Dialogic® PowerMedia™ XMS

Application Note: Running PowerMedia XMS on Amazon Web Services

November 2016 Rev 1.0

www.dialogic.com

Copyright and Legal Notice

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

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

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

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

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 6700 Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, PowerVille, PowerNova, MSaaS, ControlSwitch, I-Gate, Mobile Experience Matters, Network Fuel, Video is the New Voice, Making Innovation Thrive, Diastar, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, NaturalAccess and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 6700 Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

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

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

Table of Contents

Revision History

Revision	Release Date	Notes
1.0	November 2016	Initial version of this document.
Last modified: November 2016		

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

1. Overview

This guide provides instructions on running Dialogic® PowerMedia™ Extended Media Server (also referred to herein as "PowerMedia XMS" or "XMS") on Amazon Web Services (AWS) Elastic Compute Cloud (EC2) and Virtual Private Cloud (VPC).

You can choose to run XMS on EC2 with or without creating a VPC. The simpler method is running XMS on EC2 without creating a VPC. For this method, a public, pre-built AWS image containing a working PowerMedia XMS with a 4-port trial license built into the image is used.

To license XMS for more ports, XMS must be run on a VPC. This will allow a more realistically sized license to be used with XMS and will preserve the licensing when the XMS image is terminated.

The information in this guide is intended to be used for testing only (not for production). If considering XMS as part of an AWS media server solution, it is best to run tests with your own application server, cloud-based or otherwise, and at densities suitable for a production situation.

This guide is organized in the following sections:

- Starting XMS Instance in Amazon EC2
- Creating XMS Instance in Amazon VPC
- Reaching XMS System Using SSH
- Verifying XMS Operation
- Running XMS Verification Demos
- Obtaining Higher Density License for XMS Running in Amazon VPC

For questions regarding AWS, consult the AWS documentation at http://aws.amazon.com/documentation.

Note: A working familiarity with AWS and an AWS account is presumed.

2. Starting XMS Instance in Amazon EC2

Follow this section to start PowerMedia XMS with a 4-port trial license. If you want to use a larger license, refer to Creating an XMS Instance in an Amazon VPC. The procedure here corresponds to the AWS steps used to launch an AMI.

Step 1: Choose an Amazon Machine Image (AMI)

To choose an Amazon Machine Image (AMI), perform the following procedure:

1. Log in to your AWS account and then log in to the console.
2. Confirm that the geographic region is accurate. The AMI for XMS is located in these AWS Regions:
    - US West (N. California)
    - US East (N. Virginia)
    - EU (Frankfurt)
    - Asia Pacific (Singapore)
    - South America (Sao Paulo)
3. In the console, click **Services > EC2**.
4. In the EC2 console, find the desired public Dialogic AMI that follows the naming convention dialogic_xms_*releasenumber_buildnumber* (e.g., dialogic_xms_3.2_GA).

    Note: There is not a publicly available Dialogic account but rather a public, community image that is run under your account.
5. Once the AMI is located, launch the instance.

Step 2: Choose an Instance Type

If not using a VPC, the XMS image uses a 4-port verification license. The verification license can accommodate four simultaneous calls. To handle four video calls in a conference at a VGA (640x480) resolution, an instance type of c4.xlarge or better should be selected on the **Choose an Instance Type** page. The C series of instance types are compute optimized and suitable for video media processing.

If using a VPC, it is assumed that a 10-port license is used. This can accommodate ten simultaneous calls. To handle ten video calls in a conference at a VGA (640x480) resolution, an instance type of c4.2xlarge or better should be selected on the **Choose an Instance Type** page. The C series of instance types are compute optimized and suitable for video media processing.

Note: When using Amazon EC2 instances, there are multiple virtual machine tenants on a single host. There is no way of knowing what the other tenants are doing, how much bandwidth they are using, their clock interrupt needs, etc. Because XMS is a real-time application, it has stringent clock interrupt needs to successfully handle RTP media packets.

In Dialogic testing, XMS worked on EC2. However, on smaller instances, testing found that less than predicted densities were achieved. Occasionally, a case where media processing failed inexplicably was observed, but it could not be reproduced.

It is possible to use a dedicated host in EC2 for fully predictable performance, but that is generally not necessary.

Step 3: Configure Instance Details

When using XMS with AWS, the following settings are recommended for the **Configure Instance Details** page.

Setting	Value	Details
Number of instances	1	Leave the default value.
Purchasing option	Unselected	Leave the default value.
Network	default	Leave the default value. For the trial of XMS, using AWS-supplied networking is sufficient. A Virtual Public Cloud (VPC) is not needed. If EC2-Classic does not display as an option, it is beyond the scope of this document to describe a VPC setup. Please contact your Dialogic Sales Representative for information on configuration.
Subnet	No preference	Leave the default value.
Auto-assign Public IP	Use subnet setting (Enable)	Leave the default value.
Placement Group	No placement group	Leave the default value.
IAM role	None	Leave the default value.
Shutdown behavior	Terminate	Terminate will destroy the instance when it is stopped. If you make any changes to the running instance, you may want to select Stop.
Enable termination protection	Unselected	Leave the default value.
Monitoring	Unselected	Leave the default value.
EBS-optimized instance	Unselected	Leave the default value.
Tenancy	Shared - Run a shared hardware instance	Leave the default value.

Setting	Value	Details
Number of instances	Select the ENI just created in Create the Elastic Network Interface (ENI).	This setting is for configuring instances in VPC only. Disregard the public IP address warning.
Advanced Details	N/A	Leave the default value.

Step 4: Add Storage

For an XMS trial, a 40 GB storage size and a general purpose volume type is sufficient.

Step 5: Tag Instance

In the **Value** field, enter a name for the instance that will be recognizable when looking at the AWS console (e.g., XMS-3.2).

Step 6: Configure Security Group

On the **Configure Security Group** page in the AWS console, open AWS ports for access to XMS.

Note: This is not on the XMS system; it is AWS security.

If not using a VPC, create a security group for XMS as follows:

1. For **Assign a security group**, select **Create a new security group**.
2. Enter a descriptive name in the **Security group name** field (e.g., XMS-ports).
3. Select **Add Rule** and open the ports.

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere, or as desired
HTTP	TCP	80	Anywhere, or as desired
Custom TCP Rule	TCP	81	Anywhere, or as desired
Custom TCP Rule	TCP	161-162	Anywhere, or as desired
HTTPS	TCP	443	Anywhere, or as desired
Custom TCP Rule	TCP	444	Anywhere, or as desired

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	5060	Anywhere, or as desired
Custom TCP Rule	TCP	1080	Anywhere, or as desired
Custom TCP Rule	TCP	6789	Anywhere, or as desired
Custom TCP Rule	TCP	9004	Anywhere, or as desired
Custom TCP Rule	TCP	9876	Anywhere, or as desired
Custom TCP Rule	TCP	10080	Anywhere, or as desired
Custom TCP Rule	TCP	10443	Anywhere, or as desired
Custom TCP Rule	TCP	12000-12010	Anywhere, or as desired
Custom TCP Rule	TCP	15001	Anywhere, or as desired
Custom TCP Rule	TCP	20000	Anywhere, or as desired
Custom TCP Rule	TCP	27000-27009	Anywhere, or as desired
Custom TCP Rule	TCP	27017	Anywhere, or as desired
Custom TCP Rule	TCP	28017	Anywhere, or as desired
Custom UDP Rule	UDP	5060	Anywhere, or as desired
Custom UDP Rule	UDP	9876	Anywhere, or as desired
Custom UDP Rule	UDP	27000-27009	Anywhere, or as desired

Type	Protocol	Port Range	Source
Custom UDP Rule	UDP	49152-61344	Anywhere, or as desired

The source IP address can be left as Anywhere or, for better security, restricted to certain IP addresses.

If using a VPC, configure the security group as follows.

1. For **Assign a security group**, select **Select an existing security group**. The two security groups belonging to the VPC will be listed.
2. Select the security group that as created to open XMS ports. Do not select the default group.

Step 7: Review Instance Launch

On the **Review Instance Launch** page, ignore the notifications for improving the instance's security and for the instance's ineligibility for the free usage tier.

Verify the information on the page, and then launch the instance.

Before the instance launches, a public/private key pair must be associated with the instance. Create a new key pair or choose an existing key pair.

Note: The key pair is used to connect directly to the XMS system using SSH and will likely not be needed. However, it is not possible to start an instance without confirming that you have a valid key pair.

Once a public/private key pair is associated with the instance, "Your instance is now launching" appears on the page. Check the new XMS instance to confirm that it is running properly.

3. Creating XMS Instance in Amazon VPC

If you choose to increase the number of licensed ports for the XMS Amazon Machine Image (AMI) on the Amazon VPC, create a VPC prior to starting an XMS instance in EC2. If you choose to run XMS on EC2 using the 4-port trial license, skip to Starting an XMS Instance in Amazon EC2.

XMS licensing on AWS requires creating an Amazon Virtual Private Cloud (VPC), an associated Subnet, Elastic Network Interface (ENI), and Elastic IP Address (EIP). They are used to produce a repeatable Node ID to which the XMS license can be bound.

Once the instance is running, an XMS license can be issued for its Node ID and used whenever an XMS AMI is brought up with that same EIP associated with the VPC. The XMS system's public IP address remains the same whenever the XMS AMI is run.

The order in which the steps in this section are carried out is important because there are dependencies between the created entities. It is assumed that none of the entities created in the following procedures exist.

Create a VPC and Subnet

Perform the following procedure to create a VPC with a single public subnet:

1. Log in to your AWS account and then log in to the console.
2. Confirm that the geographic region is located in one of these AWS Regions:
    - US West (N. California)
    - US East (N. Virginia)
    - EU (Frankfurt)
    - Asia Pacific (Singapore)
    - South America (Sao Paulo)
3. In the console, click **Services > VPC > Start VPC Wizard**. While all of the entities needed to run a VPC may be individually created, the VPC Wizard available in the VPC Dashboard screen will create most of them automatically, along with the VPC. The automatic configuration is adequate for an XMS without unusual networking requirements.

Note: Create VPC in the VPC Dashboard is not the VPC Wizard.

Step 1: Select a VPC Configuration

Select **VPC with a Single Public Subnet** and then click **Select**.

Step 2: VPC with a Single Public Subnet

1. Enter a name for the VPC in the VPC name field. The other fields can be left at the default values.
2. Click Create VPC to create the VPC.
3. After the VPC is successfully created, click Services > VPC > Subnets.
4. Note the subnet ID created for the VPC.

Create the VPC Security Group

A default security group is created as part of running the VPC Wizard. However, it should not be used. A new security group must be created.

Create a security group for XMS as follows:

1. Click **Services > VPC >Security Groups**.
2. Click **Create Security Group**.
3. Enter information in the **Name tag**, **Group name**, and **Description** fields as desired. This information is for descriptive purposes only.
4. In the **VPC** field, select the VPC that was just created, and then click **Yes, Create**.
5. Once the group is created, click the **Inbound Rules** tab, and then click **Edit**.
6. Add the following rules. The source IP address can be left as 0.0.0.0/0 (anywhere) or, for security reasons, restricted to certain IP addresses.

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere, or as desired
HTTP	TCP	80	Anywhere, or as desired
Custom TCP Rule	TCP	81	Anywhere, or as desired
Custom TCP Rule	TCP	161-162	Anywhere, or as desired
HTTPS	TCP	443	Anywhere, or as desired
Custom TCP Rule	TCP	444	Anywhere, or as desired
Custom TCP Rule	TCP	5060	Anywhere, or as desired
Custom TCP Rule	TCP	1080	Anywhere, or as desired
Custom TCP Rule	TCP	6789	Anywhere, or as desired
Custom TCP Rule	TCP	9004	Anywhere, or as desired
Custom TCP Rule	TCP	9876	Anywhere, or as desired
Custom TCP Rule	TCP	10080	Anywhere, or as desired
Custom TCP Rule	TCP	10443	Anywhere, or as desired
Custom TCP Rule	TCP	12000-12010	Anywhere, or as desired
Custom TCP Rule	TCP	15001	Anywhere, or as desired

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	20000	Anywhere, or as desired
Custom TCP Rule	TCP	27000-27009	Anywhere, or as desired
Custom TCP Rule	TCP	27017	Anywhere, or as desired
Custom TCP Rule	TCP	28017	Anywhere, or as desired
Custom UDP Rule	UDP	5060	Anywhere, or as desired
Custom UDP Rule	UDP	9876	Anywhere, or as desired
Custom UDP Rule	UDP	27000-27009	Anywhere, or as desired
Custom UDP Rule	UDP	49152-61344	Anywhere, or as desired

7. Click **Save** to save the ports just added to the group.

Create the Elastic Network Interface (ENI)

The Elastic Network Interface (ENI), along with the Elastic IP address (EIP), make up a permanent network interface to which the XMS license will be bound. Create the ENI address first.

Network interface creation is done in EC2:

1. Click **Services > EC2 > Network Interfaces**.
2. Click **Create Network Interface**.
3. Enter a description in the **Description** field.
4. Select the subnet that was created as part of the VPC in the **Subnet** field.
5. Leave the **Private IP** field at the default (auto assign).
6. Select the XMS security group that was just created for the VPC, and then click **Yes, Create**. Do not use the default security group.

Create the Elastic IP Address (EIP)

After creating the ENI address, create the EIP address:

1. Click **Services > VPC > Elastic IPs**.
2. Click **Allocate New Address**.
3. Allocate the new address. Choose either **EIP used in VPC** or **Network Platform EC2-VPC**.
4. Click **Yes, Allocate**.
5. Select the EIP just created.
6. Click **Actions > Associate Address** and then select the ENI just created.
7. Click **Associate.**

Starting Multiple Instances

If multiple XMS instances are started, each XMS must have its own network interface and EIP address. It is possible, for example, to duplicate a running instance. However, unless using a known network interface with a known VPC and a license tied to it, XMS licensing and startup will fail.

4. Reaching XMS System Using SSH

It should not be necessary to directly log into the XMS system using SSH. However, to do so, use the private key file that corresponds to the public key attached to the instance. Refer to the following example where "my-private-key.pem" is the key name and "<xms_ip_addr>" is the domain name or public address assigned to the instance by EC2:

```
> ssh –i my-private-key.pem <xms_ip_addr>
```

Log in as "ec2-user". Once in the system, commands requiring root privileges are run using "sudo".

5. Verifying XMS Operation

In the AWS console, note the XMS instance's public IP (IPv4) address. Navigate to the PowerMedia XMS Admin Console (WebGUI) using the XMS instance's public IP address (https://<xms_ip_address>). To log in, enter "superadmin" in the **Username** field and "admin" in the **Password** field. From the Console, confirm XMS is started from the **System > Services** page and confirm that the statuses of the services (except faxservice, cdrserver, and wsapiserver where applicable) are green/running.

On the **Network > NAT Configuration** page, confirm that **EC2 (public-ipv4)** is selected. By default, **EC2 (public-ipv4)** is selected for Dialogic AMIs. This option must be selected because the XMS server is behind a NAT firewall. The XMS server's private IP address is different than the public address used to access the XMS externally. This must be taken into account when delivering the RTP (media) address to the WebRTC endpoint so that the external IP address will be automatically determined and used for media connections.

For more details on accessing the XMS Admin Console and XMS configuration, refer to the *Dialogic® PowerMedia™ XMS Installation and Configuration Guide* located at http://www.dialogic.com/webhelp/XMS/3.2/XMS_InstallConfig.pdf.

6. Running XMS Verification Demos

Follow the procedures in the *Dialogic® PowerMedia™ XMS WebRTC Guide* to run the Video Play Verification Demo and the Conference Verification Demo. The guide is located here: http://www.dialogic.com/webhelp/XMS/3.2/XMS_WebRTCDemo.pdf.

The Video Play Verification Demo and the Conference Verification Demos test the functionality of the XMS running on AWS in a WebRTC scenario as follows:

- **Video Play Verification Demo** - This demo plays a video clip on a web browser or a SIP phone. It is a simple demo to test basic functionality.
- **Conference Verification Demo** - This demo allows up to four full duplex video conferees in a single conference at VGA resolution. It shows interoperability between a web browser and SIP. Inbound calls enter and leave the conference. Web page selections allow for playing a video clip into the conference and recording the conference and replaying the recording.
- **Conference Verification Demo** (for VPC) - This is a modified version of the Conference Verification Demo. It assumes at least a 10-port trial license has been activated. This demo allows up to nine full duplex video conferees in a single conference at VGA resolution. More than one conference can be run simultaneously. Each conference needs a unique ID. Follow the procedure for running the Conference Verification Demo in the *Dialogic® PowerMedia™ XMS WebRTC Demo Guide* except in the **Name of person to call** field, enter **conf=*unique_id*@xms** (e.g., **conf=1234@xms**) instead of **conf_demo**. As new conferees enter, the video tiles on the screen are automatically adjusted to accommodate them (up to nine tiles).

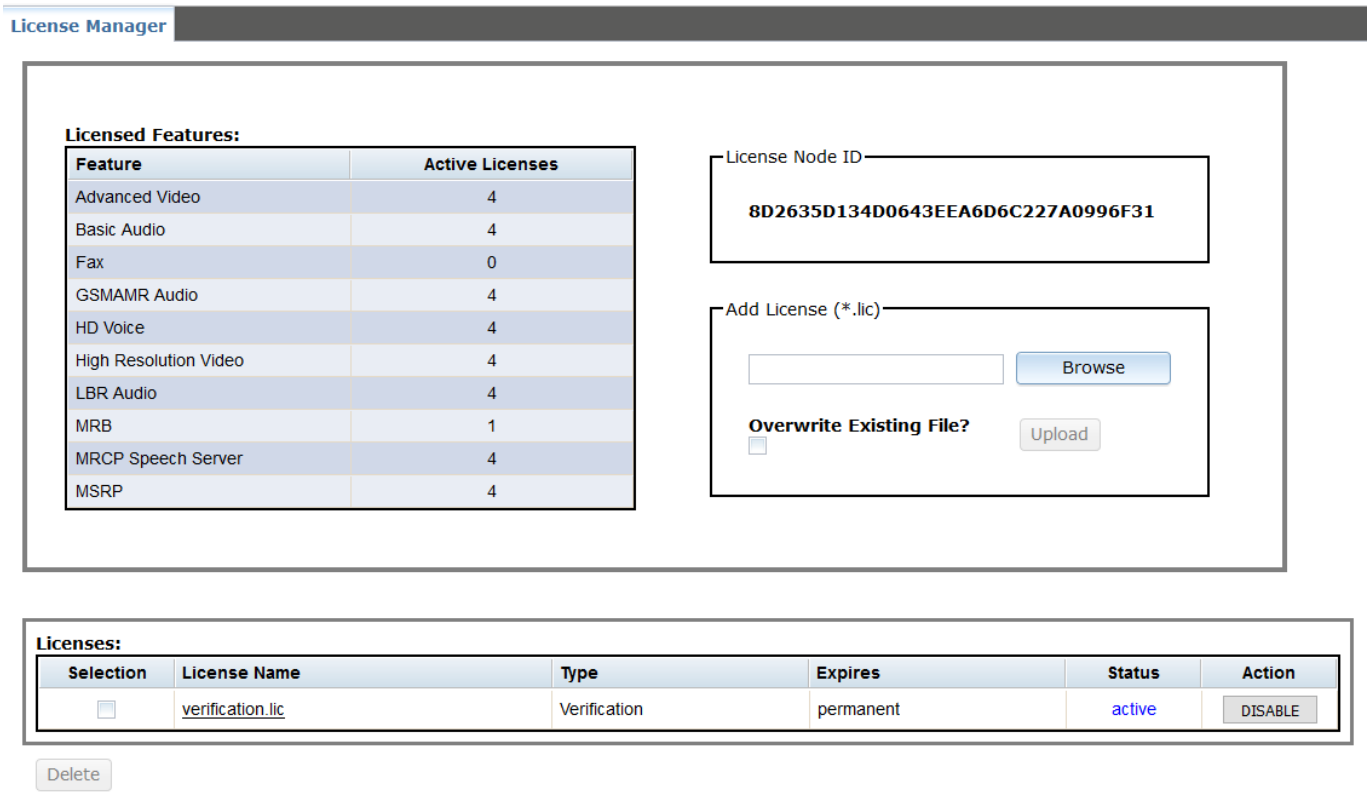
7. Obtaining Higher Density License for XMS Running in Amazon VPC

This section is covers additional procedures for licensing an XMS that is running in a VPC.

Generate the License

Now that the XMS system is running, a higher density license can be put in place.

The License Node ID used to generate the license should be obtained from the license screen.

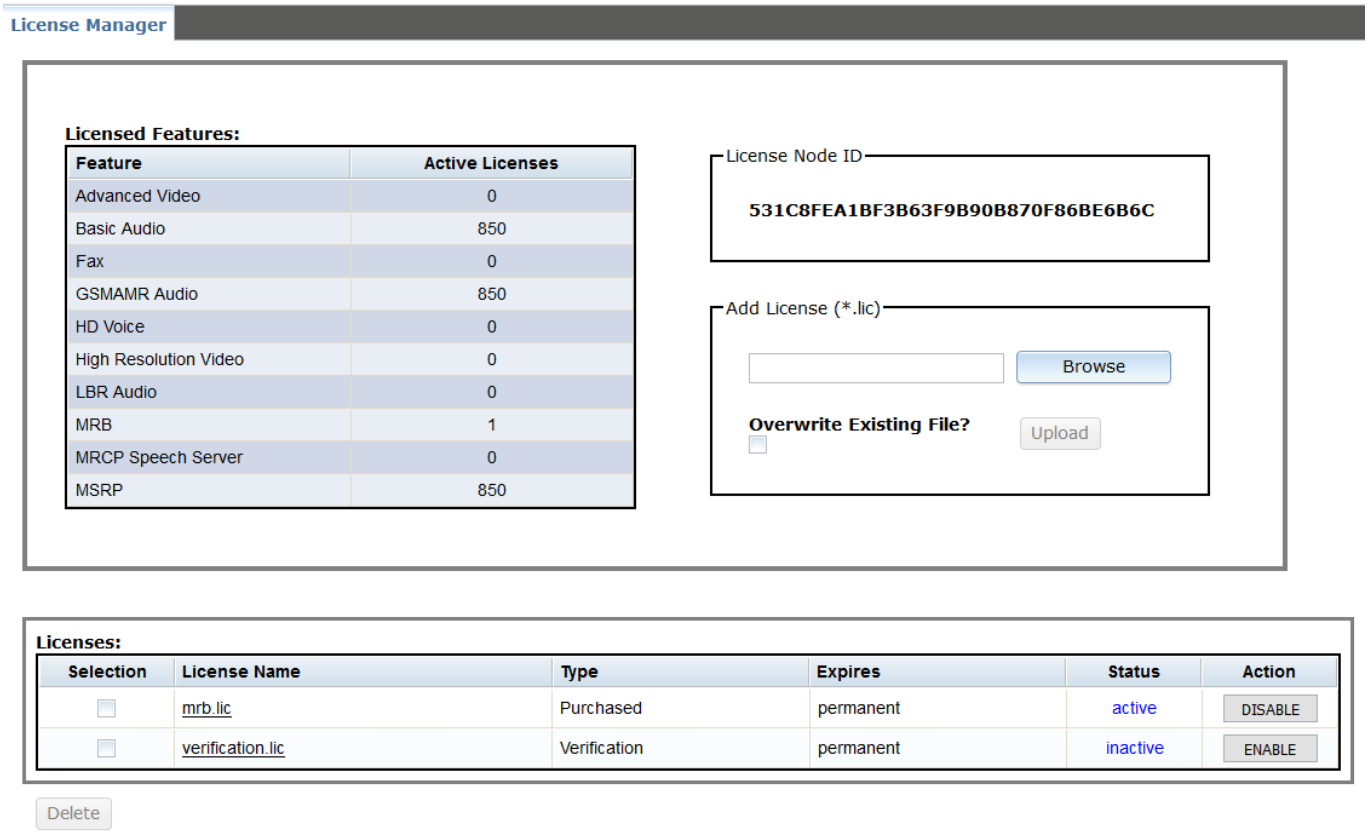


This ID is used to generate a permanent license. This is usually done through the Dialogic Product Center.

Activate the New License

Once the new license is ready and on the system running the web browser, it can be applied to the XMS image.

On the **License** page of the XMS Admin Console, click **Browse**, select the new license, and then click **Upload** to upload the new license.



Click **Disable** to disable the verification license and click **Enable** to enable the new license. Restart XMS services on the **System > Services** page.

Once the XMS services restart, the new license will be applied to the system. This can be verified on the **License** page or the **Monitor > Dashboard** page, which shows the available, used, and free licenses.

Stopping or Terminating the Modified XMS Instance on a VPC

If the newly-licensed XMS image is stopped, it will retain its licensing when the instance is restarted. If the instance is terminated, the licensing changes will be lost.

To avoid this, the licensing can be preserved if a private image/snapshot is made of the instance before it is terminated. When reused with the same VPC and EIP, licensing will remain valid.

Warning: If the EIP is released, the license will become invalid and will need to be reissued.