Hewlett Packard Enterprise

Operations Manager i

FIPS 140-2 Compliance Statement

Software version: 10.11

Document release date: August 2016

Software release date: May 2016

Contents

Summary **2**

Overview **2**

About Operations Manager i 2

Operations Agent 2

Data Flow Probe 2

About FIPS 140-2 2

FIPS 140-2 Compliant Modules and Technologies 3

OMi and FIPS 140-2 .... **4**

FIPS 140-2 Architecture 4

Acronyms **6**

References **6**

Send documentation feedback **7**

Legal notices **7**

Summary

HPE Operations Manager i complies with Federal Information Processing Standard 140-2 (FIPS 140-2), which defines the technical requirements to be used by Federal Agencies when these organizations specify cryptographic-based security systems for protection of sensitive or valuable data. The compliance of OMi with FIPS 140-2 is ensured by:

1) Integrating validated and NIST-certified third party cryptographic module(s), and using the module(s) as the only provider(s) of cryptographic services;
2) Using FIPS-approved cryptographic functions;
3) Using FIPS-approved and NIST-validated technologies;
4) Using security controls defined in NIST 800-53 (or applicable security controls such as DoD 8500.2), prescribed for cryptographic modules by FIPS 140-2 and applicable for HPE Operations Manager i design, implementation and operation.

Overview

This section describes the different elements that make up the OMi solution.

About Operations Manager i

Operations Manager i is a simplified, unified, IT operations management software. OMi provides automated monitoring, fast root cause identification and prioritization, with automated remedial action.

Operations Agent

The HPE Operations Agent helps you to monitor a system by collecting metrics that indicate the health, performance, availability, and resource utilization of essential elements of the system. When you use the Operations Agent in conjunction with OMi, you can add the capability to monitor business applications, infrastructure, as well as application workloads running on the monitored systems.

Data Flow Probe

The Data Flow Probe is the component responsible for requesting tasks from the server, scheduling and executing discovery and integration tasks, and sending the results back to the OMi server.

For details about how OMi, the Operations Agent, and the Data Flow Probe implement FIPS 140-2 requirements, see the *OMi FIPS Configuration Guide*.

About FIPS 140-2

The Federal Information Processing Standards Publication (FIPS) 140-2, “Security Requirements for Cryptographic Modules,” was issued by the National Institute of Standards and Technology (NIST) in May, 2001. The FIPS 140-2 standard specifies the security requirements for cryptographic modules used within a security system that protects sensitive or valuable data. The requirements can be found in the following documents:

- SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

  http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

- Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules

  http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

Note: In this document, the abbreviation “FIPS” means “FIPS 140-2.”

FIPS 140-2 Compliant Modules and Technologies

The benefit of using FIPS 140-2 compliant crypto modules is that the FIPS-approved crypto algorithms are deemed appropriate and that they perform the encrypt, decrypt, and hash functions correctly and in a FIPS-compliant manner.

Modes of Operation

OMi and its components can be configured and operated in the following two modes:

- FIPS-compliant mode: This mode supports FIPS 140-2 compliant cryptographic functions.
- Standard mode: This is a non-FIPS 140-2 compliant mode that uses existing or available cryptography without third-party FIPS-compliant 140-2 crypto modules.

FIPS 140-2 Compliant Third Party Modules

The Apache web server component and the HPE Shared Components are integrated with the third-party FIPS 140-2 compliant cryptographic module *OpenSSL FIPS Object Module v2.0.12.* When they are configured to operate in FIPS-compliant mode, its functions and procedures (such as SSL/TLS connections and encryption of stored sensitive data, which require cryptography such as secure hash, encryption, digital signature, and so on) use the cryptography services provided by the OpenSSL FIPS Object Module configured to run in FIPS mode.

All other OMi components are integrated with the third-party FIPS 140-2 compliant cryptographic module *RSA BSAFE Crypto-J version 6.2.1* When OMi is configured to operate in FIPS-compliant mode, its functions and procedures (such as SSL/TLS connections and encryption of stored sensitive data, which require cryptography such as secure hash, encryption, digital signature, and so on) use the cryptography services provided by RSA BSAFE Crypto-J configured to run in FIPS mode.

Details about how to configure OMi and its components to conform to FIPS 140-2 appear in *OMi FIPS Configuration Guide*.

TLS

All the OMi components communications are secured with FIPS-compliant Transport Layer Security TLS1.0 or higher. It is relying on FIPS 140-2 approved hash algorithms and symmetric and asymmetric ciphers.

- TLS handshake, key negotiation, and authentication provide data integrity and make use of secure hash, asymmetric key cryptography and digital signature
- TLS encryption of data in transit provides confidentiality and makes use of symmetric cryptography

Secure Hash

Per FIPS 140-2 standards, OMi, in the FIPS compliant mode, uses the following secure hash algorithm:

SHA-256

Symmetric Cryptography

Per FIPS 140-2 standards, OMi, in the FIPS 140-2 compliant mode, uses the following symmetric key algorithm:

AES (ECB, CBC) [256 bit key size]

Message Digest

Per FIPS 140-2 standards, OMi, in the FIPS compliant mode uses the following digital signature hash algorithm:

SHA-256

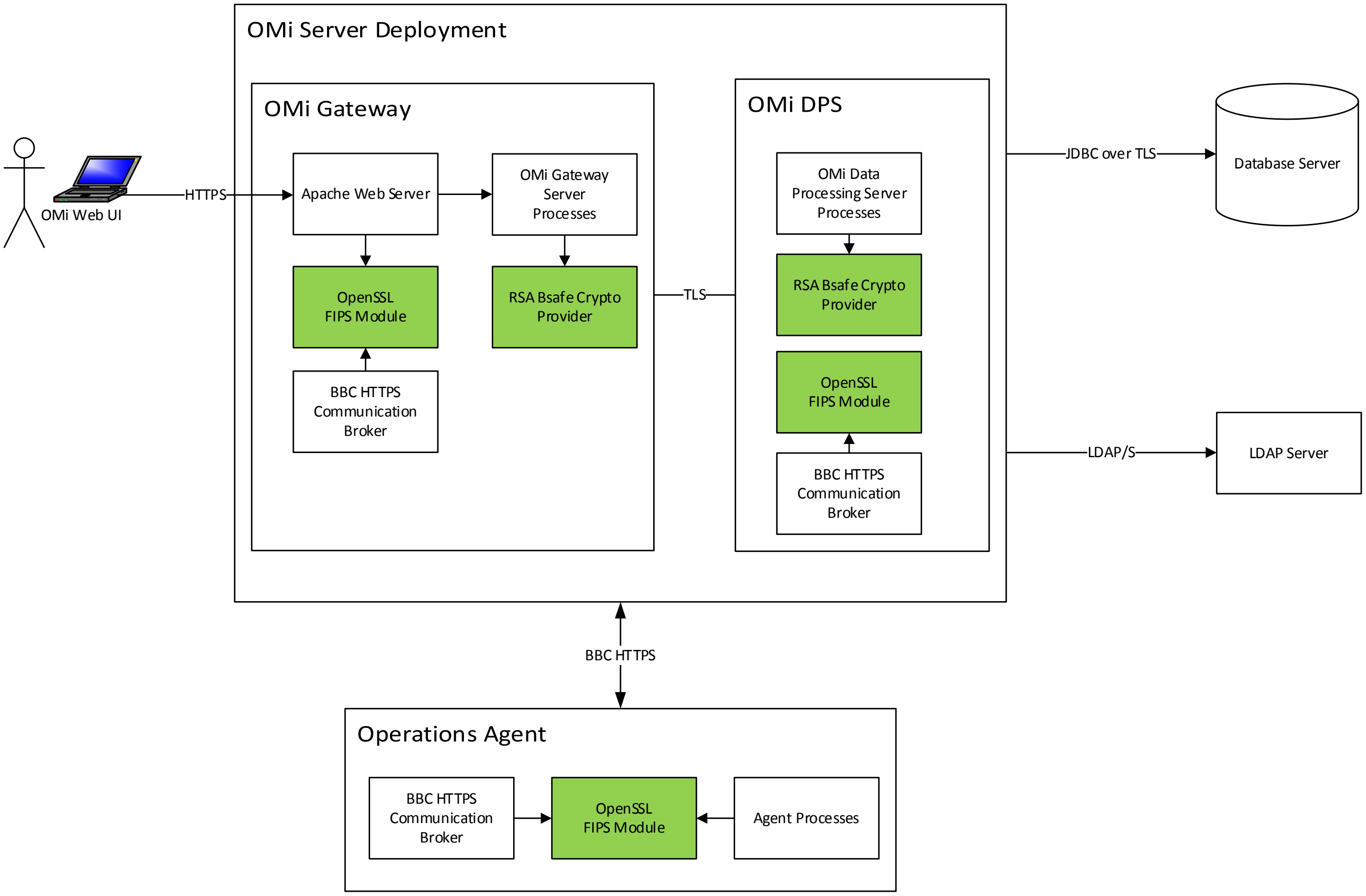
OMi and FIPS 140-2

In addition to the automated process of installing and configuring OMi in FIPS mode using the configuration wizard, you also need to manually configure the client for FIPS mode. This includes manually installing the RSA BSAFE Crypto J module on the client system.

For instructions on both manual and automated steps required to set up OMi in FIPS mode, see the *OMi FIPS Configuration Guide*.

FIPS 140-2 Architecture

All OMi instances in an OMi deployment must be run in FIPS-compliant mode. OMi does not support a deployment architecture that contains a mix of OMi instances that run in FIPS and non-FIPS mode.



Supported Platforms

See the *HPE Software Product Support Matrix* for more information.

Supported Modes and cryptography

- FIPS mode – supports FIPS 140-2. In this mode, only FIPS compliant cryptographic functions, default algorithms, and key lengths are used.
- Standard mode – non-FIPS 140-2 compliant mode, with standard existing or available cryptography without third party FIPS 140-2 crypto modules.

Design Assurance

OMi automatically uses FIPS-compliant cryptographic methods for the following:

- HTTPS communication (if configured) between clients and the OMi web server or load balancer
- HTTPS communication (if configured) between RTSM clients and RTSM
- HTTPS communication between HPE Operations Agents or Operations Connectors (OpsCx) and OMi (HTTPS required by default)
- LDAP/S communication between OMi and LDAP server
- Java keystore and Java Runtime Environment
- Policy signing
- JDBC over TLS connection with the Database server

Key Management

Many aspects of key management, such as random number and key generation, are provided by functions of RSA BSAFE Crypto-J crypto module, and thus meet FIPS 140-2 compliance requirements. The application-specific key management functions include

- Key storage, key protection, and key access functions meet FIPS 140-2 compliance requirements and use the RSA BSAFE Crypto-J module.
- Keys are generated, changed and transported in a protected manner. Keys are not available in open or stored unprotected.

Acronyms

AES
Advanced Encryption Standard.

HMAC DRBG
Keyed-hash message authentication code deterministic random bit generator, which is a random number generation algorithm.

FIPS
Federal Information Processing Standard.

IdM
Identity Management component.

JVM
Java Virtual Machine.

OMi
Operations Manager i

PKCS 12
Personal Information Exchange Syntax Standard #12.

REST
Representational State Transfer.

RSA
An algorithm for public-key cryptography. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman.

SSL
Secure Sockets Layer, which is the standard security technology for establishing an encrypted link between a web server and a browser.

TLS
Transport Security Layer.

References

OMi FIPS Configuration Guide

HPE Software Product Support Matrix

Send documentation feedback

If you have comments about this document, you can send them to ovdoc-asm@hpe.com.

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor’s standard commercial license.

Copyright notice

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation’s permission.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: https://softwaresupport.hpe.com.

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hpe.com.