Getting Started Guide:
LogRhythm Windows Appliance Software Configuration

After you complete the hardware installation of your LogRhythm Windows Appliance, this document will guide you through the initial configuration of your LogRhythm deployment.

IMPORTANT: Please work with your LogRhythm Professional Services Consultant to complete the procedures outlined in this guide.

Prerequisites

Before starting your configuration, you will need:

- The LogRhythm License file (.LIC), usually provided in an email
- The factory default password for your deployment

Configure and Start LogRhythm Components

Configure Platform Manager Services

1. On the **Start** Menu, click ↓ to open Apps, and then click **Platform Manager Configuration Manager**.
2. On the **Job Manager** tab, complete the following fields:
    - Server – the name or IP address of the Platform Manager database server
    - Password – the factory default password
3. On the **Alarming and Response Manager** tab, complete the following fields:
    - Server – the name or IP address of the Platform Manager database server
    - Password – the factory default password
4. Click **OK**.

Configure Data Processor Service

1. On the **Start** Menu, click ↓ to open Apps, and then click **Data Processor Configuration Manager**.
2. On the **General** tab, complete the following fields:
    - Server – the name or IP address of the Platform Manager database server
    - Password – the factory default password
3. Click **OK**.

Configure System Monitor Agent Service

1. On the **Start** Menu, click ↓ to open Apps, and then click **System Monitor Configuration Manager**.
2. On the **General** tab, complete the following fields:
    - Server – the name or IP address of the Data Processor server
    - System Monitor IP Address – the IP address of the System Monitor
    - Host Entity ID – default is zero for system assigned ID
3. Click **OK**.

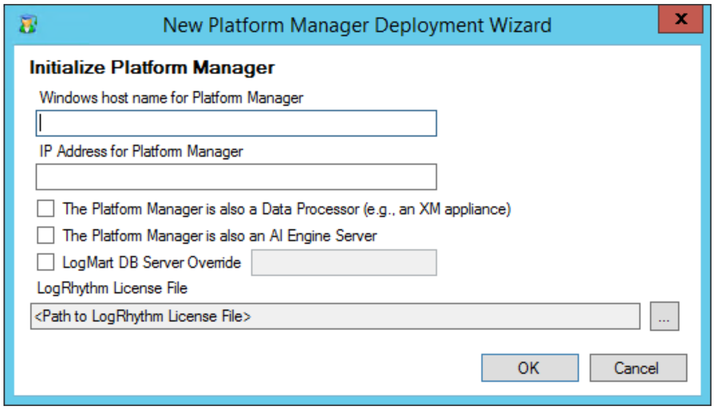
Log in to the Client Console

1. On the **Start** Menu, click ↓ to open Apps, and then click **LogRhythm Console**.
2. Complete the following fields:
    - User ID – logrhythmadmin
    - Password – the factory default password
3. Click **OK**.

Complete New Deployment Wizard

Enter the following information in the New Deployment Wizard:

1. Windows host name of the Platform Manager



New Platform Manager Deployment Wizard

Initialize Platform Manager

Windows host name for Platform Manager

IP Address for Platform Manager

□ The Platform Manager is also a Data Processor (e.g., an XM appliance)

□ The Platform Manager is also an AI Engine Server

□ LogMart DB Server Override

LogRhythm License File

<Path to LogRhythm License File>

   a. Enter the host name where the Platform Manager is located. This can be found by right-clicking My Computer and selecting Properties. Click the Computer Name tab and get the Full Computer Name up to the first period where the domain name will start.

   b. If the appliance type is XM, all LogRhythm components are contained in a single appliance.

2. IP address of the Platform Manager
   Enter the IP address where the Platform Manager is located. Appliances are shipped with two Network Interface Cards (NICs). Typically, one NIC is used for Console connections, while the other NIC is used for database intercommunications. The IP address entered here will serve as a Console connection interface.

3. The Platform Manager is also a Data Processor (e.g., an XM appliance)
   If this is an XM Appliance — all LogRhythm components are contained in a single appliance — select this checkbox.

4. The Platform Manager is also an AI Engine Server
   If AI Engine is installed on the Platform Manager — not deployed as a standalone appliance — select this checkbox.

5. LogMart DB Server Override
   If the LogMart database is installed on a different host, enter the host IP address here.

6. LogRhythm License file

   Note: This file is provided by LogRhythm Support after purchase and shipment of the appliance(s), and it is required to access and configure LogRhythm.

   a. Navigate to the location of the license file (*.lic) by clicking the ellipses at the far right.

   b. Locate and select the master license file and click **Open**. The path and file name are listed in the License File text box.

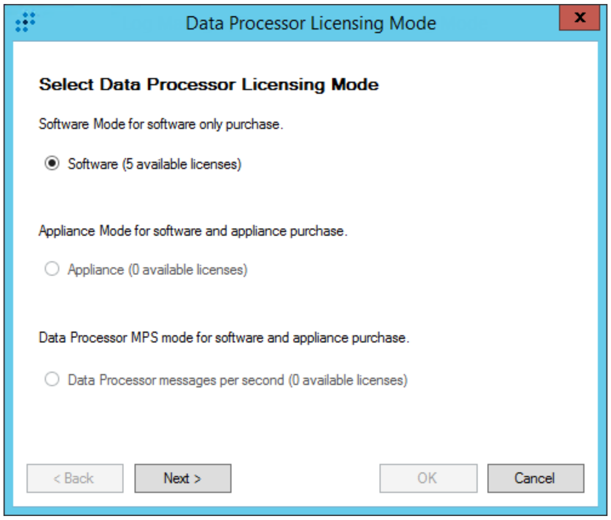
   c. Click **OK**.

8. When prompted, select the appropriate Data Processor licensing mode from the available, valid options. The mode depends on:

   a. **Software (n available licenses)** - Select this option to identify a software only purchase

   b. **Appliance Mode for software and appliance purchase** - Select this option to identify a software and appliance purchase

   c. **Data Processor MPS mode for software and appliance purchase** - Select this option to use a Messages Per Second license



Data Processor Licensing Mode

Select Data Processor Licensing Mode

Software Mode for software only purchase.

● Software (5 available licenses)

Appliance Mode for software and appliance purchase.

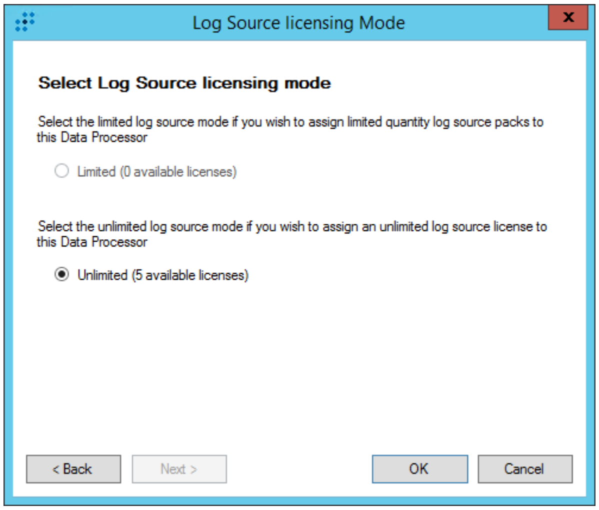
○ Appliance (0 available licenses)

Data Processor MPS mode for software and appliance purchase.

○ Data Processor messages per second (0 available licenses)

9. Click **Next**.

10. You are prompted to select the Log Source licensing mode from the available valid options: Limited or Unlimited.



Log Source licensing Mode

Select Log Source licensing mode

Select the limited log source mode if you wish to assign limited quantity log source packs to this Data Processor

○ Limited (0 available licenses)

Select the unlimited log source mode if you wish to assign an unlimited log source license to this Data Processor

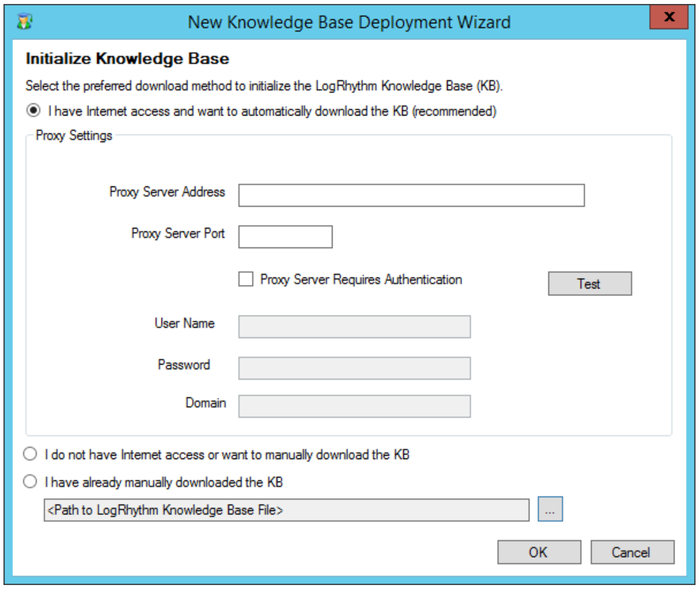
● Unlimited (5 available licenses)

11. Select the appropriate mode, and then click **OK**.

    All dialog boxes close and the main Client Console window is displayed.

Complete Knowledge Base Import Wizard

After completing the New Deployment Wizard, the New Knowledge Base Deployment Wizard is displayed.



New Knowledge Base Deployment Wizard

Initialize Knowledge Base

Select the preferred download method to initialize the LogRhythm Knowledge Base (KB).

● I have Internet access and want to automatically download the KB (recommended)

Proxy Settings

Proxy Server Address

Proxy Server Port

□ Proxy Server Requires Authentication

Test

User Name

Password

Domain

○ I do not have Internet access or want to manually download the KB

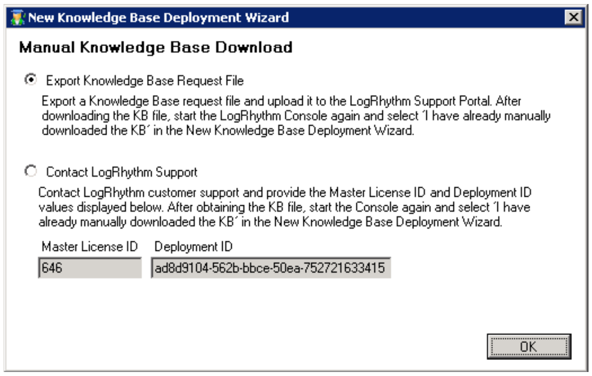
○ I have already manually downloaded the KB

<Path to LogRhythm Knowledge Base File>

OK Cancel

1. Deploy the Knowledge Base by selecting one of the three following options:
   - I have Internet access and want to automatically download the KB (recommended).
     a. Proxy Server Address - Enter the Proxy Server Address for the KB Download
     b. Proxy Server Port - Enter the port number for the server
     c. Select the Proxy Server Requires Authentication check box
     d. Enter the appropriate credentials and Host name, if necessary
     e. Click OK. The Knowledge Base is downloaded.
     f. Click OK. Proceed to the Knowledge Base Importer Wizard section.
   - I do not have Internet access or want to manually download the KB.

     The Manual Knowledge Base Download window appears.



New Knowledge Base Deployment Wizard

Manual Knowledge Base Download

● Export Knowledge Base Request File

Export a Knowledge Base request file and upload it to the LogRhythm Support Portal. After downloading the KB file, start the LogRhythm Console again and select 'I have already manually downloaded the KB' in the New Knowledge Base Deployment Wizard.

○ Contact LogRhythm Support

Contact LogRhythm customer support and provide the Master License ID and Deployment ID values displayed below. After obtaining the KB file, start the Console again and select 'I have already manually downloaded the KB' in the New Knowledge Base Deployment Wizard.

Master License ID	Deployment ID
646	ad8d9104-562b-bbce-50ea-752721633415

OK

Perform one of the following steps:

- Export Knowledge Base Request File - Select this option to export a Knowledge Base request file and upload it to the Support Portal:
    i. Click OK and download the file to your drive. The Export Successful page appears.

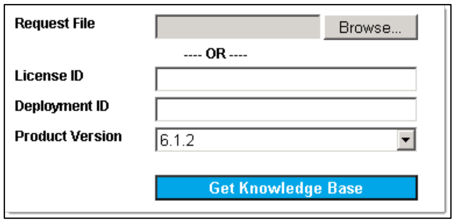
    ii. Click OK. The Knowledge Base Not Loaded page appears.

    iii. Click OK and the Console closes.

- Contact Customer Support - Select this option to obtain the Knowledge Base file from Customer Support:
    i. From a computer with Internet access, log into the Support Portal at https://support.logrhythm.com.

    ii. Go to the Downloads to section to access the latest version of the Knowledge Base.

    The request screen displays.



Request File

---- OR ----

License ID

Deployment ID

Product Version: 6.1.2

    iii. Choose from the following:

        a. Upload the Request File downloaded from the Console

        b. Enter the License ID, the Deployment ID, and the Product Version

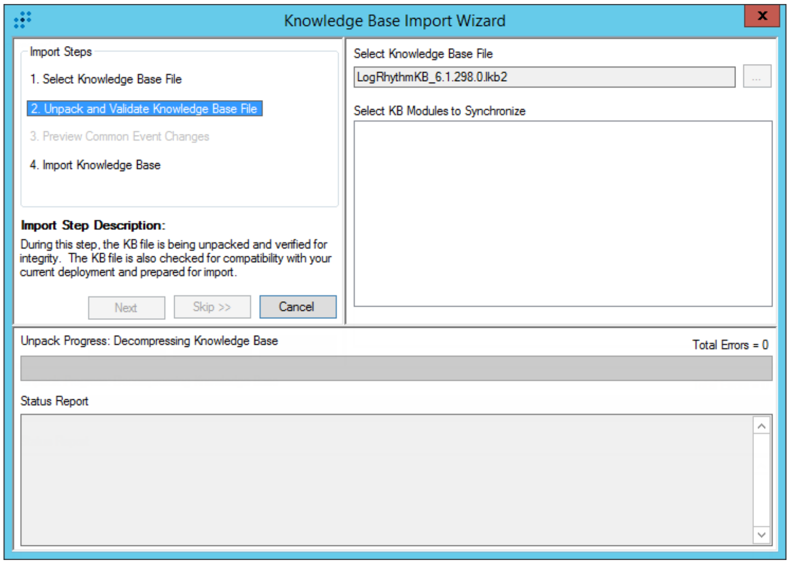
    iv. Click Get Knowledge Base.

    v. Save the Knowledge Base file and transfer it to the computer on which you are loading the Console.

    vi. Restart the Console and follow the instructions in the “I have already manually downloaded the KB section.”

- I have already manually downloaded the KB - Select this option to manually import the Knowledge Base file.

  i. The Knowledge Base Export Wizard appears and starts unpacking and validating the Knowledge Base file. The file is checked for compatibility with your current deployment and is prepared for import. This may take several minutes.


Knowledge Base Import Wizard
Import Steps
1. Select Knowledge Base File
2. Unpack and Validate Knowledge Base File
3. Preview Common Event Changes
4. Import Knowledge Base
Next
Skip >>
Cancel
Select Knowledge Base File
Select KB Modules to Synchronize
Status Report

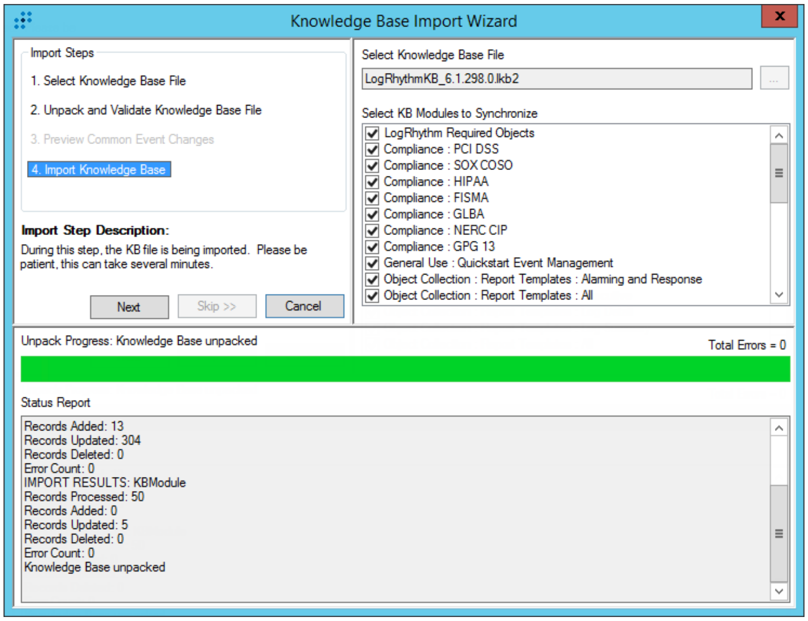
Import Step Description:
During this step, the KB file is being unpacked and verified for integrity. The KB file is also checked for compatibility with your current deployment and prepared for import.

Select Knowledge Base File: LogRhythmKB_6.1.298.0.lkb2

Unpack Progress: Decompressing Knowledge Base

Total Errors = 0

  ii. Upon completion the message Knowledge Base unpacked appears in the status. Click Next to import the Knowledge Base.


Knowledge Base Import Wizard
Import Steps
1. Select Knowledge Base File
2. Unpack and Validate Knowledge Base File
3. Preview Common Event Changes
4. Import Knowledge Base
Next
Skip >>
Cancel
Select Knowledge Base File
Select KB Modules to Synchronize
Status Report

Import Step Description:
During this step, the KB file is being imported. Please be patient, this can take several minutes.

Select Knowledge Base File: LogRhythmKB_6.1.298.0.lkb2

Select KB Modules to Synchronize:

☑ LogRhythm Required Objects
☑ Compliance : PCI DSS
☑ Compliance : SOX COSO
☑ Compliance : HIPAA
☑ Compliance : FISMA
☑ Compliance : GLBA
☑ Compliance : NERC CIP
☑ Compliance : GPG 13
☑ General Use : Quickstart Event Management
☑ Object Collection : Report Templates : Alarming and Response
☑ Object Collection : Report Templates : All

Unpack Progress: Knowledge Base unpacked

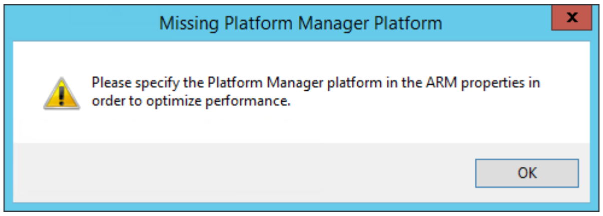
Total Errors = 0

```
Records Added: 13
Records Updated: 304
Records Deleted: 0
Error Count: 0
IMPORT RESULTS: KBModule
Records Processed: 50
Records Added: 0
Records Updated: 5
Records Deleted: 0
Error Count: 0
Knowledge Base unpacked
```

2. When the Knowledge Base Updated message is displayed, click **OK**.
3. On the Knowledge Base Import Wizard, click **Close**.

Configure the Platform

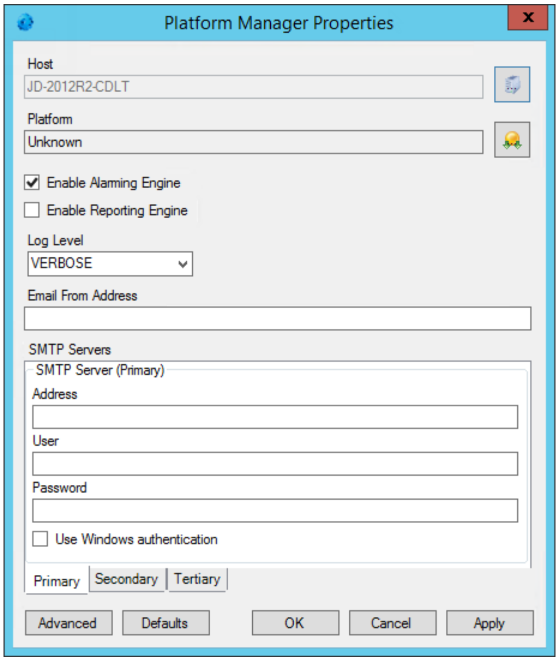
After completing the Knowledge Base import, the Missing Platform Manager Platform message is displayed.



Missing Platform Manager Platform

Please specify the Platform Manager platform in the ARM properties in order to optimize performance.

1. Click **OK**.
2. In the Platform Manager Properties dialog box, click the browse icon next to the Platform box.



Platform Manager Properties

Host: JD-2012R2-CDLT

Platform: Unknown

☑ Enable Alarming Engine

□ Enable Reporting Engine

Log Level: VERBOSE

Email From Address

SMTP Servers

SMTP Server (Primary)

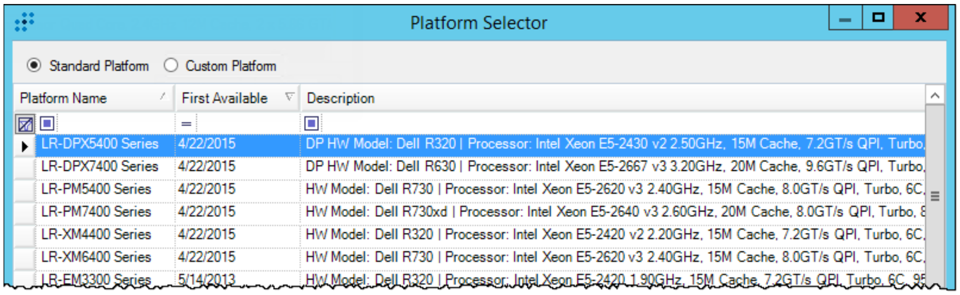
Address

User

Password

□ Use Windows authentication

3. In the Platform Selector table, select the row corresponding to your appliance, and then click **OK**.



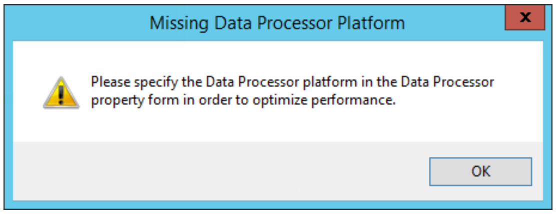
Platform Selector

● Standard Platform ○ Custom Platform

Platform Name	First Available	Description
LR-DPX5400 Series	4/22/2015	DP HW Model: Dell R320 | Processor: Intel Xeon E5-2430 v2 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo,
LR-DPX7400 Series	4/22/2015	DP HW Model: Dell R630 | Processor: Intel Xeon E5-2667 v3 3.20GHz, 20M Cache, 9.6GT/s QPI, Turbo,
LR-PM5400 Series	4/22/2015	HW Model: Dell R730 | Processor: Intel Xeon E5-2620 v3 2.40GHz, 15M Cache, 8.0GT/s QPI, Turbo, 6C,
LR-PM7400 Series	4/22/2015	HW Model: Dell R730xd | Processor: Intel Xeon E5-2640 v3 2.60GHz, 20M Cache, 8.0GT/s QPI, Turbo, 8
LR-XM4400 Series	4/22/2015	HW Model: Dell R320 | Processor: Intel Xeon E5-2420 v2 2.20GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C,
LR-XM6400 Series	4/22/2015	HW Model: Dell R730 | Processor: Intel Xeon E5-2620 v3 2.40GHz, 15M Cache, 8.0GT/s QPI, Turbo, 6C,
LR-EM3300 Series	5/14/2013	HW Model: Dell R320 | Processor: Intel Xeon E5-2420 1.90GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95

4. Enter the Email From Address, and then click **OK**.

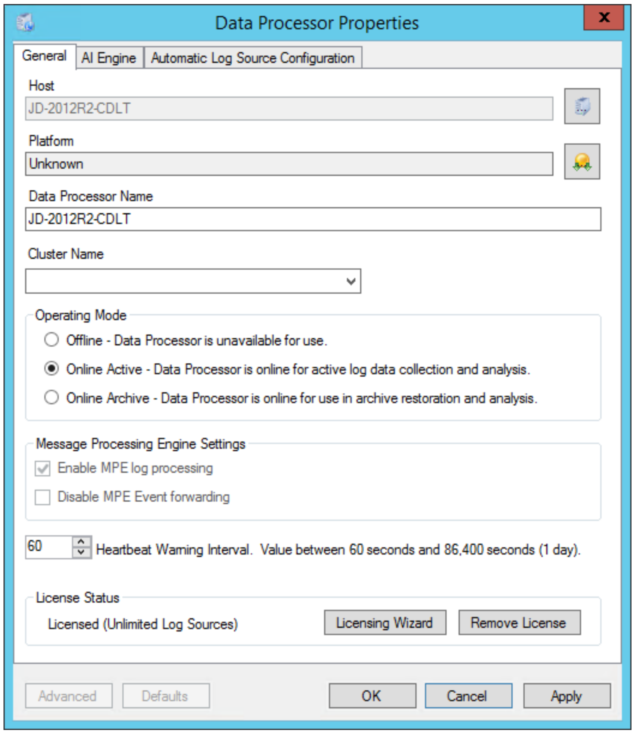
The Missing Data Processor Platform error message is displayed.



Missing Data Processor Platform

Please specify the Data Processor platform in the Data Processor property form in order to optimize performance.

5. Click **OK**.
6. In the Data Processor Properties dialog box, click the browse icon next to the Platform box.



Data Processor Properties

General | AI Engine | Automatic Log Source Configuration

Host
JD-2012R2-CDLT

Platform
Unknown

Data Processor Name
JD-2012R2-CDLT

Cluster Name

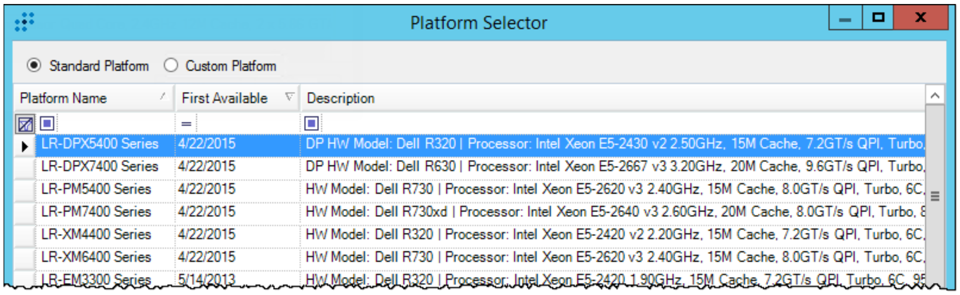
Operating Mode
○ Offline - Data Processor is unavailable for use.
● Online Active - Data Processor is online for active log data collection and analysis.
○ Online Archive - Data Processor is online for use in archive restoration and analysis.

Message Processing Engine Settings
☑ Enable MPE log processing
☐ Disable MPE Event forwarding

60 Heartbeat Warning Interval. Value between 60 seconds and 86,400 seconds (1 day).

License Status
Licensed (Unlimited Log Sources)

7. In the Platform Selector table, select the row corresponding to your appliance, and then click **OK**.

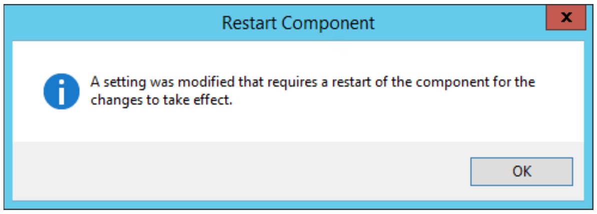


Platform Selector

● Standard Platform ○ Custom Platform

Platform Name	First Available	Description
LR-DPX5400 Series	4/22/2015	DP HW Model: Dell R320 | Processor: Intel Xeon E5-2430 v2 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo,
LR-DPX7400 Series	4/22/2015	DP HW Model: Dell R630 | Processor: Intel Xeon E5-2667 v3 3.20GHz, 20M Cache, 9.6GT/s QPI, Turbo,
LR-PM5400 Series	4/22/2015	HW Model: Dell R730 | Processor: Intel Xeon E5-2620 v3 2.40GHz, 15M Cache, 8.0GT/s QPI, Turbo, 6C,
LR-PM7400 Series	4/22/2015	HW Model: Dell R730xd | Processor: Intel Xeon E5-2640 v3 2.60GHz, 20M Cache, 8.0GT/s QPI, Turbo, 8
LR-XM4400 Series	4/22/2015	HW Model: Dell R320 | Processor: Intel Xeon E5-2420 v2 2.20GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C,
LR-XM6400 Series	4/22/2015	HW Model: Dell R730 | Processor: Intel Xeon E5-2620 v3 2.40GHz, 15M Cache, 8.0GT/s QPI, Turbo, 6C,
LR-EM3300 Series	5/14/2013	HW Model: Dell R320 | Processor: Intel Xeon E5-2420 1.90GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95

8. The Restart Component message is displayed.



Restart Component

A setting was modified that requires a restart of the component for the changes to take effect.

9. Click **OK**.

Specify Advanced Data Processor Properties

1. In the Data Processor Properties dialog box, click **Advanced**.

   The Data Processor Advanced Properties dialog box is displayed.

2. Change the ActiveArchivePath from C:\LogRhythmArchives\Active to D:\LogRhythm Archives\Active.

3. Change the InactiveArchivePath from C:\LogRhythmArchives\Inactive to D:\LogRhythmArchives\Inactive.

4. Click **OK**.

   The Restart Component message is displayed.

5. Click **OK**.

Start the Platform Manager Services

1. Click the Platform Manager tab.

2. Click Start.

Start the Data Processor Services

1. Click the Data Processors tab.

2. Select the Action box next to your Data Processor.

3. Right-click the selected Data Processor, click **Actions**, and then click **Service Start**.

Start the System Monitor Agents Services

1. Click the System Monitors tab.

2. Select the Action box next to the System Monitor Agent.

3. Right-click the selected System Monitor, click **Actions**, and then click **Service Start**.

   The System Monitor Agent is displayed in the top pane and listed as pending.

4. Select the Action box next to the pending Agent.

5. Right-click the selected Agent, and then click **Associate**.

   The “Associate New System Monitor Agent with an Existing Agent” message is displayed.

6. Select the Agent and click **OK**.

   The “Associate Successful” message is displayed.

7. Click **OK**.

Configure the Data Indexer

Accessing and configuring the Data Indexer differs slightly between Windows and Linux. Please refer to the appropriate procedure below according to your Data Indexer operating system.

Configure the Data Indexer on Windows

NOTE: You must perform these steps for each Data Indexer (XM or DPX) in your deployment. Ensure that the **LogRhythm DX – AllConf** and **LogRhythm DX – Configuration Server** services are running before trying to connect to the Data Indexer.

Configure the Data Indexer via the configuration web page hosted on the Data Indexer. Please note the following requirements:

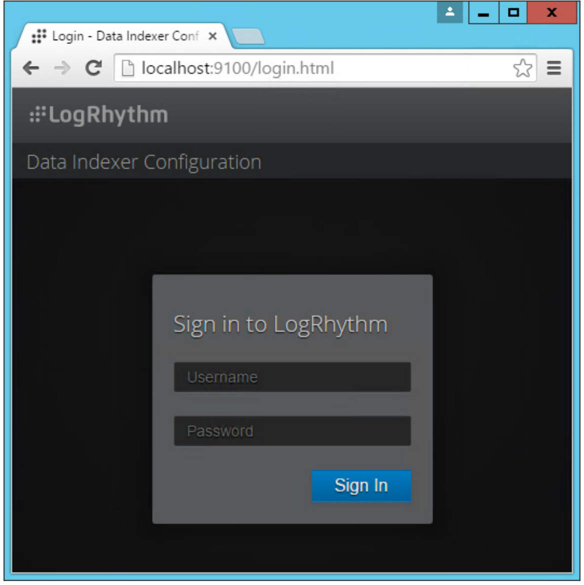
- On a Windows Data Indexer, you can only access the web page locally or through a remote desktop/terminal services session to the appliance
- You can only access the web page using **Google Chrome**, **Mozilla Firefox** (latest versions of each), or **Internet Explorer 11**.

  NOTE: Do not attempt to modify any configuration files. If you have any issues, please contact LogRhythm Support.

To access the web page and configure the Data Indexer, do the following:

1. Log in to the DPX appliance as an administrator.
2. Start one of the supported Internet browsers.
3. Type the following in the address bar: **localhost:9100**

   The Data Indexer Configuration sign in page is displayed.


Login - Data Indexer Conf
localhost:9100/login.html
LogRhythm
Data Indexer Configuration
Sign in to LogRhythm
Username
Password
Sign In

4. Type **admin** in the Username box and the LogRhythm default password in the Password box, and then click **Sign In**.

5. Modify or verify the following settings:

Anubis Config

Anubis sends logs to the Mediator in batches. The frequency at which batches are sent is determined by the Accumulator Conf settings shown below. A batch of logs will be sent when any one of the following thresholds is met: Entries to Accumulate, Max Batch Size Bytes, or Seconds To Accumulate

NOTE: The default values assume 1500 byte logs and should work well for most indexing rates.

Parameter	Value
Accumulator Conf	
Entries to Accumulate	The number of logs to accumulate before sending to the Mediator. The default is 50,000.
Max Batch Size Bytes	The maximum size in bytes that a batch of logs can become before sending to the Mediator. The default is 15,000,000.
Max Log Size Bytes	This can be left at the default value of 1,000,000.
Seconds To Accumulate	The maximum amount of time in seconds to wait before sending to the Mediator. The default is 5.
Gigawatt DB Config	
Gigawatt Db Path	This is the path to the database used for messaging within the Indexer system. **NOTE:** You can use any directory you want for Gigawatt Db, but it should **not be on the C: drive**. You should overwrite the default and change it to something like the following: D:\Logrhythm\data indexer\gigawatt\db
Relay Config	
These values can be left at their defaults.	

Carpenter Config

Parameter	Value
Db Password	This is the password used by the LogRhythmNGLM SQL account. Services on the Data Indexer use this account to connect to the EMDB and read/update tables. **NOTE:** It is highly recommended and LogRhythm best practice to change all MS SQL account passwords when setting up a deployment. After you change the LogRhythmNGLM password in Microsoft SQL Server Management Studio, you must set **Db Password** to the same value. You should change the password in Microsoft SQL Server Management Studio first, then change it on the Data Indexer page.
Db Username	This should be left unchanged unless you have renamed the LogRhythmNGLM SQL account in SQL Server Management Studio.
Emdb Host	This **must** be set to the external IP address of your Platform Manager appliance, where the EMDB database is hosted.
Minutes To Rest	This can be left at the default value.
Sql Paging Size	This can be left at the default value.

Cluster Node Config

Parameter	Value
Node Info[*n*]	
Hostname	Cannot be changed
Public IP	This **must** be set to the external IP address of your DPX appliance or server.

Elasticsearch Server Config

Parameter	Value
Elasticsearch Server Settings[*n*]	
Name	cluster.name
Value	If you only have one DPX appliance, you can leave this value at the default (logrhythm). If you have more than one DPX appliance, change this value so that each cluster name is unique. For example, logrhythm01, logrhythm02, and logrhythm03. The cluster name for each DPX appliance must be different. When you have finished making changes on the Data Indexer Configuration page, ensure that you assign the correct cluster to each Data Processor. For multiple DPX appliances, ensure that the cluster is assigned to the Data Processor running on the same appliance. For example, if clusters are named as follows: DPX-A = dxa, DPX-B = dxb, and DPX-C = dxc, Data Processor A should point to cluster dxa, Data Processor B should point to cluster dxb, and Data Processor C should point to cluster dxc.
Elasticsearch Server Settings[*n*]	
Name	path.data
Value	${DXDATAPATH}\elasticsearch\data ${DXDATAPATH} is a system variable that is created when the Data Indexer is installed. By default, ${DXDATAPATH} is set to C:\Program Files\LogRhythm\Data Indexer. This means the default data path is C:\Program Files\LogRhythm\Data Indexer\elasticsearch\data. **NOTE:** You can use any directory you want for storing Elasticsearch data, but it should **not be on the C: drive**. You should overwrite the default and change it to something like the following: D:\LRIndexer\elasticsearch\data. If you have more than one drive for data, you can specify multiple locations in the following format: D:\LRIndexer\elasticsearch\data,E:\LRIndexer\elasticsearch\data

6. Click **Submit**.

   Your changes will be pushed to the appropriate appliances and database tables, and all of the required Data Indexer services will start or restart.

Configure the Data Indexer on Linux

Whether your Linux Data Indexer cluster is one node or 3 to 10 nodes, you only have to log in to the configuration page on one of the nodes. Please note the following requirements:

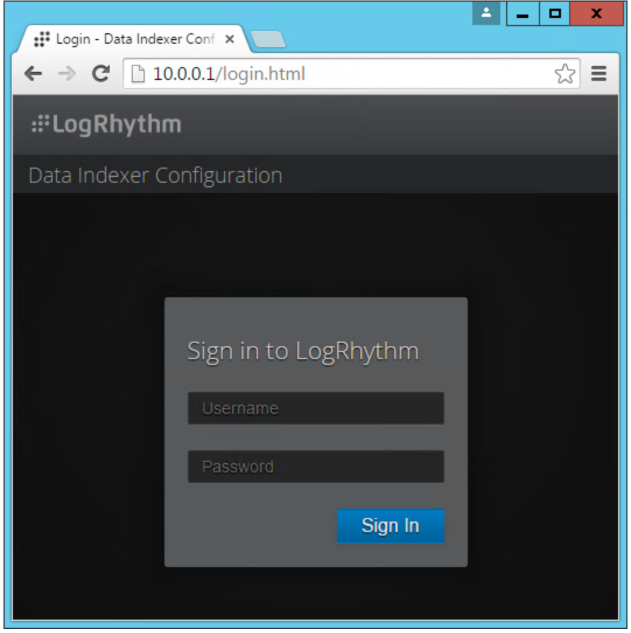
- On a Linux Data Indexer, you can only access the web page from an external computer that has access to the Data Indexer network.
- You can only access the web page using **Google Chrome**, **Mozilla Firefox** (latest versions of each), or **Internet Explorer 11**.

  NOTE: Do not attempt to modify any configuration files. If you have any issues, please contact LogRhythm Support.

To access the web page and configure the Linux cluster, do the following:

1. Log in to a Windows server with network access to the Data Indexer nodes.
2. Start one of the supported Internet browsers.
3. Type the IP address of one of the cluster nodes in the address bar, and then press **Enter**.

   The Data Indexer Configuration page is displayed.



4. Type **admin** in the username box and the LogRhythm default password in the password box, and then click **Sign In**.

5. Modify or verify the following settings:

Anubis Config

Anubis sends logs to the Mediator in batches. The frequency at which batches are sent is determined by the Accumulator Conf settings shown below. A batch of logs will be sent when any one of the following thresholds is met: Entries to Accumulate, Max Batch Size Bytes, or Seconds To Accumulate

NOTE: The default values assume 1500 byte logs and should work well for most indexing rates.

Parameter	Value
Accumulator Conf	
Entries to Accumulate	The number of logs to accumulate before sending to the Mediator. The default is 50,000.
Max Batch Size Bytes	The maximum size in bytes that a batch of logs can become before sending to the Mediator. The default is 15,000,000.
Max Log Size Bytes	This can be left at the default value of 1,000,000.
Seconds To Accumulate	The maximum amount of time in seconds to wait before sending to the Mediator. The default is 5.
Gigawatt DB Config	
Gigawatt Db Path	This can be left at the default value.
Relay Config	
These values can be left at their defaults.	

Carpenter Config

Parameter	Value
Db Password	This is the password used by the LogRhythmNGLM SQL account. Services on the Data Indexer use this account to connect to the EMDB and read/update tables. **NOTE:** It is highly recommended and LogRhythm best practice to change all MS SQL account passwords when setting up a deployment. After you change the LogRhythmNGLM password in Microsoft SQL Server Management Studio, you must set **Db Password** to the same value. You should change the password in Microsoft SQL Server Management Studio first, then change it on the Data Indexer page.
Db Username	This should be left unchanged unless you have renamed the LogRhythmNGLM SQL account in SQL Server Management Studio.
Emdb Host	This is the external IP address of your Platform Manager appliance, where the EMDB database is hosted. If you leave the default value of 127.0.0.1, the Data Indexer services will attempt to connect locally to the EMDB, but it does not exist locally.
Minutes To Rest	This can be left at the default value.
Sql Paging Size	This can be left at the default value.

Cluster Node Config

Parameter	Value
Node Info[*n*]	
Hostname	Cannot be changed
Public IP	For each node, this **must** be set to the external IP address of your Data Indexer appliance or server.

Elasticsearch Server Config

Parameter	Value
Elasticsearch Server Settings[*n*]	
Name	cluster.name
Value	If you only have one cluster, you can leave this value at the default: logrhythm If you have more than one cluster, change this value so that each cluster name is unique. For example, logrhythm01, logrhythm02, and logrhythm03.

6. Click **Submit**.

   Your changes will be pushed to the appropriate appliances and database tables, and all of the required Data Indexer services will start or restart.

Information about Automatic Maintenance

Automatic maintenance is governed by several settings in Go Maintain Config:

- **diskUtilLimt** indicates the percentage of disk utilization that triggers maintenance. The default is 80, which means that maintenance will start when the Elasticsearch data disk is 80% full.
- **indexConfigs[0]: Min** indicates the absolute minimum number of indices that are required for the active repository. The default is 2.

Maintenance is applied to the active repository, as well as archive repositories created by Second Look. When the Disk Usage Limit (**diskUtilLimit: 80**) is reached, active logs are trimmed when "max indices" is reached. Then Go Maintain deletes completed restored repositories starting with the oldest date.

The default settings prioritize restored repositories above the active log repository. Restored archived logs will be maintained at the sacrifice of active logs.

If you want to keep your active logs and delete archives for space, set your min indices equal to your max indices. This will force the maintenance process to delete restored repositories first.

Assign the Data Processor to a Data Indexer Cluster

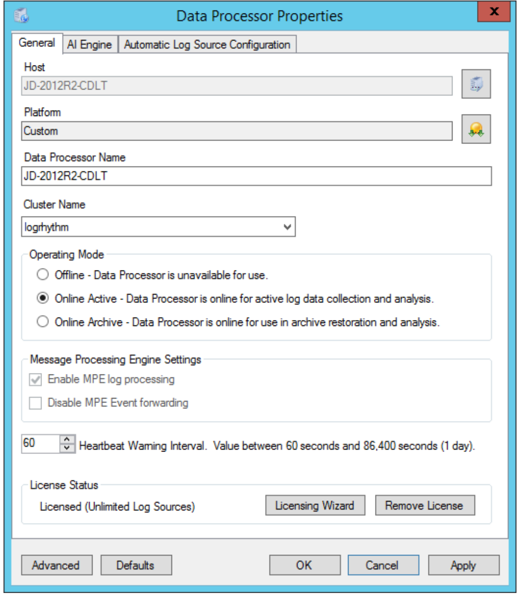
Every Data Indexer is considered to be part of a cluster, even if only a cluster of one. In LogRhythm 7.x, a new configuration option is available to assign the Data Processor to a cluster.

NOTE: You should assign all Data Processors to a cluster, offline, active, and archive. If you need to restore any data using SecondLook, the archive Data Processors must be assigned to a cluster.

To assign the Data Processor to a cluster, do the following:

1. Log in to a system where the LogRhythm 7.1.5 Client Console is installed.
2. Start the Client Console and click **Deployment Manager**.
3. Click the **Data Processors** tab.

   The Data Processor Properties dialog box is displayed.



Host
JD-2012R2-CDLT

Platform
Custom

Data Processor Name
JD-2012R2-CDLT

Cluster Name
logrhythm

Operating Mode
○ Offline - Data Processor is unavailable for use.
● Online Active - Data Processor is online for active log data collection and analysis.
○ Online Archive - Data Processor is online for use in archive restoration and analysis.

Message Processing Engine Settings
☑ Enable MPE log processing
☐ Disable MPE Event forwarding

60 Heartbeat Warning Interval. Value between 60 seconds and 86,400 seconds (1 day).

License Status
Licensed (Unlimited Log Sources) Licensing Wizard Remove License

4. Select a cluster from the **Cluster Name** list, and then click **OK**.

   NOTE: Cluster information is sent out when applying configuration changes on the Data Indexer. Refer to Configure the Data Indexer for more information.

Verify Appliance Functionality

1. Verify Log Collection via Tail (see "Configure a New Tail" in the application Help).

2. Ensure log data is being received by viewing the log data in the Tail display.

3. Configure the Tail to query all available log sources for the last 24 hours. Do not configure any filters.

4. Ensure logs are being processed by double-clicking a row in the Log/Event List pane, and checking for metadata parsing and classification. It is sufficient to just verify that there is some data loaded into the fields on the Processed Metadata Fields tab.

5. Verify Event Forwarding by opening the Personal Dashboard and viewing events as they arrive.

6. Visually check system health and status by opening the Deployment Monitor. The Deployment Monitor provides statistics about log collection and system resource usage.

NOTE: Log collection happens from the older date to the newer date. If no data is present, repeat the Tail using a timeframe further in the past. It may take your LogRhythm appliance several hours to catch up to the present after collection begins.

Additional Tasks

1. Activate and register the Microsoft Windows operating system on the appliance.

2. Ensure that you have the latest LogRhythm software, especially if there was a time lapse between the receipt and the setup of the appliance.

3. Configure log collection from additional sources.

4. Run Microsoft Windows Update to confirm that you have the latest Microsoft updates installed on the appliance.

LogRhythm Inc., 4780 Pearl East Circle, Boulder, CO 80301

www.logrhythm.com | (303) 413-8745 | support@logrhythm.com

Disclaimer
The information contained in this document is subject to change without notice. LogRhythm, Inc. makes no warranty of any kind with respect to this information. LogRhythm, Inc. specifically disclaims the implied warranty of merchantability and fitness for a particular purpose. LogRhythm, Inc. shall not be liable for any direct, indirect, incidental, consequential, or other damages alleged in connection with the furnishing or use of this information.