FIPS 140-2 Non-proprietary Security Policy

LogRhythm 6.0.4 or 6.3.4 Event Manager

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

April 15, 2016

Document Version 2.1
Module Versions 6.0.4 or 6.3.4

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 System Monitor Agents, Log Managers, Advanced Intelligence (AI) Engine Servers, Event Manager, and Consoles. Each System Monitor Agent collects log data from network sources. Each Log Manager aggregates log data from System Monitor Agents, extracts metadata from the logs, and analyzes content of logs and metadata. A Log Manager may forward log metadata to an AI Engine Server and may forward significant events to Event Manager. An AI Engine Server analyzes log metadata for complex events, which it may forward to Event Manager. Event Manager analyzes events and provides notification and reporting. LogRhythm Console provides a graphical user interface (GUI) to view log messages, events, and alerts. Console also is used to manage LogRhythm deployments. LogRhythm relies on Microsoft SQL Server. LogRhythm stores log data in SQL Server databases on Log Manager and Event Manager. It stores configuration information in SQL Server databases on Event Manager. System Monitor Agent, Log Manager, AI Engine Server, Event Manager, and Console each include a cryptographic module.

This document describes the security policy for the LogRhythm Event Manager cryptographic module. It covers the secure operation of the Event Manager cryptographic 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 Microsoft Windows Server 2008 R2 Cryptographic Primitives Library (bcryptprimitives.dll) (certificate #1336) cryptographic module.

2. Overview

The LogRhythm Event Manager cryptographic module provides cryptographic services to an Event Manager. In particular, these services support secure communication with supporting SQL Server databases.

An Event Manager is a server running the LogRhythm Alarming and Response Manager (ARM) service, Job Manager service, and Microsoft SQL Server 2008 R2. Log Managers and AI Engines process log messages and forward significant events to the Event 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 Event Manager SQL Server stores log message data (such as events and alarms) as well as configuration data for the entire LogRhythm deployment including Event Manager. Event Manager cryptographic module runs on a general purpose computer (GPC). The Event Manager operating system is Windows Server 2008 R2 SP1. The Event Manager cryptographic module was tested on an x64 processor.

The Event Manager cryptographic module is a software module. Its physical boundary is the enclosure of the standalone GPC on which the Event 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":

- 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

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

- lrjobeng.dll
- lrjobmgr.exe
- lrjobmgr.hsh
- nsoftware.IPWorks.dll
- nsoftware.IPWorksSSH.dll
- nsoftware.IPWorksSSNMP.dll

- nsoftware.System.dll
- sccscomn.dll
- scopsec.dll
- scrpteng.dll
- scshared.dll
- scvbcomn.dll
- Xceed.Compression.dll
- Xceed.Compression.Formats.dll
- Xceed.FileSystem.dll
- Xceed.GZip.dll
- Xceed.Tar.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
- LOGRHYTHM-ARM-MIB.mib
- LOGRHYTHM-MIB.mib
- LOGRHYTHM-TC.mib
- lrarmperf.dll
- scarm.exe.config
- lrhmcommgr.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
- 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
- Infragsitics2.Win.UltraWinToolbars.v9.2.dll
- Infragistics2.Win.v9.2.dll
- lrconfig.exe
- lrjobmgr.exe.config
- sccsuicomn.dll

The excluded directories (along with their subdirectories) are:

- config
- css
- html
- images
- js
- logs
- prompting
- state

The Event Manager cryptographic module relies on a cryptographic service provider from the operating system, namely BCRYPTPRIMITIVES.DLL. The cryptographic service provider from the operating system is the following FIPS 140-2 validated cryptographic module:

Microsoft Windows Server 2008 R2 Cryptographic Primitives Library
Certificate #1336

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

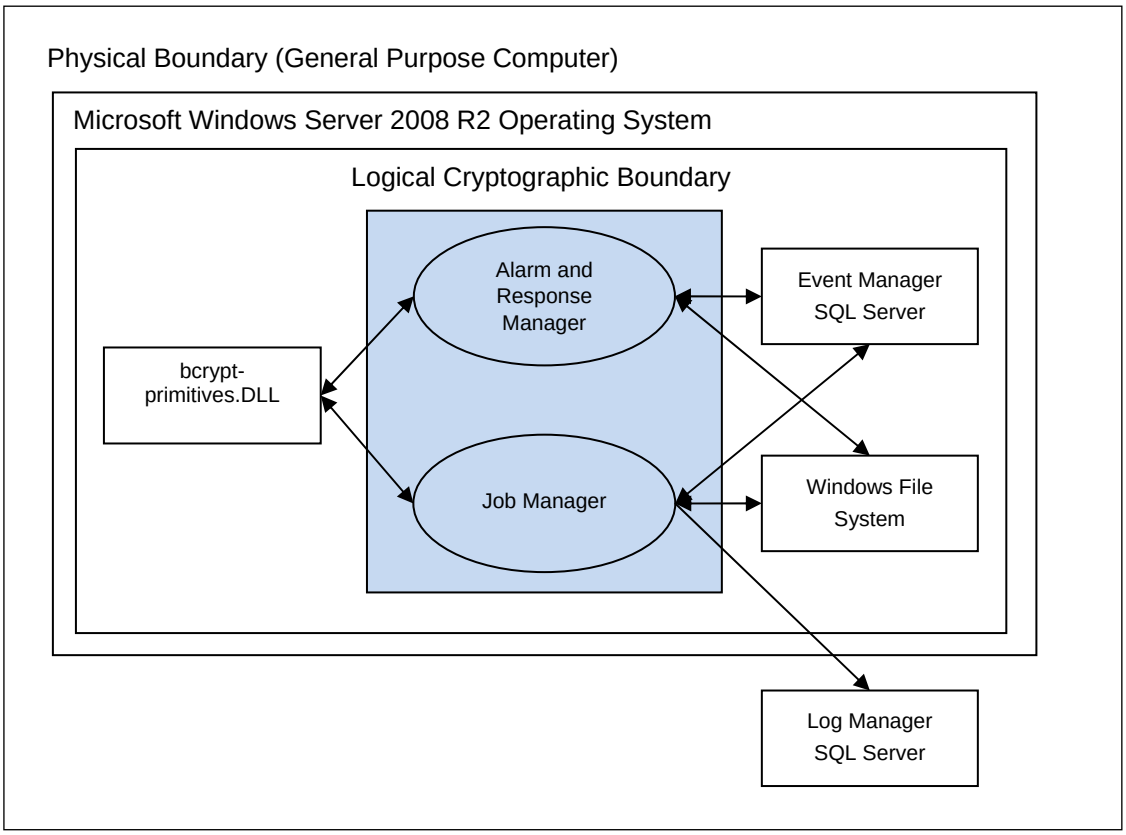

Figure 1 Cryptographic Module Boundaries

2.1. Ports and Interfaces

The Event Manager cryptographic module ports consist of one or more network interface cards (NIC) on the Event Manager GPC. NIC are RJ45 Ethernet adapters, which are connected to IP network(s).

All data enters the Event 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 Event 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 Event Manager comprises:

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

Event Manager sends alarm data to the Event 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 Event Manager cryptographic module, but configuration information reaches the module indirectly through the Event Manager SQL Server. (The Console is a separate and distinct component of a LogRhythm deployment.) The Console connects to a database on Event 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 Event Manager SQL Server serves as the control input interface. The status output interface comprises the TLS connection to the Event 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 Event Manager SQL Server using TLS, which makes it available to the Console. The Event Manager services write status information to log files in the file system and the Windows Event Log.

2.2. Modes of Operation

The Event Manager cryptographic 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 1 and Table 2 below. While the functions in Table 2 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 1 FIPS Approved Cryptographic Functions

Label	Approved Cryptographic Function	Standard
AES	Advanced Encryption Algorithm	FIPS 197
HMAC-SHA-1	Keyed-Hash Message Authentication Code SHA-1	FIPS 198-1
DRBG	Deterministic Random Bit Generator	SP 800-90A
RSA	Rivest Shamir Adleman Signature Algorithm	FIPS 186-2 (PKCS#1 v2.1 and ANSI X9.31-1998)
SHS	Secure Hash Algorithm	FIPS 180-4

Table 2 FIPS Non-Approved Cryptographic Functions

Label	Non-Approved Cryptographic Function
MD5	Message-Digest Algorithm 5
HMAC-MD5	Keyed Hash Message Authentication Code MD5

The Event Manager cryptographic 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 3 FIPS 140-2 Non-proprietary Security Policy

LogRhythm 6.0.4 or 6.3.4 Event Manager 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
Cryptographic Key Management	1
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Operational Environment	1

3. Roles

In Approved mode, Event Manager cryptographic 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 Event Manager. These are: Event Manager SQL Server and Log 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. Log Manager Generate Report

This service provides a protected communication channel to transfer log data from the Log Manager SQL Server to the Job Manager service in the Event 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 Event Manager configuration. (See service Write Event Manager Configuration.) The connection uses TLS 1.0 with cipher suites based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH _AES_128_CBC_SHA).

4.1.2. Event Manager Generate Report

This service provides a protected communication channel to transfer log data from the Event Manager SQL Server to the Job Manager service in the Event 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 Event Manager configuration. (See service Write Event Manager Configuration.) The connection uses TLS 1.0 with cipher suites based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH _AES_128_CBC_SHA).

4.1.3. Event Manager Generate Alarm

This service provides a protected communication channel to transfer log data and alarms between the Event Manager SQL Server to the ARM service in the Event Manager cryptographic module. The ARM retrieves log data from Event Manager SQL Server and identifies alarms. It writes alarms to the Event 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 Event Manager configuration. (See service Write Event Manager Configuration.) The connection uses TLS 1.0 with cipher suites based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH_AES_128_CBC_SHA).

4.1.4. Write Event Manager Configuration

This service provides a protected communication channel to transfer configuration data from the Event Manager SQL Server to the Event Manager. An operator in the Crypto Officer role sets up communication between the Event Manager and Event Manager SQL Server during deployment. (See service Configure Event Manager Communication.) After set up, an operator in the User role (that is, the Event Manager SQL Server) uses this service to propagate configuration changes to the Event Manager. The connection uses TLS 1.0 with cipher suites based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH_AES_128_CBC_SHA).

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

4.2. Crypto Officer Services

4.2.1. Configure Event Manager Communication

After the Event Manager has been installed, this service provides an operator in the Crypto Officer role with the capability to configure the Event Manager to communicate with Event Manager SQL Server. This consists of setting the IP address for the Event Manager SQL Server for both the Alarming and Response Manager and Job Manager Windows services. See [Help] section "Configure the initial connection settings for the Event Manager service." The Event Manager SQL Server provides all other configuration information. (See service Write Log Manager Configuration.)

4.2.2. Perform Self-Tests

Event 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 Event 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

Event Manager provides status information about the cryptographic module mode of operation through Event Manager log files. When the Event Manager component is started, the Event 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 Event 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 Event Manager log files. When the Event Manager component is started, the Event 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 Event Manager is encrypting communication, check the Event Manager Window services logs, scarm.log and lrjobmgr.log. The Event Manager

cryptographic module must be encrypting communications in order to be considered operating in Approved mode.

The Event Manager cryptographic module may enter an error state and stop (for example, when a self test fails). An operator in the Crypto Officer role checks the Event 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 Event Manager cryptographic 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 Event Manager cryptographic 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 Window Server 2008 R2 SP1 in a single-user environment.

2. The Event Manager cryptographic module operates in Approved mode only when used with the FIPS approved version of Microsoft Windows Server 2008 R2 Cryptographic Primitives Library (bcryptprimitives.dll) validated to FIPS 140-2 under certificate #1336 operating in FIPS mode.

3. The Event Manager cryptographic 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, Event Manager runs in a FIPS-compliant mode of operation. When communicating with other LogRhythm components, the Event Manager encrypts communication including:

   - Module to Log Manager SQL Server and
   - Module to Event 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 Event Manager cryptographic 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 Event 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 Event Manager contains the following security relevant data items:

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
Secret and Private Keys						
TLS session encryption keys	AES	128 bits	Used for TLS communication	Generated through TLS handshake	Plaintext in volatile memory	As per guidance for bound module [Win BCRYPT]
TLS session integrity keys	HMAC-SHA1	160 bits	Used for TLS communication	Generated through TLS handshake	Plaintext in volatile memory	As per guidance for bound module [Win BCRYPT]
Public Keys						
CA public key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with Event Manager SQL Server and Log 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
SQL Server public keys	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with Event Manager SQL Server and Log 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 Event 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 Event Manager in a given role performing a specific Event Manager cryptographic 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 Event Manager has no access to the SRDI.

LogRhythm Log Manager Server Access Policy [Key: r: read w: write x: execute d: delete]	Security Relevant Data Item	CA public key	SQL Server public key	TLS session encryption keys	TLS session integrity keys	Power-up integrity test key
Role/Service						
User Role						
Log Manager Generate Report		x	w,x,d	w,x,d	w,x,d	
Event Manager Generate Report		x	w,x,d	w,x,d	w,x,d	
Event Manager Generate Alarm		x	w,x,d	w,x,d	w,x,d	
Write Event Manager Configuration		x	w,x,d	w,x,d	w,x,d	
Crypto-officer Role						
Configure Event Manager Communication		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 "Installing the Components" to install LogRhythm, including Event Manager. Once Event Manager is installed, enable Approve mode as described below. See the LogRhythm Solution Software Installation Guide for more details.

The LogRhythm Event 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.

Algorithm Type	Modes/Mod sizes	Cert No.
BCRYPTPRIMITIVES.DLL Algorithms		
AES	CBC, 128 and 256-bit keys	Cert. #1168
HMAC	SHA-1	Cert. #686
SHS	SHA-1/256/384/512	Cert. #1081
DRBG	SP 800-90A CTR_DRBG (AES-256)	Cert. #23
RSA	FIPS186-2: ALG[ANSIX9.31]: Key(gen), MOD: 2048 , 3072 and 4096 bits modulus	Cert. #559
RSA	ALG [RSASSA-PKCS1_V1_5]: SIG(gen) 2048, 3072 and 4096 bits modulus, SHS: SHA-256, SHA-384 and SHA-512 SIG (ver): 1024 , 1536 , 2048 , 3072 and 4096 bits modulus , SHS: SHA-1, SHA-256, SHA-384 and SHA-512	Cert. #567

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 Event Manager.
2. Download and install cryptographic hash files for the Event 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 Event Manager. Hence, Windows FIPS security policy should be configured initially for all LogRhythm cryptographic modules in a deployment at the same time. [Help] sections "Running FIPS" and "Enabling FIPS Security Policy" cover the procedures for establishing Windows FIPS security policy across a LogRhythm deployment, including the Event 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 Event Manager cryptographic module starts. The consolidated hash file is available from the LogRhythm Support Site. [Help] section "Enabling FIPS Security Policy" 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 "Using Integrated Security 6.0" for steps to enable Integrated Security.

TLS Configuration" below describes how to enable encrypted communication

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 "Using Integrated Security 6.0" for steps to enable Integrated Security.

6.2.2. TLS Configuration

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

- Log Manager SQL Server and
- Event Manager SQL Server.

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

1. Open the Event Manager Local Configuration Manager from where the Event Manager resides by clicking Start > All Programs > LogRhythm > Event 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 Log Manager 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 Event Manager cryptographic 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 Event 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 Event 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
EM	Event Manager
GPC	General Purpose Computer
GUI	Graphical User Interface
LM	Log Manager
SIEM	Security Information Event Management
SRDI	Security Relevant Data Item
TLS [1]	Transport Layer Security

[1] 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 Communications Security Establishment Canada, 11 January 2016.

[Help] LogRhythm Help, Version 6.0.4, March 2012.
LogRhythm Help, Version 6.3.4, February 2015

[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 1*
Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, National Institute of Standards and Technology, November 2015

[Win BCRYPT] *Microsoft Windows Server 2008 R2 Cryptographic Primitives Library (bcryptprimitives.dll) Security Policy Document,* Document Version 2.3, 8 June 2011