FIPS 140-2 Non-proprietary Security Policy

LogRhythm 6.0.4 or 6.3.4 Windows System Monitor Agent

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 Windows System Monitor Agent cryptographic module. It covers the secure operation of the System Monitor Agent 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 Windows System Monitor Agent cryptographic module provides cryptographic services to a Windows System Monitor Agent. In particular, these services support secure communication with a LogRhythm Log Manager component.

A Windows System Monitor Agent is service that collects log data and forwards the data to a Log Manager 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 2008 R2 SP1. The System Monitor Agent cryptographic module was tested on an x64 processor.

The Windows System Monitor Agent cryptographic 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
- sccscomn.dll
- scmessage.dll
- scopsec.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

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
- AppUtils.dll
- ckpssl.dll
- ComUtils.dll
- cpbcrypt.dll
- cpca.dll
- cpcert.dll
- cpcryptutil.dll
- CPMIBase501.dll
- CPMIClient501.dll
- CPMIClient501.lib
- cpopenssl.dll
- cp_policy.dll
- cpprng.dll
- cpprod50.dll
- cpsic.dll
- CPSrvIS.dll
- CPSrvIS.lib
- CP_version_info.dll
- DataStruct.dll
- Encode.dll
- EventUtils.dll
- fwadb.dll
- fwsetdb.dll
- fwsmtpobj.dll
- logfilter.dll
- lrcrypt.exe
- mastersapi.dll
- messaging.dll
- ndb.dll
- objlibclient.dll

- objlib.dll
- opsec.dll
- opsecext.dll
- opsecext.lib
- opsec.lib
- OS.dll
- reg.dll
- Resolve.dll
- sccsuicomn.dll
- sicauth.dll
- sic.dll
- sicobj.dll
- skey.dll

The excluded directories (along with their subdirectories) are:

- config
- logs
- state

The Windows System Monitor Agent 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 Windows System Monitor Agent cryptographic module and the System Monitor Agent as a whole. It shows physical and logical cryptographic boundaries of the module.

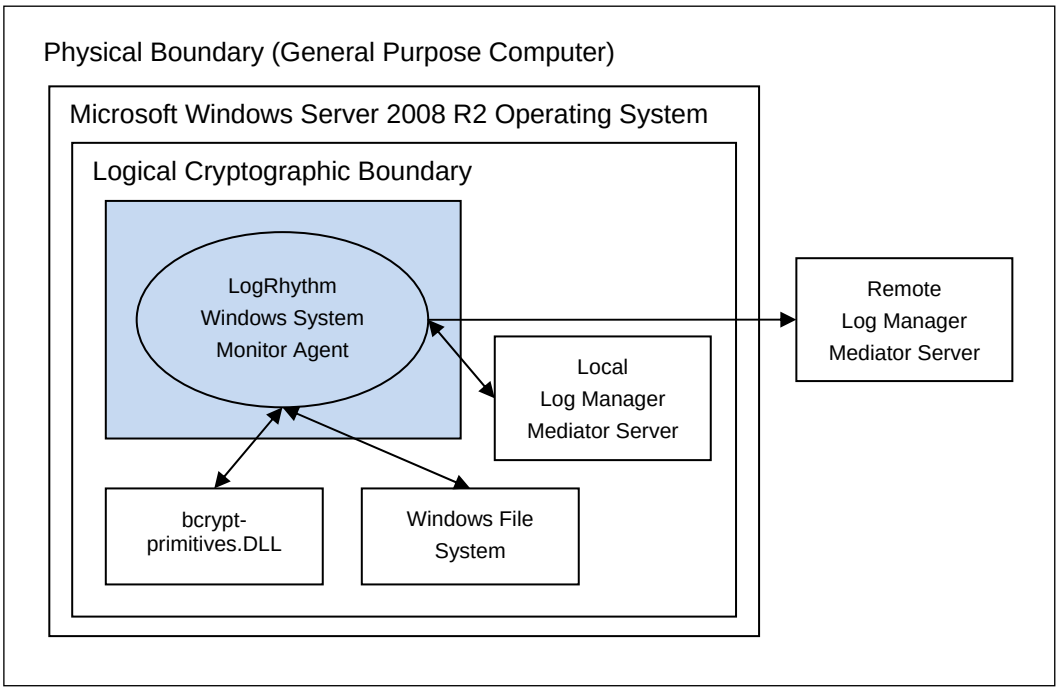

Figure 1 Cryptographic Module Boundaries

2.1. Ports and Interfaces

The Windows System Monitor Agent cryptographic 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).

All data enters the Windows 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 Log Manager over a TLS socket connection. The Console provides a graphical user interface to configure the Windows 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 Event Manager SQL Server databases, which propagate configuration information to Log Manager. In turn a Log Manager passes configuration data to its Windows System Monitor Agents as control input. Hence, the TLS connection to the Log Manager serves as the control interface. The status output interface comprises the TLS connection to the Log Manager, the local file system, and the Windows Event Log. A System Monitor Agent sends status information to its Log Manager using TLS, which relays status information to the Event Manager SQL Server. The Console reads status information from the Event Manager SQL Server. In addition, the Windows System Monitor Agent writes status information to log files in the file system and the Windows Event Log.

2.2. Modes of Operation

The Windows System Monitor Agent 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 Windows System Monitor Agent 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 Windows 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
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, Windows System Monitor Agent 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 Windows System Monitor Agent, namely Log Managers. The Log Manager 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 Windows 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 Windows System Monitor Agent cryptographic module. All log messages are considered plain text messages.

4.1.3. Log Manager Read Log Data

This service provides a protected communication channel to transfer log data collected by the System Monitor Agent to a Log Manager. An operator in the Crypto Officer role sets up communication between the System Monitor Agent and the Log Manager. (See service Configure Agent Communication.) The channel is established in accordance with the System Monitor Agent configuration (See service Write Agent Configuration). The connection uses TLS 1.0 with cipher suite 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).

LogRhythm displays log data through the Console after the data is processed by Log Manager, Event 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 Log Manager to the System Monitor Agent. An operator in the Crypto Officer role sets up communication between the System Monitor Agent and the Log Manager. (See service Configure Agent Communication.) After set up, an operator in the User role (that is, the Log Manager) uses this service to write configuration changes to the System Monitor Agent. The connection uses TLS 1.0 with cipher suite 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).

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 Log Manager.

4.2. Crypto Officer Services

4.2.1. Configure Agent Communication

After the Windows 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 Log Manager. This consists of setting the IP address for the Log Manager. System Monitor Agent authenticates the Log Manager 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 Log Manager 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 Log Manager 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 System Monitor Agent 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 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 Windows System Monitor Agent 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 Windows System Monitor Agent 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 Windows System Monitor Agent 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 Windows System Monitor Agent 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, Windows System Monitor Agent runs in a FIPS-compliant mode of operation. When communicating with Log Manager, 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 Windows System Monitor Agent and Log Manager 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 Windows System Monitor Agent and Log Manager certificates shall be at least 2048 bits.

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

8. Windows 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 Windows 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 Windows System Monitor Agent 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 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, 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 Manager	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 Manager	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 Manager	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						
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 Windows 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	Log Manager public key	CA public key	TLS session encryption keys	TLS session integrity keys	Power up integrity test key
Role/Service								
User Role								
Write Log Data								
Collect Log Data								
Log Manager Read Log Data		x	x	w,x,d	x	w,x,d	w,x,d	
Write Agent Configuration		x	x	w,x,d	x	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 "Installing the Components" to install LogRhythm, including a Windows 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 Windows 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.

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 Windows System Monitor Agent.

Enabling Windows FIPS security policy affects other LogRhythm components installed on the same GPC as the Windows 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] sections "Running FIPS" and "Enabling FIPS Security Policy" cover the procedures for establishing Windows FIPS security policy across a LogRhythm deployment, including the Windows 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 "Using Integrated Security 6.0" for steps to enable Integrated Security.

6.2.2. Starting and Stopping the Cryptographic Module

Windows System Monitor Agent cryptographic module runs as a Windows service named LogRhythm System Monitor Service. Starting the LogRhythm System Monitor Service starts the Windows 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 "Starting, Stopping, Restarting, Pausing, and Resuming Agent Services" describes Console operation. The Windows commands for starting and stopping the module are 'net start' and 'net stop,' respectively.

7. Mitigation of Other Attacks

This section is not applicable.

8. Terminology and Acronyms

Term/Acronym	Description
AIE	Advanced Intelligence Engine
CSP	Critical Security Parameter
EM	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