.

Network Tracing

Number of Files

Enter the number of network files to trace.

Size of Each File

Enter the maximum size of each file.

Start

Click **Start** to begin the network capture.

Stop

Click **Stop** to end the network capture.

Collect

Click **Collect** to collect the captured files and copy the data to the specified location.

RESTful Logs

Click **Collect** to collect the captured RESTful logs and copy the data to the specified location.

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.

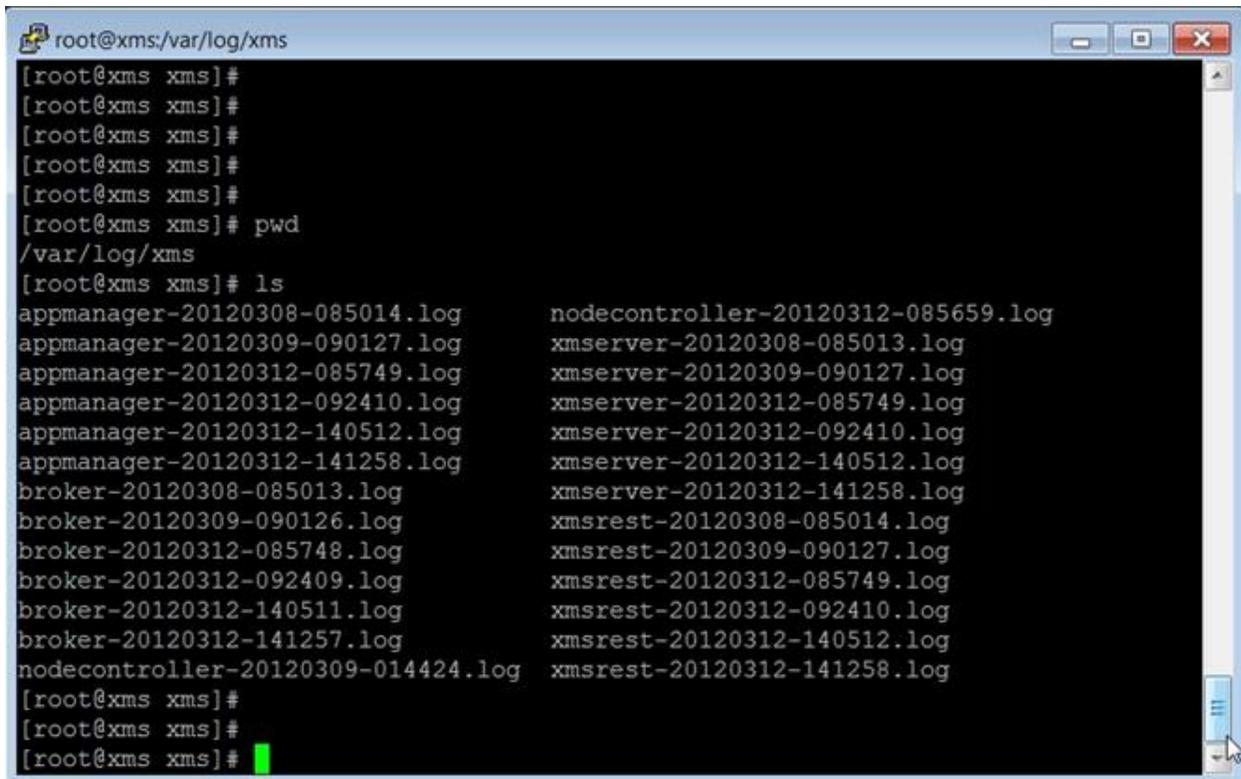
Note: RESTful logs can be collected by choosing "Collect the RESTful Logs" in the [RemoteRtfTool](#) utility available for download in the Console.

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    xmsserver-20120308-085013.log
appmanager-20120312-085749.log    xmsserver-20120309-090127.log
appmanager-20120312-092410.log    xmsserver-20120312-085749.log
appmanager-20120312-140512.log    xmsserver-20120312-092410.log
appmanager-20120312-141258.log    xmsserver-20120312-140512.log
broker-20120308-085013.log        xmsserver-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]#
```

Log File Retention

The logrotate capability in Linux is used to rotate, compress, and/or mail system log files. It is normally run from cron. It can be configured with the file `/etc/logrotate.d/xms`, which is specified in the command line when logrotate is run.

The logrotate program deletes any PowerMedia XMS log files older than seven (7) days. To modify this number, access the PowerMedia XMS logrotate configuration file and change the "maxage" field from 7 to the number of days that you wish to retain the logs.

See the example below.

```
/var/log/xms/*.log {
daily
maxage 7
missingok
rotate 0
postrotate
kill -HUP `cat /var/run/nodecontroller.pid`
kill -HUP `cat /var/run/appmanager.pid`
kill -HUP `cat /var/run/broker.pid`
kill -HUP `cat /var/run/xmsserver.pid`
kill -HUP `cat /var/run/xmsrest.pid`
endscript
}
```

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.

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 from 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.

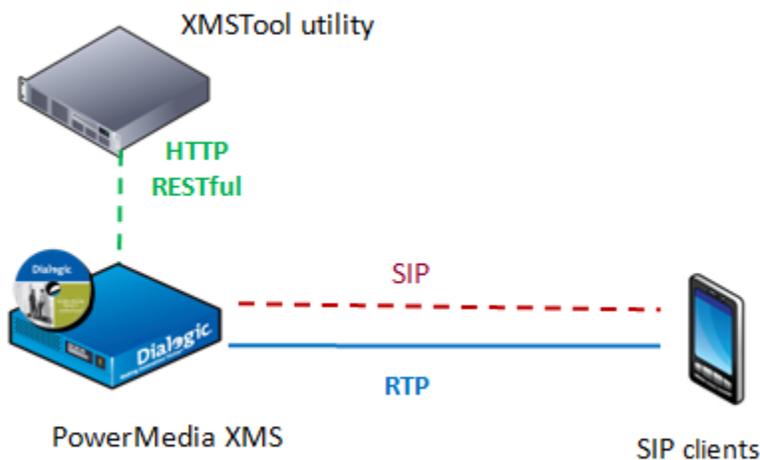
XMSTool is a Java-based test application for passing and receiving RESTful API messages to and from the PowerMedia XMS. Supported for both 1PCC and 3PCC (see the [Call Control Models](#)), it can be used to build and parse individual RESTful messages and can drive and record simple applications. The 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

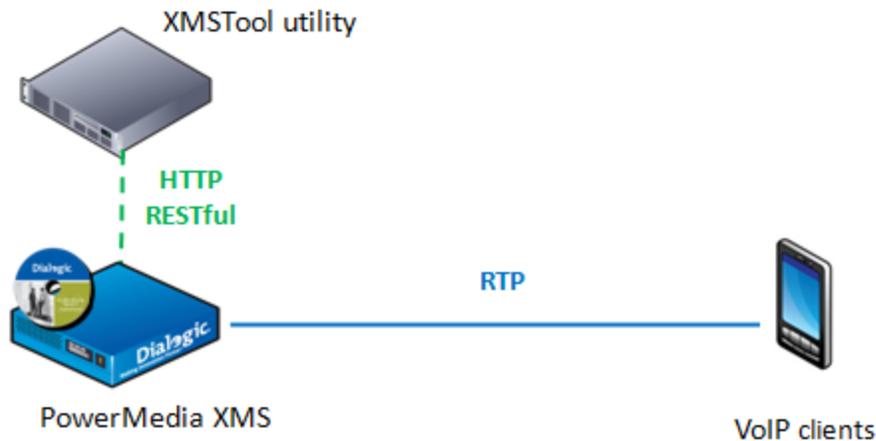
Call Control Models

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.

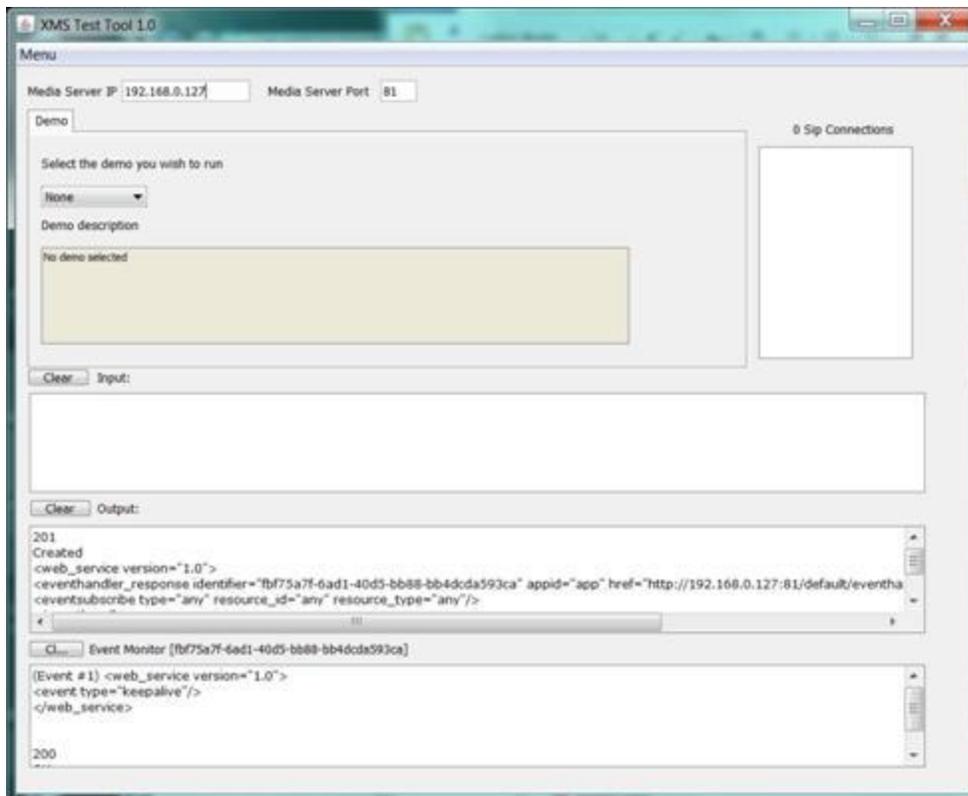
Demo/Simple Mode

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.



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>
```

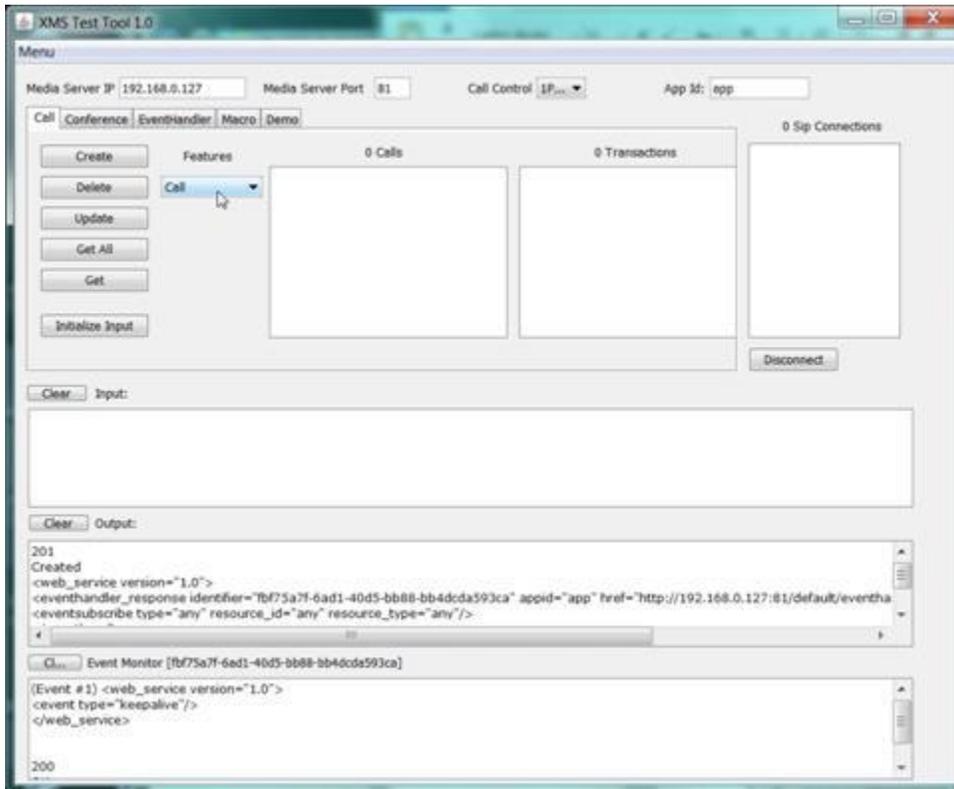
3. Access a scenario by placing a SIP video call to the IP address of PowerMedia XMS using the test name as the SIP username. For example, entering `Sip:play@192.168.1.100` will connect to the PowerMedia XMS at IP address 192.168.1.100 and execute the multimedia file "play" test scenario.
4. Stop XMSTool 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: the Call ID and the 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>

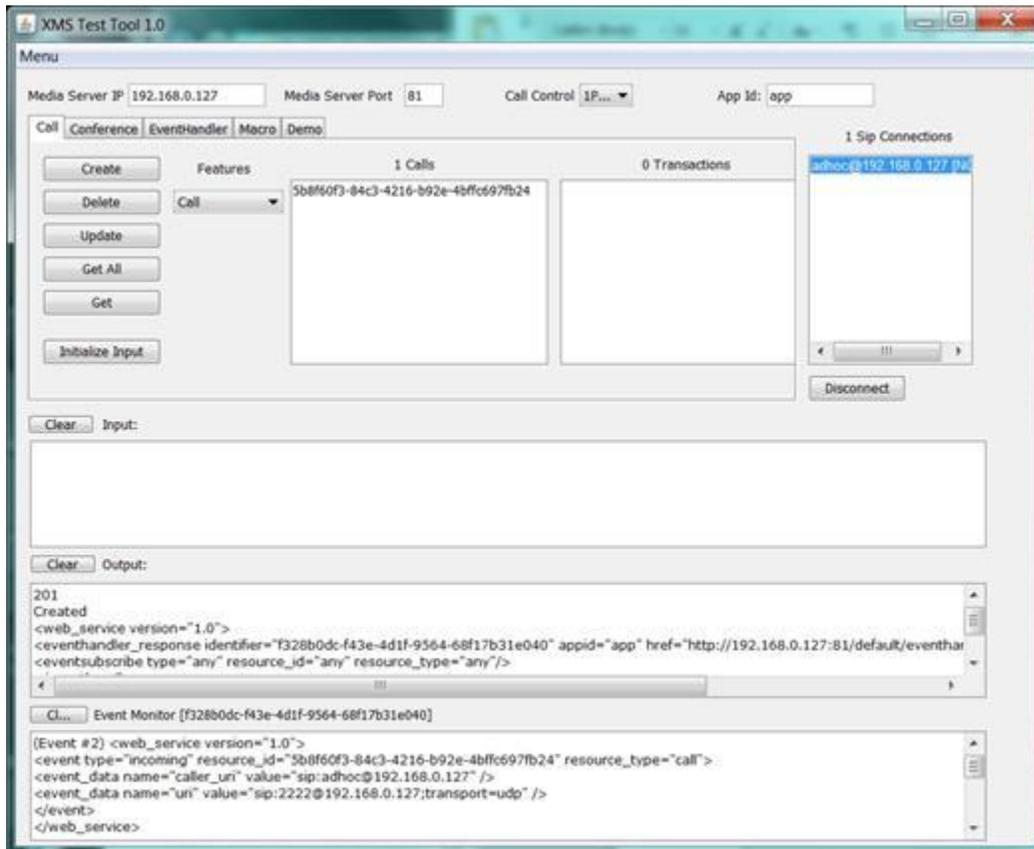
Sequence	Tasks
Delete	<ol style="list-style-type: none"> 1. Select the ID of the call or conference. 2. Click Delete to generate an HTTP DELETE for the selected entity. <p>A 200-series OK reply with no content will be displayed in the Output window.</p>

Basic Operation and Commands

The following sections provide examples of basic commands.

Receiving an Inbound Call

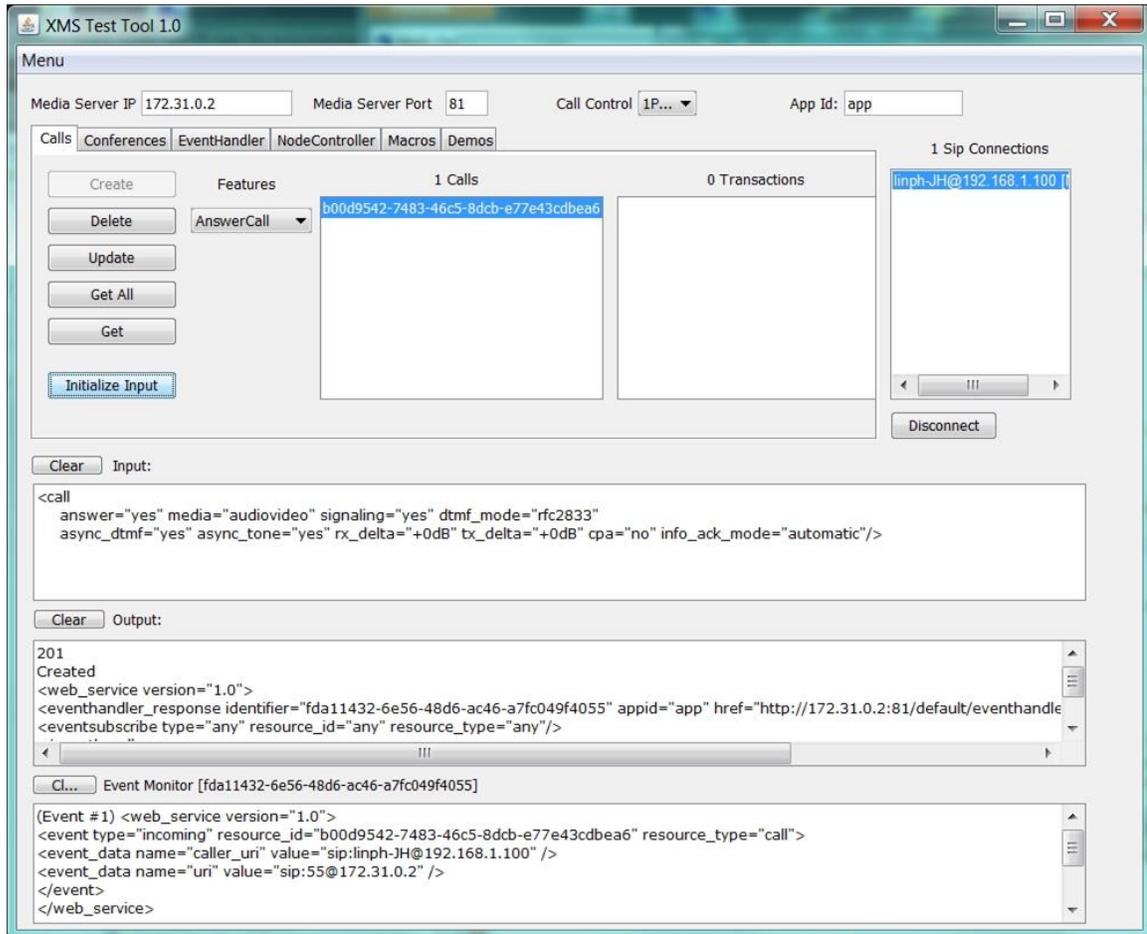
The **Call** tab is used to handle setup and teardown of a call. Inbound calls require a SIP softphone to initiate the call using any SIP username (or extension). When a call is made to the IP address of the PowerMedia XMS, notification of the call is sent to XMSTool and displayed in the Input window 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 if, for example, early media were desired. This would allow a file to be played to the caller before the call is answered.

3. 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.



4. 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:

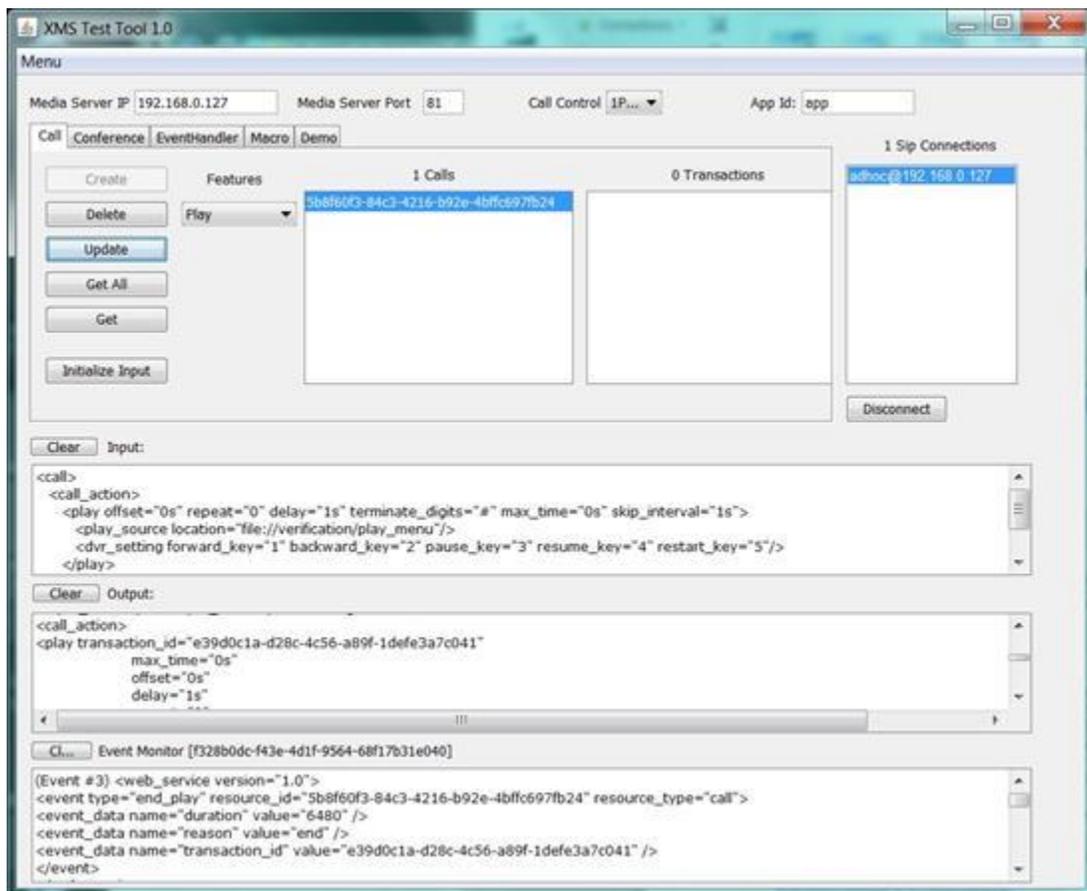
1. Click **Initialize Input** to generate a RESTful call command.
2. Edit the default command. For example, the destination_uri and source_uri should reflect the SIP address of the SIP softphone being called and the PowerMedia XMS, respectively. Other default values may be adjusted if desired.
3. Click **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.

1. 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.

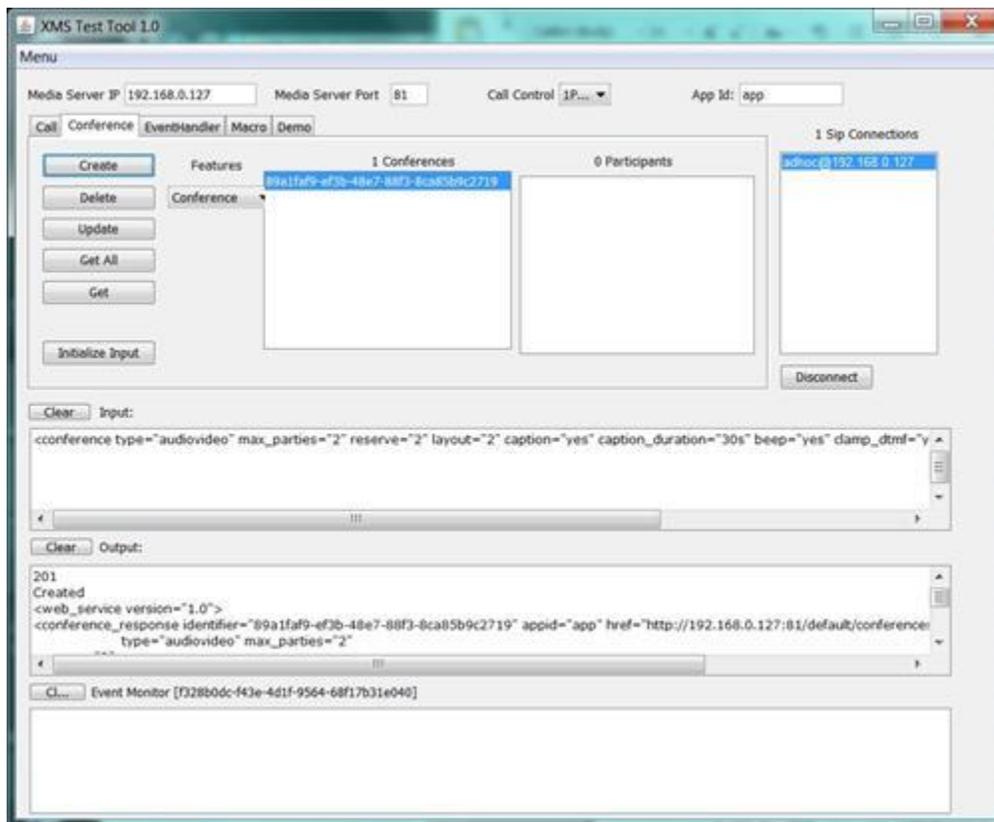


Establishing a Conference

Once a call is idle, a video conference may be started. First, create a conference in which to add the call:

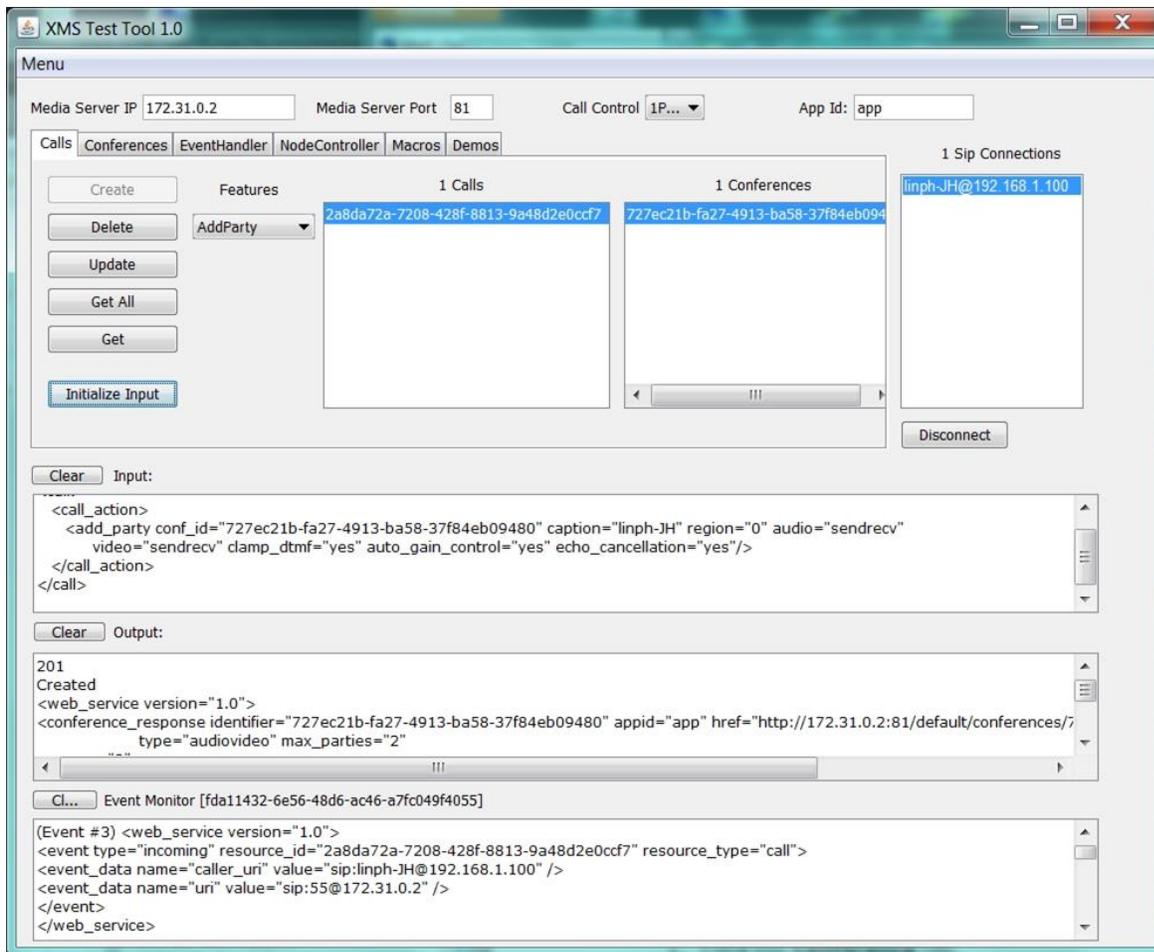
1. Click the **Conference** tab.
2. Click **Initialize Input** to get the default conference creation parameters. Edit them if desired.

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 **Conference** tab.
2. Select the call ID and click **RemoveParty** from the **Features** drop-down list. Repeat for each party in the conference.
3. Select the call ID and click **Disconnect** for each party in the conference.
4. Select the conference ID 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

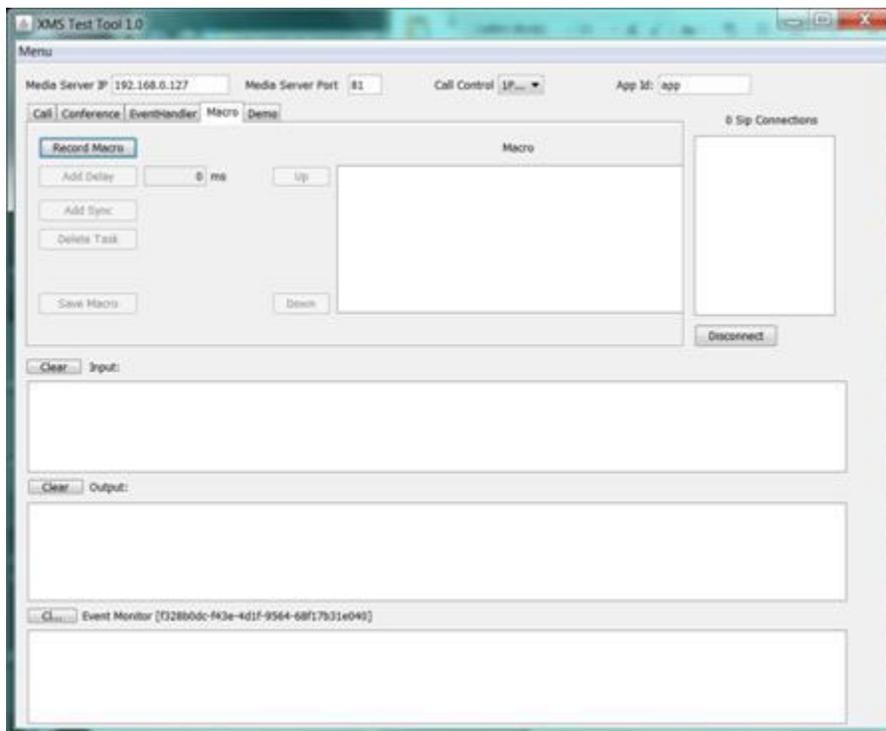
XMSTool has the ability to record a sequence of commands for an application scenario for later use. The recording can be saved and will appear in the installation's Demo directory.

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. CLI Command Scripts

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.

Mode

These CLI commands are supported only in **MSML** mode. If used in **Native** mode, the results are unpredictable.

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:

```
activatelicense-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]# activatelicense-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" />
```

```

value="40" />
        <feature id="high_res_video" display_name="High Resolution Video"
        <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"
}
```

8. 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

9. Appendix A: 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 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 	
	xmsBreachValue	Integer32	

Trap Name	Associated Variables	Type	Description
	xmsConfiguredValue	Integer32	
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 WebUI.
	xmsWebUIUserName	DisplayString	
	xmsDescription	DisplayString	
xmsWebUserProfileChanged	xmsTrapSeverity	ItuPerceivedSeverity: Warning = For changes in the web user profile	Trap is generated if user's profile is changed in WebUI.
	xmsWebUIUserName	DisplayString	
	xmsUserProfileChangeType	DisplayString	
	xmsDescription	DisplayString	
xmsServiceStatusChanged	xmsTrapSeverity	ItuPerceivedSeverity: <ul style="list-style-type: none"> Major:4 = For status (STOPPED, STARTING, STOPPING UNRESPONSIVE, OUTFSERVICE) Cleared:1 = For RUNNING status 	Trap is sent when status of a monitored service changes. If service name is "overall", it denotes overall operational status.
	xmsServiceIdentifier	DisplayString: <ul style="list-style-type: none"> broker xmserver appmanager 	

Trap Name	Associated Variables	Type	Description
	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 (e.g., "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 is generated when the CDR subsystem fails to create new CDR files.
	xmsDescription	DisplayString	
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.

Variable Name	Type	Description
xmsConferenceCallParties	Gauge32	Count of currently active conference call parties.
xmsConferenceMediaParties	Gauge32	Count of currently active conference media parties.
xmsASRTTSSessions	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.
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	<pre>SEQUENCE { xmsLicenseName xmsLicenseUsage }</pre> <p>Information of a particular license usage.</p>
xmsLicenseName	INTEGER (enumerated)	<pre>{ amraudio(1), basicaudio(2), hdaudio(3), lbraudio(4), mrcpspeech(5), basicvideo(6), hiresvideo(7) }</pre> <p>Name of the license type.</p>
xmsLicenseUsage	Gauge32	Count of licenses of a particular type currently being used.
xmsServiceUpTime	TimeTicks	Time since the services were last re-initialized.

Variable Name	Type	Description
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 B: CDR

The PowerMedia XMS CDR implementation supports stored data set record for each signaling and/or media transaction on the system.

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
	start_time	ISO Date	Call start time in GMT timezone	ISODate("2015-01-29T05:51:23.387Z")
	answer_time	ISO Date	Call answer time in GMT timezone	ISODate("2015-01-29T05:51:23.549Z")
	end_time	ISO Date	Call end time in GMT timezone	ISODate("2015-01-29T05:51:23.552Z")
	Call-ID	character string	SIP Call-ID header for this call	1-6237@10.40.2.162
	direction	character string	Direction of call with respect to XMS	"INBOUND" for incoming call and "OUTBOUND" for outgoing call
	disconnected_by	character string	Call terminating end point	"XMS" or "network"
	protocol	character string	Protocol	"SIP" or "RTCWEB"
	release_reason	character string	SIP release reason phrase	800 Bye/ 408 Request Time Out, etc.
	requesturi	character string	Request URI in initial INVITE request	sip:msml@10.40.2.183:5060

CDR Component	Field Name	Field Type	Field Description	Example Value/Range
	sip_release_code	integer	SIP release code in final SIP response	SIP 3xx, 4xx, 5xx, 6xx response or 800 for normal call termination
	state	character string	State of call signaling during the call	idle, offering, accepting, accepted, answering, answered, dialing, proceeding, ringing, connected, transferring, clearing, cleared, message
RTP Stream	dtmf_mode	character string	DTMF mode	inband, outofband, rfc2833
	start_time	ISO Date	RTP stream start time	ISODate("2015-01-29T05:51:23.544Z")
	end_time	ISO Date	RTP stream end time	ISODate("2015-01-29T05:51:23.553Z")
RTP Stream (Audio Codec)	bit_rate	integer	Bitrate of audio codec used in the call	64000
	clock_rate	integer	Clock rate of audio codec used in the call	8000
	coder_frame_size	integer	Coder frame size for audio codec used in the call	20
	direction	character string	Direction for audio RTP stream	sendrecv, sendonly, recvonly
	encoding	character string	Encoding selected for audio RTP	pcmu, pcma, etc.
	frames_per_packet	integer	Frames per packet for audio encoding	1
	local_ip	character string	Local IP for audio stream	10.40.2.183
	local_port	integer	Local port for audio stream	49158
	payload_type	integer	Audio payload type in SDP	0
	remote_ip	character string	Remote IP for audio stream	10.40.2.162

CDR Component	Field Name	Field Type	Field Description	Example Value/Range
	remote_port	integer	Remote port for audio stream	6000
	vad_enabled	integer	VAD (voice activity detection) is enabled for the call	0 or 1 (for disabled or enabled respectively)
RTP Stream (Video Codec)	bit_rate	integer	Bitrate of video codec	768000
	max_bit_rate	integer	Maximum bitrate	0
	sampling_rate	integer	Sampling rate of codec	1
	img_width	integer	Image width in video	640
	img_height	integer	Image height in video	480
	direction	character string	Direction of video RTP stream	sendrecv, sendonly, recvonly
	encoding	character string	Encoding selected for video RTP	vp8
	payload_type	integer	Payload type for video media	120
	local_ip	character string	Local IP for video stream	10.40.2.183
	local_port	integer	Local port for video stream	49158
	remote_ip	character string	Remote IP for video stream	10.40.2.162
	remote_port	integer	Remote port for video stream	6000