



Dialogic® PowerMedia™
Media Resource Broker (MRB)
Installation and Configuration Guide

Copyright and Legal Notice

Copyright © 2015-2019 Dialogic Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Corporation at the address provided below.

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

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

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

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

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

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

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

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

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

Table of Contents

1. Welcome	8
Related Information	8
2. PowerMedia MRB Installation	9
System Requirements	9
Processor Requirements	9
Disable SELinux	10
Enable NTP	10
Software Installation	10
Command Line Installation	11
Graphical Environment Installation	12
Software Updates and Uninstallation	17
MRB Adaptor Updates	17
3. PowerMedia MRB Configuration	18
MRB Login	18
Dashboard	19
Media Servers	20
Media Server Details	22
Port Usage	24
Manage Conferences	24
Call Groups	25
Manage Media Servers	26
Add a Media Server	26
Manage a Media Server	27
Aggregated Port Usage	28
HA Statistics	29
Media Server Locations	29
MRB	30
Configuration	30
Configuration Import/Export	32
Manage MRB Cluster	34
Manage Conferences	36
Unaware Mode	38
VIP	40
Network Configuration	40
VIP Status	42
SNMP	43
Notification Configuration	43
Notification Triggers	44
User Administration	44
Users	44
Add a User	45
Change a User	45
User Roles	46
Security Profiles	46
Profiles	46
Add a Trusted Certificate	47
Add a Server Certificate	47
Logging	48
Configuration	48

History	49
4. PowerMedia MRB Operations	50
Enable HTTPS with Jetty	50
Configure the Media Server Adaptor	56
Configure the Firewall	57
CentOS 7.x	57
CentOS 6.x	58
Create Self-Signed Certificates and Keys	59
Add Customized Security Profile	59
SNMP Traps	61
List of Standard MIBs	61
5. PowerMedia MRB Troubleshooting	62
Resolve the Hostname	62
6. Appendix A: Performance Tuning for RTP Proxy	63
Network Optimization at High Density	63
Network Bandwidth	63
UDP Ports	63
Network Buffering	63
Interrupt Handling	64
Coalescing	64
Queuing and Steering	64
7. Appendix B: Upgrading to PowerMedia MRB 3.5 Service Update 17	65
Prerequisites	65
Upgrade Procedure	65

Revision History

Revision	Release Date	Notes
5.0 (Updated)	July 2019	Updates for MRB version 3.5 to support PowerMedia MRB 3.5 Service Update 17. Media Servers : Updated the section. Media Server Details : Updated the section. Call Groups : Added the section. MRB Configuration : Updated the section. Manage MRB Cluster : Updated the section. Manage Conferences : Updated the section. Unaware Mode : Updated the section. VIP Network Configuration : Updated the section. Logging Configuration : Updated the section. Configure the Media Server Adaptor : Added the section. Appendix B: Upgrading to PowerMedia MRB 3.5 Service Update 17.
5.0 (Updated)	October 2018	Software Installation : Updated the Command Line Installation section.
5.0 (Updated)	February 2018	Configure the Media Server Adaptor : Added the section.
5.0 (Updated)	November 2017	PowerMedia MRB Installation : Updated the Software Installation section. PowerMedia MRB Configuration : Updated the MRB Configuration and Networking Configuration sections.
5.0	October 2017	Updates for MRB version 3.5. PowerMedia MRB Configuration : Updated the Media Servers , MRB Configuration , Manage MRB Cluster , and Networking Configuration sections.

Revision	Release Date	Notes
4.0	May 2017	<p>Updates for MRB version 3.3.</p> <p>System Requirements: Updated the operating system requirements.</p> <p>Enable NTP: Added the section.</p> <p>Software Updates and Uninstallation: Updated the section.</p> <p>PowerMedia MRB Configuration: Updated the section.</p> <p>Configuration Import/Export: Added the section.</p> <p>Predictable Network Interface Names: Added the section.</p> <p>SNMP Traps: Added the section.</p> <p>Resolve the Hostname: Updated the section.</p> <p>Network Optimization at High Density: Added the section.</p>
3.0 (Updated)	January 2017	<p>Software Installation: Updated the section.</p> <p>Media Servers: Updated the section.</p> <p>Manage Media Servers: Updated the Manage a Media Server section.</p>
3.0	November 2016	<p>Updates for MRB version 3.2.</p> <p>Media Servers:</p> <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. <p>Appendix A: Performance Tuning for RTP Proxy: Added the section.</p>
2.1	August 2016	<p>PowerMedia MRB Configuration: Added limitations to the cascading conferences feature in the MRB Configuration section.</p>
2.0	April 2016	<p>Updates for MRB version 1.5.</p> <p>Create Self-Signed Certificates and Keys: Added the section.</p>

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>Enable HTTPS with Jetty: Relocated the section.</p> <p>Configure the Firewall: Added the section.</p> <p>Resolve the Hostname: Added the section.</p> <p>Add Customized Security Profile: Added the section.</p>
1.0	October 2015	Initial release of this document.
Last modified: July 2019		

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

1. Welcome

This Installation and Configuration Guide provides information about installing 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*, *Dialogic® PowerMedia™ Media Resource Broker (MRB) Technology Guide*, and PowerMedia XMS Release 3.5 documentation at <http://www.dialogic.com/manuals/xms/xms3-5>.
- 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 System	Community ENTERprise Operating System (CentOS) 7.3 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 7.3, 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 PowerMedia 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.

Enable NTP

To ensure time synchronization between the HA MRB nodes, proceed as follows on both nodes:

1. Ensure the `ntp` package is installed. If not, run the `"yum install ntp"` command.
2. Open the `/etc/ntp.conf` file and add an entry for the ntp time server using the syntax `"server <nt-server-address>"` (e.g., `server 192.168.2.x`).
3. Enable the `ntpd` startup service using the `"systemctl enable ntpd"` command.
4. Start the ntp daemon using the `"systemctl start ntpd"` command.

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.x

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

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

CentOS 6.x

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 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 example after the procedure for details.

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

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

Note: Edit 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. Press **y** to enable or press **n** to disable the Media Proxy, 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** to accept.
6. Select the target path. Change the path, or press **Enter** to use the default path, and press **1** to accept.
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-3.5.0.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
[/usr/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: Edit 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.

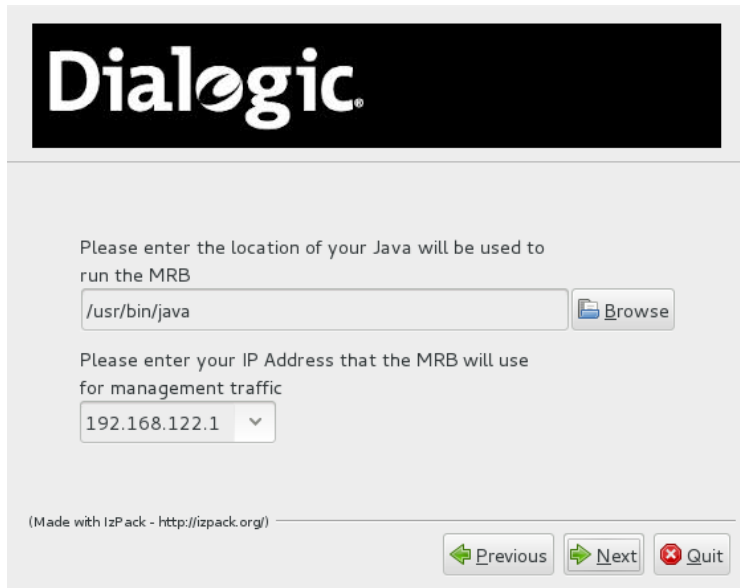


4. Click **Next** to proceed to the next step if no packages are required. If prompted, install the required packages using the yum install command. Refer to the following example to install the glib2-devel and glibc-devel packages:

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



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., */usr/bin/java*).
 - Enter the IP address that will be used for management traffic.



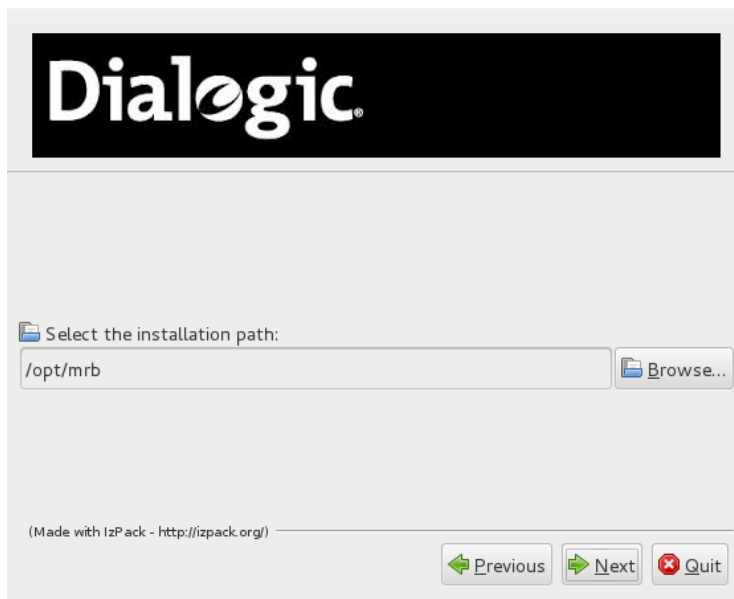
The screenshot shows a Dialogic installer window. At the top is the Dialogic logo. Below it, the text reads: "Please enter the location of your Java will be used to run the MRB". There is a text input field containing "/usr/bin/java" and a "Browse" button. Below this, the text reads: "Please enter your IP Address that the MRB will use for management traffic". There is a text input field containing "192.168.122.1" and a dropdown arrow. At the bottom left, it says "(Made with IzPack - http://izpack.org/)". At the bottom right are three buttons: "Previous", "Next", and "Quit".

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



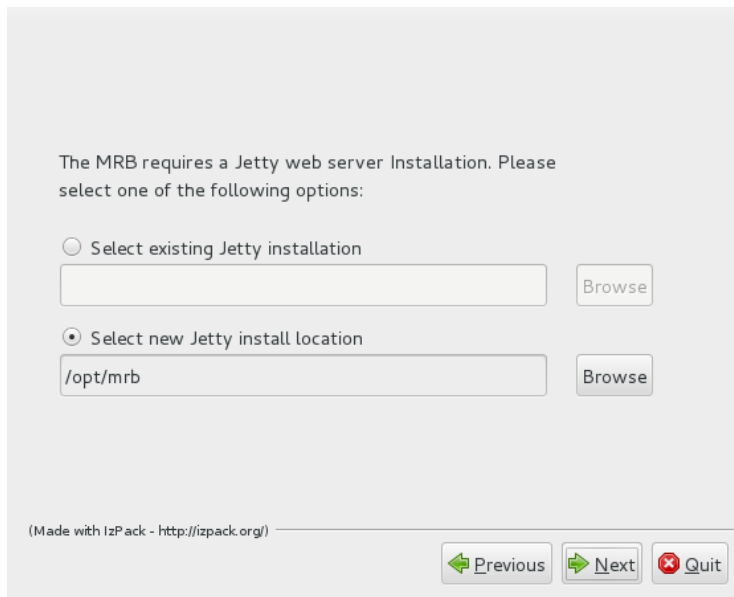
The screenshot shows a Dialogic installer window. At the top is the Dialogic logo. Below it, the text reads: "Please read the following license agreement carefully:". There is a large empty rectangular box for the license agreement. Below this box are two radio buttons: the first is selected and labeled "I accept the terms of this license agreement.", and the second is labeled "I do not accept the terms of this license agreement.". At the bottom left, it says "(Made with IzPack - http://izpack.org/)". At the bottom right are three buttons: "Previous", "Next", and "Quit".

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

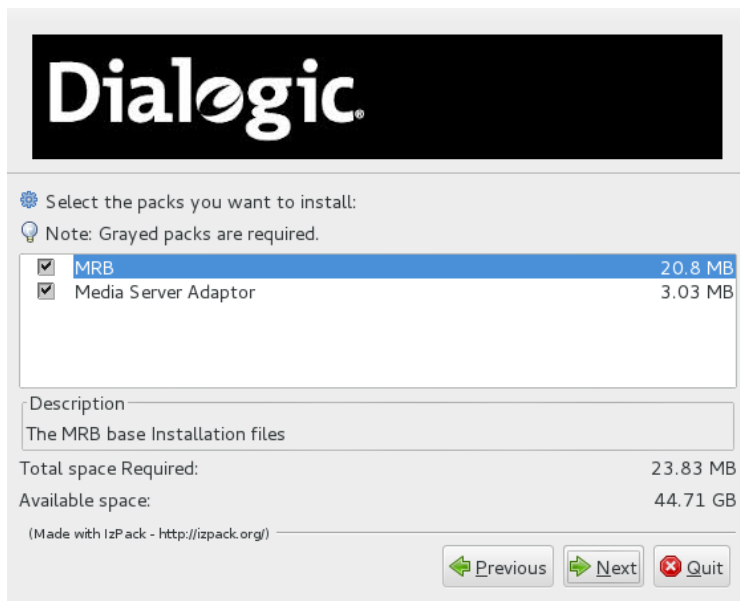


8. Set the Jetty web server preferences, and then click **Next**:

- **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.



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
```

Important: Prior to uninstalling the existing MRB software, capture the existing configuration settings (e.g., via screen dumps). The configuration settings need to be reapplied after the new MRB software has been installed.

To ease the process of updating MRB, use the configuration import/export functionality available on the MRB console. For more information, refer to [Configuration Import/Export](#).

Note: 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 PowerMedia 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 PowerMedia 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 PowerMedia XMS machine.
4. Run the installer using the following command:

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

Note: Edit 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 MRB console is a web-based user interface used to manage MRB. 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 [Enable HTTPS with Jetty](#). For details on configuring the firewall, refer to [Configure the Firewall](#).

The procedure for configuring the MRB should always be as follows:

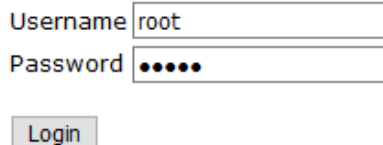
- Configure VIP.
- Click **Add MRB Node** to add MRB Node 2 (Slave).
- Configure MRB Node 2 to ensure the **SIP Hostname and port** is bound to the correct IP address (a restart is required if change is made).
- Any configuration changes should be made on MRB Node 1. MRB Node 2 should not be modified apart from in a failure situation.
- Restart MRB Node 1.
- Restart MRB Node 2.

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



Username

Password

Note: If the error message "Lost connection to MRB on localhost:5100" is displayed when attempting to log in, refer to [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.

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

Dashboard

Media Servers

- [Manage Media Servers](#)
- [Aggregated Port Usage](#)
- [HA Statistics](#)
- [Media Server Locations](#)

MRB

- [Configuration](#)
- [Manage MRB Cluster](#)
- [Manage Conferences](#)
- [Unaware Mode](#)

VIP

- [Networking Configuration](#)
- [VIP Status](#)

SNMP

- [Notification Configuration](#)
- [Notification Triggers](#)

User Administration

- [Users](#)
- [User Roles](#)

Security Profiles

- [Profiles](#)



Logging

- [Configuration](#)
- [History](#)

Dashboard

When logging in to the MRB console, the **Dashboard** page is displayed. On this page, 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.

MRB Dashboard

Cluster Overview
 **Master** 192.168.188.202:5100
 **Slave** 192.168.188.205:5100

JVM
JVM Vendor Oracle Corporation
JVM Version Java HotSpot(TM) 64-Bit Server VM version 25.92-b14
Java Version Java Virtual Machine Specification version 1.8
O/S Linux 3.10.0-327.28.2.el7.x86_64

Process
Up Time 000:01:48:17
Start Time Mon, 1 Oct 2018 13:24:54 UTC

Processor
Number of Processors 2
Architecture amd64
Number of Threads 354
Peak Number of Threads 355

Heap Memory
Initial 256.0 MB
Current 83.41 MB
Maximum 2048.0 MB
Committed 256.0 MB

Non Heap Memory
Initial 2.44 MB
Current 70.51 MB
Maximum -0.0 MB
Committed 72.69 MB

Errors
[Clear](#)
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).

Note: While the MRB does perform load balancing of calls between PowerMedia XMS systems, the granularity of the load balancing is based on 1 second intervals.

Media Servers

Status	Media Server Detail	Host	Location	Response Time (ms)	Manage	Port Usage	Conferences	Call Groups
	Dialogic PowerMedia XMS	10.20.245.92	London	91	Manage	View	Manage	View

[Add Media Server](#)

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> <p>A yellow traffic light could indicate that either a media server is full or that it is gracefully shutting down, which 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.
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.
Manage	A hyperlink to view and manage the media server. Refer to Manage a Media Server for more information.
Port Usage	A hyperlink to view specific port usage information for the media server. Refer to Port Usage for more information.
Conferences	A hyperlink to view and manage conferences that are currently active on the MRB. Refer to Manage Conferences for more information.
Call Groups	A hyperlink to view the call groups for the media server, displaying the call group name and number of calls in each group on the chosen media server. Refer to Call Groups for more information.

Media Server Details

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

Media Server Details

Status

Name

Identifier

Version

Up Time

Time Zone


CPU Load

Memory

Supported Audio Codecs

Supported Video Codecs

Running Status



[Dialogic PowerMedia XMS](#)

1 10.20.245.92:5070

3.5.20036

026:04:27:27

Coordinated Universal Time

t1=1.17, t5=1.22, t15=1.2

Total=0.01 MB Used=0 MB [used=25%]

G722, PCMU, PCMA, opus, EVS, AMR-WB, AMR, G729, GSM-EFR, GSM, iLBC, G723, G726-32

VP8, VP9, H264, MP4V-ES, H263-2000, H263-1998, H263

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
msrpserver	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
wsapiserver	WS Api Server	RUNNING
xmcsd	Metrics Export Service	STOPPED
xmserver	Signaling and Media Service	RUNNING
xmsrest	RESTful Call/Media Control Service	RUNNING

Restart Machine

Restart Services

Start Services

Stop Services

Graceful Shutdown

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.
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	The reported running status of the media resource. 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., PowerMedia XMS).

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







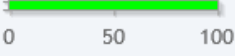


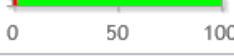



Item	Description
Restart Machine	The media resource restarts.
Restart Services	The services running on the media resource restart.
Start Services	The services on the media resource start.
Stop Services	The services running on the media resource stop.
Graceful Shutdown	The media resource does not accept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

Port Usage

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

Port Usage

Location: London Hostname: 10.20.245.92 Port: 5070

Codec	Used		Codec	Used	
AMR	0/100		AMR-WB	0/10	
EVS	0/10		G722	0/10	
G723	0/100		G726-32	0/100	
G729	0/100		GSM	0/100	
GSM-EFR	0/100		PCMA	2/100	
PCMU	2/100		iLBC	0/100	
opus	0/10				

[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.
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 the media server **Manage** hyperlink in the "Conferences" column. The **Manage Conferences** page provides a list of conferences that are active on the media resource.

Manage Conferences

Location: London Hostname: 10.20.245.92 Port: 5070

Number of Active Bridged Calls: 0

Conference ID	Conference Name	Number Of Calls	Priority	Call Group	End Calls
No records found.					

[Back](#) [End All Conferences](#) 

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.
Call Group	The name of the call group.
End Calls	End a specific conference instance by clicking the link.

Call Groups

To access the **Call Groups** page from the **Media Servers** page, click on the media server **View** hyperlink in the "Call Groups" column. The **Call Groups** page provides a list of call groups that are active on the media resource.

Call Groups

Location: London Hostname: 10.20.245.92 Port: 5070

Call Group	Number Of Calls
No records found.	

[Back](#)

The following information is provided.

Item	Description
Call Group	The name of the call group.
Number of Calls	The number of active calls currently participating in a call group.

Manage Media Servers

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

Media Servers

Status	Media Server Detail	Host	Location	Response Time (ms)	Manage	Port Usage	Conferences	Call Groups
	Dialogic PowerMedia XMS	10.20.245.92	London	91	Manage	View	Manage	View





[Add Media Server](#)

Add a Media Server

To add a media server, proceed as follows:

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

Add Media Server

Host	<input type="text"/>	
Port	<input type="text" value="5070"/>	
Listen on TLS	<input type="checkbox"/>	
Location	<input type="text" value="London"/>	

[Add](#)

[Cancel](#)





2. Enter the host address for **Host** and the port number for **Port**.
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 **Manage** hyperlink of the media server in the **Manage** column that needs to be configured. The **Media Server** page appears.

Media Server - 10.20.245.92

Host	<input type="text" value="10.20.245.92"/>	
Port	<input type="text" value="5070"/>	
Listen on TLS	<input type="checkbox"/>	
Location	<input type="text" value="London"/>	
<div><input type="button" value="Cancel"/> <input type="button" value="Take off line"/> <input type="button" value="End all conferences on MS"/></div>		

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, **Take off line** must be selected to take the media server out of service. The traffic light turns gray. When **Take off line** 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.

Aggregated Port Usage

The **Media Server Aggregated Port Usage** 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., PowerMedia XMS Resource Meters).

Media Server Aggregated Port Usage

General Info	
Active Media Servers	1

Audio Codecs

Codec	Used		Codec	Used	
AMR	0/100		AMR-WB	0/10	
EVS	0/10		G722	0/10	
G723	0/100		G726-32	0/100	
G729	0/100		GSM	0/100	
GSM-EFR	0/100		PCMA	2/100	
PCMU	2/100		iLBC	0/100	
opus	0/10				

Video Codecs

Codec	Used		Codec	Used	
H263	0/10		H263-1998	0/10	
H263-2000	0/10		H264	0/10	
MP4V-ES	0/10		VP8	0/10	
VP9	0/10				

Active Resource Meters

Active Resource Meter	Value
Fax Sessions	0
ASR / TTS Sessions	0
Conference Media Parties	0
Conference Parties	0
Conference Rooms	0
Media Transactions	0
RTP Sessions	0
Signaling Sessions	2

Groups Resource Meters

Groups Resource Meter	Value
No records found.	

HA Statistics

The **Media Server 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.

Media Server HA Statistics

Time/Date	Failed MS	Type (Manual/Automatic)	Total Calls	Successful Moves	Failed Moves
<i>No moves to report on.</i>					

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.

Media Server Locations

The **Media Server 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 **Create New Location**. An existing location can be edited by clicking **Manage** hyperlink and removed by clicking **Delete** hyperlink.

Media Server Locations

Location	Description	Location Group Size	Manage
London		1	Manage
New York		0	Manage

[Create New Location](#)

MRB

Configuration

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

MRB Configuration

General Configuration

System Description	<input type="text" value="Default Configuration Set"/>	
Push Route	<input type="text"/>	
Preserve Request URI	<input type="checkbox"/>	
Adaptor Poll Period	<input type="text" value="0.2"/>	
Enable MS Allocation Buffer	<input type="checkbox"/>	
MS Allocation Buffer Size	<input type="text" value="4"/>	
HTTP Call Control API REST Port	<input type="text" value="8181"/>	
HTTP Call Control API Keepalive Period	<input type="text" value="120"/>	
MS Failure Timeout	<input type="text" value="1"/>	
Session Timeout	<input type="text" value="1800"/>	
SIP Media Proxy Enabled	<input type="checkbox"/>	
Full Call Replication	<input checked="" type="checkbox"/>	
Process SIP Calls Statefully	<input checked="" type="checkbox"/>	

LifeCycle Control

Configuration Import / Export

The following configuration options are available.

Item	Description
System Description	The name used to describe the MRB system.

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>In some deployment architectures, it can be a requirement that all requests targeted at a media server traverse an intermediary network element, like a Serving Call Session Control Function (S-CSCF) for example, as part of the onward journey to a media server. This configuration item can be used to push preloaded SIP Route headers for all requests targeted at a media server when deploying in architectures such as IP Multimedia Subsystem (IMS).</p>
Preserve Request URI	<p>Enables preservation of the Request URI between incoming and outgoing SIP requests.</p> <p>If enabled, the Request URI for any outgoing request will be the Request URI of the incoming request. A route header containing the selected media server will also be added to ensure correct routing.</p>
Adaptor Poll Period	The value in seconds for the statistics retrieval period from the media servers being managed by the MRB.
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 functionality is useful in call flows such as transcoding.
MS Allocation Buffer Size	The number of calls to be batched to a specific media server if the MS allocation buffer is enabled.
HTTP Call Control API REST Port	Configures the port to be used when accessing the call control RESTful API. Refer to the <i>Dialogic® PowerMedia™ XMS RESTful API User's Guide</i> .
HTTP Call Control API Keepalive Period	Sets the frequency of keepalive events down any eventhandler connection in the call control RESTful API, which can be used to detect MRB node failover and accepts values (in seconds) in a range from 1 to 600.
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.
MS Failure Timeout	The minimum duration (in seconds) that must elapse after MS failure detection before the MS will be marked as failed. The minimum is 1 and maximum is 30.

Item	Description
Session Timeout	The maximum amount of time (in seconds) that can occur between refresh requests in a dialog before the session will be considered timed out (minimum is 90).
Full Call Replication	<p>If enabled, all calls coming into the MRB will be replicated to the other MRB node in the HA pair immediately. If it is disabled, the MRB will only replicate conference calls and joined calls at the point in which the MRB knows the call is creating the conference or joining the call.</p> <p>If the active MRB node (the node in control of the VIP) fails and full replication is enabled, the backup MRB will have the state for all calls when it takes over the VIP. Without the option enabled, only calls that have created or joined options will be maintained after an MRB node failover.</p> <p>Note that enabling this value has no impact on which calls are moved to a new MS when the MS failover is triggered.</p>
Process SIP Calls Statefully	<p>If enabled, the default SIP calls are processed statefully. If it is disabled, the default SIP calls are processed statelessly.</p> <p>This can be overridden on a per call basis by the SIP P-MRB header.</p> <p>When using SIP calls with 1PCC mode of the call control RESTful API, they must be stateful.</p>

Click **Save** to save the configuration or click **Cancel** to abort the operation.

From the **LifeCycle Control** section, click **Restart Master** to restart the MRB Node 1 (Master) or click **Restart Slave** to restart the MRB Node 2 (Slave).

Configuration Import/Export

The **Configuration Import/Export** section allows for importing and exporting configuration.

Configuration Import / Export

Export Config Import Config Browse... No file selected.

The configuration import/export functionality is intended to ease the process of updating MRB. The MRB configuration should be exported prior to an update and then subsequently imported once the update has been completed. For more information on updating MRB, refer to [Software Updates and Uninstallation](#).

The configuration import/export functionality may only be applied when:

- Updating between minor releases of the MRB.
- The system configuration is to remain the same (e.g., host environment, IP addresses, network interfaces).

Configuration Export

To export the configuration from a running MRB installation, perform the following procedure:

- Click **Configuration** from side-bar menu.
- Click **Export Config** from **Configuration Import/Export** section and save the file in a suitable location.

Note: The file name includes the time and date of the download. This may be used to identify the correct file when performing a configuration import.

The exported file will contain the following information:

- System Configuration (e.g., VIPs, Service Nodes)
- High Availability Configuration
- Media Server Configuration
- Security Profiles (Trusted/Server Certificates)

Software Update

Once the configuration export process has been completed, the MRB software can be updated. The update should be performed as normal, making sure each node has been updated to the same version before the nodes are started. For more information on updating MRB, refer to [Software Updates and Uninstallation](#).

Prior to importing a configuration file, each node should be started using the default configuration. No attempt should be made to either pair the nodes or set any configuration values at this time.

Configuration Import

To import a configuration file into a running MRB installation, perform the following procedure:



- Click **Configuration** from side-bar menu.
- Click **Browse** from **Configuration Import/Export** section and select the configuration file to be imported. Click **Open** to choose the configuration file.
- Click **Import Config** from **Configuration Import/Export** section to import the configuration file.
- A summary of the configuration import will be displayed. Click **Apply Imported Configuration** if the summary is correct.
- A warning message will be displayed asking for confirmation to apply the imported configuration. Click **OK** to confirm.


The configuration will then be applied, and each node will be automatically restarted. Any resources required by the MRB will be automatically created and once each node has completed its restart, the system will be fully operational.

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	Management Mode	
	mrbs-192.168.188.202:5100	192.168.188.202:5100	Master	Manage
	new Mrb	192.168.188.205:5100	Slave	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.

MRB Node - new Mrb

Node	
Name	<input type="text" value="new Mrb"/> 
Inbound Signalling Node Address	
Inbound Address	<input type="text" value="192.168.188.205"/> 
Inbound SIP Port	<input type="text" value="5060"/> 
Inbound SIP TLS Port	<input type="text" value="5061"/> 
Outbound Signalling Node Address	
Outbound Address	<input type="text" value="192.168.188.205"/> 
Outbound SIP Port	<input type="text" value="5070"/> 
Outbound SIP TLS Port	<input type="text" value="5071"/> 
Management Address	
Management Address	<input type="text" value="192.168.188.205"/> 
Management JMX Port	<input type="text" value="5100"/> 
Management SIP Port	<input type="text" value="5080"/> 
Security	
Listen on TLS	<input type="checkbox"/> 
Security Profile	<input type="text" value="v"/> 

[Back](#) [Save and Restart](#) [Delete](#)

The following configuration options are available.

Item	Description
Node	
Name	The name/identifier of MRB node in the cluster.
Inbound Signalling Node Address	
Inbound Address	The local IP address for inbound SIP interaction.
Inbound SIP Port	The local port for inbound SIP interaction.
Inbound SIP TLS Port	If Listen on TLS is selected, this is the local port for inbound SIP TLS interaction.
Outbound Signalling Node Address	
Outbound Address	The local IP address for outbound SIP interaction.
Outbound SIP Port	The local port for outbound SIP interaction.
Outbound SIP TLS Port	If Listen on TLS is selected, this is the local port for outbound SIP TLS interaction.
Management Address	
Management Address	The local IP address for management traffic.
Management JMX Port	The local port for JMX management traffic.
Management SIP Port	The local port for SIP management traffic.
Security	
Listen on TLS	A check box that enables or disables listen on TLS. Enabling this functionality results in TLS communication between MRB nodes within the cluster.

Item	Description
Security Profile	<p>If Listen on TLS is selected, this is the security profile used for SIP TLS interaction.</p> <p>Note: Refer to Create Self-Signed Certificates and Keys and Add Customized Security Profile for guidelines on adding customized security profiles.</p>

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

Manage Conferences

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

Manage Conferences

Manage Conferences Configuration

Enable Conference Clean Up ☐ ⓘ
Cascade Conferences ☒ ⓘ
Save Cancel

Conference Mix High Availability

Media Server Failover Policy: ☐ Move Calls ☒ End Calls ☐ Leave Calls on Failed MS ⓘ
RTP Failure Detection ☐ ⓘ
Detection Period ⓘ
Save Cancel

The following configuration options are available.

Item	Description
Manage Conferences Configuration	
Enable Conference Clean Up	<p>Enabling this functionality results in all conferences being cleaned up when the MRB connects. When the PowerMedia XMS transitions from a failed or offline state to an active state, the MRB cleans up conferences on the given PowerMedia XMS.</p>
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 functionality, refer to the following limitations:</p> <ul style="list-style-type: none"> Active speaker notifications from the PowerMedia XMS for that conference will not be correct. Video conference cascading is not supported. Only audio conferences can be cascaded.

Item	Description
Conference Mix High Availability	
Media Server Failure Policy	<p>Select an option from the radio buttons indicating what to do on media server failure.</p> <ul style="list-style-type: none"> • Move Calls - Select this option to move calls to another media server. • End Calls - Select this option to end all calls and conferences, notifying clients by sending BYEs for SIP calls and "resource_ended" events for call control RESTful API calls and conferences. • Leave Calls on Failed MS - Select this option to leave the calls on the failed media server. If the failure was due to a network outage, the media server may come back and start processing the same calls without issue.
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.

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

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)

Conferencing

Enabled	<input checked="" type="checkbox"/>
Location	No specific location ▾
Number of Audio Ports	1
Default Audio Codec	PCMU ▾
Number of Video Ports	1
Default Video Codec	No video (use audio) ▾
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

IVR

Enabled	<input type="checkbox"/>
Location	No specific location ▾
Number of Audio Ports	1
Default Audio Codec	PCMU ▾
Number of Video Ports	1
Default Video Codec	No video (use audio) ▾
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

Item	Description
Enabled	A check box that enables or disables unaware mode.
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>
Number of Audio Ports	Specify the number of audio ports required in association with the request.
Default Audio Codec	Specify the default audio codec in association with the request.
Number of Video Ports	Specify the number of video ports required in association with the request.
Default Video Codec	Specify the default video codec in association with the request.

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




VIP

Network Configuration



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

VIP Network Configuration




Inbound Signalling VIP

Inbound Signalling Network Interface	<input type="text" value="eth0"/>	
	192.168.188.202	
Inbound Signalling Address	<input type="text" value="192.168.188.244"/>	
Inbound Signalling NAT Address	<input type="text"/>	




Outbound Signalling VIP

Outbound Signalling Network Interface	<input type="text" value="eth0"/>	
	192.168.188.202	
Outbound Signalling Address	<input type="text" value="192.168.188.245"/>	

Management VIP

Management Network Interface	<input type="text" value="eth0"/>	
	192.168.188.202	
Allow Admin Traffic Segregation	<input type="checkbox"/>	
Management Address	<input type="text"/>	

Ports

VIP Manager Listening Port	<input type="text" value="5111"/>	
Signalling VIP SIP Port	<input type="text" value="5060"/>	
Signalling VIP SIP TLS Port	<input type="text" value="5061"/>	

Media VIPs

	VIP Address	NAT Address	Remove	
<input type="text" value="eth0"/>	<input type="text" value="192.168.188.230"/>	<input type="text"/>	<input type="button" value="Remove"/>	

The following configuration options are available.

Item	Description
Inbound Signalling VIP	
Inbound Signalling Network Interface	The interface name for inbound signalling VIP.
Inbound Signalling Address	MRB Virtual IP address for inbound signalling (e.g., SIP/HTTP).
Inbound Signalling NAT Address	The address used in RTP signaling when MRB is deployed behind external NAT.
Outbound Signalling VIP	
Outbound Signalling Network Interface	The interface name for outbound signalling VIP.
Outbound Signalling Address	MRB Virtual IP address for outbound signalling (e.g., SIP/HTTP).
Management VIP	
Note: The Management VIP will not be assigned until the MRB has been paired and configured for HA. Refer to Manage MRB Cluster for details on how to set up.	
Management Network Interface	The interface name for management VIP.
Allow Admin Traffic Segregation	A check box that enables or disables admin traffic segregation. If enabled, the MRB will allow Admin UI network traffic to be segregated by allowing a VIP to be provisioned on different network to one hosting the traffic VIP.
Management Address	MRB Virtual IP address for management UI.
Ports	
VIP Manager Listening Port	The port on which the MRB communicates with the VIP Manager process.
Signalling VIP SIP Port	The accompanying SIP port for inbound and outbound signalling VIP addresses.
Signalling VIP SIP TLS Port	The accompanying SIP TLS port for inbound and outbound signalling VIP addresses.

Item	Description
Media VIPs	
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.
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.
NAT Address	The address for NAT. This configuration option is available if the Media Proxy feature is enabled during the installation.

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

Predictable Network Interface Names

CentOS 7.x uses predictable network interface names. This means the interface names on the active and backup nodes may be different; the VIPs require the same interface name on the active and backup nodes.

If the OS chooses different network interface names for the interfaces that are used for the VIPs, then perform the following procedure to rename the interface names (to ensure they are the same on both nodes):

1. Run the "cd /etc/sysconfig/network-scripts" command.
2. Find the network interface name that needs to work with MRB ("enp0s3" used in the following example which will be changed to "eth0").
3. Run the "mv ifcfg-enp0s3 ifcfg-eth0" command.
4. Edit the *ifcfg-eth0* to:
 - Add the HWADDR of the interface (e.g., add an entry using the syntax "HWADDR=01:00:27:0d:6c:c2").
 - Change the values for NAME and DEVICE to "eth0".
5. Reboot.

VIP Status

The **VIP Manager** 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	Controlling Node Candidates
192.168.188.230	192.168.188.202	2
192.168.188.244	192.168.188.202	2
192.168.188.245	192.168.188.202	2

[Restart VIP Manager](#)

Click **Restart VIP Manager** to restart the VIP Manager.

SNMP

Notification Configuration


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

SNMP Notification Configuration


Primary SNMP Trap Receiver

Enabled


☐



Destination hostname



Destination port




Save


Cancel

Additional SNMP Trap Receiver


Additional Destination hostname



Additional Destination port



SNMP Community Name



Save

Cancel

The following configuration options are available.

Item	Description
Primary SNMP Trap Receiver	
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 SNMP Trap Receiver	
Additional Destination hostname	An additional location that can optionally be provisioned to send MRB SNMP traps.
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.

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

Notification Triggers

The **SNMP Notification Triggers** page provides a list of events that can appear in the MRB log files and also raise SNMP traps.

SNMP Notification Triggers

A location has been deleted	<input checked="" type="checkbox"/>	A MS has been detected as alive	<input checked="" type="checkbox"/>
An MRB node push route is now set	<input type="checkbox"/>	A user has logged into the admin console	<input checked="" type="checkbox"/>
A user has been changed	<input checked="" type="checkbox"/>	A location has been added	<input checked="" type="checkbox"/>
A MS is now online	<input checked="" type="checkbox"/>	An MRB node is now online	<input type="checkbox"/>
A user has been deleted	<input checked="" type="checkbox"/>	VIP Manager detailed logging configured	<input type="checkbox"/>
MRB signalling vip sip port configured	<input type="checkbox"/>	A MS has been detected as failed	<input checked="" type="checkbox"/>
A user role has been changed	<input checked="" type="checkbox"/>	MRB detailed logging configured	<input type="checkbox"/>
MRB media vips configured	<input type="checkbox"/>	MRB signalling vip sip tls port configured	<input type="checkbox"/>
A user role has been deleted	<input checked="" type="checkbox"/>	A MRB node has stopped	<input checked="" type="checkbox"/>
MRB use reinvites for moves configured	<input type="checkbox"/>	An MRB node has been changed	<input checked="" type="checkbox"/>
A MS is now offline	<input checked="" type="checkbox"/>	VIP manager port set	<input type="checkbox"/>
A user has been added	<input checked="" type="checkbox"/>	A MRB node has started	<input checked="" type="checkbox"/>
A MRB node has failed to start	<input checked="" type="checkbox"/>	An MRB node has been forced to master	<input checked="" type="checkbox"/>
Inbound Signalling VIP interface name set	<input type="checkbox"/>	MRB outbound signalling vip address configured	<input type="checkbox"/>
A location has been changed	<input checked="" type="checkbox"/>	An MRB node has been added to the cluster	<input checked="" type="checkbox"/>
An MRB node is now offline	<input type="checkbox"/>	A MS has been changed	<input checked="" type="checkbox"/>
MS has high port usage	<input checked="" type="checkbox"/>	MRB inbound signalling vip address configured	<input type="checkbox"/>
MRB stack logging configured	<input type="checkbox"/>	This Node has been promoted and now hosts the VIP	<input checked="" type="checkbox"/>
MRB HA connection failed	<input type="checkbox"/>	An MRB node has been deleted	<input checked="" type="checkbox"/>
A MS has been added	<input checked="" type="checkbox"/>	VIP Admin interface name set	<input type="checkbox"/>
MRB cascade conferences configured	<input type="checkbox"/>	MRB Admin vip address configured	<input type="checkbox"/>
A users password has been changed	<input checked="" type="checkbox"/>	This Node no longer hosts the VIP	<input checked="" type="checkbox"/>
A user role has been added	<input checked="" type="checkbox"/>	SNMP traps configuration has been changed	<input checked="" type="checkbox"/>
A MS has been deleted	<input checked="" type="checkbox"/>	Outbound Signalling VIP interface name set	<input type="checkbox"/>
MRB HA connection succeeded	<input type="checkbox"/>		

Click **Save** to save the configuration settings.

User Administration

Users

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

User Administration

Description	User Name	Role	Manage
Root User	root	Super user	<button>Manage</button>
Low Privileges User	nst		<button>Manage</button>

Add User

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 **Add User**. Clicking **Cancel** 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"/>	

Add user Cancel

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

Back Update Delete

User Roles

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

User Roles

Role Name	User	MRB	Media Servers	Edit	Delete
Super user	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[Fixed Role]	[Fixed Role]
Low privileges	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	[Fixed Role]	[Fixed Role]

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.

Security Profiles

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 [Create Self-Signed Certificates and Keys](#) and [Add Customized Security Profile](#) for guidelines on adding customized security profiles.

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

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

Security Profiles

Profile Name	Server Certificates	Trust Certificates	Actions
<input type="text" value="Security Profile"/>	<input type="button" value="Add"/> <input type="button" value="Delete"/>	<input type="button" value="Add"/> <input type="button" value="Delete"/>	<input type="button" value="Save"/> <input type="button" value="Delete"/>
<input type="button" value="Add Profile"/> <input type="button" value="Cancel"/>			

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 "Trust Certificates" and "Server Certificates".

The following configuration options are available.



Item	Description
Delete	The Delete causes the appropriate certificate to be removed from the profile.
Add	The Add causes the appropriate certificate to be added to the profile. Refer to Add a Trusted Certificate and Add a Server Certificate 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 **Add** in the "Trust Certificates" column. 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 **Save** to add the certificate or **Cancel** to return to the previous page.




Add Trusted Certificate

Alias	<input type="text"/>	
Certificate File	<input type="button" value="Browse..."/> No file selected.	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>		

Add a Server Certificate

To add a server certificate, click **Add** in the "Server Certificates" column. 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 **Save** to add the certificate or **Cancel** to return to the previous page.

Add Server Certificate





Alias	<input type="text"/>	
Certificate File	<input type="button" value="Browse..."/> No file selected.	
Private Key	<input type="button" value="Browse..."/> No file selected.	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>		

Logging

Configuration

The **Logging Configuration** page allows for logging to be configured.

Logging Configuration

MRB	
Enable Detailed Logging	<input checked="" type="checkbox"/> 
Stack Logging	<input type="checkbox"/> 
SIP Message Logging	<input type="checkbox"/> 
VIP Manager	
Enable Detailed Logging	<input type="checkbox"/> 
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

The following configuration options are available.

Item	Description
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.
VIP Manager	
Enable Detailed Logging	Allows a user to turn on and off detailed logging. This option does not require a restart.

Click **Save** to save the configuration or **Cancel** to abort the operation.

History

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

Logging History

Entries Per Page <input type="text" value="20"/> Update				
Time/Date	Who	Event	Description	Other Information
2:31:55 PM Oct 1, 2018	root	console.login	A user has logged into the admin console	
2:30:49 PM Oct 1, 2018	root	console.login	A user has logged into the admin console	
1:56:59 PM Oct 1, 2018	root	console.login	A user has logged into the admin console	
1:27:04 PM Oct 1, 2018	system	health.mrb.ha.connected	MRB HA connection succeeded	192.168.188.205:5100
1:25:56 PM Oct 1, 2018	system	health.mrb.ha.lostconnection	MRB HA connection failed	192.168.188.205:5100
1:25:29 PM Oct 1, 2018	system	health.mrb.ha.connected	MRB HA connection succeeded	192.168.188.205:5100
1:25:20 PM Oct 1, 2018	system	vip.manager.now.hosting.vip	This Node has been promoted and now hosts the VIP	vip:192.168.188.245 interface:eth0 application id:192.168.188.244:5060 created 2018-10-01 13:25:20.343
1:25:20 PM Oct 1, 2018	system	vip.manager.now.hosting.vip	This Node has been promoted and now hosts the VIP	vip:192.168.188.244 interface:eth0 application id:192.168.188.244:5060 created 2018-10-01 13:25:20.129
1:25:19 PM Oct 1, 2018	system	vip.manager.now.hosting.vip	This Node has been promoted and now hosts the VIP	vip:192.168.188.244 interface:eth0 application id:192.168.188.244:5060 created 2018-10-01 13:25:19.919
1:25:19 PM Oct 1, 2018	system	vip.manager.now.hosting.vip	This Node has been promoted and now hosts the VIP	vip:192.168.188.244 interface:eth0 application id:192.168.188.244:5060 created 2018-10-01 13:25:19.805
1:25:19 PM Oct 1, 2018	system	vip.manager.now.hosting.vip	This Node has been promoted and now hosts the VIP	vip:192.168.188.244 interface:eth0 application id:192.168.188.244:5060 created 2018-10-01 13:25:19.598
1:25:15 PM Oct 1, 2018	system	vip.manager.now.hosting.vip	This Node has been promoted and now hosts the VIP	vip:192.168.188.230 interface:eth0 application id:192.168.188.244:5060 created 2018-10-01 13:25:15.367
1:25:10 PM Oct 1, 2018	system	admin.mrb.cluster.node.force	An MRB node has been forced to master	JsonManagementHostAndPort [host=192.168.188.202, sipPort=5080, jmxPort=5100]
1:25:10 PM Oct 1, 2018	system	vip.manager.now.hosting.vip	This Node has been promoted and now hosts the VIP	vip:192.168.188.245 interface:eth0 application id:192.168.188.244:5060 created 2018-10-01 13:25:10.932
1:24:56 PM Oct 1, 2018	system	start	starting	Start

Search Page 1 of 1 [Previous page](#) [Next page](#) [Clear](#)

4. PowerMedia MRB Operations

Enable 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-----
MIIEogIBAAKCAQEAR653O+uwL0Ohoq8OQFadub9MMilqak2tDhI9k25N5iZgElkL
:
RldsDTpOMqikPFbT1aw98mNTcSMFiOiUcg07AEswqYfuuc8iR44=
-----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/QOOF0Y1ITVchhbBjRgYcnEVp7dUPSEWum
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.pl12 -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 *sslContextFactory* 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:1vn1zl01x8e1vnw1vn61x8glzlulvn4</Set>
<Set name="KeyManagerPassword">OBF:1u2ulwml1z7s1z7a1wn1lu2g</Set>
<Set name="TrustStore"><Property name="jetty.home" default="." />/etc/keystore</Set>
<Set name="TrustStorePassword">OBF:1vn1zl01x8e1vnw1vn61x8glzlulvn4</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:11fg1mmcldi01x0r1z0f1z0f1x1vldgm1mi11lc2
MD5:c0e1ec92ed0dc1b26daa291604cd0d69
```

- c. Update the *ssl/ContextFactory* 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:11fg1mmcldi01x0r1z0f1z0f1x1vldgm1mi11lc2</Set>
<Set name="KeyManagerPassword">OBF:11fg1mmcldi01x0r1z0f1z0f1x1vldgm1mi11lc2</Set>
<Set name="TrustStore"><Property name="jetty.home" default="." />/etc/myCompany-
Jetty.jks</Set>
<Set name="TrustStorePassword">OBF:11fg1mmcldi01x0r1z0f1z0f1x1vldgm1mi11lc2</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 (e.g., 8888 is the standard Jetty port for MRB console 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.

Configure the Media Server Adaptor

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
```


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.x 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 RHEL 7.x 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
```

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
```

Add 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
mr-146.152.124.92:5070-146.152.124.92:5070:Master

Name	<input type="text" value="mr-146.152.124.92:507"/>	
SIP Hostname and port	<input type="text" value="146.152.124.92:5070"/>	
Listen on TLS	<input type="checkbox"/>	
TLS port	<input type="text" value="5061"/>	
Security Profile	<input type="button" value="v"/>	
JMX Hostname and port	<input type="text" value="146.152.124.92:5100"/>	
Paired MRB node ID	<input type="button" value="not HA v"/>	
<input type="button" value="Back"/> <input type="button" value="Save and Restart"/> <input type="button" value="Delete"/>		

- b. Select **Listen on TLS**.
 - c. In the **Security Profile** down-down list, select the security profile.
 - d. Click **Save and Restart**.
 - 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.

SNMP Traps

The PowerMedia MRB SNMP implementation supports SNMPv2. The standard MIBs are located on your system.

There are two additional MIB files that are not located in the standard MIBs directory. The two MIB files ("NST-MIB" and "MRB-MIB") must be loaded into a network manager in order to decode SNMP traps. "NST-MIB" is a parent file. "MRB-MIB" is a file specific to the PowerMedia MRB. These MIBs are located in the following location on the PowerMedia MRB installation:

```
/opt/mrb
```

SNMP traps are raised in response to certain system events. Details and a description of each trap may be found within the "MRB-MIB" file.

List of Standard MIBs

MIB	Description
EtherLike-MIB	Defines generic objects for Ethernet like network interfaces (RFC 3635)
HOST-RESOURCES-MIB	Management of host systems (RFC - many)
IF-MIB	Defines generic objects for network interface sub-layers (RFC 2863)
IP-MIB	Management of IP and ICMP implementation (RFC 4293)
IPV6-MIB	Management of IPv6 implementation
TCP-MIB	Management of TCP implementation (RFC 4022)
UDP-MIB	Management of UDP implementation (RFC 4113)
RFC1213-MIB	Defines MIB-II (RFC 1213)

5. PowerMedia MRB Troubleshooting

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
```

6. Appendix A: Performance Tuning for RTP Proxy

The MRB RTP proxy uses the `rtppengine` utility to relay RTP and RTCP between the remote endpoints and the media servers controlled by the MRB. The feature can place significant resource demands on the 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 an MRB configured to proxy RTP.

Network Optimization at High Density

For optimal network performance at high density, it is necessary to use 2 VIPs per NIC.

Using a second NIC allows maximum density for many 720p video sessions as a single 10 GB link reached capacity before the CPU usage maxed out on the MRB.

It is necessary to set the following network parameters on all NICs:

- `txqueuelen`, set using `ifconfig`, should be increased from the default of 1000 to 10000 or more.
- interrupt coalescence, configured using `ethtool -C`, should have `adaptive-rx` set to off and `rx-usecs` set to the maximum.
- ring buffers, configured using `ethtool -G`, should be set to the maximum allowable values for rx and tx.
- channels, configured using `ethtool -L`, should be set to the number of physical CPU cores. It is possible to set it to a higher value, but this appears to have no effect.

Network Bandwidth

With a 1 GB NIC, the 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 MRB with two distinct Media VIPs. Failure to do so may cause `rtppengine` 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: The 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 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.

7. Appendix B: Upgrading to PowerMedia MRB 3.5 Service Update 17

This section provides additional configuration required to upgrade to PowerMedia MRB 3.5 Service Update 17 (also referred to herein as "MRB 3.5 SU17") from previous MRB 3.5 release.

Prerequisites

Make sure to take screenshots or mark down all relevant VIP addresses and cluster configuration from the respective screens.

With MRB 3.5 SU17 comes the addition of "Outbound Signalling VIP" field. The network administrator must assign a new VIP address for use with the MRB before the upgrade can take place.

Upgrade Procedure

Proceed as follows to upgrade to MRB 3.5 SU17:

1. Export your current configuration so there is a backup file if you need to roll back to a previous MRB 3.5 release or have a reference point for configuration.
 - Navigate to the **MRB Configuration** page and click **Export Config** from **Configuration Import/Export** section. Save the file in a suitable location.
2. Uninstall the MRBs - `/opt/mrb/uninstall-mrb.sh`.
3. Install the MRB on respective nodes.
4. Log in to MRB console.
5. Navigate to the **VIP Network Configuration** page.
 - The "Traffic VIP Address" field from previous MRB 3.5 release is now called "Inbound Signalling Address" field. Enter the address from "Traffic VIP Address" field in the "Inbound Signalling Address" field.
 - Enter the newly assigned VIP (see [Prerequisites](#) section) in the "Outbound Signalling Address" field.
 - The "Admin UI VIP Address" field from previous MRB 3.5 release is now called "Management Address" field. Enter the address from "Admin UI VIP Address" field in the "Management Address" field.
 - The media VIP addresses can be added from **Media VIPs** section and is no longer restricted to two media VIP addresses.
 - Click **Save and Restart** to save configuration settings and restart.

6. Navigate to the **Manage MRB Cluster** page and click **Add MRB Node**. The procedure to set up HA cluster is now slightly different in MRB 3.5 SU17.
 - The "Inbound Address" field is your inbound traffic interface address. This is the address from the "SIP Hostname and port" field on the **Manage MRB Cluster** page in previous MRB 3.5 release.
 - The "Outbound Address" field is your inbound traffic interface address. This is the address from the "SIP Hostname and port" field on the **Manage MRB Cluster** page in previous MRB 3.5 release.
 - The "Management Address" field is your management interface address set at installation time for the MRB. This is the address from the "JMX Hostname and port" field on the **Manage MRB Cluster** page in previous MRB 3.5 release.
 - Click **Save and Restart** to save configuration settings and restart.

Note: When upgrading to MRB 3.5 SU17, the inbound VIP address will be updated to bind on port 5060 instead of port 5070 by default. The application configuration must be updated to reflect the port change.