FIPS 140-2 Non-proprietary Security Policy

LogRhythm 7.8.0 Data Processor

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

June 29, 2022

Document Version 1.2
Module Version 7.8.0

LogRhythm™
The Security Intelligence Company

Prepared by:

leidos

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

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

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 Data Processor 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

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

2. Overview

The Module provides cryptographic services to a Data Processor. In particular, these services support secure communication with other LogRhythm components (System Monitor Agents, Data Indexers and AI Engine Servers) and SQL Server databases.

A Data Processor is a server running the LogRhythm Mediator Server service and Microsoft SQL Server 2019. The Mediator Server service processes log messages. The Data Processor SQL Server stores log messages as well as metadata the Mediator extracts from logs. Data Processor runs on a general purpose computer (GPC). The Data Processor operating system is Windows Server 2019 (x64). The Data Processor cryptographic 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 Data Processor cryptographic module is a software module. Its physical boundary is the enclosure of the standalone GPC on which the Data Processor runs. The software within the logical cryptographic boundary consists of all software assemblies for the Mediator Server service. The Mediator Server software consists of the following files in "C:\Program Files\ LogRhythm\LogRhythm Data Processor":

- lrgeoip.dll
- lrhmcommgr.dll
- nsoftware.IPWorks.dll
- nsoftware.IPWorksSSH.dll
- nsoftware.IPWorksSSL.dll
- nsoftware.IPWorksSSNMP.dll
- nsoftware.System.dll
- Xceed.Compression.dll
- Xceed.Compression.Formats.dll
- Xceed.FileSystem.dll
- Xceed.GZip.dll
- Xceed.Tar.dll
- sccscomn.dll
- scmedeng.dll
- scmedsvr.exe
- scmedsvr.hsh
- scmessage.dll
- scmpeeng.dll
- scopsec.dll
- scshared.dll
- scvbcomn.dll

Other files and subdirectories of "C:\Program Files\LogRhythm\LogRhythm Data Processor" are outside the logical cryptographic boundary. The excluded files are:

- EULA.rtf

- lrconfig.exe
- lrmedperf.dll
- scmedsvr.exe.config
- sccsuicomn.dll
- Infragistics2.Shared.v9.2.dll
- Infragistics2.Win.Misc.v9.2.dll
- Infragistics2.Win.UltraWinDataSource.v9.2.dll
- Infragistics2.Win.UltraWinEditors.v9.2.dll
- Infragistics2.Win.UltraWinGrid.v9.2.dll
- Infragistics2.Win.UltraWinTabControl.v9.2.dll
- Infragistics2.Win.UltraWinToolbars.v9.2.dll
- Infragistics2.Win.v9.2.dll

The excluded directories (along with their subdirectories) are:

- config
- logs
- state

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

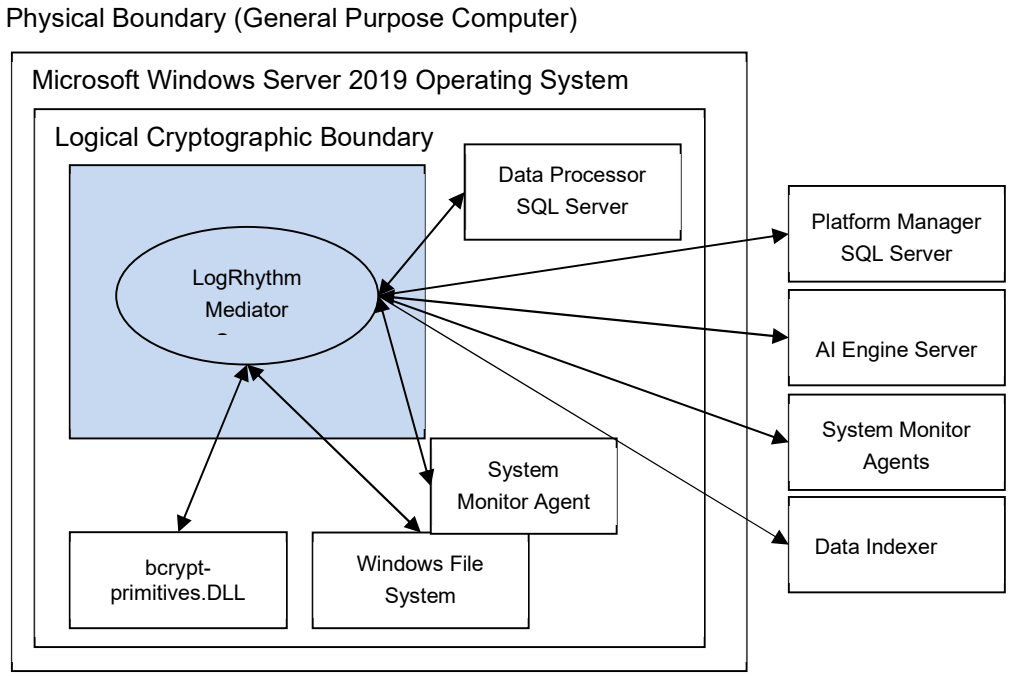

Figure 1 Cryptographic Module Boundaries

2.1. Ports and Interfaces

The Module ports consist of one or more network interface cards (NIC) on the Data Processor 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
4 x 10GbE Ethernet Ports	Data Input, Data Output, Control Input, Status Output
1 x Dedicated iDRAC Ethernet Port	N/A – Not used by module
1 x Dedicated iDRAC direct USB Ports	N/A – Not used by module
2 x USB 2.0 Ports	N/A – Not used by module

2 x USB 3.0 Ports	N/A – Not used by module
1 x Serial Port	N/A – Not used by module
1 x VGA Port	N/A – Not used by module

All data enters the Data Processor Server physically through the NIC and logically through the GPC's network driver interface 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 Data Processor is made up of log messages. System Monitor Agents collect log messages and send them to the Data Processor over a TLS socket connection. Data Processor can archive log data to the Windows file system. Data output from Data Processor comprises log data sent to AI Engine Server and to SQL Servers as well as data written to the local file system. Data Processor sends log data to the AI Engine Server over a TLS socket connection. Data Processor sends raw log data to the Data Processor SQL Server and event data to the Platform Manager SQL Server using TLS connections. Log data output to the local file system consists of archive plain text log data, suspense log files, and unprocessed logs. The Console provides a graphical interface to configure the Data Processor 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 Platform Manager SQL Server and stores configurations in a database. The Mediator service retrieves the 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 Data Processor sends status information to Platform Manager SQL Server using TLS, which makes it available to the Console. The Data Processor writes 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

Label	Approved Cryptographic Function	Standard
AES	Advanced Encryption Algorithm	FIPS 197

Label	Approved Cryptographic Function	Standard
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 LogRhythm Data Processor 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
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. Roles are assumed implicitly, since the module does not provide user authentication.

1. User Role: Operators with the User role are other components of a LogRhythm deployment configured to interact with the Data Processor. These are: System Monitor Agents, AI Engine Server, Data Processor SQL Server, and Platform Manager 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. Agent Write Log Data

This service provides a protected communication channel to transfer log data collected by the System Monitor Agent to a Data Processor. The channel is established in accordance with the Data Processor configuration. (See service Write Data Processor Configuration.) Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

4.1.2. Read Agent Configuration

This service provides a protected communication channel to transfer configuration data from a Data Processor to the System Monitor Agent. The channel is established in accordance with the Data Processor configuration. (See service Write Data Processor Configuration.) Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

4.1.1. AI Engine Server Read Log Data

This service provides a protected communication channel to transfer log data from Data Processor to an AI Engine Server. The channel is established in accordance with the Data Processor configuration set. (See service Write Data Processor 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 Read Log Data

This service provides a protected communication channel to transfer log data from the Data Processor to Platform Manager SQL Server. An operator in the Crypto Officer role sets up communication between the Data Processor and the Platform Manager SQL Server. (See service Configure Data Processor Communication.) The channel is established in accordance with the Data Processor configuration. (See service Write Data Processor Configuration.) Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

4.1.3. Data Processor Read/Write Log Data

The Mediator Server service stores log data and metadata in Data Processor SQL Server databases and Data Indexer Elasticsearch database. This service provides a protected communication channel to transfer log data between the Data Processor and Data Processor SQL Server, and the Data Processor and Elasticsearch server. The channel is established in accordance with the Data Processor configuration. (See service Write Data Processor 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 Data Processor Configuration

This service provides a protected communication channel to transfer configuration information from the Platform Manager SQL Server to the Data Processor. An operator in the Crypto Officer role sets up communication between the Data Processor and the Platform

Manager SQL Server. (See service Configure Data Processor 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 Data Processor. Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

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

4.1.5. Seal Archive File

The Data Processor can archive log data to a file in the file system. In a process called sealing, the Data Processor computes and stores a cryptographic hash of an archive file. Data Processor uses SHA-1 for the cryptographic hash. It stores the hash value in an Platform Manager SQL Server database. The Data Processor performs the Archive Sealing service in accordance with the Data Processor configuration. (See service Write Data Processor Configuration.)

4.2. Crypto Officer Services

4.2.1. Configure Data Processor Communication

After the Data Processor has been installed, this service provides an operator in the Crypto Officer role with the capability to configure the Data Processor to communicate with Platform Manager. This consists of setting the IP address for the Platform Manager. Data Processor authenticates the AI Engine Server for TLS sessions. Optionally, a Crypto Officer may pre-place a user-provided certificate on the Data Processor for mutual authentication of TLS sessions with the AI Engine Server. The Platform Manager SQL Server provides all other configuration information. (See service Write Data Processor Configuration.)

4.2.2. Perform Self-Tests

Data Processor module performs a (start-up) power-on software integrity 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 Data Processor will not be able to receive logs and cannot output data to SQL Server databases 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

Data Processor provides status information about the cryptographic module mode of operation through Data Processor log file. When the Data Processor component is started, the Mediator service writes a message to the log indicating the mode of operation, for example:

Mediator running in FIPS mode: YES

To determine whether Data Processor is in Approved mode, an operator in the Crypto Officer role checks the Mediator Server service log, scmedsvr.log.

Similarly, LogRhythm provides information about communication encryption through Data Processor log files. When the Data Processor component is started, the Mediator service writes a message to the log file indicating whether encryption is being used, for example.

Mediator using encryption for SQL Server communications: YES

To determine whether Data Processor is encrypting communication, check the Mediator Server service log, scmedsvr.log. The Module must be encrypting communication in order to be considered operating in Approved mode.

The Module may enter an error state and stop (for example, when a power-up integrity test fails). An operator in the Crypto Officer role checks the Mediator log file (scmedsvr.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 AI Engine Server cryptographic 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

4. When installed on a system where FIPS is enabled, Data Processor runs in a FIPS-compliant mode of operation. When communicating with other LogRhythm components, the Data Processor encrypts communication including:

   - Module to System Monitor Agent
   - Module to Data Processor SQL Server
   - Module to Platform Manager SQL Server
   - Module to AI Engine Server

5. The Module operates in Approved mode only when using pre-placed, user-provided certificates for TLS communication with the Mediator service. Dynamically-generated, self-signed certificate for the Mediator service shall not be used in Approved mode. See [Help] section "Certificate Configuration for LogRhythm Component Connections" for detailed configuration instructions. [Help] section "Common Access

Card (CAC) Use" covers operational requirements for user-provided certificates (for example, extended key usage values).

6. In accordance with [SP 800-57 P3] and [SP 800-131A] (key length transition recommendations), the size of TLS public/private keys provided for Data Processor, Windows System Monitor Agents, AI Engine Server, and SQL Servers shall be at least 2048 bits.

7. In accordance with [SP 800-57 P3] (key length transition recommendations), the size of public/private keys for the CA issuing Data Processor, Windows System Monitor Agents, AI Engine Server, and SQL Server certificates shall be at least 2048 bits.

8. The module does not support unidirectional System Monitor Agents in Approved mode.

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 Data Processor's Security Relevant Data Items (SRDI) 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 Data Processor contains the following security relevant data items:

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
Secret and Private Keys						
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]
	AES CBC	128-bits, 256-bits	Used for TLS communication			

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
TLS session encryption keys				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]
Public Keys						
TLS public key	RSA	2048-bits, 3072-bits	Used for TLS communication with AI Engine Server, Windows System Monitor Agents, Data Indexer, and SQL Servers	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
Windows System Monitor Agent public keys	RSA	2048-bits, 3072-bits	Used for TLS communication with Windows System Monitor Agents	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCRYPT]
AI Engine Server public key	RSA	2048-bits, 3072-bits	Used for TLS communication with AI Engine Server	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCRYPT]
Data Indexer Public Key	RSA	2048-bits, 3072-bits	Used for TLS communication with Data Indexer	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCRYPT]
CA public key	RSA	2048-bits, 3072-bits	Used for TLS communication with AI Engine Server, Windows System Monitor Agents, and SQL Servers	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 Data Processor SQL Server and Platform Manager SQL Server	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCRYPT]
Other Keys/CSPs						
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 Data Processor 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 Data Processor in a given role performing a specific Data Processor 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 Data Processor 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 public key	Windows System Monitor Agent public keys	AI Engine Server public key	Data Indexer Public Key	CA public key	SQL Server public keys	TLS Pre-master Secret	TLS Master Secret	TLS Session encryption keys	TLS Session Integrity seys	Power-up integrity test key
Role/Service													
User Role													
Agent Write Log Data		x	x	w,x,d			x		w,x,d	w,x,d	w,x,d	w,x,d	
Read Agent Configuration		x	x	w,x,d			x		w,x,d	w,x,d	w,x,d	w,x,d	
AI Engine Server Read Log Data		x	x		w,x,d		x		w,x,d	w,x,d	w,x,d	w,x,d	
Platform Manager Read Log Data		x	x				x	w,x,d	w,x,d	w,x,d	w,x,d	w,x,d	
Data Processor Read/Write Log Data		x	x			w,x,d	x	w,x,d	w,x,d	w,x,d	w,x,d	w,x,d	
Write Data Processor Configuration		x	x				x	w,x,d	w,x,d	w,x,d	w,x,d	w,x,d	
Seal Archive File		x	x				x	w,x,d	w,x,d	w,x,d	w,x,d	w,x,d	
Crypto-officer Role													
Configure Data Processor Communication		r,w,d	r,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 a Data Processor. Once Data Processor is installed, enable Approve mode as described below. See the LogRhythm Solution Software Installation Guide for more details.

The LogRhythm Data Processor 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.
BCRYPTPRIMITIVES.DLL Algorithms		
AES	CBC, 128 and 256-bit keys	Cert. #C211
CVL[1]	TLS 1.0/1.1 and TLS 1.2 KDF	Cert. #C211
DRBG	SP 800-90A CTR_DRBG (AES-256)	Cert. #C211
HMAC	SHA-1, SHA-256	Cert. #C211
SHS	SHA-1/256/384/512	Cert. #C211
RSA	ALG [RSASSA-PKCS1_V1_5]: SIG(gen) 2048 and 3072 bits modulus, SHS: SHA-256, SHA-384 and SHA-512 SIG (ver): 1024, 2048 and 3072 bits modulus, SHS: SHA-1, SHA-256, SHA-384 and SHA-512	Cert. #C211
Triple-DES[2]	Triple-DES-CBC, 192-bits	Cert. #C211

[1] This protocol has not been reviewed or tested by the CAVP and CMVP

[2] 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 2^20 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 Data Processor.
2. Providing public key certificate for the Mediator service to support encrypted communication.
3. Enabling encrypted communication between LogRhythm components.

Enabling Windows FIPS security policy affects other LogRhythm components installed on the same GPC as the Data Processor. 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 Data Processor cryptographic module.

[Help] section "Certificate Configuration for LogRhythm Component Connections" covers providing public key certificates as well as configuring Data Processor to use the certificate.

Section "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 Data Processor and other LogRhythm components. Protection is provided by TLS. In particular, the Data Processor module supports TLS between itself and the following external components:

- System Monitor Agents,
- AI Engine Server,
- Data Indexer API Gateway,
- Data Processor SQL Server, and
- Platform Manager SQL Server.

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

1. Open the Data Processor Local Configuration Manager from where the Data Processor resides by clicking Start > All Programs > LogRhythm > Data Processor Configuration Manager.

2. Select the General tab and check 'Encrypt all communication.'
3. 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.'
4. 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 a Windows service *scmedsvr*. Starting service *scmedsvr* starts the Data Processor cryptographic module. Similarly, stopping service *scmedsvr* 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 Data Processor 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
AIE	Advanced Intelligence Engine
CSP	Critical Security Parameter
EM	Platform Manager
GPC	General Purpose Computer
GUI	Graphical User Interface
LM	Data Processor
Mediator Server service	System Monitor Agents collect logs and send them to a Mediator Server service, which processes the logs
SIEM	Security Information Event Management
SRDI	Security Relevant Data Item
TLS [3]	Transport Layer Security

[3] 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 Transitions: Recommendation for 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 ncryptsslp.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