



Dialogic® PowerMedia™ Media Resource Broker (MRB)

Installation and Configuration Guide

Copyright and Legal Notice

Copyright © 2015-2018 Dialogic Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Corporation at the address provided below.

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

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

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

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

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

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

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

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

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

Table of Contents

1. Welcome	7
Related Information.....	7
2. PowerMedia MRB Installation	8
System Requirements	8
Processor Requirements	8
Disable SELinux	9
Software Installation.....	9
Command Line Installation	9
Graphical Environment Installation	11
Software Updates and Uninstallation	16
MRB Adaptor Updates	16
3. PowerMedia MRB Configuration	17
MRB Login	17
Dashboard	18
Media Servers	19
Media Server Details	20
Port Usage.....	23
Manage Conferences	24
Manage Media Servers	25
Add a Media Server.....	25
Manage a Media Server	26
Resource Summary	27
MS HA Statistics.....	28
Locations.....	28
User Administration	29
Add a User.....	29
Change a User	29
User Roles	30
User Policies	30
MRB Configuration.....	31
Manage Conferences.....	32
Manage MRB Cluster	33
Networking Configuration	35
VIP Status	36
SNMP Configuration	36
SNMP Notifications.....	37
Selection Algorithms	37
Unaware Mode	38
Security Profiles	39
Add a Trusted Certificate	40
Add a Server Certificate	40
Logging.....	41
4. Appendix A: Enabling HTTPS with Jetty	42
5. Appendix B: Configure the Firewall	49
CentOS 7.x.....	49
CentOS 6.x.....	50
6. Appendix C: Resolve the Hostname	51

7.	Appendix D: Create Self-Signed Certificates and Keys	52
8.	Appendix E: Add a Customized Security Profile	53
9.	Appendix F: Performance Tuning for the RTP Proxy	55
	Network Bandwidth	55
	UDP Ports	55
	Network Buffering	55
	Interrupt Handling	55
	Coalescing	55
	Queuing and Steering	56
10.	Appendix G: Media Server Adaptor Configuration	57

Revision History

Revision	Release Date	Notes
3.0 (Updated)	February 2018	Appendix G: Media Server Adaptor Configuration : Added the section.
3.0 (Updated)	January 2017	Software Installation : Updated the section. Media Servers : Updated the section. Manage Media Servers : Updated the Manage a Media Server section.
3.0	November 2016	Updates for MRB version 3.2. Media Servers : <ul style="list-style-type: none">• Added a note requiring media servers to be configured to accept SIP on both UDP and TCP.• Added a note requiring MSML Services to be enabled and running when using PowerMedia XMS systems with an MRB.• Added a note about MRB utility calls when using PowerMedia XMS. Appendix F: Performance Tuning for the RTP Proxy : Added the section.
2.1	August 2016	PowerMedia MRB Configuration : Added limitations to the cascading conferences feature in the MRB Configuration section.
2.0	April 2016	Updates for MRB version 1.5. Appendix D: Create Self-Signed Certificates and Keys : Added the section.

Revision	Release Date	Notes
1.0 (updated)	January 2016	<p>System Requirements: Updated the operating system and software requirements.</p> <p>Software Installation: Updated the section.</p> <p>Software Updates and Uninstallation: Added the section.</p> <p>PowerMedia MRB Configuration: Updated the Add a Trusted Certificate to change the name from "Client" to "Trusted".</p> <p>MRB Adaptor Updates: Updated the section.</p> <p>Appendix A: Enabling HTTPS with Jetty: Relocated the section.</p> <p>Appendix B: Configure the Firewall: Added the section.</p> <p>Appendix C: Resolve the Hostname: Added the section.</p> <p>Appendix E: Add a Customized Security Profile: Added the section.</p>
1.0	October 2015	Initial release of this document.
Last modified: February 2018		

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 and configuring the Dialogic® PowerMedia™ Media Resource Broker (also referred to herein as "PowerMedia MRB" or "MRB").

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

Related Information

See the following for additional information:

- *Dialogic® PowerMedia™ Media Resource Broker (MRB) Quick Start Guide* and PowerMedia XMS 3.2 documentation at <http://www.dialogic.com/manuals/xms/xms3.2.aspx>.
- Media Resource Brokering at <http://tools.ietf.org/html/rfc6917>.
- Media Server Control Markup Language (MSCML) and Protocol at <http://tools.ietf.org/html/rfc5022>.
- Media Server Markup Language (MSML) at <http://tools.ietf.org/html/rfc5707>.
- Basic Network Media Services with SIP at <http://tools.ietf.org/html/rfc4240>.
- An Interactive Voice Response (IVR) Control Package for the Media Control Channel Framework at <http://tools.ietf.org/html/rfc6231>.
- A Mixer Control Package for the Media Control Channel Framework at <http://tools.ietf.org/html/rfc6505>.
- Media Control Channel Framework at <http://tools.ietf.org/html/rfc6230>.

2. PowerMedia MRB Installation

System Requirements

The system requirements are as follows.

Component	Requirement
Operating Systems	Community ENTERprise Operating System (CentOS) 7.x and 6.4 (or later) Red Hat Enterprise Linux (RHEL) 7.x and 6.4 (or later) Oracle Linux 6.4 Note: When installing the MRB on CentOS 7.x, the CentOS net-tools package must be installed.
Software	Install the latest update of Java Runtime Environment (JRE) version 8 on the target installation machine. By default, the JRE should be installed within the /opt directory (unpack tar.gz). As of April 2016, obtain the latest Oracle JRE 8 update at the following location: http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html . Note: The JRE is not required if the latest Oracle Java Development Kit (JDK) version 8 is installed.
Memory	MRB and MRB adaptor require 2 GB RAM each

Processor Requirements

The MRB processor requirements are dependent on the number of XMS it will support, and the calls per second it is required to process.

Configuration	Max Calls Per Second (CPS)	Processor
Low Density (1-7 XMS Clusters)	Up to 250 CPS	*Intel Xeon E3-1220v2 uni-processor (3.10 GHz, 4 cores) or better
High Density (8-15 XMS Clusters)	Up to 500 CPS	*Intel Xeon E5-2609v2 dual-processor (2.50 GHz, 4 cores/socket) or better
*Comparable systems can be used based on capacity requirements. For more demanding workloads, such as complex IVR systems or voicemail applications that result in a large amount of SIP traffic or demand fast response times, a more robust system may be required.		

Disable SELinux

SELinux is not currently supported and must be disabled. To disable SELinux, proceed as follows:

1. Edit the `/etc/selinux/config` file as a root user.
2. Find the line with the key **SELINUX=** and replace the value after the equals sign with **disabled**.
3. Save the file and reboot the operating system.

Software Installation

During the software installation, there will be a prompt to install any required packages.

The hiredis packages are required when the Media Proxy is enabled and can be retrieved from the following locations.

Note: The hiredis packages are not included as part of the standard CentOS repo and will need to be installed manually.

CentOS 7

http://dl.fedoraproject.org/pub/epel/7/x86_64/h/hiredis-0.12.1-1.el7.x86_64.rpm

http://dl.fedoraproject.org/pub/epel/7/x86_64/h/hiredis-devel-0.12.1-1.el7.x86_64.rpm

CentOS 6

http://www.dialogic.com/files/xms/mrb/C6/hiredis/hiredis-0.10.1-3.el6.x86_64.rpm

http://www.dialogic.com/files/xms/mrb/C6/hiredis/hiredis-devel-0.10.1-3.el6.x86_64.rpm

Install the required packages if prompted using the "yum install <package name>" command. Refer to the following example.

```
yum install hiredis
yum install hiredis-devel
```

There are two methods to install the PowerMedia MRB depending on the available capabilities of the environment:

- [Command Line Installation](#)
- [Graphical Environment Installation](#)

Command Line Installation

To install the MRB, proceed as follows. Refer to the image after the procedure for details.

1. Run the following command to execute the installer file:

```
java -jar dialogic-mrb-installer-<version>.jar -console
```

Note: Alter the command line as necessary to match the version and path of your Java executable.

2. Press **1** and then **Enter** to install the MRB.
3. Disable the Media Proxy [n] and press **Enter**. By default, it is disabled [n].
4. Enter the location of the Java install (JRE or JDK) that will be used to run the MRB and press **Enter**.
5. Enter the management interface IP address, or press **Enter** to use the default values, and press **1**.

6. Select the target path. Change the path, or press **Enter** to use the default path, and press **1**.
7. Press **1** or **2** to set your Jetty web server preference, and press **Enter**:
 - Press **1** to create a new installation of the Jetty web server. Select this option if you do not use a Jetty instance on your server already.
 - Press **2** to install the MRB Admin UI within an existing Jetty instance. Select this option if you use a Jetty instance on your server already.
8. Follow the on-screen instructions until the installation process is complete. When the installation process is complete, the installation details will be displayed.

The following example is from the command line installation.

```
[root@osboxes opt]# java -jar dialogic-mrb-installer-3.2.0.jar -console
* Press 1 if you would like to install the Media Resource Broker
* Press 2 if you would like to install the MRB Adaptor
1

The Media Proxy enables the MRB to proxy media sent between MRB clients and the media server. It
provides:
* The ability to move calls between media servers faster than when the originator of the call
needs to be reinvited.
* The only way of moving calls to a new media server when the MRB client doesn't support
reinviting.

Warning : The Media Proxy is a controlled introduction feature and will impact the performance of
the MRB if enabled

Would you like to enable the Media Proxy [y/n][default:n]
n

Please enter the location of your Java JRE install that will be used to run the MRB
[/opt/jre1.8.0_111/bin/java]

The list of available IP Addresses are as follows:
192.168.122.1
Please enter your IP Address that the MRB will use for management traffic. [192.168.122.1]

press 1 to accept, 2 to reject, 3 to redisplay
1
Select target path [/opt/mrb]

press 1 to continue, 2 to quit, 3 to redisplay
1
* Press 1 if you would like to create a new installation of the Jetty web server
* Press 2 if you would like to install the MRB Admin UI within an existing Jetty instance
1
Please enter a path where you would like to install the jetty web server [default: /opt/mrb]:

Select the packs you want to install:

[<required>] MRB (The MRB base Installation files)
[<required>] Media Server Adaptor (The Media Server Adaptor base installation files)

...pack selection done.
press 1 to continue, 2 to quit, 3 to redisplay
1
[ Starting to unpack ]
[ Processing package: MRB (1/2) ]
[ Processing package: Media Server Adaptor (2/2) ]
[ Unpacking finished ]

Install of the MRB successfully complete.
The MRB has been installed at the following location - /opt/mrb

You can now view the web admin ui at the following URL:
http://192.168.122.1:8888/mrb
```

```
Login details are as follows  
Username : root  
Password : admin  
  
[ Console installation done ]
```

Graphical Environment Installation

To install the MRB using the graphical environment, proceed as follows.

1. Run the following command to execute the installer file:

```
java -jar dialogic-mrb-installer-<version>.jar
```

Note: Alter the command line as necessary to match the version and path of your Java executable.

2. Select **Media Resource Broker** to install the MRB, and then click **Next**.



3. Read the information on the **Installing the Media Proxy** window. To proceed without enabling the Media Proxy feature, click **Next**. To enable the Media Proxy feature, select **Enable Media Proxy**, and then click **Next**.

Warning: The Media Proxy is a controlled introduction feature and will impact the performance of the MRB if enabled.

Note: If using the MRB to make RESTful and WebRTC calls, the Media Proxy feature must be enabled.

Dialogic

Installing the Media Proxy

The Media Proxy enables the MRB to proxy media sent between MRB clients and the media server. It provides:

- The ability to move calls between media servers faster than when the originator of the call needs to be reinvited.
- The only way of moving calls to a new media server when the MRB client doesn't support reinviting.

Warning : The Media Proxy is a controlled introduction feature and will impact the performance of the MRB if enabled

(Made with IzPack - <http://izpack.org/>)

Previous

Next

Quit

4. Click **Next** to proceed to the next step if no packages are required. If prompted, install the required packages using the yum install command. Refer to the following example to install the glib2-devel and glibc-devel packages.

```
yum install glib2-devel glibc-devel
```

Dialogic

The following packages are required by OS for install of MRB and must be installed to continue with the installation

No additional packages are required. You may continue with install

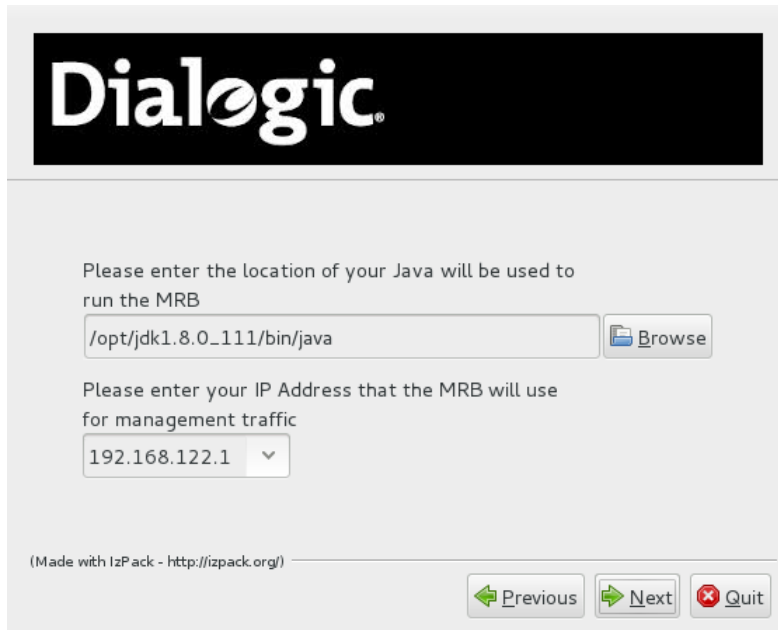
(Made with IzPack - <http://izpack.org/>)

Previous

Next

Quit

5. Enter the following information or use the default values, and then click **Next**:
- Enter the location of the Java install (JRE or JDK) that will be used to run the MRB (e.g., /opt/jdk1.8.0_111/bin/java).
 - Enter the IP address that will be used for management traffic.



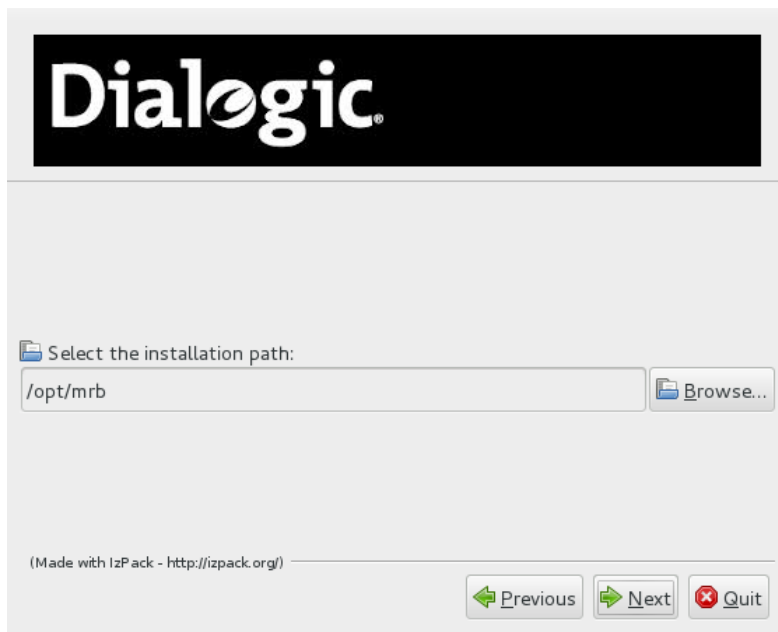
The Dialogic installer window for step 5 features a black header with the Dialogic logo. Below the header, the text "Please enter the location of your Java will be used to run the MRB" is displayed. A text input field contains the path "/opt/jdk1.8.0_111/bin/java", and a "Browse" button is to its right. Below this, the text "Please enter your IP Address that the MRB will use for management traffic" is shown. A dropdown menu displays "192.168.122.1". At the bottom, a small text line reads "(Made with IzPack - http://izpack.org/)", and three buttons labeled "Previous", "Next", and "Quit" are positioned on the right.

6. Review the license agreement if populated, accept the terms, and then click **Next**.



The Dialogic installer window for step 6 has a black header with the Dialogic logo. Below the header, the text "Please read the following license agreement carefully:" is followed by a large, empty rectangular box for the license agreement. Below the box, there are two radio button options: "I accept the terms of this license agreement." (which is selected) and "I do not accept the terms of this license agreement." At the bottom, a small text line reads "(Made with IzPack - http://izpack.org/)", and three buttons labeled "Previous", "Next", and "Quit" are positioned on the right.

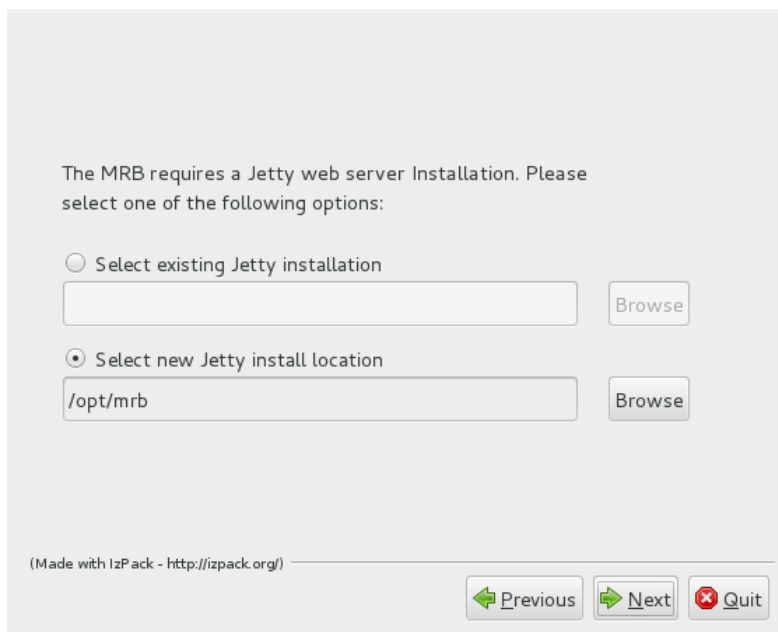
7. Select the installation path, and then click **Next**.



The image shows a window titled "Dialogic" with a black header. Below the header, there is a text box labeled "Select the installation path:" containing the text "/opt/mrb". To the right of the text box is a "Browse..." button. At the bottom of the window, there is a footer that says "(Made with IzPack - http://izpack.org/)" and three buttons: "Previous", "Next", and "Quit".

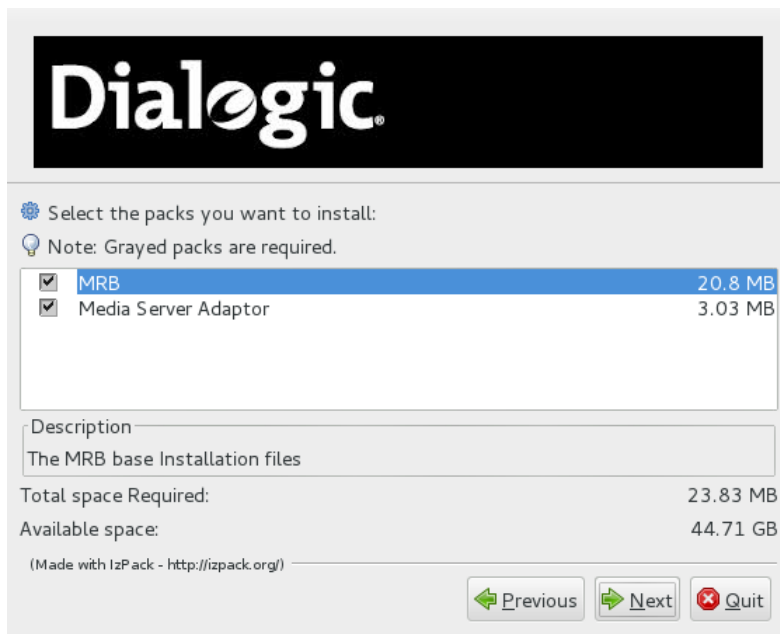
8. Set the Jetty web server preferences, and then click **Next**:

- **Select new Jetty install location** - Choose this option if there is not a Jetty instance on the server already. If you do not know if Jetty has been previously installed, select this option.
- **Select existing Jetty installation** - Choose this option if there is a Jetty instance on the server already.



The image shows a window titled "Dialogic" with a black header. Below the header, there is a text box labeled "Select the installation path:" containing the text "/opt/mrb". To the right of the text box is a "Browse..." button. At the bottom of the window, there is a footer that says "(Made with IzPack - http://izpack.org/)" and three buttons: "Previous", "Next", and "Quit".

9. Select the packs to install, and then click **Next**.



10. When the installation process is complete, click **Next** to view the installation details.



Software Updates and Uninstallation

To update the MRB software, the existing MRB software must be uninstalled and the new MRB software must be installed following the [Software Installation](#) procedure. The location of the MRB uninstall script is as follows:

```
/opt/mrb/uninstall-mrb.sh
```

If the MRB console WAR file is installed on an existing Jetty instance (as opposed to being installed on the Jetty that is part of the MRB installation), the uninstall script will not remove the MRB console WAR file from the existing Jetty install.

MRB Adaptor Updates

Note: PowerMedia XMS versions 3.0 and higher automatically update the MRB adaptor at the same time as the other XMS components. This procedure is not normally required.

Using the following procedure, update the MRB adaptor on PowerMedia XMS if there is a version mismatch or a recommended update:

1. Log in to the XMS machine that the MRB adaptor is installed on.
2. Stop the MRB adaptor using the **service adaptor stop** command.
3. Copy the MRB installer to the XMS machine.
4. Run the installer using the following command:

```
java -jar dialogic-mrb-installer-<version>.jar
```

Note: Alter the command line as necessary to match the version and path of your Java executable.

5. On the installer product selection screen, select **Media Server Adaptor**.
6. Select the defaults for the **Select Java** and **Management JMX IP Address** options.
7. When prompted to select the target path, accept the default location `-/opt/adaptor`.
8. When prompted to overwrite existing files in the target install directory, select **Yes** and continue with the installation.

3. PowerMedia MRB Configuration

The PowerMedia MRB console (also referred to herein as "MRB console") is a web-based user interface used to manage PowerMedia MRB. PowerMedia MRB configuration is done through the MRB console. HTTPS is not enabled by default on the administrator user interface. For details on setting up HTTPS, refer to [Appendix A: Enabling HTTPS with Jetty](#). For details on configuring the firewall, refer to [Appendix B: Configure the Firewall](#).

MRB Login

Proceed as follows to log in to the MRB console.

1. Launch the **MRB Login** page in a web browser using one of the following URLs:
`http://{server_address}:8888/mrb` or `https://{server_address}:8443/mrb`.

MRB Login

Welcome to the Dialogic MRB

Username	<input type="text" value="root"/>
Password	<input type="password" value="....."/>
<input type="button" value="Login"/>	

Note: If the error message "Lost connection to MRB on localhost:5100" is displayed when attempting to log in, refer to [Appendix C: Resolve the Hostname](#).

2. When logging in to the MRB console for the first time, enter **root** in the **Username** field and **admin** in the **Password** field. Once logged in to the MRB console, you can add different users by going to the [User Administration](#) page if desired.
3. Click **Login**. The MRB console opens and the **Dashboard** page appears. Refer to [Dashboard](#) for more information.
4. To make changes to the MRB console, click **Unlock Config**.

The side-bar menu of the console contains hyperlinks to each of the configuration pages. They are as follows:


- [Dashboard](#)
- [Media Servers](#)
- [Manage Media Servers](#)
- [Resource Summary](#)
- [MS HA Statistics](#)
- [Locations](#)
- [User Administration](#)
- [User Roles](#)
- [User Policies](#)
- [MRB Configuration](#)
- [Manage Conferences](#)


- [Manage MRB Cluster](#)
- [Networking Configuration](#)
- [VIP Status](#)
- [SNMP Configuration](#)
- [SNMP Notifications](#)
- [Selection Algorithms](#)
- [Unaware Mode](#)
- [Security Profiles](#)
- [Logging](#)

Dashboard

When logging in to the MRB console, the **Dashboard** page is displayed. On this page, PowerMedia MRB operation can be verified. The status of the MRB is shown in the **Status** field using a traffic light system. A green status indicates the MRB node is running and functional. A red status indicates that the MRB node is not running or is in an error state and is subsequently unavailable.

Dashboard

Status	MRB			
	Hostname	192.168.2.74:5070		
	Status	Active		
	HA Enabled	<input type="checkbox"/>		
	Up Time	000:00:26:15		
	Start Time	Tue, 7 Jul 2015 09:25:13 BST		
	JVM Vendor	Oracle Corporation		
	JVM Version	Java HotSpot(TM) 64-Bit Server VM version 24.51-b03		
	Java Version	Java Virtual Machine Specification version 1.7		
	Operating System Version			
	Number of Processors	Number of Threads	506	
	Architecture	Peak Number of Threads	507	
	Heap Size		Non Heap Size	
	Initial	256.0 MB	Initial	22.44 MB
	Current	108.99 MB	Current	24.89 MB
	Maximum	2048.0 MB	Maximum	130.0 MB
	Committed	256.0 MB	Committed	25.0 MB

Status	Paired MRB	
	Hostname	192.168.2.117:5070
	Status	Active

Errors

No errors

Media Servers




The **Media Servers** page provides a summary of the configured media server resources that are being managed by the MRB application.

Note: The media servers must be configured to accept SIP on both UDP and TCP when working with the MRB.

Note: When using an MRB with PowerMedia XMS systems, the MSML Service on the PowerMedia XMS systems must be enabled and running.

Note: Each MRB will create a utility call to each PowerMedia XMS that it is load balancing. If the MRB configuration is high availability (HA), there will be two utility calls on each PowerMedia XMS (one for each MRB). These utility calls will use one basic audio license each (one signaling and one RTP resource).

Media Servers

Status	Media Server Detail	Host	Port	Listen On Tls ?	TLS Port	Location	Response Time (ms)	Port Usage	Conferences
	Dialogic PowerMedia XMS	192.168.2.112	5070	false		New York	4	View Port Usage	Manage Conferences
	Dialogic PowerMedia XMS	192.168.2.12	5070	false		New York	1	View Port Usage	Manage Conferences
	Dialogic PowerMedia XMS	192.168.2.59	5070	false		New York	1	View Port Usage	Manage Conferences

The following information is provided.

Item	Description
Status	<p>A traffic light system that illustrates the current status of a media server. Green signals that the media server is online and in service. Red signals that the media server is offline and not in service. Yellow signals that the media server is full and unable to accept new calls. Gray signals that the media server has been taken offline manually by the system administrator.</p> <p>If the traffic light has a warning symbol in front of it, there is a version mismatch between the MRB and the MRB adaptor running on the particular media server. In this scenario, the MRB and MRB adaptor versions can be viewed as a tooltip by hovering over the traffic light.</p>
Media Server Detail	A hyperlink that allows specific media server information to be viewed on a separate page. Refer to Media Server Details for more information.
Host	The hostname/IPv4 of the media server being managed.
Port	The port that the MRB adaptor is listening on.
Listen On TLS	Whether or not the media server has been set up to communicate over a Transport Layer Security (TLS) channel.

Item	Description
TLS Port	The port that the media server is using to receive encrypted SIP signaling requests via TLS.
Location	The primary location of the media server. This information is entered when adding the media server.
Response Time (ms)	The responsiveness of the media server based on keep-alive probes.
Port Usage	A hyperlink to view specific port usage information for the media server. More information is provided in the Port Usage section.
Conferences	A hyperlink to view and manage conferences that are currently active on the MRB. Refer to Manage Conferences for more information.


The **Media Servers** page provides hyperlinks for additional configuration options:

- [Media Server Details](#)
- [Port Usage](#)
- [Manage Conferences](#)

Media Server Details

To access the **Media Server Details** page from the **Media Servers** page, click on the name of the media server in the "Media Server Detail" column. The **Media Server Detail** page displays information for a specific media resource instance.

Media Server Details

Status 
Name [Dialogic PowerMedia XMS](#)
Identifier 192.168.2.12:5070 2
Version 2.4.9750
Up Time 119:00:15:52
Time Zone Greenwich Mean Time
CPU Load t1=0.03, t5=0.03, t15=0.0
Memory Total=31.23 MB Used=3.44 MB [used=11%]
Supported Audio Codecs PCMU, PCMA, G726-32, AMR, G723, G729, iLBC, GSM, GSM-EFR
Supported Video Codecs H264, MP4V-ES, H263, H263-1998, H263-2000, VP8

Running Status **RUNNING**

Service Name	Description	Status
appmanager	Application Interface Service	RUNNING
broker	Message Routing Service	RUNNING
cdrserver	CDR Service	STOPPED
eventmanager	Event Manager	RUNNING
faxservice	FAX Service	STOPPED
hmp	Media Processing Service	RUNNING
httpclient	HTTP Client	RUNNING
mrcpclient	MRCP Client	RUNNING
msml	MSML Service	RUNNING
msrpservice	MSRP Service	RUNNING
netann	NETANN Service	RUNNING
perfmanager	Performance Manager	RUNNING
rtcweb	RTCWeb Signaling Service	RUNNING
verification	System/Application Verification Service	RUNNING
vxml	VXML Service	RUNNING
xmsserver	Signaling and Media Service	RUNNING
xmsrest	RESTful Call/Media Control Service	RUNNING
xmssysstats	System Statistics Collector Service	RUNNING

MS License File No file chosen

The following information is provided.

Item	Description
Status	Traffic light illustration of the current connection status between the MRB and the media resource instance.
Name	The name provided by the media resource for display purposes.
Identifier	The unique IP address and port combination for the media resource.
Version	The media resource version currently running.
Up Time	The reported up time of the media resource.

Item	Description
Time Zone	The reported time zone of the media resource.
CPU Load	The details of the recent average CPU load levels.
Memory	Total and used memory values of the media resource.
Supported Audio Codecs	A reported list of audio codecs supported on the media resource.
Supported Video Codecs	A reported list of video codecs supported on the media resource.
Running Status	<p>The reported running status of the media resource.</p> <p>A table is included to convey the status of individual services running on the media resource instance. This table is only available for selected media servers (e.g., Dialogic PowerMedia XMS).</p>

To perform direct actions on the media resource, select one of the following buttons.

Item	Description
Restart Machine	The media resource restarts.
Restart Services	The services running on the media resource restart.
Start Services	The services on the media resource start.
Stop Services	The services running on the media resource stop.
Graceful Shutdown	The media resource does not accept any new traffic and stops service when the active calls are completed.

The MRB does not need licensing because it obtains licensing information from the XMS that it is provisioned with. To upload and apply a Media Server License file to the media server, proceed as follows:

1. Click the **Choose File** button and select the desired Media Server License file.
2. Click **Apply** to save the changes or click **Cancel** to abort the operation.

Port Usage

To access the **Port Usage** page from the **Media Servers** page, click on a media server's **View Port Usage** hyperlink. The **Port Usage** page provides information on an MRB-managed media server.

Port Usage

Location: New York Hostname: 192.168.2.59 Port: 5070

Mixer Ports

Codec	Available Mixer Ports	Used Mixer Ports	Total Mixer Ports
G723	500	0	500
G726-32	500	0	500
PCMU	500	0	500
G729	500	0	500
AMR	500	0	500
MP4V-ES	300	0	300
H264	300	0	300
GSM-EFR	500	0	500
iLBC	500	0	500
GSM	500	0	500
H263-2000	300	0	300
H263-1998	300	0	300

IVR Ports

Codec	Available IVR Ports	Used IVR Ports	Total IVR ports
G723	500	0	500
G726-32	500	0	500
PCMU	500	0	500
G729	500	0	500
AMR	500	0	500
MP4V-ES	300	0	300
H264	300	0	300
GSM-EFR	500	0	500
iLBC	500	0	500
GSM	500	0	500
H263-2000	300	0	300
H263-1998	300	0	300

[Back](#)

Port usage information is split into IVR ports and Mixer ports. The following information is provided for both categories.

Item	Description
Codec	The codec used for the reported figures.
Available IVR/Mixer Ports	The reported number of available IVR/Mixer ports on a media resource.

Item	Description
Used IVR/Mixer Ports	The reported number of IVR/Mixer ports currently in use on a media resource.
Total IVR/Mixer Ports	The reported total number of IVR/Mixer ports supported on a media resource.

Manage Conferences

To access the **Manage Conferences** page from the **Media Servers** page, click on a media server's **Manage Conferences** hyperlink. The **Manages Conferences** page provides a list of conferences that are active on the media resource.

Manage Conferences

Location: New York Hostname: 192.168.2.112 Port: 5070

Number of Active Bridged Calls: 0

Conference Id	Conference Name	Number Of Calls	Priority	End Calls
2857		1	100	End




The following information is provided.

Item	Description
Conference ID	The unique identifier for the conference instance being hosted on the media resource.
Conference Name	An optional text tag to provide a more meaningful reference to a conference instance.
Number of Calls	The number of active calls currently participating in a conference instance.
Priority	The priority associated with a conference instance. Priority is taken into account when moving conference instances across media resources. A conference call with a priority of "1" is moved first, a conference call with a priority of "100" is moved last, and a conference call with a priority of "0" is not moved at all. The default value is 100.
End Calls	End a specific conference instance by clicking the link.

Manage Media Servers

The **Manage Media Servers** page allows new and existing media servers to be configured.

Manage Media Servers

Status	Media Server Detail	Host	Port	Listen On Tls ?	TLS Port	Location	
	Dialogic PowerMedia XMS	192.168.2.112	5070	false		New York	Manage
	Dialogic PowerMedia XMS	192.168.2.12	5070	false		New York	Manage
	Dialogic PowerMedia XMS	192.168.2.59	5070	false		New York	Manage

Add Media Server

Add a Media Server

To add a media server, proceed as follows:

1. Click the **Add Media Server** button on the **Manage Media Servers** page. The **Add Media Server** page appears.

Add Media Server

Host ?

Port ?

Listen on TLS ☐ TLS Port ?

Location ?

2. Enter the host address and the port number.
3. Select **Listen on TLS** if the media server is set up to use TLS communications. The **TLS Port** field reflects the SIP port being used by the MRB adaptor for the media server.
4. Select the location of the media server.
5. Click **Add** to finish adding a new media server. The new media server will appear on the **Manage Media Servers** page. Click **Cancel** to abort the operation.


Manage a Media Server


To manage a media server, proceed as follows:


1. Click the **Manage** hyperlink of the media server that needs to be configured. The **Media Server** page appears.


Media Server


Media Server **192.168.2.59:5070 3**

Status 

Host 

Port 

Listen on TLS ☐ TLS Port 

Location 

2. Click one of the following buttons:
 - **Cancel** navigates back to the **Manage Media Servers** page.
 - **Take off line** takes the media server offline and allows further administration tasks to occur.
 - **End all conferences on MS** allows the user to terminate all conference instances that are currently being hosted on the selected media server.

To make and apply changes, the **Take off line** button must be selected to take the media server out of service. The traffic light turns gray. When the **Take off line** button is clicked, the following buttons appear:

- **Cancel** navigates back to the **Manage Media Servers** page.
 - **Save** saves the media server configuration changes.
 - **Bring online** returns the media server to active service. Click this after changes have been made to apply them.
 - **Delete** removes the media server from the MRB pool.
 - **Move calls to another MS** moves all active conference calls from the selected media server to an alternative media server (if available). An algorithm is used to select a new media server, and if an appropriate match is found, the calls are relocated.
3. Make changes to the configuration of the media server as necessary.
 4. Click **Bring online** to apply the changes.
 5. Click **Save** to save the changes and return to the **Manage Media Servers** page.












Resource Summary

The **Resource Summary** page provides an aggregated view of media server resources available within the MRB cluster. The total number of active media servers is shown at the top of the page. Aggregated port usage information is provided for each codec (audio and video). Other totals are also displayed on this page (e.g., XMS Resource Meters).



Aggregated Media Server Information

General Info	
Active Media Servers	3

Audio Codecs

Codec	Ports	Used	Free	
AMR	1500	0	1500	
AMR-WB	500	0	500	
G722	500	0	500	
G723	1500	0	1500	
G726-32	1500	0	1500	
G729	1500	0	1500	
GSM	1500	0	1500	
GSM-EFR	1500	0	1500	
Opus	500	0	500	
PCMA	1500	79	1421	
PCMU	1500	79	1421	
iLBC	1500	0	1500	

Video Codecs

Codec	Ports	Used	Free	
H263	610	0	610	
H263-1998	610	0	610	

MS HA Statistics

The **MS HA Statistics** page provides information that enables an administrator to view the outcome of when conference calls are moved between media servers following media server failures.

MS HA Statistics

Time/Date	Failed MS	Type (Manual/Automatic)	Total Calls	Successful Moves	Failed Moves
06/07/2015 16:04:25,645	Dialogic PowerMedia XMS (192.168.2.112:5070, New York)	Automatic	0	0	0
06/07/2015 16:06:09,842	Dialogic PowerMedia XMS (192.168.2.112:5070, New York)	Automatic	0	0	0

The following information is provided.

Item	Description
Time/Date	The time and date that the move call operation occurred.
Failed MS	The identity of the source media server where calls are moved from.
Type (Manual/Automatic)	The type of move call operation that took place: either a Manual Move (as a result of user intervention) or an Automatic Move (as a result of media server failure).
Total Calls	The total number of calls that were attempted to be moved.
Successful Moves	The number of successful calls that were moved as part of a move call operation.
Failed Moves	The number of calls that were moved unsuccessfully as part of a move call operation.

Locations

The **Locations** page provides a list of valid locations that media server resources can reside within the MRB managed pool and accompanying statistics. Groups of media servers that are labeled with the same location can be provided with certain functionalities. In addition, messages can be steered to a preferred location. An administrator can create additional locations by clicking the **Add Location** button. An existing location can be edited using the **Edit** hyperlink and deleted using the **Delete** hyperlink.

Locations

	Location name	Notes	No. MSs	No. MSs on line	No. MSs off line			
Edit	New York		3	3	0	Delete		
Edit	London		0	0	0	Delete		

[Add Location](#)

User Administration

The **User Administration** page allows users of the MRB to be provisioned and managed. An administrator can create additional users by clicking the **Add User** button. An existing user can be deleted clicking the **Delete** hyperlink and edited using the **Change** hyperlink.

User Administration

Name	Username	Role		
	root	Super user	Delete	Change
	nst	Low privileges	Delete	Change

Add a User

The **Add User** page allows users of the MRB to be provisioned and the user role to be set. To successfully create a user, all of the fields must be populated. The administrator must then click the **Add user** button. Clicking the **Cancel** button aborts the addition of a new user to the MRB.






Add user

Username	<input type="text"/>	
Real name	<input type="text"/>	
Password	<input type="password"/>	
Repeat Password	<input type="password"/>	
User role	<input type="text" value="Low privileges"/>	

Change a User

The **Change User** page provides identical user manipulation options as provided by the **Add User** page. Click **Update** when the changes have been made.

User Details

Username	<input type="text" value="root"/>	
Existing password	<input type="password" value="*****"/>	
Real name	<input type="text"/>	
Password	<input type="password"/>	
Repeat Password	<input type="password"/>	
User role	<input type="text" value="Super user"/>	

User Roles

The **User Roles** page allows you to adjust the user settings. An administrator can create additional user roles by clicking the **Add Role** button, adjusting the settings, and then clicking the **Save** hyperlink. An existing user can edit by clicking the **Edit** hyperlink, adjusting the settings, and then clicking the **Save** hyperlink. An existing user can be deleted using the **Delete** hyperlink.

User Roles

	Role name	User	MRB	Media Servers	
Edit	New Role	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete
	Low privileges	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Super user	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

[Add Role](#)

The following user settings are available.


Item	Description
User	Allows a user to create, edit, add, and delete new users.
MRB	Allows a user to configure an MRB cluster, SNMP trap configuration, MRB configuration (e.g., log levels), etc.
Media Servers	Allows a user to create and add a media server and conduct media server related tasks.

User Policies

The **User Policies** page allows user policies of the MRB to be edited. To change the **User idle time before logout** and the **Minimum password length** fields, click **Update**, make the changes, and click **Save** to save the changes.

User Policies

User idle time before logout 







Minimum password length 

[Update](#)

MRB Configuration

The **MRB Configuration** page allows for MRB-specific information to be provisioned.

MRB Configuration

Push Route	<input type="text"/>	
Adaptor Poll Period	<input type="text" value="0.2"/>	
Enable Detailed Logging	<input checked="" type="checkbox"/>	
Stack Logging	<input type="checkbox"/>	
SIP Message Logging	<input checked="" type="checkbox"/>	
Enable MS Allocation Buffer	<input checked="" type="checkbox"/>	
MS Allocation Buffer Size	<input type="text" value="4"/>	
Cascade Conferences	<input checked="" type="checkbox"/>	
HTTP Call Control API REST Port	<input type="text" value="8181"/>	
SIP RTP Proxy	<input checked="" type="checkbox"/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Restart"/> <input type="button" value="Shutdown"/>		

The following configuration options are available.

Item	Description
Push Route	<p>Enables the MRB to insert a specified preloaded SIP Route header in all outgoing SIP INVITE requests, thus forcing the next hop destination. For example, if "sip:s-cscf@dialogic.com" is specified, the following SIP Route header would be inserted in all outgoing initial SIP INVITE requests:</p> <p>Route: <sip:s-cscf@dialogic.com;lr></p> <p>Because it can be a requirement that all requests traverse the Serving Call Session Control Function (S-CSCF) as part of the onward journey, preloaded SIP Route headers can be pushed for all outgoing initial SIP INVITE requests when deploying in an IP Multimedia Subsystem (IMS) architecture.</p>
Adaptor Poll Period	The value in seconds for the statistics retrieval period from the media servers being managed by the MRB.
Enable Detailed Logging	Allows a user to turn on and off detailed logging. This option does NOT require a restart.
Stack Logging	Allows a user to turn on and off full logging output to the log files. This option does NOT require a restart. This option should only be enabled under the guidance of Dialogic support.
SIP Message Logging	Allows a user to turn on and off SIP message logging output to the log files. This option does NOT require a restart.
Enable MS Allocation Buffer	Enables the administrator to intentionally skew the media server selection algorithm such that batches of requests arrive at a single instance with a specified period of time as determined by the MS Allocation Buffer Size. This feature is useful in call flows such as transcoding.


Item	Description
MS Allocation Buffer Size	The number of calls to be batched to a specific media server if the MS allocation buffer is enabled.
Cascade Conferences	<p>Overflow facility that will use ports on an alternative media resource for a conference instance if none are available to join new participants. This is achieved by cascading mixes across two media resources.</p> <p>Note: If using this feature, refer to the following limitations:</p> <ul style="list-style-type: none"> Active speaker notifications from the XMS for that conference will not be correct. Video conference cascading is not supported. Only audio conferences can be cascaded.
HTTP Call Control API REST Port	Configures the port to be used when accessing the HTTP Call Control REST API. Refer to the <i>Dialogic® PowerMedia™ XMS RESTful API User's Guide</i> at http://www.dialogic.com/webhelp/XMS/3.2/XMS_RESTfulAPIUser.pdf .
SIP RTP Proxy	This configuration option is available if the Media Proxy feature is enabled during the installation. When SIP RTP Proxy is enabled, SIP media traffic utilizes the RTP proxy and does not re-INVITE clients on MRF failure.

Click **Save** to save the configuration, **Cancel** to abort the operation, **Restart** to restart the MRB, and **Shutdown** to turn off the MRB.



Manage Conferences

The **Manage Conferences** page provides configuration options related specifically to conferencing.

Manage Conferences

Conference Clean Up ☒ 

Conference Mix High Availability

Enable Mix HA ☒ 
 RTP Failure Detection ☒
 Detection Period 
 SIP Re-invite on RTP Failure ☒

The following configuration options are available.



Item	Description
Conference Clean Up	Enabling this feature results in all conferences being cleaned up when the MRB connects. When an XMS transitions from a failed or offline state to an active state, the MRB cleans up conferences on the given XMS.
Enable Mix HA	The MRB will attempt to preserve conference calls on detection of failure of a media server.
RTP Failure Detection	The MRB creates a single RTP stream to each provisioned media server for monitoring. The MRB will look for breaks in RTP as an indicator of media server failure.
Detection Period	The period in milliseconds that the MRB looks for break in RTP in conjunction with the RTP Failure Detection feature.
SIP Re-invite on RTP Failure	On detecting an RTP failure, the MRB will send an additional re-INVITE to check the media server's health if this feature is provisioned.


Click **Save** to save configuration settings or click **Cancel** to return to the previous page.

Manage MRB Cluster

The **Manage MRB Cluster** page is used to configure a Highly Available (HA) pair of MRB nodes.

Manage MRB cluster

Status	Name	Host	Total SIP Calls	Management Mode	
	MRB-backup	192.168.2.117:5070	0	Slave	Manage
	mrB	192.168.2.74:5070	0	Master	Manage

[Add MRB Node](#) 

The **Manage MRB Cluster** page provides a status overview of an MRB cluster deployment and the currently configured nodes. It provides two main options: **Manage**, which allows manipulation of an existing MRB node in a cluster, and **Add MRB Node**, which allows the addition of a new MRB node in a cluster. Both navigate to the same page.

MRB node

MRB node new MRB-192.168.2.117:5070:Slave

Name	MRB-backup	✓
SIP Hostname and port	192.168.2.117:5070	✓
Listen on TLS	<input type="checkbox"/>	
TLS port	5061	✓
Security Profile	▼	✓
JMX Hostname and port	192.168.2.117:5100	✓
Paired MRB node ID	not HA ▼	✓
Management mode	Slave	
MRB/MLF	Mrb ▼	
<input type="button" value="Back"/> <input type="button" value="Save"/> <input type="button" value="Delete"/>		

The following configuration options are available.










Item	Description
Name	Supplies the name of the MRB node in a cluster.
SIP Hostname and port	Supplies the SIP hostname/address and port being used by the MRB node.
Listen on TLS	Whether or not this MRB node is set up to communicate over a TLS channel.
TLS Port	If Listen on TLS is selected, this is the port used for TLS data.
Security Profile	If Listen on TLS is selected, this is the security profile to be used to provide the MRB node's certificate/key. Note: Refer to Appendix D: Create Self-Signed Certificates and Keys and Appendix E: Add a Customized Security Profile for guidelines on adding customized security profiles.
JMX Hostname and port	Supplies the Java Management Technology (JMX) hostname and port being used by the MRB node.
Paired MRB node ID	Allows two MRB nodes (active and standby) to be linked in an HA pair.
Management mode	Displays the current management mode of the MRB node (active or standby).
MRB/MLF	Reserved for future use.

Click **Back** to return to the **Manage MRB Cluster** page. Click **Save** to save configuration settings. Click **Delete** to remove the MRB node.

Networking Configuration

The **Networking Configuration** page is used to manage listening and communication interfaces.

Networking Configuration

VIP Manager Listening Port	<input type="text" value="5111"/>	
External Load Balancer	<input checked="" type="checkbox"/>	
Traffic VIP Address	<input type="text"/>	
Traffic VIP Port	<input type="text" value="0"/>	
Traffic VIP Interface	<input type="text" value="enp0s3"/>	
Media VIP Address 1	<input type="text"/>	
Media VIP Interface 1	<input type="text" value="enp0s3"/>	
Media VIP Address 2	<input type="text"/>	
Media VIP Interface 2	<input type="text" value="enp0s3"/>	

The following configuration options are available.

Item	Description
VIP Manager Listening Port	The port on which the MRB communicates with the VIP Manager process.
External Load Balancer	Specifies if the MRB is being deployed with an external Load Balancer. Checking this option means the MRB will not configure the traffic VIP directly, since traffic will be routed through the load balancer, which will control the VIP.
Traffic VIP Address	MRB Virtual IP address for call traffic (i.e., SIP/HTTP).
Traffic VIP Port	The accompanying port for the traffic VIP address.
Traffic VIP Interface	The interface name for the SIP VIP.
Media VIP Address	A VIP address used for the RTP proxy such that media will continue to flow via the MRB when node failure occurs or a user is moving RESTful and WebRTC calls. This configuration option is available if the Media Proxy feature is enabled during the installation.

Item	Description
Media VIP Interface	The interface that will be used to provide the media VIP. This configuration option is available if the Media Proxy feature is enabled during the installation.

Click **Save** to save the configuration settings and click **Cancel** to return to the previous page.

VIP Status

The **VIP Status** page provides the current state of the VIP Manager process. The page also contains up-to-date information regarding the VIPs managed by the MRB cluster. The page lists each VIP and the IP address of the node currently serving the VIP.

VIP Manager - Running








VIP	Controlling Node IP Address
192.168.2.171	192.168.2.74
192.168.2.172	192.168.2.74

[Restart VIP Manager](#)

SNMP Configuration

The **SNMP Configuration** page allows for SNMP-related provisioning.

MRB Notifications Configuration

Enabled	<input type="checkbox"/>	
Destination hostname	<input type="text"/>	
Destination port	<input type="text" value="162"/>	
Additional Destination hostname	<input type="text"/>	
Additional Destination port	<input type="text"/>	
SNMP Community Name	<input type="text" value="public"/>	
Java class name for notifications	<input type="text" value="com.nstechnologies.commo"/>	

[Save](#) [Cancel](#)

The following configuration options are available.

Item	Description
Enabled	A check box that enables or disables MRB notifications.
Destination hostname	The host to send MRB SNMP traps.
Destination port	The port to send MRB SNMP traps.
Additional Destination hostname	An additional location that can optionally be provisioned to send MRB SNMP traps.

Item	Description
Additional Destination port	An additional port associated with the Additional Destination hostname field to send MRB SNMP traps.
SNMP Community Name	The community name for SNMP notifications.
Java class name for notifications	Allows custom notifications to be sent. The field contains the Java class name to be used instead of the default SNMP traps.

Click **Save** to save the configuration settings. Click **Cancel** to return to the previous page.

SNMP Notifications

The **SNMP Notifications** page provides a list of events that can appear in the MRB log files and also raise SNMP traps. Click **Save** to save the configuration settings.

SNMP Notifications

Event	Send Notification
MRB HA connection failed	<input type="checkbox"/>
A user role has been changed	<input checked="" type="checkbox"/>
MRB HA connection succeeded	<input type="checkbox"/>
MRB stack logging configured	<input type="checkbox"/>
A MS has been added	<input checked="" type="checkbox"/>
A location has been deleted	<input checked="" type="checkbox"/>
A location has been added	<input checked="" type="checkbox"/>
MRB media vips configured	<input type="checkbox"/>
A user has been deleted	<input checked="" type="checkbox"/>
A user has logged into the admin console	<input checked="" type="checkbox"/>
A MRB node has stopped	<input checked="" type="checkbox"/>
VIP interface name set	<input type="checkbox"/>
A MRB node has failed to start	<input checked="" type="checkbox"/>
An MRB node has been deleted	<input checked="" type="checkbox"/>
A user has been changed	<input checked="" type="checkbox"/>
A user has been added	<input checked="" type="checkbox"/>
An MRB node has been forced to master	<input checked="" type="checkbox"/>
A MS is now offline	<input checked="" type="checkbox"/>
MRB traffic vip port configured	<input type="checkbox"/>
MRB cascade conferences configured	<input type="checkbox"/>
A MS has been deleted	<input checked="" type="checkbox"/>
A user role has been added	<input checked="" type="checkbox"/>

Save

Selection Algorithms

Reserved for future use.

Unaware Mode

The **Unaware Mode** page provides default properties for an incoming call if the call's values cannot be determined from other mechanisms such as the SIP P-MRB header.

Unaware Mode (IUMM)

Default Option

The default option used by the MRB in Unaware Mode is: Conferencing

Conferencing

Location

Audio

Video

IVR

Location

Audio

Video

The same settings are available for the **Conferencing** and **IVR** sections. The following configuration options are as follows.

Item	Description
Location	<p>Set the default location for a request, which is used for appropriate media server selection. Select from a drop-down list of valid locations that have been provisioned for the MRB.</p> <p>If the value No specific location is selected from the drop-down list, no explicit default location is set for request processing. Therefore, the MRB location routing is not applied to newly received requests and all media server instances are considered as part of the selection process regardless of location.</p>
Audio	<p>Number of Ports: Specify the number of audio ports required in association with the request.</p> <p>Default Codec: Specify the default audio codec in association with the request.</p>
Video	<p>Number of Ports: Specify the number of video ports required in association with the request.</p> <p>Default Codec: Specify the default video codec in association with the request.</p>

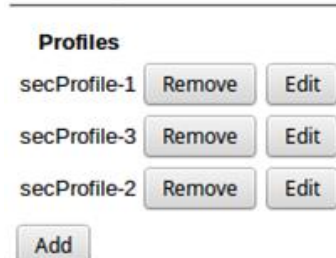
Click **Make Default** to make Conferencing or IVR the default for unaware mode. Click **Save** to save the configuration settings. Click **Cancel** to return to the previous page.

Security Profiles

The **Security Profiles** page enables the MRB to be configured for secure protocol communication, such as Transport Layer Security (TLS), over transports such as SIP. Security profiles are only relevant to TLS connections.

Note: Refer to [Appendix D: Create Self-Signed Certificates and Keys](#) and [Appendix E: Add a Customized Security Profile](#) for guidelines on adding customized security profiles.

Security Profiles



The screenshot shows a section titled "Profiles" with a list of three security profiles: secProfile-1, secProfile-3, and secProfile-2. Each profile has "Remove" and "Edit" buttons next to it. Below the list is an "Add" button.

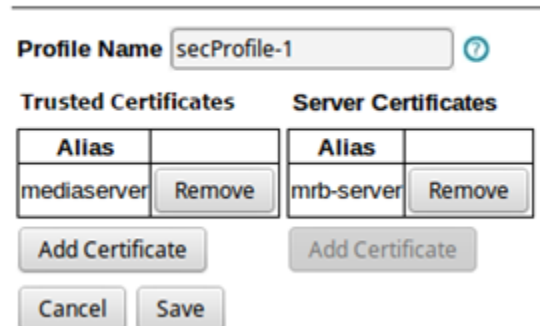
Profiles	
secProfile-1	<button>Remove</button> <button>Edit</button>
secProfile-3	<button>Remove</button> <button>Edit</button>
secProfile-2	<button>Remove</button> <button>Edit</button>

Add

This page displays the current set of security profiles that are configured for the MRB. To remove a security profile, click **Remove**. To edit a security profile, click **Edit**. To add a security profile, click **Add**.

The **Add** button allows a new security profile to be created. When the **Add** button is clicked, the **Security Profile** page appears.

Security Profile



The screenshot shows the "Security Profile" page. At the top is a "Profile Name" field with the value "secProfile-1" and a help icon. Below this are two columns: "Trusted Certificates" and "Server Certificates". Each column has a table with "Alias" and "Remove" buttons. The "Trusted Certificates" table has one entry with alias "mediaserver". The "Server Certificates" table has one entry with alias "mrb-server". Below each table is an "Add Certificate" button. At the bottom are "Cancel" and "Save" buttons.

Profile Name: ?

Trusted Certificates	
Alias	
mediaserver	<button>Remove</button>

Add Certificate

Server Certificates	
Alias	
mrb-server	<button>Remove</button>

Add Certificate

Cancel Save

The **Security Profile** page allows both client and server certificates to be added to the profile.

Note that a security profile requires exactly one server certificate entry but can have 0 to n trusted certificates configured. The existing certificates that have been assigned to the security profile are listed under the column headers "Trusted Certificate" and "Server Certificate".

The following configuration options are available.

Item	Description
Remove	The Remove button causes the appropriate certificate to be deleted from the profile.
Add Certificate	The Add Certificate button causes the appropriate certificate to be added to the profile. Refer to the Add a Trusted Certificate and Add a Server Certificate sections that follow for more information.

When you are finished making changes to the **Security Profiles** page, click **Save** to save the configuration settings. If invalid data is provided, an error message appears. If this occurs, validate the data and click **Save** again. Click **Cancel** to return to the previous page without saving pending changes.

Add a Trusted Certificate

To add a trusted certificate, click the **Add Certificate** button and enter a valid alias on the **Add Trusted Certificate** page. Click **Browse** to find and select the appropriate certificate file (locally stored). This is the SSL certificate file (X.509) for a secure connection to any nodes (required for SSL re-encryption mode). When the alias and certificate file have been added, click **Add** to add the certificate or **Cancel** to return to the previous page.

Add Trusted Certificate



Add a Server Certificate

To add a server certificate, click the **Add Certificate** button and enter a valid alias on the **Add Server Certificate** page. Click **Browse** to find and select the appropriate certificate file (stored locally). This is the signed certificate containing the public key, which is sent to the client when a SSL connection is made. Click **Browse** to find and select the appropriate private key file (stored locally). This is the complementary private key used for encryption when an SSL connection is made. This must be a DER file in PKCS8 format. When the alias and certificate file have been added, click **Add** to add the certificate or **Cancel** to return to the previous page.

Add Server Certificate



Logging

The **Logging** page displays the log and allows different search settings to be applied to the log. To apply search settings, click **Update**.

Logging

No entries per page

Page 1 of 1

Time/Date	Who	Event	Description	Other information
9:32:55 AM Jul 7, 2015	system	health.ms.alive	A MS has been detected as alive	192.168.2.59:5070 3
9:32:54 AM Jul 7, 2015	system	admin.ms.add	A MS has been added	Media Server 0 192.168.2.59:5070
9:26:58 AM Jul 7, 2015	root	console.login	A user has logged into the admin console	

4. Appendix A: Enabling HTTPS with Jetty

Proceed as follows to configure Jetty to enable a secure connection. If an existing private key or company certificate is being used, skip steps 1 and 2 as necessary.

1. Create a private key using the following command and entering a pass phrase in the output.

```
$ openssl genrsa -des3 -out myCompany.key
```

Sample Output

```
Generating RSA private key, 2048 bit long modulus
.....+++
...+++
e is 65537 (0x10001)
Enter pass phrase for myCompany.key: [pwJetty123]
Verifying - Enter pass phrase for myCompany.key: [pwJetty123]
```

This creates the private key file *myCompany.key*. Verify the private key using the following command.

```
$ openssl rsa -in myCompany.key -check
```

Sample Output

```
Enter pass phrase for myCompany.key: [pwJetty123]
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAr6530+uwL0Ohoq8OQFadub9MMilqak2tDhI9k25N5iZgElkL
: :
RldsDTpOMqikPFbTlAw98mNTcSMFiOiUcg07AEswqYfuuc8iR44=
-----END RSA PRIVATE KEY-----
```

2. Create a certificate using the private key that was just created and enter the applicable information.

```
$ openssl req -new -x509 -key myCompany.key -out myCompany.crt
```

Sample Output

```
Enter pass phrase for myCompany.key: [pwJetty123]
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:UK
State or Province Name (full name) [Some-State]:myState
Locality Name (eg, city) []:myTown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:myCompany
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:myServer.com
```

```
Email Address []:me@company.com
```

This creates the certificate file *myCompany.crt*. Verify the certificate using the following command.

```
$ openssl x509 -in myCompany.crt -text -noout
```

Sample Output

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 17639746180074664251 (0xf4ccf7b0ff67713b)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=UK, ST=myState, L=myTown, O=myCompany, OU=Engineering,
CN=myServer.com/emailAddress=me@company.com
Validity
Not Before: Sep 2 07:18:47 2015 GMT
Not After : Oct 2 07:18:47 2015 GMT
Subject: C=UK, ST=myState, L=myTown, O=myCompany, OU=Engineering,
CN=myServer.com/emailAddress=me@company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:af:ae:77:3b:eb:b0:2f:43:a1:a2:af:0e:40:56:
: :
57:38:3a:84:c4:0d:24:3b:2c:8f:e1:c3:b5:56:0a:
fe:23
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
39:09:70:E1:9A:99:A6:DE:90:CB:AF:70:6E:D4:A9:74:68:71:11:C1
X509v3 Authority Key Identifier:
keyid:39:09:70:E1:9A:99:A6:DE:90:CB:AF:70:6E:D4:A9:74:68:71:11:C1
X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
7a:d9:c5:c4:3a:93:77:35:b9:de:57:96:c5:36:fa:26:ab:63:
: :
6b:b4:de:06:1a:65:c8:36:9a:85:7a:83:79:04:ee:9f:f3:89:
c9:83:23:e0
```

3. Add the certificate to the keystore using the following command and enter the applicable information.

```
$ keytool -keystore myCompany-Jetty.jks -import -alias myCompany -file myCompany.crt -trustcacerts
```

Sample Output

```
Enter keystore password: [pwJetty123]
Re-enter new password: [pwJetty123]
Owner: EMAILADDRESS=me@company.com, CN=myServer.com, OU=Engineering, O=myCompany,
L=myTown, ST=myState, C=UK
```

```

Issuer: EMAILADDRESS=me@company.com, CN=myServer.com, OU=Engineering, O=myCompany,
L=myTown, ST=myState, C=UK
Serial number: f4ccf7b0ff67713b
Valid from: Wed Sep 02 08:18:47 BST 2015 until: Fri Oct 02 08:18:47 BST 2015
Certificate fingerprints:
MD5: 66:D1:81:98:12:05:CC:7C:7C:9B:1E:2F:44:1F:9D:29
SHA1: CF:E8:39:E0:E7:7F:B0:96:CE:80:72:7E:4B:C0:4A:2B:D2:DB:94:DA
SHA256:
A0:34:77:FA:67:0D:54:AC:14:6D:EF:98:6C:A7:AB:1C:01:7A:99:6D:08:85:B1:3E:8D:02:6E:28:65:39
:74:31
Signature algorithm name: SHA256withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 39 09 70 E1 9A 99 A6 DE 90 CB AF 70 6E D4 A9 74 9.p.....pn..t
0010: 68 71 11 C1 hq..
]
]
#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 39 09 70 E1 9A 99 A6 DE 90 CB AF 70 6E D4 A9 74 9.p.....pn..t
0010: 68 71 11 C1 hq..
]
]
Trust this certificate? [no]: yes
Certificate was added to keystore

```

This creates the keystore file *myCompany-Jetty.jks*. Verify the keystore contents using the following command.

```
$ keytool -list -keystore myCompany-Jetty.jks
```

Sample Output

```

Enter keystore password: [pwJetty123]
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
mycompany, 02-Sep-2015, trustedCertEntry,
Certificate fingerprint (SHA1):
CF:E8:39:E0:E7:7F:B0:96:CE:80:72:7E:4B:C0:4A:2B:D2:DB:94:DA

```

4. Create a Certificate Signing Request (CSR) using the following command and enter the applicable information.

```
$ openssl req -new -key myCompany.key -out myCompany.csr
```

Sample Output

```
Enter pass phrase for myCompany.key: [pwJetty123]
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:UK
State or Province Name (full name) [Some-State]:myState
Locality Name (eg, city) []:myTown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:myCompany
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:myServer.com
Email Address []:me@company.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:pwJetty123
An optional company name []:
```

This creates the CSR file *myCompany.csr*. Verify the contents of the CSR using the following command.

```
$ openssl req -text -noout -verify -in myCompany.csr
```

Sample Output

```
verify OK
Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=UK, ST=myState, L=myTown, O=myCompany, OU=Engineering,
CN=myServer.com/emailAddress=me@company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:af:ae:77:3b:eb:b0:2f:43:a1:a2:af:0e:40:56:
: :
57:38:3a:84:c4:0d:24:3b:2c:8f:e1:c3:b5:56:0a:
fe:23
Exponent: 65537 (0x10001)
Attributes:
challengePassword :unable to print attribute
Signature Algorithm: sha256WithRSAEncryption
8f:65:04:17:24:b4:3f:32:0c:87:75:22:8b:21:a8:ca:98:62:
```

```
: :
55:21:82:5a:8c:e9:18:8e:b7:98:53:32:7a:7f:77:5e:55:08:
7f:76:96:e2
```

5. Create a PKCS12 bundle containing the private key and its x509 certificate using the following command and enter the applicable information.

```
$ openssl pkcs12 -inkey myCompany.key -in myCompany.crt -export -out myCompany.p12
```

Sample Output

```
Enter pass phrase for myCompany.key: [pwJetty123]
Enter Export Password: [pwJetty123]
Verifying - Enter Export Password: [pwJetty123]
```

This creates the PKCS12 bundle file *myCompany.p12*. Verify the contents of the PKCS12 bundle using the following command.

```
$ openssl pkcs12 -info -in myCompany.p12
```

Sample Output

```
Enter Import Password: [pwJetty123]
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
localKeyID: CF E8 39 E0 E7 7F B0 96 CE 80 72 7E 4B C0 4A 2B D2 DB 94 DA
subject=/C=UK/ST=myState/L=myTown/O=myCompany/OU=Engineering/CN=myServer.com/emailAddress=me@company.com
issuer=/C=UK/ST=myState/L=myTown/O=myCompany/OU=Engineering/CN=myServer.com/emailAddress=me@company.com
-----BEGIN CERTIFICATE-----
MIID9zCCAt+gAwIBAgIJAPTm97D/Z3E7MA0GCSqGSIb3DQEBCwUAMIGRMQswCQYD
: :
CTgULXcnl6Zyxm9E1P1XjWXpmCBtSTMUOoNR1YBV8LmLCo+LsGu03gYaZcg2moV6
g3kE7p/zicmDI+A=
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
localKeyID: CF E8 39 E0 E7 7F B0 96 CE 80 72 7E 4B C0 4A 2B D2 DB 94 DA
Key Attributes: <No Attributes>
Enter PEM pass phrase: [pwJetty123]
Verifying - Enter PEM pass phrase: [pwJetty123]
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI4W6snmuYS6ICAggA
: :
Ks7khnExAVuwu5/kbxBH90rf/cFFMQ/QOFOYlITVchhbBjRgYcnEVp7dUPSEWum
a5E=
-----END ENCRYPTED PRIVATE KEY-----
```

6. Insert the PKCS12 bundle in the keystore using the following command and enter the applicable information.

```
$ keytool -importkeystore -srckeystore myCompany.p12 -srcstoretype PKCS12 -destkeystore myCompany-Jetty.jks
```

Sample Output

```
Enter destination keystore password: [pwJetty123]
Enter source keystore password: [pwJetty123]
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

This updates keystore file *myCompany-Jetty.jks*. Verify the contents of the updated keystore using the following command.

```
$ keytool -list -keystore myCompany-Jetty.jks
```

Sample Output

```
Enter keystore password: [pwJetty123]
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 2 entries
mycompany, 02-Sep-2015, trustedCertEntry,
Certificate fingerprint (SHA1):
CF:E8:39:E0:E7:7F:B0:96:CE:80:72:7E:4B:C0:4A:2B:D2:DB:94:DA
1, 02-Sep-2015, PrivateKeyEntry,
Certificate fingerprint (SHA1):
CF:E8:39:E0:E7:7F:B0:96:CE:80:72:7E:4B:C0:4A:2B:D2:DB:94:DA
```

7. Copy the updated keystore to an area that can be used by the Jetty installation.

```
$ cp myCompany-Jetty.jks <jetty-install-dir>/etc/
```

8. Update the Jetty SSL config file to use the new keystore as follows:

- a. Locate the *ssl/ContextFactory* block in **<jetty-install-dir>/etc/jetty-ssl.xml**.

```
<New id="sslContextFactory" class="org.eclipse.jetty.http.ssl.SslContextFactory">
<Set name="KeyStore"><Property name="jetty.home" default="." />/etc/keystore</Set>
<Set name="KeyStorePassword">OBF:1vnY1zl01x8e1vnw1vn61x8glzlulvn4</Set>
<Set name="KeyManagerPassword">OBF:1u2ulwml1z7s1z7a1wnl1u2g</Set>
<Set name="TrustStore"><Property name="jetty.home" default="." />/etc/keystore</Set>
<Set name="TrustStorePassword">OBF:1vnY1zl01x8e1vnw1vn61x8glzlulvn4</Set>
</New>
```

Note: The passwords are listed in obfuscated form. Jetty provides a utility within the installation to generate obfuscated passwords.

- b. In the Jetty install directory, run the following command using the passwords created in the previous steps. Note the value of the obfuscated (OBF) version of the password.

```
$ java -cp lib/jetty-util-8.1.10.v20130312.jar
org.eclipse.jetty.util.security.Password pwJetty123
```

Sample Output

```
pwJetty123
OBF:1lfglmmcldi01x0r1z0f1z0f1x1vldgmlmi11lc2
MD5:c0e1ec92ed0dc1b26daa291604cd0d69
```

- c. Update the *sslContextFactory* configuration accordingly. Note that the password and keystore locations have been updated.

```
<New id="sslContextFactory" class="org.eclipse.jetty.http.ssl.SslContextFactory">
<Set name="KeyStore"><Property name="jetty.home" default="." />/etc/myCompany-
Jetty.jks</Set>
<Set name="KeyStorePassword">OBF:1lfglmmcldi01x0r1z0f1z0f1x1vldgmlmi11lc2</Set>
<Set name="KeyManagerPassword">OBF:1lfglmmcldi01x0r1z0f1z0f1x1vldgmlmi11lc2</Set>
<Set name="TrustStore"><Property name="jetty.home" default="." />/etc/myCompany-
Jetty.jks</Set>
<Set name="TrustStorePassword">OBF:1lfglmmcldi01x0r1z0f1z0f1x1vldgmlmi11lc2</Set>
</New>
```

- d. In the Jetty startup file (**<jetty-install-dir>/start.ini**), look for the following line: # etc/jetty-ssl.xml. Uncomment and save.
9. Validate the changes. Take note of the Jetty ports (i.e., 8888 is the standard Jetty port for MRB/LB UI and 8443 is the standard default HTTPS port).

```
$ netstat -nlp | grep -E '8888|8443'
```

If 8443 is not an appropriate secure port, change it using the following procedure:

- a. Restart Jetty to apply the changes using the following command.

```
$ service jetty restart
```

- b. Verify that Jetty is listening on its secure port using the following command.

```
$ netstat -nlp | grep -E '8888|8443'
```

- c. Using a web browser, navigate to the new secure port: https://<Jetty-IP>:8443/. The default Jetty landing page should appear.

After validating the changes, you can change the secure port by updating the Port value in the **<jetty-install-dir>/etc/jetty-ssl.xml** *Ss/SelectChannelConnector* class element. Follow step 9 to validate and restart Jetty after changing the secure port.

5. Appendix B: Configure the Firewall

Configure the firewall to allow HTTP, HTTPS, FTP, etc. It is easier to disable the firewall for testing. The procedure differs between [CentOS 7.x](#) and [CentOS 6.x](#). Refer to the applicable procedure to configure the firewall.

CentOS 7.x

Note: CentOS 7 installs and enables the "firewalld" service by default.

```
systemctl stop firewalld.service
systemctl disable firewalld.service
rm '/etc/systemd/system/basic.target.wants/firewalld.service'
rm '/etc/systemd/system/dbusorg.fedoraproject.FirewallD1.service'
```

To configure the firewall, the following ports need to be opened for MRB: 8888/tcp (for HTTP), 8443/tcp (for HTTPS), 5070/tcp, 5070/udp, 5100/tcp, 5111/tcp, 12000-12010/tcp, 5060/tcp, 5060/udp, 1081/tcp, 8081/tcp, and 8000/tcp.

The firewall is configured with the "firewall-cmd" command in Centos 7.x (see Red Hat 7 firewall configuration). To view the current state of the firewall, use the following command:

```
firewall-cmd --state
running
```

To find the current default "zone" that is in use, use the following command:

```
firewall-cmd --get-default-zone
public
```

To list the configuration for the default zone the interface uses, use the following command:

```
firewall-cmd --zone=public --list-all
public (default, active)
  interfaces: ens32
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

To add rules, use the following commands.

Note: Each "add-port" command shown below should return "success".

```
firewall-cmd --zone=public --add-port=8888/tcp --permanent
firewall-cmd --zone=public --add-port=8443/tcp --permanent
firewall-cmd --zone=public --add-port=5070/tcp --permanent
firewall-cmd --zone=public --add-port=5070/udp --permanent
firewall-cmd --zone=public --add-port=5060/tcp --permanent
firewall-cmd --zone=public --add-port=5060/udp --permanent
firewall-cmd --zone=public --add-port=5100/tcp --permanent
firewall-cmd --zone=public --add-port=5111/tcp --permanent
firewall-cmd --zone=public --add-port=1081/tcp --permanent
firewall-cmd --zone=public --add-port=8081/tcp --permanent
firewall-cmd --zone=public --add-port=8000/tcp --permanent
firewall-cmd --zone=public --add-port=12000-12010/tcp --permanent
firewall-cmd --reload
```

To allow communication between the MRB nodes in an HA pair, add a "Rich Rule." This allows certain MRB nodes to access to all ephemeral ports. On each MRB node in an HA pair, the following rule must be entered and the IP address of the paired node on each MRB machine must be provided:

```
firewall-cmd --zone=public --permanent --add-rich-rule='rule family="ipv4" source
address="[paired_mrb_node_ip_address]" accept'
firewall-cmd --reload
```

Check the service:

```
systemctl status firewalld.service
firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
  Active: active (running) since Thu 2015-11-12 10:31:33 GMT; 39min ago
Main PID: 6891 (firewalld)
  CGroup: /system.slice/firewalld.service
          â€”6891 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
Nov 12 10:31:32 mc-mrb.lonlab.dialogic.com systemd[1]: Starting firewalld - dynamic firewall
daemon...
Nov 12 10:31:33 mc-mrb.lonlab.dialogic.com systemd[1]: Started firewalld - dynamic firewall
daemon.
```

The final configuration is as follows:

```
firewall-cmd --zone=public --list-all
public (default, active)
  interfaces: ens32
  sources:
  services: dhcpv6-client ssh
  ports: 5060/tcp 12000-12010/tcp 5070/tcp 8888/tcp 5070/udp 8081/tcp 8443/tcp 5100/tcp 8000/tcp
12000/tcp 12001/tcp 5100/udp 5060/udp 5111/tcp 1081/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

CentOS 6.x

To allow access to the loopback interface for VIP interaction, use the following rule:

```
iptables -I INPUT -i lo -j ACCEPT
```

On each MRB node in an HA install, the following command must be entered to allow communication between the MRB nodes in an HA pair. The IP address of the paired node on each MRB machine must be provided:

```
iptables -I INPUT -p tcp -s [paired_mrb_node] -j ACCEPT
```

Before configuring the firewall ports, the following iptables rule must be applied to allow already-established connections on the MRB machine:

```
iptables -I INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
```

To open specific MRB ports, use the following iptables ACCEPT rules:

```
iptables -I INPUT -i eth0 -p tcp --dport 1081 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 5060 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 5070 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p udp --dport 5060 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 5060 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p udp --dport 5070 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 5100 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 5111 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 8000 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 8181 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 8888 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 8443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth0 -p tcp --dport 12000:12001 -m state --state ESTABLISHED -j ACCEPT
```

To list the firewall rules and opened ports, the following commands are used:

```
iptables -L -v -n
```

and

```
iptables -t nat -L -v -n
```

6. Appendix C: Resolve the Hostname

The PowerMedia MRB software needs to be able to resolve the hostname otherwise the error "Lost connection to MRB on localhost:5100" is displayed in the MRB console when attempting to log in and an error is displayed in *opt/mrb/mrb.out* every few seconds.

MRB Login

Welcome to the Dialogic MRB

Lost connection to MRB on localhost:5100

Try again

This is an example of the error message in *opt/mrb/mrb.out* when "mc-mrb" is the hostname and "mc-mrb3.lonlab.dialogic.com" is the FQDN.

```
Error: Exception thrown by the agent : java.net.MalformedURLException: Local host name unknown:
java.net.UnknownHostException: mc-mrb3.lonlab.dialogic.com: mc-mrb3.lonlab.dialogic.com: Name or
service not known
```

To resolve the hostname, edit the */etc/hosts* file so that the hostname and FQDN are included.

This is an example of an incorrect */etc/hosts* file when "mc-mrb" is the hostname and "mc-mrb3.lonlab.dialogic.com" is the FQDN. The hostname and FQDN are not in the file.

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4::1 localhost
localhost.localdomain localhost6 localhost6.localdomain6
```

This is an example of a correct */etc/hosts* file when "mc-mrb" is the hostname and "mc-mrb3.lonlab.dialogic.com" is the FQDN. The hostname and FQDN have been added to the file.

```
127.0.0.1 mc-mrb mc-mrb3.lonlab.dialogic.com localhost localhost.localdomain localhost4
localhost4.localdomain4::1 mc-mrb mc-mrb3.lonlab.dialogic.com localhost localhost.localdomain
localhost6 localhost6.localdomain6
```

7. Appendix D: Create Self-Signed Certificates and Keys

Proceed as follows to create self-signed certificates and keys.

1. Create a self-signed key.

```
keytool -genkey -keyalg RSA -alias server -keystore keystore.jks -storepass password  
-validity 360 -keysize 2048
```

To view the contents of this key, use the following command.

```
keytool -list -keystore keystore.jks
```

2. Export the key from keytool in PKCS12 format.

```
keytool -importkeystore -srckeystore keystore.jks -destkeystore inter.p12 -deststoretype  
PKCS12
```

To view the contents of this keystore, use the following command.

```
keytool -list -keystore inter.p12 -storetype PKCS12
```

3. Convert the key to PEM format.

```
openssl pkcs12 -in inter.p12 -out inter.pem -nodes
```

To view the PEM certificate, use the following command.

```
openssl x509 -in inter.pem
```

To view the contents of the PEM certificate, use the following command.

```
openssl x509 -in inter.pem -noout -text
```

4. Create a DER file.

```
openssl pkcs8 -topk8 -nocrypt -in inter.pem -outform der -out server.der
```

To view the contents of the PKCS8 unencrypted DER file, use the following command.

```
openssl pkcs8 -inform der -nocrypt -in server.der
```

5. Export the signed certificate.

```
keytool -export -keystore keystore.jks -alias server -file server.crt
```

To view the contents of the certificate, use the following command.

```
openssl x509 -in server.crt -noout -text -inform der
```

8. Appendix E: Add a Customized Security Profile

This section provides guidelines on adding a customized security profile.

1. Unzip the certificate bundle and locate the CRT file. The MRB does not accept CSR files to create a security profile. The MRB requires a PEM Certificate to be provided.
2. Obtain the private key as a DER file in PKCS8 format. If the private key is already a DER file, proceed to step 3. If the private key must be converted to a DER file, use the following command where "msaasmrb01.key" is an example of a file that needs to be converted to a DER file and "msaasmrb.der" is an example of the converted DER file:

```
$ openssl pkcs8 -topk8 -nocrypt -in msaasmrb01.key -outform der -out msaasmrb.der
```

3. In the MRB console, create an MRB security profile:
 - a. On the **Security Profiles** page, click **Add**.
 - b. In the **Profile Name** field, enter a name for the security profile.
 - c. In the **Server Certificates** section, click **Add Certificate**.

Add Server Certificate

Alias	<input type="text"/>	?
Certificate File	<input type="button" value="Choose File"/> No file chosen	?
Private Key	<input type="button" value="Choose File"/> No file chosen	?
<input type="button" value="Cancel"/> <input type="button" value="Add"/>		







- d. Enter a valid alias.
- e. In the **Certificate File** field, browse for the CRT file obtained in step 1 and select it.
- f. In the **Private Key** field, browse for the DER file obtained in step 2 and select it.
- g. Click **Add**, and then click **Save**. The new security profile should now be on the listed on the **Security Profiles** page.

4. For each MRB listed on the **Manage MRB Cluster** page of the MRB console, add the MRB security profile:

- a. Click **Manage**.

MRB node

MRB node new MRB-146.152.124.36:5070:Master

Name	<input type="text" value="new MRB"/>	
SIP Hostname and port	<input type="text" value="146.152.124.36:5070"/>	
Listen on TLS	<input checked="" type="checkbox"/>	
TLS port	<input type="text" value="5061"/>	
Security Profile	<input type="text" value="▼"/>	
JMX Hostname and port	<input type="text" value="146.152.124.36:5100"/>	
Paired MRB node ID	<input type="text" value="mrb 146.152.124.39:5070"/>	
Management mode	Master	
MRB/MLF	<input type="text" value="Mrb"/>	
<input type="button" value="Back"/> <input type="button" value="Save"/> <input type="button" value="Delete"/>		

- b. Select **Listen on TLS**.
 - c. In the **Security Profile** dropdown list, select the security profile.
 - d. Click **Save**.
 - e. Restart the MRB from the **MRB Configuration** page.
5. Confirm the security profile was successfully added by making an encrypted call from your client to the configured TLS port.

9. Appendix F: Performance Tuning for the RTP Proxy

The PowerMedia MRB RTP proxy uses the `rtengine` utility to relay RTP and RTCP between the remote endpoints and the media servers controlled by the PowerMedia MRB. The feature can place significant resource demands on the PowerMedia MRB machine, including network bandwidth and CPU time. The following sections provide the steps that need to be taken to work around some of the limitations that have been observed when testing thousands of audio calls through a PowerMedia MRB configured to proxy RTP.

Network Bandwidth

With a 1 GB NIC, the PowerMedia MRB has been observed to lose packets at less than 5,000 G.711 calls. During the observed packet loss, multiple VIPs were in use but they used the same physical NIC, which was saturated. To resolve this limitation, use a machine with a 10 GB NIC.

UDP Ports

Each leg of a call can use up to four UDP ports (audio, video, and an RTCP port for each of these). It is important to properly configure the PowerMedia MRB with two distinct Media VIPs. Failure to do so may cause `rtengine` to run out of usable ports and subsequent calls will fail.

Network Buffering

Network cards buffer a number of Ethernet frames internally. If these buffers overflow, packets are dropped. To minimize this risk, configure the hardware ring buffers to the maximum allowed values.

View the current settings using the following command:

```
ethtool -g <network device>
```

Then, set rx and tx to the maximum:

```
ethtool -G <network device> [rx|tx] <value>
```

Note: Inside a virtual machine, it was not possible to use `ethtool` for this setting, but it may be possible to configure this on the VM host.

Interrupt Handling

Coalescing

Incoming and outgoing packets trigger hardware interrupts. These consume CPU time, which is noted in the `%si` column.

To reduce the number of times the interrupt handler is called, interrupt coalescing can be configured. Interrupt coalescing allows the data to be buffered for a short period of time while more work arrives. The work is then all handled in a single interrupt.

Check the current interrupt coalescing settings using the following command:

```
ethtool -c <network device>
```

If "Adaptive RX" (or TX) is enabled, disable it:

```
ethtool -C <network device> adaptive-rx off
```

Note: Adaptive-rx is intended to keep latency low while increasing the coalescing parameters as needed. During testing, this rarely got above 32us even under heavy load. Disabling adaptive-rx and forcing rx-usecs to the maximum gave the best performance.

Then, set rx-usecs and tx-usecs to the maximums (rx-usecs-high, tx-usecs-high):

```
ethtool -C <network device> rx-usecs <value>
```

Note: It was not possible to set interrupt coalescing on a VM system and setting it on the host was not observed to have much effect.

Queuing and Steering

When interrupts are handled, they are not always handled evenly on all processors. This can cause a problem because one CPU may max out, which causes packets to be lost or other processes on the PowerMedia MRB to be delayed. In order to reduce the likelihood of this occurring, RSS (receive side scaling) can be configured and/or RPS (receive packet steering) can be enabled. On the non-VM systems that were tested, RSS was enabled by default. The queues are in the following directory: `/sys/class/net/<network device>/queues/`.

In each of these queues, there is an `rps_cpus` or `xps_cpus` file. This file specifies which CPU(s) handles packets for the queue. The CPUs are specified as a bitmask in hexadecimal format. For example, to use CPUs 0,1,6,7, the bitmask is set to 0..011000011 or 000000C3 (for 32 processors). For more than 32 processors, the bitmask is comma separated. If the bitmask is set to 0, RPS is disabled.

For more information on RSS, refer to the following link:

http://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Performance_Tuning_Guide/network-rss.html.

For more information on RPS, refer to the following link:

http://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Performance_Tuning_Guide/network-rps.html.

10. Appendix G: Media Server Adaptor Configuration

The media server (MS) adaptor can be configured to set the bind address in the adaptor properties file after installation.

- To change the listen address of the MS adaptor, edit "listenHostname" parameter in the */etc/sysconfig/adaptor.properties* file to supply an IP address.

```
listenHostname=192.168.x.x
```

- Once the change has been made, restart the MS adaptor to bind to the provided IP address.

```
service adaptor restart
```