Hewlett Packard
Enterprise

IT Business Analytics

Software Version: 10.10

Linux operating system

FIPS 140-2 Compliance Statement

Document Release Date: February 2016

Software Release Date: February 2016

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.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

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: https://softwaresupport.hp.com/.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport logon page.

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

Support

Visit the HP Software Support site at: https://softwaresupport.hpe.com.

This website provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport logon page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HP Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this website is http://h20230.www2.hp.com/sc/solutions/index.jsp.

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

FIPS 140-2 Compliance Statement

FIPS 140-2 Compliance Statement

HPE IT Business Analytics (ITBA) complies with the 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 ITBA 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, prescribed for cryptographic modules by FIPS 140-2 and applicable for ITBA design, implementation and operation.

About IT Business Analytics

- ITBA is a young product and considered to be the leading IT product today, measuring and optimizing the cost, risk quality and value of IT services and processes. The first release was on June 2011. ITBA biggest differentiator from the competition is usability and content. ITBA has tight integrations with HPESW products. ITBA 10 is already bundled with Project and Portfolio Management (PPM), Service Manager (SM), Application Lifecycle Management (ALM), Cloud Service Automation (CSA), and Amazon Web Services (AWS). ITBA is currently in the middle of transition from being a Dashboard tool for senior managers to a leading Business Analytics tool for mid-layer managers as well. ITBA is on top of Vertica DB, meaning that it will deal with large amount of data. It has amazing Time-to-Value and provides a stable foundation for Self-Service Analytics capabilities.

  ITBA is in competition with very powerful self-service analytic tools such as Tableau, QlikView, which provide easy ways to manage, view and analyze the data, along with BI tools such as VMWare ITBM and MooD BI.

- For more details about how ITBA implements FIPS 140-2 requirements, see "ITBA and FIPS140-2" on page 7.

FIPS 140-2 Compliance Statement

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 standard specifies the security requirements for cryptographic modules utilized 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

FIPS 140-2 Compliant Module and Technologies

The benefits of using FIPS 140-2 validated crypto module is that the crypto algorithms are deemed appropriate and that they perform the encrypt/decrypt/hash functions correctly.

Modes of Operation

ITBA can be configured and can operate in two modes:

- **FIPS-compliant mode.** Supports FIPS 140-2 compliant cryptographic functions. The default FIPS 140-2 compliant algorithms and key length are configurable. It provides flexibility for products integration and meeting the higher cryptographic security standards of NSA Suite B cryptography (http://www.nsa.gov/ia/programs/suiteb_cryptography/) in addition to FIPS 140-2 compliance.
- **Standard mode.** Non-FIPS 140-2 compliant mode which utilizes existing cryptography available without 3rd party FIPS 140-2 crypto modules.

FIPS 140-2 Validated Third Party Module

ITBA is integrated with 3rd party FIPS 140-2 validated cryptographic module ***RSA BSAFE Crypto-J***. Its compliance was validated according to Cryptographic Module Validation Program (CMVP http://csrc.nist.gov/groups/STM/cmvp/index.html) and certified on Intel/Windows with Sun JRE 6.0 platform by NIST (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1786). When ITBA is configured to operate in FIPS-compliant mode, its functions and procedures - like

FIPS 140-2 Compliance Statement

SSL/TLS connections, which require cryptography such as secure hash, encryption, digital signature etc. – make use of the crypto services provided by ***RSA BSAFE Crypto-J***. It supports FIPS 140-2 compliance of ITBA.

Details about how to configure ITBA and its components to conform to FIPS 140-2 standard appear in the installation guides for the product(s):

- ITBA *Installation Guide*.

TLS/SSL3.x

All the ITBA components communications are secured with FIPS-compliant Transport Layer Security TLS1.0/SSL3.1 or higher. They are relying on FIPS 140-2 approved hash algorithms and symmetric and asymmetric ciphers.

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

Secure Hash

Per FIPS 140-2 standards, ITBA, in the FIPS 140-2 compliant mode, can be configured to use the following secure hash algorithms:

SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256

Symmetric Cryptography

Per FIPS 140-2 standards, ITBA, in the FIPS 140-2 compliant mode, can be configured to use the following symmetric key algorithms:

AES (ECB, CBC, CFB, OFB, CTR, CCM, GCM, XTS) [128, 192, 256 bit key sizes]

Triple-DES (ECB, CBC, CFB, OFB)

Message Digest

Per FIPS 140-2 standards, ITBA, in the FIPS 140-2 compliant mode, can be configured to use the following digital signature algorithms:

SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256

FIPS 140-2 Compliance Statement

Digital Signature

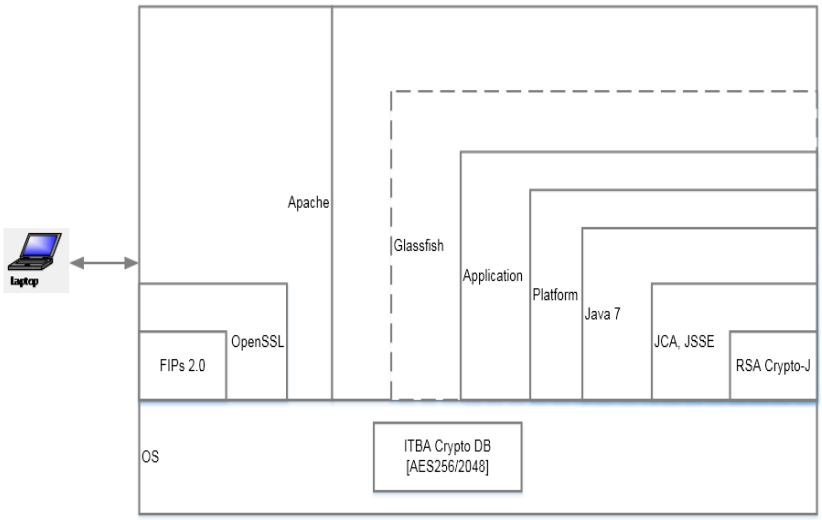
Per FIPS 140-2 standards, ITBA, in the FIPS 140-2 compliant mode, can be configured to use the following digital signature algorithms:

RSA X9.31, PKCS #1 V.1.5, RSASSA-PSS; DSA; ECDSA

ITBA and FIPS140-2

ITBA is expected to operate on General Purpose Systems with no additional physical security controls. ***RSA BSAFE Crypto-J*** crypto module installed on such platforms provides validation to Level 1 FIPS 140-2 compliant crypto services.

FIPS 140-2 Architecture



Supported Platforms

Refer to the ITBA *Support Matrix* document for a comprehensive list of supported platforms.

Also refer to the document ITBA *Open Source and Third Party Software Licenses* for a comprehensive list of 3rd Party SW used by ITBA including the JDK.

Supported Modes and Cryptography

- **FIPS mode.** Supports FIPS 140-2. In this mode, all cryptographic functions, default algorithms and key length are configurable.

FIPS 140-2 Compliance Statement

- **Standard mode.** Non-FIPS 140-2 compliant mode, with standard existing cryptography available without 3rd party FIPS 140-2 crypto modules.

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, thus meet FIPS 140-2 compliance requirements. The application-specific key management functions include

- **Key Generation.** All private and public key used by ITBA are generated during installation time. This is an automatic process which does not require any inputs from the user.
- **Key Storage.** The private keys are stored in a 3DES encrypted, password protected file.
- **Key Protection.** The password to the ITBA management DB is required to access its contents.
- **Key Access.** Only a valid user in ITBA server can access ITBA management.

Design Assurance

The RSA Bsafe Crypto-J module is packaged in ITBA and installed by the ITBA installer as JAR files provided by the vendor. The configuration parameters to use the crypto modules in ITBA and parameters to enable or disable FIPS mode is supplied to the modules as part of the Java runtime environment security configuration. The crypto modules are loaded by the ITBA modules that use them for FIPS enabled crypto functions by loading the modules as their primary crypto providers. This vendor recommended method of priority loading is also controlled by the Java Runtime security settings. Further, the RSA Bsafe Crypto-J modules are loaded only if FIPS mode is enabled.

FIPS mode is enabled in ITBA during installation. It is one of the installation interview questions. Once enabled, FIPS mode cannot be disabled.

Risk Mitigation

Physical or remote access to ITBA server and access to root user password is required to gain access to the password protected file and the crypto modules. Further, the password to the management DB is required to access its contents.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on FIPS 140-2 Compliance Statement (IT Business Analytics 10.10)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to SW-Doc@hpe.com.

We appreciate your feedback!

Hewlett Packard
Enterprise