FIPS 140-2 Non-proprietary Security Policy

LogRhythm 7.8.0 Console

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 Console 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 Console. In particular, these services support secure communication with SQL Server databases in a LogRhythm deployment.

A Console is a Windows application used to access log data collected and processed by a LogRhythm deployment as well as to configure the deployed components. The Console obtains log data from Data Processor SQL Server. It manages deployed components through the Platform Manager SQL Server. The Module runs on a general purpose computer (GPC). The Console operating system is Microsoft 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 Console runs. The software within the logical cryptographic boundary consists of all software assemblies for the Console application. The Console application software consists of the following files in "C:\Program Files\LogRhythm\LogRhythm Console":

- ChartFX.Designer.dll
- ChartFX.WinForms.Adornments.dll
- ChartFX.WinForms.Annotation.dll
- ChartFX.WinForms.Base.dll
- ChartFX.WinForms.Data.dll
- ChartFX.WinForms.dll
- ChartFX.Wizard.dll
- clrzmq.dll
- Google.ProtocolBuffers.dll
- Infragistics.Shared.dll
- Infragistics.Win.dll
- Infragistics.Win.Misc.dll
- Infragistics.Win.UltraWinDataSource.dll
- Infragistics.Win.UltraWinDock.dll
- Infragistics.Win.UltraWinEditors.dll
- Infragistics.Win.UltraWinExplorerBar.dll
- Infragistics.Win.UltraWinGauge.dll
- Infragistics.Win.UltraWinGrid.dll
- Infragistics.Win.UltraWinListView.dll
- Infragistics.Win.UltraWinMaskedEdit.dll
- Infragistics.Win.UltraWinStatusBar.dll
- Infragistics.Win.UltraWinTabbedMdi.dll
- Infragistics.Win.UltraWinTabControl.dll
- Infragistics.Win.UltraWinToolbars.dll
- Infragistics.Win.UltraWinTree.dll
- libzmq.dll

- log4net.dll
- LogRhythm.Business.dll
- LogRhythm.CrossCutting.dll
- LogRhythm.Data.Components.dll
- LogRhythm.Data.dll
- LogRhythm.Data.Entities.dll
- LogRhythm.Data.Interfaces.dll
- LogRhythm.DTO.dll
- LogRhythm.IdentityInference.dll
- LogRhythm.Presentation.dll
- LogRhythm.Protobuffers.dll
- lrautormdneng.dll
- lrconsole.exe
- lrconsole.hsh
- lrgeoip.dll
- lrhmcommgr.dll
- lrhmschema.dll
- lrhmui.dll
- lrHostWiz.dll
- lrsecurity.dll
- MindFusion.Common.dll
- MindFusion.Diagramming.dll
- MindFusion.Diagramming.WinForms.dll
- MindFusion.Diagramming.WinForms.Overview.dll
- MindFusion.Graphs.dll
- MindFusion.Svg.dll
- Newtonsoft.Json.dll
- nsoftware.IPWorks.dll
- nsoftware.IPWorksSSH.dll
- nsoftware.IPWorksSSL.dll
- nsoftware.IPWorksSSNMP.dll
- nsoftware.System.dll
- RestClients.dll
- scarcstr.dll
- sccscomn.dll
- sccsuicomn.dll
- scmpeeng.dll
- scrpteng.dll
- scshared.dll
- scuicomn.dll
- scvbcomn.dll
- SimpleInjector.dll

- SimpleInjector.Extensions.LifetimeScoping.dll
- Xceed.Compression.dll
- Xceed.Compression.Formats.dll
- Xceed.FileSystem.dll
- Xceed.GZip.dll
- Xceed.Tar.dll
- Xceed.Zip.dll

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

- EULA.rtf
- LogRhythmHelp.chm

The excluded directories (along with their subdirectories) are:

- config
- images2
- logs

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

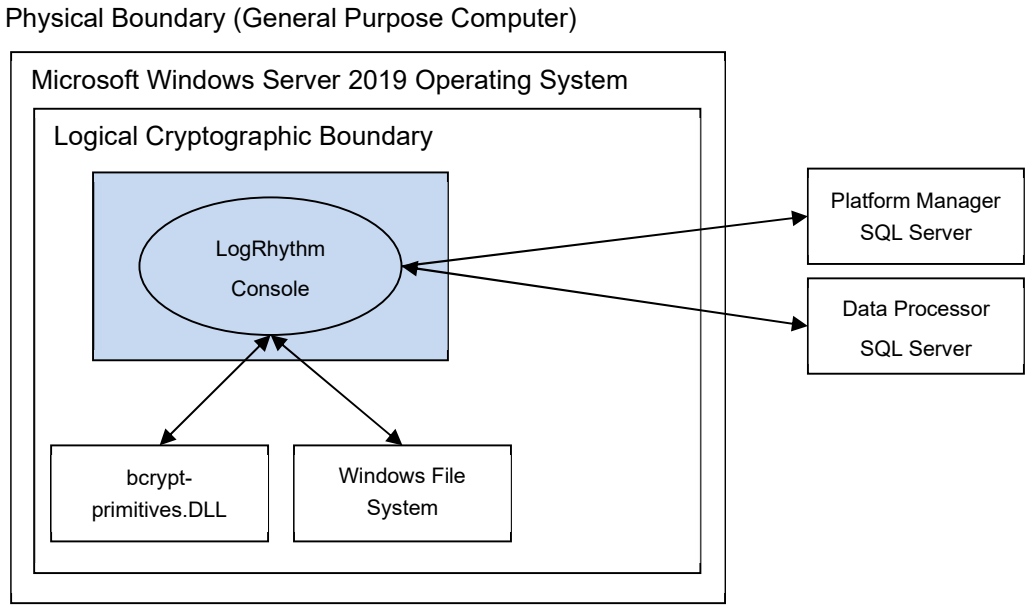

Figure 1 Cryptographic Module Boundaries

2.1. Ports and Interfaces

The Module ports consist of one or more network interface cards (NIC) on the Console GPC, a keyboard, a mouse, and video output. NICs 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 Console application through the NIC, keyboard, and mouse. Data enters physically through the NIC and logically through the GPC's network driver interfaces to the module. All data exits the Console through the NIC and video output. Hence, the NIC, keyboard, mouse, and video 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 Console is made up of log data (such as raw log messages and alarms). The Data Processor SQL Server and Platform Manager SQL Server transfer log data (raw log messages and alarms, respectively) to the Console over TLS socket connections. Console can restore log data that Data Processor has archived in the Windows file system. Data output from the Console comprises log data presented to an operator as well as data written to the local file system (for example, reports). Console presents log data to an operator through the graphical user interface described in [Help]. Console writes reports and state information to files in the local file system. The Console graphical interface also serves as the control interface. At application startup, Console reads preferences and state information from the Windows file system and prompts the operator for session control settings: "Login with Windows account" and "Encrypt all communications." The status output interface comprises the Console "About LogRhythm" dialog box and the Windows Event Log. The Console displays mode and encryption status information in the "About LogRhythm" dialog box. The Console writes status information to the graphical user interface and the Windows Event Log.

2.2. Modes of Operation

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

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

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

Label	Approved Cryptographic Function	Standard
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 Console 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, the Module supports four roles which correspond to the FIPS 140-2 Crypto Officer and User roles. Roles are assumed implicitly, since the module does not provide user authentication.

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.

User Role: Operators with the User role are other components of a LogRhythm deployment configured to interact with the Module. These are: Data Indexer and Platform Manager. The User Role can be further divided into the following LogRhythm Roles

Table 6 LogRhythm User roles

LogRhythm Role	Description
LogRhythmGlobalAdmin	Allows for complete read and write access to both the configuration of the module and the data it collects.
LogRhythmRestrictedAdmin	Allows for read and write access to configuration changes and the data as permitted by LogRhythmGlobalAdmin.
LogRhythmGlobalAnalyst	Allows for read only access to all data and configuration resources.
LogRhythmRestrictedAnalyst	Allows for read only access to data and configuration as permitted by LogRhytmGlobalAdmin.

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. Read/Export Log Data

This service provides an operator with a protected communication channel for reading log data. An operator reads log data from a Data Indexer SQL Server with the Console application. The Console displays log data to the operator and can export the data to the Windows file system as a report. The Module provides the cryptographic functions for a TLS connection between the Console and the SQL Server. Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

4.1.2. Read LogRhythm Configuration

This service provides an operator with a protected communication channel for reading configuration information for each of the LogRhythm components. The Console connects to the Platform Manager SQL Server database using TLS and reads configuration information. Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

4.1.3. Perform Self-Tests

Console 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 Console will not be able to receive input 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.

4.1.4. Show FIPS Status

LogRhythm provides status information about the cryptographic module mode of operation through the Console itself. To determine whether the LogRhythm Console is running in FIPS mode, click Console Help menu item About LogRhythm and view the FIPS mode message.

Similarly, LogRhythm provides information about communication encryption through the Console. To determine whether the LogRhythm Console is encrypting Console communication, click Console Help menu item About LogRhythm and view the encryption message. 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 self test fails). The Console displays an error dialog box when it stops. To determine the cause of a Console failure, an operator checks the Console error dialog box for error messages to determine the cause of the cryptographic module's error state.

4.2. Crypto Officer Services

4.2.1. Read/Export Log Data

An operator in the Crypto Officer role has access to the User role Read/Export Log Data service described above.

4.2.2. Read LogRhythm Configuration

An operator in the Crypto Officer role has access to the User role Read LogRhythm Configuration service described above.

4.2.3. Perform Self-Tests

An operator in the Crypto Officer role has access to the User role Perform Self-Tests service described above.

4.2.4. Show FIPS Status

An operator in the Crypto Officer role has access to the User role Show FIPS Status service described above.

4.2.5. Write LogRhythm Configuration

This service provides an operator in the Crypto Officer role with a protected communication channel for writing configuration information for each of the LogRhythm components. The Console connects to the Platform Manager SQL Server database using TLS and writes configuration information. Please see Appendix A for the list of supported cipher suites used in the TLS 1.0/1.2 connections.

4.2.6. Verify Archive File Seal

An operator in the Crypto Officer role can restore a previously archived log data from a file. Archive files reside on the Data Processor and are restored to a Data Processor SQL Server database. This service provides the capability to validate the integrity of an archive file. Console uses SHA-1 for the cryptographic hash. It recalls the original hash value from the Platform Manager SQL database.

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 Window 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 communicating with other LogRhythm components in Approved mode, the Console encrypts communication including:

   - Module to Data Processor SQL Server and

   - Module to Platform Manager SQL Server.

5. In accordance with [SP 800-57 P3] and [SP 800-131A] (key length transition recommendations), the size of TLS public/private keys provided for SQL Servers shall be at least 2048 bits.

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

5.2. Identification and Authentication Policy

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

5.3. Access Control Policy and SRDIs

This section specifies the LogRhythm Console'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 Console contains the following security relevant data items:

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
Secret and Private Keys						
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 Processors and Platform Manager SQL Server	N/A (entered through Windows operating system)	Volatile memory and the operating system	As per guidance for bound module [Win BCRYPT] and Windows operating system guidance

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
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]
Platform Manager 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 Data Processor SQL Server and Platform Manager SQL Server	N/A (entered through Windows operating system)	Volatile memory and the operating system	As per guidance for bound module [Win BCRYPT] and Windows operating system guidance
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 Console 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 Console in a given role performing a specific Console 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 Pre-master Secret	TLS Master Secret	TLS session encryption keys	TLS session integrity keys	TLS public key	Data Indexer public key	Platform Manager public key	CA public key	SQL Server public keys	Power-up integrity test key
Role/Service											
User Role											
Read/Export Log Data		w,x,d	w,x,d	w,x,d	w,x,d	r	r	r	x	w,x,d	

LogRhythm Data Processor Server Access Policy [Key: r: read w: write x: execute d: delete]	Security Relevant Data Item	TLS Pre-master Secret	TLS Master Secret	TLS session encryption keys	TLS session integrity keys	TLS public key	Data Indexer public key	Platform Manager public key	CA public key	SQL Server public keys	Power-up integrity test key
Read LogRhythm Configuration		w,x,d	w,x,d	w,x,d	w,x,d	r	r	r	x	w,x,d	
Perform Self Tests											x
Show FIPS Status											
Crypto-officer Role											
Read/Export Log Data		w,x,d	w,x,d	w,x,d	w,x,d	r	r	r	x	w,x,d	
Read LogRhythm Configuration		w,x,d	w,x,d	w,x,d	w,x,d	r	r	r	x	w,x,d	
Perform Self Tests											x
Show FIPS Status											
Write LogRhythm Configuration		w,x,d	w,x,d	w,x,d	w,x,d	r	r	r	x	w,x,d	
Verify Archive Seal		w,x,d	w,x,d	w,x,d	w,x,d	r	r	r	x	w,x,d	

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 Console. Once Console is installed, enable Approve mode as described below. See the LogRhythm Solution Software Installation Guide for more details.

The LogRhythm Console 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.

Algorithm Type	Modes/Mod sizes	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	Triple-DES-CBC, 192-bits	Cert. #C211

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

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 Console,
2. Using a Windows account to login to Console, and
3. Enabling encrypted communication between LogRhythm components.

Enabling Windows FIPS security policy affects other LogRhythm components installed on the same GPC as the Console. Hence, Approved mode 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 Approved mode across a LogRhythm deployment, including the Module.

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

See section "Starting and Stopping the Cryptographic Module" below for instructions for using a Windows account to login to Console and for encrypting all Console communication.

6.2.2. Starting and Stopping the Cryptographic Module

The Console is a Windows application. To start the Console:

1. Go to Start > All Programs > LogRhythm > LogRhythm Console.

The LogRhythm log in window is displayed.

2. Select 'Login with Windows account'
3. Select 'Encrypt all communications'
4. Complete other local options as described in [Help] section "Log in to the Client Console"
5. Click OK.

The Console application starts.

See [Help] section "Client Console Administrator Guide" for additional instructions for the first time Console starts.

To stop the Console, select File menu option Exit.

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
PM	Platform Manager
SIEM	Security Information Event Management
SRDI	Security Relevant Data Item
TLS [2]	Transport Layer Security

[2] 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