

# **FIPS 140-2 Non-proprietary Security Policy**

## **LogRhythm 7.8.0 Platform Manager**

---

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

August 3, 2022

Document Version 1.2  
Module Version 7.8.0



Prepared by:



Accredited Testing & Evaluation Labs  
6841 Benjamin Franklin Drive  
Columbia, MD 21046

© Copyright 2022 LogRhythm, Inc.

**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.

**Trademark**

LogRhythm is a registered trademark of LogRhythm, Inc. All other company or product names mentioned may be trademarks, registered trademarks, or service marks of their respective holders.

## Table of Contents

1.	Introduction.....	4
2.	Overview.....	5
2.1.	Ports and Interfaces .....	10
2.2.	Modes of Operation.....	12
2.3.	Module Validation Level.....	12
3.	Roles .....	14
4.	Services .....	15
4.1.	User Services.....	15
4.2.	Crypto Officer Services .....	16
5.	Policies.....	18
5.1.	Security Rules.....	18
5.2.	Identification and Authentication Policy.....	19
5.3.	Access Control Policy and SRDIs .....	19
5.4.	Physical Security .....	21
6.	Crypto Officer Guidance.....	22
6.1.	Secure Operation Initialization Rules.....	22
6.2.	Approved Mode .....	24
7.	Mitigation of Other Attacks .....	26
8.	Terminology and Acronyms.....	27
9.	References.....	28
	Appendix A: TLS Cipher Suites.....	29

# 1. Introduction

LogRhythm is an integrated log management and security information event management (SIEM) solution. It is a distributed system containing several cryptographic modules, which support secure communication between components. A LogRhythm deployment is made up of distributed components including Advanced Intelligence (AI) Engine Servers, Consoles (Client/Web), Data Indexers, Data Processors, a Platform Manager, and System Monitor Agents. An AI Engine Server analyzes log metadata for complex events, which it may forward to Platform Manager. A LogRhythm Console provides a graphical user interface (GUI) to view log messages, events, and alerts. LogRhythm Consoles are also used to manage LogRhythm deployments. Data Indexers deliver distributed and highly scalable indexing of machine and forensic data. Data Indexers run Elasticsearch and LogRhythm services to provide raw log and metadata persistence and search capabilities. Indexers can be clustered to enable high availability and improved performance. A Data Processor aggregates log data from System Monitor Agents, extracts metadata from the logs, forwards logs/metadata to Elasticsearch for persistence and search, and analyzes content of logs and metadata. A Data Processor may forward log metadata to an AI Engine Server and may forward significant events to Platform Manager. A Platform Manager manages configuration, alarms, notifications, and case and security incident management. A System Monitor Agent collects log data from network sources. LogRhythm relies on Microsoft SQL Server. LogRhythm stores log data in SQL Server databases on Data Processor and Platform Manager. It stores configuration information in SQL Server databases on Platform Manager. System Monitor Agent, Data Processor, AI Engine Server, Platform Manager, and Console each include a cryptographic module.

This document describes the security policy for the LogRhythm Platform Manager cryptographic module (hereafter referred to as “Module”). It covers the secure operation of the Module including initialization, roles, and responsibilities for operating the product in a secure, FIPS-compliant manner. This module is validated at Security Level 1 as a multi-chip standalone module. The module relies on the following cryptographic modules for the corresponding LogRhythm versions:

**Table 1 Bounded Modules**

<b>LogRhythm version</b>	<b>Cryptographic Module</b>
7.8.0	Microsoft Windows Server 2019 Cryptographic Primitives Library (bcryptprimitives.dll) (CMVP Certificate #3197)

## 2. Overview

The Module provides cryptographic services to a Platform Manager. In particular, these services support secure communication with supporting SQL Server databases and API Gateways.

A Platform Manager is a server running the LogRhythm Alarming and Response Manager (ARM) service, Job Manager service, and Microsoft SQL Server 2019. Data Processors and AI Engines process log messages and forward significant events to the Platform Manager. The Alarming and Response Manager service processes events using alarm rules and takes appropriate responses, such as sending email to recipients on a notification list. The Job Manager service provides the capability to schedule, run, and deliver report packages. The Platform Manager SQL Server stores log message data (such as events and alarms) as well as configuration data for the entire LogRhythm deployment including Platform Manager. Module runs on a general purpose computer (GPC). The Platform Manager operating system is Windows Server 2019 (x64). The Module was tested on a Dell PowerEdge R740 Server with an Intel Xeon Silver 4114 processor, both with and without PAA (AES-NI acceleration).

The Module is a software module. Its physical boundary is the enclosure of the standalone GPC on which the Platform Manager runs. The software within the logical cryptographic boundary consists of all software assemblies for the Alarming and Response Manager service and for the Job Manager service. The ARM software consists of the following files in “C:\Program Files\LogRhythm\LogRhythm Alarming and Response Manager”:

- clrzmq.dll
- LogRhythm.CrossCutting.dll
- lrsecurity.dll
- nsoftware.IPWorks.dll
- nsoftware.IPWorksSSH.dll
- nsoftware.IPWorksSSNMP.dll
- nsoftware.System.dll
- RestClients.dll
- scarmeng.dll
- scarm.exe
- scarm.hsh
- sccscomn.dll
- scshared.dll
- scvbcomn.dll
- Xceed.Compression.dll
- Xceed.Compression.Formats.dll
- Xceed.FileSystem.dll
- Xceed.GZip.dll
- Xceed.Tar.dll
- Xceed.Zip.dll

The Job Manager software consists of the following files in “C:\Program Files\LogRhythm\LogRhythm Job Manager”:

- Clrzmq.dll
- Google.ProtocolBuffers.dll
- LogRhythm.Business.dll
- LogRhythm.CrossCutting.dll
- LogRhythm.Data.dll
- LogRhythm.DTO.dll
- LogRhythm.Protobuffers.dll
- Lrconfig.exe
- lrjobeng.dll
- lrjobmgr.exe
- lrjobmgr.hsh
- lrsecurity.dll
- Newtonsoft.Json.dll
- nsoftware.IPWorks.dll
- nsoftware.IPWorksSSH.dll
- nsoftware.IPWorksSSNMP.dll
- nsoftware.System.dll
- RestClients.dll
- scscomn.dll
- scrpteng.dll
- scshared.dll
- scvbcomn.dll
- Xceed.Compression.dll
- Xceed.Compression.Formats.dll
- Xceed.FileSystem.dll
- Xceed.GZip.dll
- Xceed.Tar.dll
- Xceed.Zip.dll

Other files and subdirectories of “C:\Program Files\LogRhythm\LogRhythm Alarming and Response Manager” are outside the logical cryptographic boundary. The excluded files are:

- EULA.rtf
- Google.ProtocolBuffers.dll
- Logger.Log4net
- LOGRHYTHM-ARM-MIB.mib
- LOGRHYTHM-MIB.mib
- LOGRHYTHM-TC.mib
- LogRhythm.Business.dll

- LogRhythm.Data.dll
- LogRhythm.DTO.dll
- LogRhythm.Protobuffers.dll
- log4net.dll
- lrarmperf.dll
- Newtonsoft.Json.dll
- scarm.exe.config
- SimpleInjector.dll
- SimpleInjector.Extensions.LifetimeScoping.dll

The excluded directories (along with their subdirectories) are:

- config
- logs
- state

Other files and subdirectories of “C:\Program Files\LogRhythm\LogRhythm Job Manager” are outside the logical cryptographic boundary. The excluded files are:

- EULA.rtf
- Infragistics.Shared.dll
- Infragistics.Win.dll
- Infragistics.Win.Misc.dll
- Infragistics.Win.UltraWinDataSource.dll
- Infragistics.Win.UltraWinEditors.dll
- Infragistics.Win.UltraWinGrid.dll
- Infragistics.Win.UltraWinTabControl.dll
- Infragistics.Win.UltraWinToolbars.dll
- libzmq.dll
- Logger.Log4Net.config
- log4net.dll
- lrconfig.exe.config
- lrconfig.visualelementsmanifest.xml
- lrjobmgr.exe.config
- lrjobsvc.visualelementsmanifest.xml
- sccsuicmn.dll
- SimpleInjector.dll
- SimpleInjector.Extensions.LifetimeScoping.dll

The excluded directories (along with their subdirectories) are:

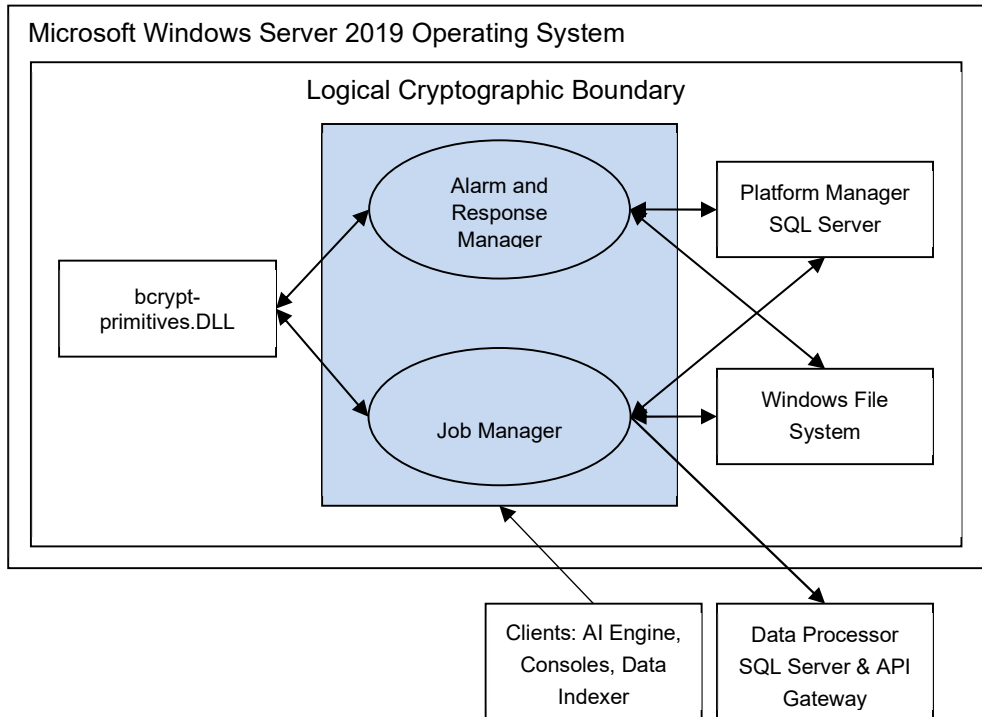
- config
- logs

- state



Figure 1 Cryptographic Module Boundaries illustrates the relationship between the Module and the Platform Manager as a whole. It shows physical and logical cryptographic boundaries of the module.

Physical Boundary (General Purpose Computer)



**Figure 1 Cryptographic Module Boundaries**

## 2.1. Ports and Interfaces

The Module ports consist of one or more network interface cards (NIC) on the Platform Manager GPC. NIC are RJ45 Ethernet adapters, which are connected to IP network(s). The specific ports on the tested platform as well as the mappings to the logical interfaces are as follows:

**Table 2: Physical to Logical Interface Mappings**

Physical Interface	Logical Interface
<b>4 x 10GbE Ethernet Ports</b>	Data Input, Data Output, Control Input, Status Output
<b>1 x Dedicated iDRAC Ethernet Port</b>	N/A – Not used by module
<b>1 x Dedicated iDRAC direct USB Ports</b>	N/A – Not used by module
<b>2 x USB 2.0 Ports</b>	N/A – Not used by module
<b>2 x USB 3.0 Ports</b>	N/A – Not used by module
<b>1 x Serial Port</b>	N/A – Not used by module
<b>1 x VGA Port</b>	N/A – Not used by module

All data enters the Platform Manager Server physically through the NIC and logically through the GPC's network driver interfaces to the module. Hence, the NIC correspond to the data input, data output, control input, and status output interfaces defined in [FIPS 140-2]. Although located on the same GPC as the cryptographic module, the Windows operating system file system and Windows Event Log are outside the logical cryptographic boundary. Hence, the file system and Windows Event Log also present data input, data output, control input, and status output logical interfaces.

Data input to Platform Manager is made up of log message data, which the ARM and Job Manager services retrieve from SQL Server databases over a TLS socket connection. Data output from Platform Manager comprises:

- Alarm data sent to Platform Manager SQL Server,
- Reports sent to the Windows file system and to a NIC, and
- Alarm notifications sent to a NIC.

Platform Manager sends alarm data to the Platform Manager SQL Server using TLS connections. It exports reports as files to the Windows file system and as plain text email messages to a NIC. It sends notifications to a NIC as plain text email messages and SNMP traps. The Console provides a graphical interface to configure the Platform Manager cryptographic module, but configuration information reaches the module indirectly through

the Platform Manager SQL Server. (The Console is a separate and distinct component of a LogRhythm deployment.) The Console connects to a database on Platform Manager SQL Server and stores configurations. The Alarming and Response Manager and Job Manager services retrieve their configuration information from the database. Hence, the TLS connection to the Platform Manager SQL Server serves as the control input interface. The status output interface comprises the TLS connection to the Platform Manager SQL Server, the local file system, and the Windows Event Log. The Alarming and Response Manager and Job Manager services send status information to Platform Manager SQL Server using TLS, which makes it available to the Console. The Platform Manager services write status information to log files in the file system and the Windows Event Log.

## 2.2. Modes of Operation

The Module has two modes of operation: Approved and non-Approved. Approved mode is a FIPS-compliant mode of operation. The module provides the cryptographic functions listed in Table 3 and Table 4 below. While the functions in Table 4 are not FIPS- Approved, they are allowed in Approved mode of operation when used as part of an approved key transport scheme where no security is provided by the algorithm.

**Table 3 FIPS Approved Cryptographic Functions (please see section 6.1 for specific modes used).**

Label	Approved Cryptographic Function	Standard
AES	Advanced Encryption Algorithm	FIPS 197
CVL	Transport Layer Security Key Derivation Function	SP 800-135 Rev. 1
DRBG	Deterministic Random Bit Generator	SP 800-90A Rev. 1
HMAC	Keyed-Hash Message Authentication Code	FIPS 198-1
RSA	Rivest Shamir Adleman Signature Algorithm	FIPS 186-4
SHS	Secure Hash Algorithm	FIPS 180-4
Triple-DES	Triple Data Encryption Algorithm	SP 800-67 Rev. 2

**Table 4 FIPS Non-Approved Cryptographic Functions**

Label	Non-Approved Cryptographic Function
MD5	Message-Digest Algorithm 5
NDRNG	The module depends on the Cryptographic Primitives Library (Cert. #3197) for AES-CTR DRBG Entropy Input. The DRBG is provided at least 256 bits of entropy from the NDRNG
RSA	Key Wrapping using PKCS 1 v1.5

The Module does not implement a bypass capability.

## 2.3. Module Validation Level

The module meets an overall FIPS 140-2 compliance of Security Level 1.

**Table 5 FIPS 140-2 Non-proprietary Security Policy**

### LogRhythm 7.8.0 Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1

<b>Security Requirements Section</b>	<b>Level</b>
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

### **3. Roles**

In Approved mode, Module supports two roles: User and Crypto Officer.

1. User Role: Operators with the User role are other components of a LogRhythm deployment configured to interact with the Platform Manager. These are: Platform Manager SQL Server and Data Processor SQL Server.
2. Crypto Officer Role: Operators with the Crypto Officer role have direct access to the cryptographic module. Responsibilities of the Crypto Officer role include initial configuration, on-demand self test, and status review.

## **4. Services**

In Approved mode, the services available to an operator depend on the operator's role. Roles are assumed implicitly.

### **4.1. User Services**

#### **4.1.1. Data Processor Generate Report**

This service provides a protected communication channel to transfer log data from the Data Processor SQL Server to the Job Manager service in the Platform Manager cryptographic module. The Job Manager formats the data as a report. It writes the report to the Windows file system or a NIC (as a plain text email message). The channel is established in accordance with the Platform Manager configuration using TLS. (See service Write Platform Manager Configuration.) Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

#### **4.1.2. Platform Manager Generate Report**

This service provides a protected communication channel to transfer log data from the Platform Manager SQL Server to the Job Manager service in the Platform Manager cryptographic module. The Job Manager formats the data as a report. It writes the report to the Windows file system or a NIC (as a plain text email message). The channel is established in accordance with the Platform Manager configuration using TLS. (See service Write Platform Manager Configuration.) Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

#### **4.1.3. Platform Manager Generate Alarm**

This service provides a protected communication channel to transfer log data and alarms between the Platform Manager SQL Server to the ARM service in the Platform Manager cryptographic module. The ARM retrieves log data from Platform Manager SQL Server and identifies alarms. It writes alarms to the Platform Manager SQL Server and sends alarm notifications to a NIC (as a plain text email message or SNMP trap). The channel is established in accordance with the Platform Manager configuration using TLS. (See service Write Platform Manager Configuration.) Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

#### **4.1.4. Write Platform Manager Configuration**

This service provides a protected communication channel to transfer configuration data from the Platform Manager SQL Server to the Platform Manager. An operator in the Crypto Officer role sets up communication between the Platform Manager and Platform Manager SQL Server during deployment using TLS. (See service Configure Platform Manager Communication.) After set up, an operator in the User role (that is, the Platform Manager SQL Server) uses this service to propagate configuration changes to the Platform Manager. Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

Note that a Platform Manager's configuration originates from the Console. The Console transfers the configuration information to the Platform Manager SQL Server.

## **4.2. Crypto Officer Services**

### **4.2.1. Configure Platform Manager Communication**

After the Platform Manager has been installed, this service provides an operator in the Crypto Officer role with the capability to configure the Platform Manager to communicate with Platform Manager SQL Server. This consists of setting the IP address for the Platform Manager SQL Server for both the Alarming and Response Manager and Job Manager Windows services. See [Help] section “Update the IP Address of the Platform Manager” The Platform Manager SQL Server provides all other configuration information. (See service Write Data Processor Configuration.)

### **4.2.2. Perform Self-Tests**

Platform Manager module performs a (start-up) power-on software integrity self test to verify the integrity of the component software. If the module fails a software integrity test, it reports status indicating which failure occurred and transitions to an error state, in which the module ceases to continue processing. The Platform Manager will not be able to receive logs and cannot output data to SQL Server database when it is in an error state.

An operator can run the software integrity test on demand by stopping and starting the module. The system integrity test will always run at startup regardless of FIPS Mode.

### **4.2.3. Show FIPS Status**

Platform Manager provides status information about the cryptographic module mode of operation through Platform Manager log files. When the Platform Manager component is started, the Platform Manager Window services write messages to the logs indicating the mode of operation, for example:

```
ARM running in FIPS mode: YES  
Job Manager running in FIPS mode: YES
```

To determine whether Platform Manager is in Approved mode, an operator in the Crypto Officer role checks the ARM and Job Manager service logs, scarm.log and lrjobmgr.log.

Similarly, LogRhythm provides information about communication encryption through Platform Manager log files. When the Platform Manager component is started, the Platform Manager Windows services write messages to the log files indicating whether encryption is being used, for example.

```
ARM using encryption for SQL Server communications: YES  
Job Manager using encryption for SQL Server communications: YES
```

To determine whether Platform Manager is encrypting communication, check the Platform Manager Window services logs, scarm.log and lrjobmgr.log. The Module must be encrypting communications in order to be considered operating in Approved mode.

The Module may enter an error state and stop (for example, when a self test fails). An operator in the Crypto Officer role checks the Platform Manager log files (scarm.log and lrjobmgr.log)



and the Windows Event Log for error messages to determine the cause of the cryptographic module's error state.

## 5. Policies

### 5.1. Security Rules

In order to operate the Module securely, the operator should be aware of the security rules enforced by the module. Operators should adhere to rules required for physical security of the module and for secure operation.

The Module enforces the following security rules when operating in Approved mode (its FIPS compliant mode of operation). These rules include both security rules that result from the security requirements of FIPS 140-2 and security rules that LogRhythm has imposed.

1. Approved mode is supported on Windows Server 2019 (10.0.17763) in a single-user environment.
2. The Module operates in Approved mode only when used with the FIPS approved version of the bounded modules identified in Table 1 operating in FIPS mode.
3. The Module is in Approved mode only when it operates in the environment of BCRYPTPRIMITIVES, namely:
  - i) FIPS approved security functions are used and Windows is booted normally, meaning Debug mode is disabled and Driver Signing enforcement is enabled;
  - ii) One of the following DWORD registry values is set to 1:
    - (1) HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled
    - (2) HKLM\SYSTEM\CurrentControlSet\Policies\Microsoft\Cryptography\Configuration\SelfTestAlgorithms
    - (3) HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy
    - (4) HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\MDEnabled
4. When installed on a system where FIPS is enabled, Platform Manager runs in a FIPS-compliant mode of operation. When communicating with other LogRhythm components, the Platform Manager encrypts communication including:
  - Module to Data Processor SQL Server and
  - Module to Platform Manager SQL Server
5. In accordance with [SP 800-57 P3] and [SP 800-131A] (key length transition recommendations), the size of TLS public/private keys provided for SQL Servers shall be at least 2048 bits.

6. In accordance with [SP 800-57 P3] (key length transition recommendations), the size of public/private keys for the CA issuing SQL Server certificates shall be at least 2048 bits.

## 5.2. Identification and Authentication Policy

The Module does not provide operator authentication. Roles are assumed implicitly. Operating system and SQL Server authentication mechanisms were not within the scope of the validation.

## 5.3. Access Control Policy and SRDIs

This section specifies the LogRhythm Platform Manager's Security Relevant Data Items as well as the access control policy enforced by the LogRhythm.

### 5.3.1. Cryptographic Keys, CSPs, and SRDIs

While operating in a FIPS-compliant manner, the LogRhythm Platform Manager contains the following security relevant data items:

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
<b>Secret and Private Keys</b>						
TLS private key	RSA	2048-bits, 3072-bits	Used for TLS session establishment	External (entered through Windows operating system)	Volatile memory and the operating system	As per guidance for bound module [Win BCRYPT] and Windows operating system guidance
TLS Pre-master Secret	Symmetric	384-bits	Used for TLS Master Secret derivation	Generated internally via DRBG (client), Generated externally (server)	Plaintext in volatile memory	As per guidance for bound module [Win BCRYPT]
TLS Master Secret	Symmetric	384-bits	Used for TLS session key derivation	Derived from Pre-master Secret	Plaintext in volatile memory	As per guidance for bound module [Win BCRYPT]
TLS session encryption keys	AES CBC	128-bits, 256-bits	Used for TLS communication	Generated through TLS handshake via SP 800-135 KDF	Plaintext in volatile memory	As per guidance for bound module [Win BCRYPT]
	Triple-DES CBC	192-bits				
TLS session integrity keys	HMAC-SHA1, SHA-256	160-bits, 256-bits	Used for TLS communication	Generated through TLS handshake via SP 800-135 KDF	Plaintext in volatile memory	As per guidance for bound module [Win BCRYPT]
<b>Public Keys</b>						

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
TLS public key	RSA	2048-bits, 3072-bits	Used for TLS communication with Data Processors and Platform Manager SQL Server	N/A (entered through Windows operating system)	Volatile memory and the operating system	As per guidance for bound module [Win BCrypt] and Windows operating system guidance
CA public key	RSA	2048-bits, 3072-bits	Used for TLS communication with Platform Manager SQL Server and Data Processor SQL server	N/A (entered through Windows operating system)	Volatile memory and the operating system	As per guidance for bound module [Win BCrypt] and Windows operating system guidance
SQL Server public keys	RSA	2048-bits, 3072-bits	Used for TLS communication with Platform Manager SQL Server and Data Processor SQL server	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCrypt]
<b>Other Keys/CSPs</b>						
Power-up integrity test key	HMAC-SHA1	160 bits	Used to verify integrity of cryptographic module image on power up	Preplaced in module by LogRhythm	Obscured in volatile memory	Re-initialize module

### 5.3.2. Access Control Policy

The Platform Manager allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the Platform Manager in a given role performing a specific Module service. The permissions are categorized as a set of four separate permissions: read, write, execute, delete (r, w, x, and d, respectively, in the table). If no permission is listed, then an operator outside the Platform Manager has no access to the SRDI.

LogRhythm Data Processor Server Access Policy  [Key: r: read w: write x: execute d: delete]	Security Relevant Data Item	TLS private key	TLS Pre-master Secret	TLS Master Secret	TLS session encryption keys	TLS session integrity keys	TLS Public Key	CA public key	SQL Server public key	Power-up integrity test key
	Role/Service									
User Role										

LogRhythm Data Processor Server Access Policy	Security Relevant Data Item	TLS private key	TLS Pre-master Secret	TLS Master Secret	TLS session encryption keys	TLS session integrity keys	TLS Public Key	CA public key	SQL Server public key	Power-up integrity test key
[Key: r: read w: write x: execute d: delete]										
Data Processor Generate Report			w,x,d	w,x,d	w,x,d	w,x,d	w,x,d	x	w,x,d	
Platform Manager Generate Report			w,x,d	w,x,d	w,x,d	w,x,d	w,x,d	x	w,x,d	
Platform Manager Generate Alarm			w,x,d	w,x,d	w,x,d	w,x,d	w,x,d	x	w,x,d	
Write Platform Manager Configuration		r,x	w,x,d	w,x,d	w,x,d	w,x,d	w,x,d	x	w,x,d	
<b>Crypto-officer Role</b>										
Configure Platform Manager Communication		w,d						r,w,d		
Perform Self Tests										x
Show FIPS Status										

## 5.4. Physical Security

This section is not applicable.

## 6. Crypto Officer Guidance

### 6.1. Secure Operation Initialization Rules

The LogRhythm software is delivered with the LogRhythm Appliance or standalone as part of the LogRhythm Solution Software (LRSS).

LRSS is the software-only solution for installation and configuration on your own dedicated custom hardware or a supported virtualization platform. Follow the instructions in [Help] section “Install LogRhythm” to install LogRhythm, including Platform Manager. Once Platform Manager is installed, enable Approve mode as described below. See the LogRhythm Solution Software Installation Guide for more details.

The LogRhythm Platform Manager provides the cryptographic functions listed in section Modes of Operation above. The following table identifies the FIPS algorithm certificates for the Approved cryptographic functions along with modes and sizes. Note that while the algorithm certificates list more modes and options than what is contained in the table below, that the algorithms listed in the table are the only ones utilized by the module.

**Table 6 Cryptographic Algorithms**

Algorithm Type	Modes/Mod sizes	Algorithm Cert No.	Usage
BCRYPTPRIMITIVES.DLL Algorithms			
AES	CBC, 128 and 256-bit keys	Cert. #C211	Encryption and Decryption in TLS
CVL <sup>1</sup>	TLS 1.0/1.1 and TLS 1.2 KDF	Cert. #C211	TLS Master Secret and Session Key Derivation
DRBG	SP 800-90A CTR_DRBG (AES-256)	Cert. #C211	Random Number Generation
HMAC	SHA-1, SHA-256	Cert. #C211	Module Integrity and TLS Integrity
SHS	SHA-1/256/384/512	Cert. #C211	Prerequisite for CVL, HMAC, RSA
RSA	ALG [RSASSA-PKCS1_V1_5]: SIG(gen) 2048 and 3072 bits modulus, SHS: SHA-256, SHA-384 and SHA-512	Cert. #C211	Digital Signature Generation and Verification in TLS

---

<sup>1</sup> This protocol has not been reviewed or tested by the CAVP and CMVP

	SIG (ver): 1024, 2048 and 3072 bits modulus, SHS: SHA-1, SHA-256, SHA-384 and SHA-512		
Triple-DES <sup>2</sup>	Triple-DES-CBC, 192-bits	Cert. #C211	Encryption and Decryption in TLS

---

<sup>2</sup> The use of Triple-DES as part of the IETF Protocols TLS 1.0 and TLS 1.2 (RFC 2246 and 5246) limits the use of a single key to no more than 2<sup>20</sup> encryptions.

## **6.2. Approved Mode**

### **6.2.1. Establishing Approved Mode**

Establishing Approved mode entails:

1. Enabling Windows FIPS security policy on the GPC hosting the Platform Manager.
2. Download and install cryptographic hash files for the Platform Manager cryptographic module.
3. Enabling encrypted communication between LogRhythm components.

Enabling Windows FIPS security policy affects other LogRhythm components installed on the same GPC as the Platform Manager. Hence, Windows FIPS security policy should be configured initially for all LogRhythm cryptographic modules in a deployment at the same time. [Help] section “Federal Information Processing Standards (FIPS)” cover the procedures for establishing Windows FIPS security policy across a LogRhythm deployment, including the Platform Manager cryptographic module.

In Approved mode, Alarming and Response Manager and Job Manager must use a consolidated cryptographic hash file to verify the integrity of both applications when the Module starts. The consolidated hash file is available from the LogRhythm Support Site. [Help] section “Federal Information Processing Standards (FIPS)” contains instructions for downloading and installing the consolidated hash file.

Section “When FIPS mode is enabled on a host, all LogRhythm services will connect to SQL Server using Windows Integrated Security regardless of what is configured in their INI files. See [Help] section “Integrated Security” for steps to enable Integrated Security.

TLS Configuration” below describes how to enable encrypted communication. Only those ciphersuites specified in “Appendix A: TLS Cipher Suites” may be used in the approved mode.

When FIPS mode is enabled on a host, all LogRhythm services will connect to SQL Server using Windows Integrated Security regardless of what is configured in their INI files. See [Help] section “Integrated Security” for steps to enable Integrated Security.

### **6.2.2. TLS Configuration**

The cryptographic module supports protected communication between the Platform Manager and other LogRhythm components. Protection is provided by TLS. In particular, the Platform Manager module supports TLS between itself and the following external components:

- Data Processor SQL Server,
- Platform Manager SQL Server, and
- API Gateways (HTTPS)

In Approved mode, TLS communication is required between all components. Enable TLS communication for the Platform Manager cryptographic module:



1. Open the Platform Manager Local Configuration Manager from where the Platform Manager resides by clicking Start > All Programs > LogRhythm > Platform Manager Configuration Manager.
2. Select the Alarming and Response Manager tab and check 'Encrypt all communication.'
3. Select the Job Manager tab and check 'Encrypt all communication.'
4. To restart the Data Processor when the Local Configuration Manager exits, select the Windows Service tab and check 'Start (or restart) the service when the configuration is saved.'
5. Click OK to save the settings and exit.

The TLS communication is not enabled and the module is not in Approved mode until the module is restarted.

### **6.2.3. Starting and Stopping the Cryptographic Module**

The Module runs as two Windows services: *LogRhythm Alarming and Response Server* and *LogRhythm Job Manager*. Starting services *LogRhythm Alarming and Response Server* and *LogRhythm Job Manager* starts the Platform Manager cryptographic module. Similarly, stopping services *LogRhythm Alarming and Response Server* and *LogRhythm Job Manager* stops the cryptographic module. Use the LogRhythm Console, Windows Service Control Manager (SCM), or Windows command line to start or stop the cryptographic module. [Help] section "Start, Stop, and Restart Platform Manager Services" describes Console operation. The Windows commands for starting and stopping the module are 'net start' and 'net stop,' respectively.

## **7. Mitigation of Other Attacks**

This section is not applicable.

## 8. Terminology and Acronyms

Term/Acronym	Description
ARM	Alarm And Response Manager
CSP	Critical Security Parameter
DP	Data Processor
GPC	General Purpose Computer
GUI	Graphical User Interface
PM	Platform Manager
SIEM	Security Information Event Management
SRDI	Security Relevant Data Item
TLS <sup>3</sup>	Transport Layer Security

---

<sup>3</sup> This protocol has not been reviewed or tested by the CAVP and CMVP.

## 9. References

- [FIPS 198-1] *Federal Information Processing Standards Publication: The Keyed-Hash Message Authentication Code (HMAC)*, Information Technology Laboratory National Institute of Standards and Technology, July 2008.
- [FIPS 140-2] *Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules*, Information Technology Laboratory National Institute of Standards and Technology, 25 May 2001.
- [FIPS 140-2 IG] *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, National Institute of Standards and Technology Canadian Centre for Cyber Security, 4 May 2021
- [Help] LogRhythm NextGen SIEM 7.8.0 Documentation, Version 7.8.0.
- [SP 800-57 P3] *NIST Special Publication 800-57 Part 3, Revision 1 Recommendation for Key Management Part 3: Application-Specific Key Management Guidance*, National Institute of Standards and Technology, January 2015
- [SP 800-131A] *NIST Special Publication 800-131A, Revision 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths*, National Institute of Standards and Technology, March 2019
- [Win BCRYPT] *Cryptographic Primitives Library (bcryptprimitives.dll and ncryptssp.dll) in Microsoft Windows 10 Home Edition (32-bit version) Windows 10 Pro Edition (64-bit version) Windows 10 Enterprise Edition (64-bit version) Windows 10 Education Edition (64-bit version) Windows 10 S Edition (64-bit version) Windows 10 Mobile Microsoft Surface Hub Windows Server Standard Core Windows Server Datacenter Core Microsoft Azure Data Box Edge*, Document Version 1.4, 7 May 2020

## Appendix A: TLS Cipher Suites

Below is a list of the supported TLS Cipher Suites:

TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.2, TLS 1.0
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.2, TLS 1.0
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.2, TLS 1.0