

FIPS 140-2 Non-proprietary Security Policy
LogRhythm 6.0.4 or 6.3.4 AI Engine Server

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



© Copyright 2012, 2016 LogRhythm, Inc. All rights reserved.

This document contains proprietary and confidential information of LogRhythm, Inc., which is protected by copyright and possible non-disclosure agreements. The Software described in this Guide is furnished under the End User License Agreement or the applicable Terms and Conditions (“Agreement”) which governs the use of the Software. This Software may be used or copied only in accordance with the Agreement. No part of this Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than what is permitted in the Agreement.

Disclaimer

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

Trademark

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

Table of Contents

1.	Introduction.....	4
2.	Overview.....	5
2.1.	Ports and Interfaces.....	7
2.2.	Modes of Operation.....	8
2.3.	Module Validation Level.....	9
3.	Roles.....	10
4.	Services.....	11
4.1.	User Services.....	11
4.2.	Crypto Officer Services.....	11
5.	Policies.....	13
5.1.	Security Rules.....	13
5.2.	Identification and Authentication Policy.....	14
5.3.	Access Control Policy and SRDIs.....	14
5.4.	Physical Security.....	16
6.	Crypto Officer Guidance.....	17
6.1.	Secure Operation Initialization Rules.....	17
6.2.	Approved Mode.....	18
7.	Mitigation of Other Attacks.....	20
8.	Terminology and Acronyms.....	21
9.	References.....	22

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 AI Engine Server cryptographic module. It covers the secure operation of the AI Engine Server 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 AI Engine Server cryptographic module provides cryptographic services to an AI Engine Server. In particular, these services support secure communication with LogRhythm Log Managers and Event Manager SQL Server databases.

An AI Engine Server is a server running the LogRhythm AI Engine Communication Manager (LRAIEComMgr) and AI Engine (LRAIEEngine) services. The AI Engine Communication Manager service marshals log message data received from Log Managers. The AI Engine service processes the log message data. AI Engine Server cryptographic module runs on a general purpose computer (GPC). The AI Engine Server operating system is Windows Server 2008 R2 SP1. The AI Engine Server cryptographic module was tested on an x64 processor.

The AI Engine Server cryptographic module is a software module. Its physical boundary is the enclosure of the standalone GPC on which the AI Engine Server services run. The software within the logical cryptographic boundary consists of all software assemblies for the AI Engine Communications Manager service and the AI Engine service. The AI Engine Server cryptographic module software consists of the following files in “C:\Program Files\LogRhythm\LogRhythm AI Engine”:

- LRAIEComMgr.exe
- lraiecommgr.hsh
- LRAIEEngine.exe
- lraieengine.hsh
- lrhmcommgr.dll
- lrhmengine.dll
- lrhmenginesvr.dll
- lrhmschema.dll
- nsoftware.IPWorks.dll
- nsoftware.IPWorksSSH.dll
- nsoftware.IPWorksSSL.dll
- nsoftware.IPWorksSSNMP.dll
- nsoftware.System.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 AI Engine” are outside the logical cryptographic boundary. The excluded files are:

- EULA.rtf
- LRAIEComMgr.exe.config
- LRAIEEngine.exe.config
- lrconfig.exe
- lrhmperf.dll
- AIEngine001.lrhmc.cs
- AIEngine001.lrhmc.dll
- DocumentFormat.OpenXml.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
- lrmuicomn.dll
- sccscomn.dll
- sccsuicomn.dll

The excluded directories (along with their subdirectories) are:

- config
- logs
- state

The AI Engine Server cryptographic module relies on a cryptographic service provider (CSP) from the operating system, namely BCRYPTPRIMITIVES.DLL. The CSP 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 AI Engine Server cryptographic module and the AI Engine Server as a whole. It shows physical and logical cryptographic boundaries of the module.

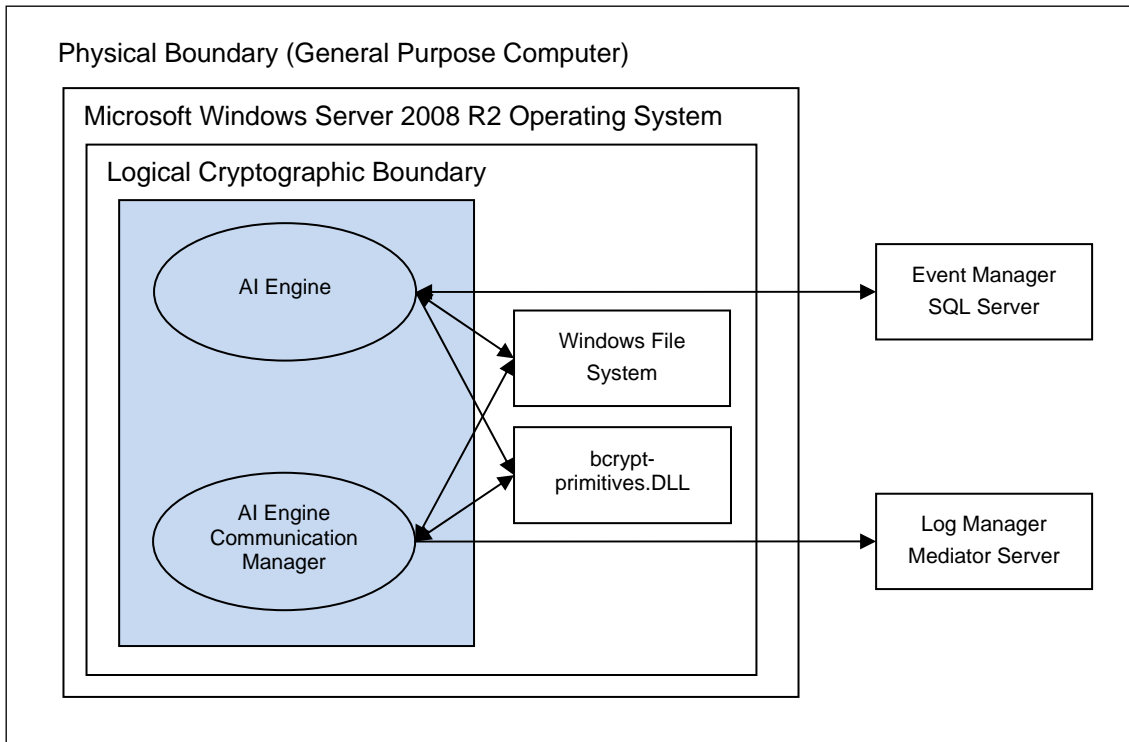


Figure 1 Cryptographic Module Boundaries

2.1. Ports and Interfaces

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

All data enters the AI Engine 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 AI Engine is made up of log message data. Log Manager processes log messages collected by System Monitor Agents and sends log message data to the AI Engine

Communications Manager over a TLS socket connection. Data output from AI Engine Server comprises log message data sent to Event Manager SQL Server as well as data written to the local file system. AI Engine Server sends event data to the Event Manager SQL Server over a TLS socket connection. Data output to the local file system consists of suspense log files and unprocessed logs. The Console provides a graphical interface to configure the AI Engine Server 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 Event Manager SQL Server and stores configurations in a database. The AI Engine service retrieves the 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 AI Engine Server sends status information to Event Manager SQL Server using TLS, which makes it available to the Console. The AI Engine Server writes status information to log files in the file system and the Windows Event Log.

2.2. Modes of Operation

The AI Engine Server 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 AI Engine Server 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 LogRhythm 6.0.4 or 6.3.4 AI Engine Server 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, AI Engine Server cryptographic 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 AI Engine Server. These are: Log Manager and Event 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 Write Log Data

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

This service provides a protected communication channel to transfer log message data to the Event Manager SQL Server from the AI Engine Server. The channel is established in accordance with the AI Engine Server configuration. (See service Write AI Engine Server 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. Write AI Engine Server Configuration

This service provides a protected communication channel to transfer configuration data from the Event Manager SQL Server to the AI Engine Server. An operator in the Crypto Officer role sets up communication between the AI Engine Server and the Event Manager SQL Server during deployment. After set up, the Event Manager SQL Server uses this service to propagate configuration changes to the AI Engine Server. 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 AI Engine Server'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 AI Engine Server Communication

After the AI Engine Server has been installed, this service provides an operator in the Crypto Officer role with the capability to configure the AI Engine Server to communicate with Event Manager. This consists of setting the IP address for the Event Manager. The Event Manager SQL Server provides all other configuration information. (See service Write AI Engine Server Configuration.)

4.2.2. Perform Self-Tests

AI Engine Server module performs a (start-up) power-on software integrity self test to verify the integrity of the module 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 AI Engine Server will not be able to receive logs and cannot output data to an 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

AI Engine Server provides status information about the cryptographic module mode of operation through AI Engine Server log files. When the AI Engine Server component is started, the AI Engine Server processes write messages to the logs indicating the mode of operation, for example:

```
AI Engine Server running in FIPS mode: YES
AI Engine Communication Manager running in FIPS mode: YES
```

To determine whether AI Engine Server is in Approved mode, an operator in the Crypto Officer role checks the AI Engine Server process logs, LRAIEComMgr.log and LRAIEEngine.log.

Similarly, LogRhythm provides information about communication encryption through AI Engine Server log files. When the AI Engine Server component is started, the AI Engine Server processes write messages to the log files indicating whether encryption is being used, for example.

```
AI Engine Server using encryption for SQL Server communications: YES
```

To determine whether AI Engine Server is encrypting communication, check the AI Engine Server service logs, LRAIEComMgr.log and LRAIEEngine.log. The AI Engine Server cryptographic module must be encrypting communications in order to be considered operating in Approved mode.

The Log 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 AI Engine Server log files (LRAIEComMgr.log and LRAIEEngine.log) and the Windows Event Log for error messages to determine the cause the cryptographic module's error state.

5. Policies

5.1. Security Rules

In order to operate the AI Engine Server 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 AI Engine Server 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 AI Engine Server 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 AI Engine Server 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\SelfTestAlgorithms
4. When installed on a system where FIPS is enabled, AI Engine Server runs in a FIPS-compliant mode of operation. When communicating with other LogRhythm components, the AI Engine Server encrypts communication including:
 - Module to Log Manager
 - Module to Event Manager SQL Server
5. The AI Engine Server cryptographic module operates in Approved only when using a pre-placed, user-provided certificate for TLS communication with AI Engine Communication Manager. Dynamically-generated, self-signed certificate for the AI

Engine Communication Manager shall not be used in Approved mode. See [Help] section “Configure LogRhythm to use Specific User Provided TLS Certificates” 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 AI Engine Server, Log Manager, 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 AI Engine Server, Log Manager, and SQL Server certificates shall be at least 2048 bits.

5.2. Identification and Authentication Policy

The AI Engine Server 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 AI Engine Server’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 AI Engine Server 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, 4096-bits	Used for TLS session establishment	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
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						
TLS public key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with Log Managers and Event 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
Log Manager public key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with Log Managers	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCRYPT]
CA public key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with Log Managers and Event 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 key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with Event 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 AI Engine Server cryptographic module 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 AI Engine Server in a given role performing a specific AI Engine Server 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 Log Manager has no access to the SRDI.

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

The LogRhythm AI Engine Server 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 AI Engine Server.
2. Providing public key certificate for the AI Engine Communication Manager to support encrypted communication.
3. Download and install cryptographic hash files for the AI Engine Server cryptographic module.
4. Enabling encrypted communication between LogRhythm components.

Enabling Windows FIPS security policy affects other LogRhythm components installed on the same GPC as the AI Engine Server. 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 AI Engine Server cryptographic module.

[Help] section “Public Key Enabled (PKE)” covers providing public key certificates as well as configuring AI Engine Communication Manager to use the certificate.

In Approved mode, AI Engine Communication Manager and AI Engine must use a consolidated cryptographic hash file to verify the integrity of both applications when the AI Engine Server 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 “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 AI Engine Server and other LogRhythm components. Protection is provided by TLS. In particular, the AI Engine Server module supports TLS between itself and the following external components:

- Log Manager and
- Event Manager SQL Server.

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

1. Open the AI Engine Server Local Configuration Manager from where the AI Engine Server resides by clicking Start > All Programs > LogRhythm > AI Engine Configuration Manager.
2. Select the General tab and check 'Encrypt all communication.'
3. To restart the AI Engine Server 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 AI Engine Server cryptographic module runs as two Windows services: *LRAIEngine* and *LRAIComMgr*. Starting services *LRAIEngine* and *LRAIComMgr* starts the AI Engine Server cryptographic module. Similarly, stopping services *LRAIEngine* and *LRAIComMgr* 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 "Restart AI Engine Servers" 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	Cryptographic Service Provider
EM	Event Manager
GPC	General Purpose Computer
GUI	Graphical User Interface
LM	Log Manager
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 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