Dialogic® PowerMedia™ XMS

Quick Start Guide

Copyright and Legal Notice

Table of Contents

Revision History

Revision	Release Date	Notes
05-2701-017	October 2017	Updates to support PowerMedia XMS Release 3.5. System Requirements: Added note in the Operating System section. Licensing: Updated the section.
05-2701-016 (Updated)	August 2017	System Requirements: Added httpd requirement and note in the Operating System section.
05-2701-016	June 2017	Updates to support PowerMedia XMS Release 3.4.
05-2701-015	May 2017	Updates to support PowerMedia XMS Release 3.3. Reserved Ports: Updated the section.
05-2701-014	November 2016	Updates to support PowerMedia XMS Release 3.2.
05-2701-013 (Updated)	May 2016	Supported Virtual Machines: Added the recommended number of VMs.
05-2701-013	March 2016	Updates to support PowerMedia XMS Release 3.1. System Requirements: Updated the operating system requirements. ISO Method: Updated the section. Connecting to the Console: Updated screenshots and content because the Mode tab has been removed as a result of legacy MSML mode no longer being supported.
05-2701-012	October 2015	Updates to support PowerMedia XMS Release 3.0. PowerMedia XMS Overview: Updated the section. Installing PowerMedia XMS: Updated the System Requirements and Supported Virtual Machines.
05-2701-011 (Updated)	April 2015	RESTful Verification: Updated with information on the XMSTool and clarification on the verification demo.
05-2701-011	February 2015	Updates to support PowerMedia XMS Release 2.4. Installing PowerMedia XMS: Updated list of supported processors. RPM Method: Added table of reserved ports.
05-2701-010	September 2014	Updates to support PowerMedia XMS Release 2.3.

Revision	Release Date	Notes
05-2701-009	May 2014	Installing PowerMedia XMS: Updated list of supported operating systems and added new section for supported virtual machines.
05-2701-008	February 2014	Updates to support PowerMedia XMS Release 2.2. Verification Options and WebRTC Verification: Removed note that the WebRTC verification demos are video-only. Supported on audio and video.
05-2701-007	November 2013	Verification Options and WebRTC Verification: Added note that the WebRTC verification demos are video-only.
05-2701-006	October 2013	Updates to support PowerMedia XMS Release 2.1.
05-2701-005	March 2013	Overview of PowerMedia XMS: Updated with clarification that NETANN and VXML media options are currently audio-only. VoiceXML (VXML): Updated with clarification that VXML is audio-only. Verification Options: Updated with clarification that VXML verification demos are audio-only.
05-2701-004	February 2013	Updates to support PowerMedia XMS Release 2.0. Installing PowerMedia XMS: Added a note regarding Internet Explorer and file renaming at download. Configuring PowerMedia XMS: Added sections for Network Announcement (NETANN), VoiceXML (VXML), and Media Resource Control Protocol (MRCP). RESTful Verification: Updated section. Logging: Updated section.
05-2701-003	August 2012	Installing PowerMedia XMS: Added information to the RPM Method section.
05-2701-002	July 2012	General update to support PowerMedia XMS Release 1.1. This is a 64-bit only release. Installing PowerMedia XMS: Updated and added a stand-alone RPM Method section.
05-2701-001	March 2012	Initial release of this document.
Last modified: October 2017		

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

1. Welcome

This Quick Start Guide provides instructions necessary to install and configure the Dialogic® PowerMedia™ Extended Media Server (also referred to herein as "PowerMedia XMS" or "XMS"). This guide will also show how to get the PowerMedia XMS running with a simple Verification Demo, and then allows you to try sample applications or to start developing your own.

The basic operation of the system is contained in this guide, which is primarily intended for users who do not have extensive experience working with PowerMedia XMS. For advanced operation, refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide*.

2. PowerMedia XMS Overview

Overview of PowerMedia XMS

Dialogic's PowerMedia XMS is a highly scalable, software-only media server that enables standards-based, real-time multimedia communications solutions for IMS, MRF, Enterprise, and WebRTC applications on premise or in the cloud. Built on 15+ years of software media processing experience, PowerMedia XMS is trusted by world-class service providers and large enterprises to power millions of rich media sessions.

With an extensive list of successful implementations that include MRF for VoLTE, carrier hosted contact centers, enterprise communications, voice messaging and "mission critical" next-generation 911 services, PowerMedia XMS has proven to be a key building block to new and innovative applications. When deployed with the optional Dialogic® PowerMedia™ Media Resource Broker (MRB), PowerMedia XMS scales to meet growing service-provider and business requirements.

PowerMedia XMS energizes application delivery by boosting performance with:

- State of the art mixing of media-rich communications
- Software providing a seamless transition to virtualization and cloud delivery
- Telco hardened scalability
- Supercharged WebRTC integration

PowerMedia XMS elevates what developers can create for their customers, from virtually any development environment, on virtually any network, and connecting to virtually any type of communication endpoint.

PowerMedia XMS is a powerful next-generation software-only media server or software Media Resource Function (MRF) IMS network element that enables standards-based, real-time multimedia communications solutions for SIP and WebRTC for mobile and broadband environments. PowerMedia XMS enables high density real-time multimedia communication functions including inbound and outbound session/call control, audio/video play and record, transcoding, transrating, transizing of video streams, multimedia conference mixing, content streaming, and a wide range of advanced supporting functions for communication sessions.

PowerMedia XMS is controlled by the business logic of applications deployed on SIP application servers and web application servers. PowerMedia XMS offers multiple media control protocols that can be used in a variety of network infrastructures. For example, a SIP application server (AS) can drive PowerMedia XMS using the MSML control interface or use the PowerMedia XMS VoiceXML (VXML) browser to execute VXML scripts and invoke MRCP speech services, like ASR and TTS. For Web 2.0 and Cloud development, a web application written in an appropriate language can control PowerMedia XMS using the HTTP RESTful interface. Similarly, the JSR 309 Connector Software for PowerMedia XMS (JSR 309 Connector) can enable Java EE developers to control real-time applications from converged application servers.

The MSML, JSR 309 Connector, VXML, RESTful, and NETANN interfaces support multimedia—both audio and video, using a variety of codecs. All PowerMedia XMS APIs provide support for handling RTP media, security (via DTLS/SRTP), and ICE negotiation from WebRTC media sources.

PowerMedia XMS provides powerful and user-friendly OA&M functionality, and can be managed remotely through a web-based operator console and the HTTP RESTful Management interface.

A wide variety of SIP endpoints can be handled by PowerMedia XMS, resulting in the delivery of rich full-duplex audio and video media streams to a variety of fixed and mobile devices. With the additional support for WebRTC media, PowerMedia XMS provides the power to mix diverse streams and enable connectivity between legacy networks, endpoints, and WebRTC.

The following figure illustrates an example of a video conferencing delivery platform for a PowerMedia XMS-based multimedia conferencing solution.
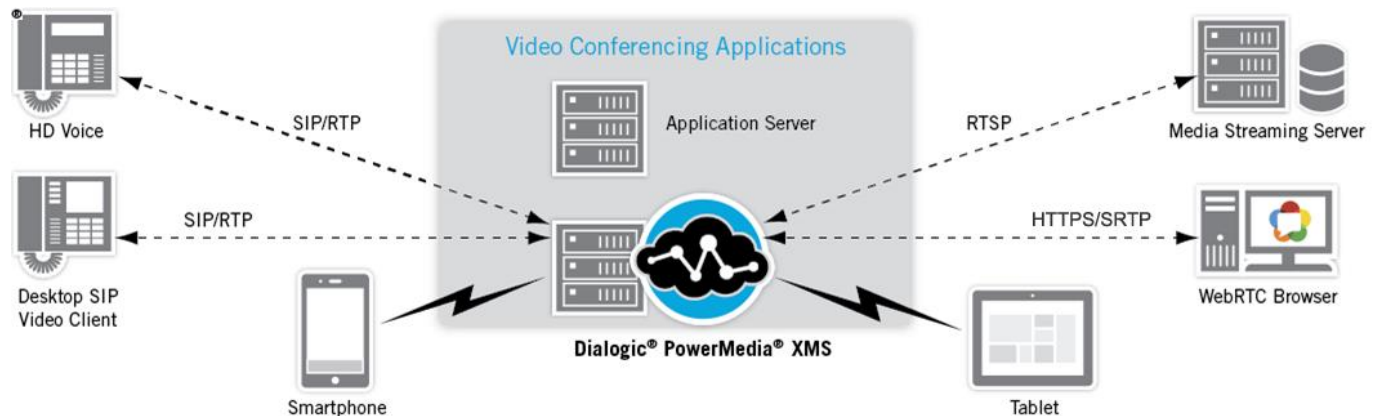
Related Information

See the following for additional information:

- PowerMedia XMS product page at http://www.dialogic.com/xms.

- PowerMedia XMS datasheet at http://www.dialogic.com/~/media/products/docs/media-server-software/12888-powermedia-xms-ds.pdf.

- PowerMedia XMS Developer portal at http://www.dialogic.com/developer.

- PowerMedia XMS Release 3.5 documentation at http://www.dialogic.com/manuals/xms/xms3-5.

- Dialogic Service Center at http://www.dialogic.com/support.

3. 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-3.5.xxxx-x86_64.iso* and *dialogic_xms_3.5.xxxx.tgz* where "xxxx" indicates the version number.

There are two installation methods available:

- ISO Method
- RPM Method (used for a CentOS or RHEL installation)

System Requirements

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

Item	Requirement
Hardware	Intel Architecture-based server
Operating System	**Note:** 32-bit operating systems are not supported. **ISO Method Installation:** Community ENTerprise Operating System (CentOS) 7.x **RPM Method Installation:** • CentOS 7.x and 6.4 (or later) • Red Hat Enterprise Linux (RHEL) 7.x and 6.4 (or later) • Oracle Linux 6.4 • Oracle Linux 7.2 with Unbreakable Enterprise Kernel (UEK) Release 4 Before running the RPM Method installation, the following packages, available from the OS distributor, must first be installed: • perl-core • openssl version 1.0.1e or higher • httpd-2.2.15-60.el6.centos.4.x86_64 or higher **Note:** If using CentOS 6.x, please ensure that the installed version (2.2.15) and release (60.el6.centos.4) of httpd is *httpd-2.2.15-60.el6.centos.4.x86_64* or higher. **Note:** The WebGUI requires a minimum version of TLS 1.2. If using CentOS 6.x, please ensure that the installed version of httpd is *httpd-2.2.15-60.el6.centos.4.x86_64* or higher. If the CentOS 6.x httpd package is not updated, the XMS installation logs will indicate that "httpd may fail to start" and the WebGUI will be unresponsive. The failure message will also appear in */var/log/messages* when trying to start httpd or reboot the system.

Item	Requirement
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

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

Supported Virtual Machines

The supported virtual machines (VM) are as follows:

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

It is recommended to use two VMs when running XMS. If more than two VMs are used, there may be performance issues.

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 is 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.

Refer to the *Dialogic® PowerMedia™ XMS Application Note: Optimizing VMware Host Hardware and Virtual Machine to Reduce Latency* for more information.

Cloud Environments

The qualified cloud environments include the following:

- Amazon Web Services (AWS)

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

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

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

Supported Web Browsers

Browser Support for PowerMedia XMS Admin Console

The following web browsers are supported:

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

Browser Support for WebRTC

The following web browsers are supported:

- Mozilla Firefox
- Google Chrome

Note: Other release lines of Mozilla Firefox (Nightly) and Google Chrome (Canary) may also work. However, other release lines are subject to frequent change and may not work correctly.

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.

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

- Burn the .ISO image to a bootable DVD.
- Place the .ISO image in a virtual datastore and point the DVD drive to that location. This method is helpful for remote installations. Refer to "Appendix A: ISO Method for Remote Installation" of the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide* for details.

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

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

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

2. Use the .ISO image to create the PowerMedia XMS installation DVD.

3. Ensure the target system on which PowerMedia XMS will be installed is connected to your network.

4. Boot the target PowerMedia XMS system from the installation DVD. The DVD will install CentOS operating system and required software.

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

5. Perform licensing and configuration.

Getting and Burning the .ISO File

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

1. Download a single .ISO file, which contains CentOS and PowerMedia XMS packages. Go to http://www.dialogic.com/products/media-server-software/xms for information about downloading the .ISO file.

2. Using a DVD drive that has write capabilities, along with the appropriate DVD burning software, burn the .ISO image onto a bootable DVD.

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

Booting the System from the DVD

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

Once the bootable DVD is created, proceed as follows:

1. Insert the bootable DVD in the system drive on which the installation will be done and boot the system from the DVD.

2. Press **Enter** at the boot prompt.

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

Setting the IP Address

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

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

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

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

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

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

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

Refer to the following guidelines:

- For parameters ending with "_addr", enter the ipv4 addresses.

- The first double colon (::), which is between "<ip_addr>" and "<gateway_addr>", defaults to no peer. Unlike other instances of double colons in the syntax, this double colon does not represent a missing (i.e., not entered) parameter.

- The second double colon (::), which is between "<hostname>" and "none", means the default Ethernet device is automatically obtained. The default Ethernet device is automatically obtained because the parameter was not entered.

- "none" means that a static IP address is being set up.

- It is recommended to set the DNS ("nameserver=<ip_addr>") as part of the installation. The "nameserver=" parameter is separate from the "ip=" parameter.

Refer to the following example for setting up a static IP address of 192.168.1.200 with a gateway of 192.168.1.1, a netmask of 255.255.255.0, a system name of "server.xms30.com", the default Ethernet device found on the system, and a DNS of 8.8.8.8.

```
ip=192.168.1.200::192.168.1.1:255.255.255.0:server.xms30.com::none nameserver=8.8.8.8
```

For complete information on all available parameters, refer to the "Chapter 20. Boot Options" section of the Red Hat Documentation:
http://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Installation_Guide/chap-anaconda-boot-options.html#tabl-boot-options-network-formats.

Completing the Installation

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

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

RPM Method

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.

Ensure that your PowerMedia XMS system firewall is configured accordingly.

For more information about the RPM Method, refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide*.

Reserved Ports

The default PowerMedia XMS configuration uses the following reserved ports:

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

Service	Port
WebRTC (all processes)	1080
WebUI (nodecontroller, lighttpd, httpd)	81, 10443, 9004 (lighttpd) 10080 (nodecontroller)

4. PowerMedia XMS Configuration

Configuring PowerMedia XMS

PowerMedia XMS configuration and operation is done though a secure web-based GUI called the PowerMedia XMS Admin Console (also referred to herein as "Console"). 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.

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 on the **Lock Symbol > Certificate Information > Details > CopytoFile** 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 pop-up 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.
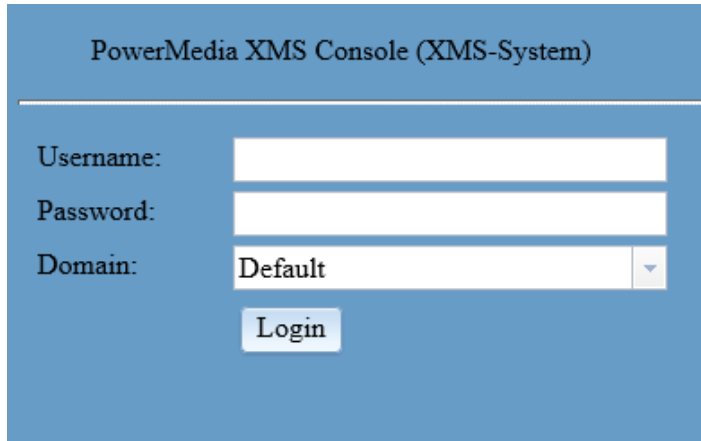
Note: A permanent, publicly accessible PowerMedia XMS should have a valid certificate from a signed certificate authority. Refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide* for more information.

Connecting to the Console

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.

   PowerMedia XMS Console (XMS-System)

Username:	
Password:	
Domain:	Default
	Login

2. Enter "superadmin" for the **Username** field and "admin" for the **Password** field. The superadmin user allows access to all configuration functions available on the Console.

3. Click **Login**. After user information is authenticated, you are logged on to the initial **General** page of the **Systems** menu.

4. 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.

On the **System > General** page, verify system data and system operation by noting that PowerMedia XMS is in a RUNNING state.

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

XMS	
release	3.5.17943 GA
state	RUNNING
System	
os release	CentOS Linux release 7.0.1406 (Core)
os version	Linux 3.10.0-123.el7.x86_64
uptime	0 days 11 hours 57 minutes 22 seconds
cpu load	T1=32.709999 , T5=28.48 ,T15=27.559999
memory	total:15886 MB used:6445 MB
System Storage	
/dev/sda2 (/)	total: 10230 MB, used: 4592 MB
/dev/sda5 (/var)	total: 83980 MB, used: 66310 MB
/dev/sda1 (/boot)	total: 124 MB, used: 74 MB
System Time	
time	Tue Oct 17 11:51:00 2017
zone	America/New_York

On the **System > Services** page, the status will indicate **Mandatory Services** and **Optional Services** are RUNNING as well.

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

Overall Status: RUNNING
Graceful Shutdown Timeout (seconds): 120

[Restart] [Stop] [Graceful Shutdown] [Refresh]

Mandatory Services:

Service Name	Description	Status
hmp	Media Processing Service	RUNNING
broker	Message Routing Service	RUNNING
xmserver	Signaling and Media Service	RUNNING
appmanager	Application Interface Service	RUNNING

Optional Services:

Service Name	Description	On Start Enabled	Status
eventmanager	Event Manager	☑	RUNNING
perfmanager	Performance Manager	☑	RUNNING
httpclient	HTTP Client	☑	RUNNING
mrcpclient	MRCP Client	☑	RUNNING
rtcweb	RTCWeb Signaling Service	☑	RUNNING
xmsrest	RESTful Call/Media Control Service	☑	RUNNING
netann	NETANN Service	☑	RUNNING
vxml	VXML Service	☑	RUNNING
msml	MSML Service	☑	RUNNING
msrpservice	MSRP Service	☑	RUNNING
faxservice	Fax Service	☐	STOPPED
verification	System/Application Verification Service	☑	RUNNING
xmssysstats	System Statistics Collector Service	☑	RUNNING
cdrserver	CDR Service	☑	RUNNING
wsapiserver	WS Api Server	☐	STOPPED

OS Services:

Service Name	Description	On Boot Enabled	Status
adaptor	MRB Adaptor Service	⬤	⬤

Licensing

PowerMedia XMS comes with a 4-port verification license to get started. The name of the license file is *verification.lic*. This evaluation license is not intended to provide access to all product capability.

Note: As of PowerMedia XMS Release 3.5, the LBR Audio codecs (G.723, G.726, G.729ab, or iLBC), the GSMAMR Audio codecs (GSM-FR, GSM-EFR, or AMR-NB), and the AMR-WB codec are no longer enabled in the verification license. Please contact Dialogic inside sales (insidesales@dialogic.com) for a trial license with these codec capabilities.

On the **License > License Manager** page, you can view the licensed features currently enabled on PowerMedia XMS. In addition, you can find the 33-byte License Node ID, which is required to obtain a PowerMedia XMS 3.x License.

License Manager

Licensed Features:

Feature	Active Licenses
Advanced Video	8
Basic Audio	4
Fax	0
GSMAMR Audio	4
HD Voice	4
High Resolution Video	4
LBR Audio	4
MRB	1
MRCP Speech Server	4
MSRP	4

License Node ID

84CC16FFC19716A71E647EFA5FF711057

Add License (*.lic)

[   ] Browse

Overwrite Existing File? ☐   Upload

Licenses:

Selection	License Name	Type	Expires	Status	Action
☐	verification.lic	Verification	permanent	active	DISABLE

Delete

Proceed as follows to activate the PowerMedia XMS 3.x License using the 33-byte License Node ID:

1. After PowerMedia XMS installation is complete, retrieve the License Node ID from the **License Manager** page in the PowerMedia XMS Admin Console or from the RESTful Management API.

2. Use the License Node ID to generate the license file.

3. Apply and activate the license file.

Note: If upgrading from PowerMedia XMS 2.x to PowerMedia XMS 3.x, PowerMedia XMS 2.x licenses must be upgraded to use the 33-byte License Node ID. Customers with valid support agreements can upgrade their license through the Dialogic Product Center with a valid account or by contacting an authorized Dialogic distributer.

For detailed License Manager actions and other Console operations, refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide*.

5. PowerMedia XMS Verification

Verification Options

The following table shows the options for verifying the operation of PowerMedia XMS depending on the desired application technology.

Application	Considerations
Web Real-Time Communication (WebRTC)	The following WebRTC verification demos are available. These demos are installed by default on the system and are activated using a specific URI. • Video Play Verification Demo • Conference Verification Demo • Join Verification Demo • WebRTC to SIP Verification Demo
Network Announcement (NETANN)	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.
Voice Extensible Markup Language (VXML)	Two VXML verification scripts, including all required media, are included in the PowerMedia XMS distribution. These verification demos are audio-only. One script plays and records audio files to verify operation, and the second script requires a Media Resource Control Protocol (MRCP) server for Automatic Speech Recognition (ASR) and Text-to-Speech (TTS). **Note:** Do not attempt to run the second verification script until basic operation of PowerMedia XMS has been verified.
Representational State Transfer (RESTful)	Included with PowerMedia XMS distribution, this Java-based RESTful application provides the same play/record demo as the basic VXML script. However, this verification demo uses both audio and video. **Note:** This option requires a Java Runtime Environment.
Media Server Markup Language (MSML)	A separate MSML application server is required to verify PowerMedia XMS operation. For this reason, using one of the supplied VXML or RESTful applications is suggested.

WebRTC Verification

The following WebRTC verification demos are available. These demos are installed by default on the system and are activated using a specific URI.

- Video Play Verification Demo – plays a video clip into browser or SIP phone.
- Conference Verification Demo – four (4) party conferencing demo that shows interoperability between Chrome, Firefox, and SIP. Inbound calls enter and leave the conference. Web page selections allow for playing a video clip into the conference and recording the conference and replaying the recording.
- Join Verification Demo – two SIP or WebRTC inbound video calls are joined together and then unjoined when one hangs up.
- WebRTC to SIP Verification Demo – allows a SIP URL to be dialed from a WebRTC screen. When the SIP call is answered, the two endpoints are joined together. When either call hangs up, the other caller will be disconnected and the demo reset.

Refer to the *Dialogic® PowerMedia™ XMS WebRTC Demo Guide* and *Dialogic® PowerMedia™ XMS WebRTC JavaScript API User's Guide* for more information.

NETANN Verification

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.

By default, any SIP call whose URL begins with sip:annc or sip:conf= will be directed to the NETANN service.

Refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide* and *Dialogic® PowerMedia™ XMS Basic Network Media Services with SIP User's Guide* for more information.

VXML Verification

Two VXML demos are available to verify VXML. The first is a simple audio-only IVR script to take menu choices via DTMF and play and record audio. It uses audio prompts already installed on the media server, and will be automatically accessed when a SIP call is made to the default "dialog" user. This demo requires only the verification license that is automatically installed on PowerMedia XMS.

The second demo is a company directory application. This demo requires:

- An operating MRCP ASR/TTS server for voicing prompts and recognizing responses.
- A 4-port (or greater) trial or permanent license that must be manually installed on PowerMedia XMS using the Console. The license is required for call transfer functionality.

The demo is located on the PowerMedia XMS server in the default VXML script directory: */var/lib/xms/vxml/www/vxml/company_directory.vxml*.

To test the transfer function part of the demo, the script must be modified so that the "transferaddr" VXML variable at the top of the script is set to a SIP address that is waiting to accept a call. A call can then be placed to the application. The employee can be selected by DTMF extension or by name.

If the extension is not answered, an option of leaving voicemail will be presented. The message will be replayed/re-recorded until the caller chooses to save it.

Refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide* and *Dialogic® PowerMedia™ XMS VoiceXML Reference Guide* for more information.

RESTful Verification

PowerMedia XMS comes with RESTful Client verification demo. This verification demo is a Java application that can be run from a system with a Java Runtime Environment (JRE). The usual choice would be the system used for the Console via a web browser.

Starting the 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.

To use the XMSTool utility, access the **Downloads > Tools** page from the Console and click on **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.

Starting the Demo

The verification demo is available through the Console's **Downloads** page. Before running the demo, you must set up a SIP softphone to receive calls. For more information, see Verification Using a SIP Softphone. Be sure to have a SIP softphone ready before running the demo.

To run the demo, follow these steps:

1. From the Console, click **Downloads > Tools** page.

2. Select the **XMS Verification Demo**.

3. Save the **XMS Verification Demo** file to your local location from the pop up window. The demo file is a .zip file.

4. Unzip the file.

5. Navigate to the top level directory.

6. From the top level directory, run the tools as follows:

   ```
   > java –jar dist/XMSVerificationDemo.jar –g –m <xms_ip_address>
   ```

The Demo's main screen will appear. It includes a Call State to show progress. All messages sent and received will appear in their respective boxes.
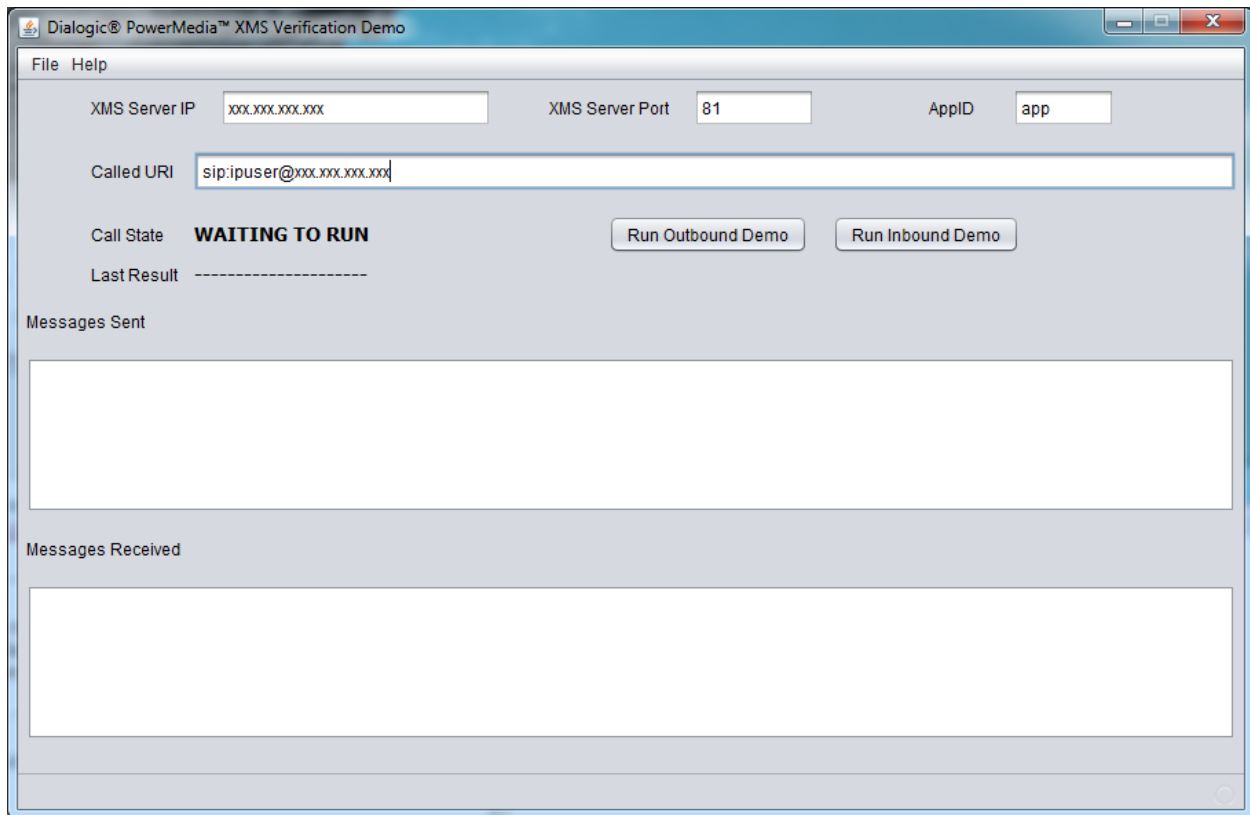
Running the Demo

The demo can be run in either an Inbound mode where the PowerMedia XMS will expect a call from a SIP softphone, or in an Outbound mode where it will place a call to a SIP softphone.

Run the Inbound demo as follows:

1. Indicate the name of the PowerMedia XMS IP address in the space provided.

2. Click **Run Inbound Demo**. The Call State should change to WAITING FOR CALL.

3. Place a call from your SIP softphone to the PowerMedia XMS IP address.

Run the Outbound demo as follows:

1. Indicate the name of your PowerMedia XMS IP address in the space provided.

2. Set the Called SIP URI to your SIP softphone's URI.

3. Click **Run Outbound Demo**. The Call State should change to OUTBOUND CALL STARTED.

In either the inbound or outbound case, a greeting should be seen and heard. The demo's progress can be determined by viewing the Call State and Last Result status.

Sent and received messages also provide the call status.

The demo leads the caller through several menus, and allows several multimedia clips to be played, or a multimedia recording to be made and replayed. If the verification demo is not successful, an error will appear on the screen and messages will be captured in the *verification.log* file. This log file is located in the */dist* directory from where the .jar file was executed.

Refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide* and *Dialogic® PowerMedia™ XMS RESTful API User's Guide* for more information.
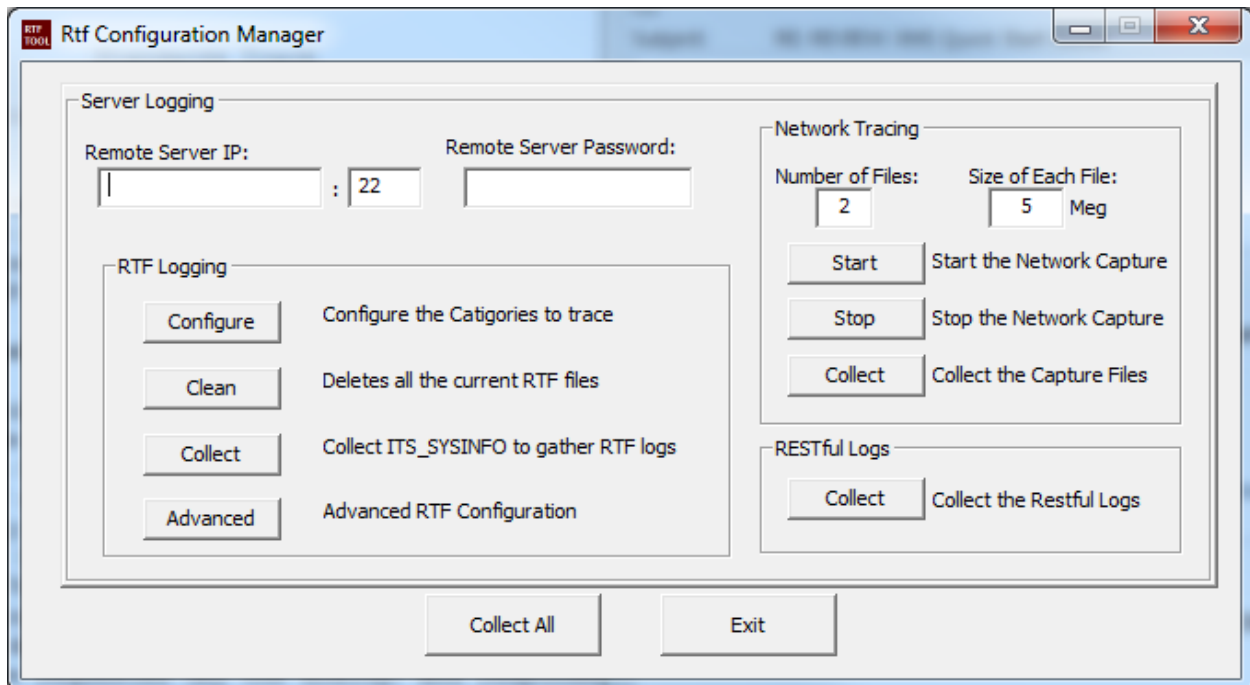
Logging

Most PowerMedia XMS subsystems produce their own log files, which are updated on a regular basis or whenever a subsystem is restarted. Always look for the log with the current time/date stamp.

PowerMedia XMS logs are accessed through the RemoteRtfTool utility. To use the RemoteRtfTool utility, access the **Downloads > Tools** page from the Console and click on **Window Logger Manager Tool** (*RemoteRtfToolInstaller.msi*) to download and install the file.
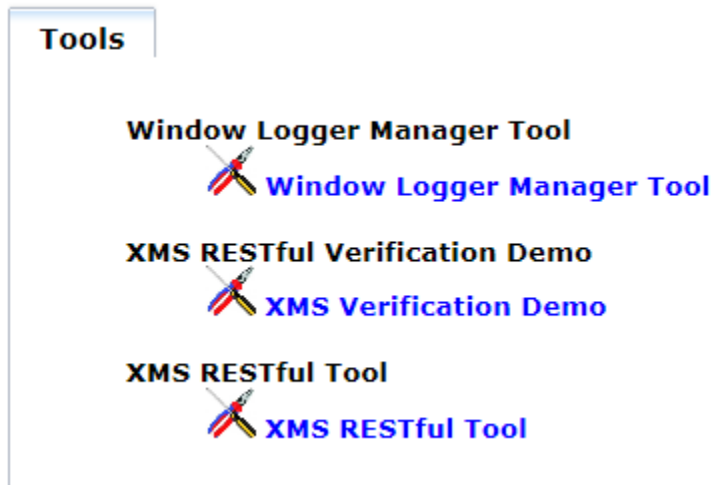
The Rtf Configuration Manager window allows access to the logs.

To access the logs:

1. Enter the **Remote Server IP** and **Remote Server Password**.

2. Click **Collect** from either the RTF Logging or RESTful Logs sections.

3. To view a specific file, click the box to the left of the file to select it.

4. Click **View**.

For additional information about log files and the information they contain, refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide*.

Verification Using a SIP Softphone

This section provides details for verifying PowerMedia XMS using a SIP softphone. Instructions for download, install, and use are included in this section.

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.

The PowerMedia XMS may be directly dialed by IP address as shown above, with a SIP URL such as 100@192.168.0.126.