FIPS 140-2 Non-proprietary Security Policy

LogRhythm 7.8.0 System Monitor Agent

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

July 6, 2022

Document Version 1.2
Module Version 7.8.0

Prepared by:

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 System Monitor Agent 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 System Monitor Agent. In particular, these services support secure communication with a LogRhythm Data Processor component.

A System Monitor Agent is service that collects log data and forwards the data to a Data Processor for processing and analysis. Remote hosts and devices can send logs to an Agent (for example, as syslog messages). An Agent also can collect log data (for example, from Windows Event Logs and SQL Trace files). System Monitor Agent runs on a general purpose computer (GPC). The System Monitor Agent 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 Agent runs. The software within the logical cryptographic boundary consists of all software assemblies for the System Monitor Agent component and cryptographic service provider from the operating system. The System Monitor Agent software consists of the following files in "C:\Program Files (x86)\LogRhythm\LogRhythm System Monitor Agent":

- nsoftware.IPWorksSSNMP.dll
- nsoftware.IPWorksSSL.dll
- sccscomn.dll
- scmessage.dll
- scshared.dll
- scsmeng.dll
- scsm.exe
- scsm.hsh
- scusbmon.dll
- scvbcomn.dll
- lrqualys.dll
- lrnessus.dll
- lrvulncommon.dll
- Xceed.Compression.dll
- Xceed.Compression.Formats.dll
- Xceed.FileSystem.dll
- Xceed.GZip.dll
- Xceed.Tar.dll
- Xceed.Zip.dll
- LRAgentEvents.dll
- LRAgentMFLib.dll
- LRAgentMFInterface.dll
- LRAgentMFInterop.dll
- Microsoft.IdentityModel.Clients.ActiveDirectory.Platform.dll

- Microsoft.IdentityModel.Clients.ActiveDirectory.dll
- lrsourcefire.dll
- lrsecurity.dll
- lrsalesforce.dll
- lrrapid7.dll
- lrokta.dll
- lroffice365.dll
- lrip360.dll
- lreeye.dll
- lrcradlepoint.dll
- lrbox.dll
- lrautormdneng.dll
- lramazonwebservices.dll
- AWSSDK.dll
- Lrcrypt.exe
- Chkptconsole.exe

Other files and subdirectories of "C:\Program Files (x86)\LogRhythm\LogRhythm System Monitor Agent" are outside the logical cryptographic boundary. The excluded files are:

- EULA.rtf
- lrconfig.exe
- lrsmwperf.dll
- scsm.exe.config
- SmartThreadPool.dll
- Newtonsoft.Json
- Logger.Log4net
- log4net.dll
- lrconfig.visualelementsmanifest.xml
- lrcrypt.exe.xml
- scsmwsvc.visualelementsmanifest.xml

The following directories, their subdirectories, and their files in C:\Program Files (x86)\LogRhythm\LogRhythm System Monitor Agent are **Included** in the cryptographic boundary:

- LRAgentMF

The excluded directories (along with their subdirectories) are:

- config
- logs
- state

Figure 1 Cryptographic Module Boundaries illustrates the relationship between the Windows Module and the System Monitor Agent as a whole. It shows physical and logical cryptographic boundaries of the module.

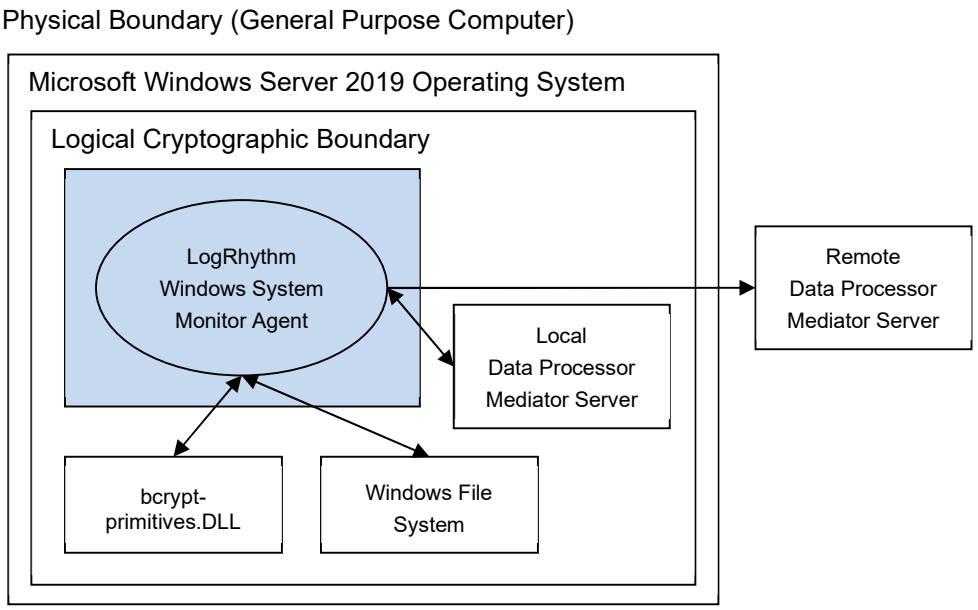

Figure 1 Cryptographic Module Boundaries

2.1. Ports and Interfaces

The Module ports consist of one or more network interface cards (NIC) on the System Monitor Agent 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 System Monitor Agent physically through the NIC and logically through the GPC's network driver interfaces to the module or through the Windows file system. Hence, the NIC and Windows file system 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 System Monitor Agent is made up of log messages. An Agent may pull data, for example, from flat files, Windows Event Logs, and database log message sources. Other log sources such as syslog and Netflow devices send log messages to an Agent. Data output from a System Monitor Agent is the log data it sends to a Data Processor over a TLS socket connection. The Console provides a graphical user interface to configure the System Monitor Agent cryptographic module, but the configuration information reaches the module indirectly. (The Console is a separate and distinct component of a LogRhythm deployment.) The Console connects to Platform Manager SQL Server databases, which propagate configuration information to Data Processor. In turn a Data Processor passes configuration data to its System Monitor Agents as control input. Hence, the TLS connection to the Data Processor serves as the control interface. The status output interface comprises the TLS connection to the Data Processor, the local file system, and the Windows Event Log. A System Monitor Agent sends status information to its Data Processor using TLS, which relays status information to the Platform Manager SQL Server. The Console reads status information from the Platform Manager SQL Server. In addition, the System Monitor Agent 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 (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

Label	Approved Cryptographic Function	Standard
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 System Monitor Agent 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 System Monitor Agent, namely Data Processors. The Data Processor executes the Mediator Server as a Windows service under an account defined by an operator in the Crypto Officer role.

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. Write Log Data

This service supports remote hosts and devices that send logs to a System Monitor Agent. An Agent can accept log messages sent via syslog, Netflow, sFlow, and SNMP.

4.1.2. Collect Log Data

An Agent also can collect log data from local and remote sources. Examples of local sources include files in the Windows file system and the Windows Event Log. Remote sources include:

- Databases (via open database connectivity),
- Check Point devices (via Open Platform for Security Log Export API),
- Cisco intrusion detection system devices (via Security Device Event Exchange), and
- Remote Windows Event Logs (via remote procedure call)
- QualysGuard Security and Compliance suite servers, and
- Nessus vulnerability scanner servers.

This service does not use cryptographic functions of the System Monitor Agent cryptographic module. All log messages are considered plain text messages.

4.1.3. Data Processor Read Log Data

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

LogRhythm displays log data through the Console after the data is processed by Data Processor, Platform Manager, and (optionally) an AI Engine Server.

4.1.4. Write Agent Configuration

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

System Monitor Agent's configuration originates from the Console. The Console transfers the configuration information to the Event Manager SQL Server, which relays the information the Data Processor.

4.2. Crypto Officer Services

4.2.1. Configure Agent Communication

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

4.2.2. Perform Self-Tests

System Monitor Agent 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 System Monitor Agent will not be able to receive logs and cannot output data to a Data Processor when it is in an error state.

An operator in the Crypto Officer role 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

System Monitor Agent provides status information about the cryptographic module mode of operation through System Manager Agent log file. When the System Monitor Agent component is started, the agent service writes a message to the log indicating the mode of operation, for example:

Agent running in FIPS mode: YES

To determine whether a System Monitor Agent is in Approved mode, an operator in the Crypto Officer role checks the agent service log, scsm.log.

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 agent log file (scsm.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\MDMEnabled

4. When installed on a system where FIPS is enabled, System Monitor Agent runs in a FIPS-compliant mode of operation. When communicating with Data Processor, a System Monitor Agent encrypts communication.
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 System Monitor Agent and Data Processor 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 System Monitor Agent and Data Processor certificates shall be at least 2048 bits.

7. The module does not support unidirectional mode in Approved mode.

8. System Monitor Agent supports encrypted communication from log sources: Check Point firewalls, Cisco intrusion detection systems, QualysGuard Security and Compliance suite, and Nessus vulnerability scanners. The cryptography used to support encrypted communication from log sources is not within the scope of the System Monitor Agent cryptographic module. Consequently, encrypted communication from log sources is considered plain text for this validation.

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 System Monitor Agent's Security Relevant Data Items (SRDIs) 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 System Monitor Agent 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]
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]
Public Keys						
TLS public key	RSA	2048-bits, 3072-bits	Used for TLS communication with Data Processor	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
Data Processor public key	RSA	2048-bits, 3072-bits	Used for TLS communication with Data Processor	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 Data Processor	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
Other Keys/CSPs						

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
Power-up integrity test key	HMAC-SHA1	160-bits	Used to verify integrity of cryptographic module image	Preplaced in module by LogRhythm	Obscured in volatile memory	Re-initialize module

5.3.2. Access Control Policy

The System Monitor Agent 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 System Monitor Agent in a given role performing a specific System Monitor Agent 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 System Monitor Agent has no access to the SRDI.

LogRhythm Window System Monitor Agent Access Policy [Key: r: read w: write x: execute d: delete]	Security Relevant Data Item	TLS private key	TLS public key	Data Processor public key	CA public key	TLS Pre-master Secret	TLS Master Secret	TLS session encryption keys	TLS session integrity keys	Power up integrity test key
Role/Service										
User Role										
Write Log Data										
Collect Log Data										
Data Processor Read Log Data		x	x	w,x,d	x	w,x,d	w,x,d	w,x,d	w,x,d	
Write Agent Configuration		x	x	w,x,d	x	w,x,d	w,x,d	w,x,d	w,x,d	
Crypto-officer Role										
Configure Agent 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 "Getting Started with LogRhythm Enterprise" to install LogRhythm, including a System Monitor Agent. Once System Monitor Agent is installed, enable Approve mode as described below. See the LogRhythm Solution Software Installation Guide for more details.

The LogRhythm System Monitor Agent 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

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

Triple-DES[2]	Triple-DES-CBC, 192-bits	Cert. #C211

[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 System Monitor Agent.

Enabling Windows FIPS security policy affects other LogRhythm components installed on the same GPC as the System Monitor Agent. 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 System Monitor Agent cryptographic module.

If the System Monitor Agent service will perform remote event log collection, then it must be configured to use Windows Integrated Security. See [Help] section "Integrated Security" for steps to enable Integrated Security.

Only those ciphersuites specified in "Appendix A: TLS Cipher Suites" may be used in the approved mode.

6.2.2. Starting and Stopping the Cryptographic Module

System Monitor Agent cryptographic module runs as a Windows service named LogRhythm System Monitor Service. Starting the LogRhythm System Monitor Service starts the System Monitor Agent cryptographic module. Similarly, stopping the LogRhythm System Monitor Service 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 "Stop, Start, and Restart Agent Services on Windows" 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
DP	Data Processor
GPC	General Purpose Computer
GUI	Graphical User Interface
Mediator Server service	System Monitor Agents collect logs and send them to a Mediator Server service, which processes the logs
PM	Platform Manager
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 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