



Hewlett Packard
Enterprise

IT Business Analytics

Software Version: 10.10

Linux operating system

Security Guide

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

© 2011-2016 Hewlett Packard Enterprise Development LP

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>.

Contents

Welcome to This Guide	5
Introduction	5
Secure Implementation and Deployment	6
Technical System Landscape	6
Security in ITBA Configurations	6
External Authentication	7
Common Security Considerations	7
Business Analytics Security Parameters	8
Secure File Storage	8
Secure Debug Features	8
Installation Security	9
Supported Operating Systems	9
Web Server Security Recommendations	9
Apache Web Server	9
Database Security Recommendations	10
PostgreSQL	10
Vertica	10
Application Server Security Recommendations	10
Best Practices	10
Network and Communication Security	12
Secure Topology	12
FAQ	12
Administration Interface	13
User Management and Authentication	14
Authentication Model	14
Best Practices	14
User Management Model	16
Authentication Administration and Configurations	16
Authorization	17
Authorization Model	17
Authorization Configuration	17
FAQ	17

Data Integrity	19
Encryption	20
TLS/SSL Data Transmission	20
Encryption of stored database fields	20
Logs	21
Log and Trace Model	21
FAQ	21
Send Documentation Feedback	22

Welcome to This Guide

Introduction

This guide is intended for Business Analytics (ITBA) implementers and system administrators who need to implement their ITBA environment in a secure manner.

Secure Implementation and Deployment

This section provides information on implementing and deploying Business Analytics in a secure manner.

This section includes the following topics:

Technical System Landscape	6
Security in ITBA Configurations	6
External Authentication	7
Common Security Considerations	7

Technical System Landscape

ITBA is a suite of enterprise applications based on various industry standard technologies. ITBA is written in Java and utilize Java EE and SE technologies and JavaScript.

For more information about typical deployment schemes and options, see the *Support Matrix* or the *Installation Guide*.

Security in ITBA Configurations

ITBA configurations may be deployed in the following two implementations. For more information, see Performance and Sizing in the *Support Matrix*.

1. **2 Servers Configuration** (1 server with ITBA, 1 server with DWH, and Vertica, 1 optional server with BOE)
2. **4 Servers Configuration** (1 server with ITBA and DWH, 3 servers with Vertica, 1 optional server with BOE)

All of these implementations share the same basic out-of-the-box security configuration options.

1. TLS/SSL security was enabled between the browser and the ITBA server by default.
2. ITBA requires users to enter user name and password credentials to gain access to the application.

External Authentication

With additional configuration, it is possible to supplement or replace the default authentication & authorization provider for ITBA by using a variety of industry-standard protocols and tools such as LDAP and Single Sign-On. For additional information on these options, see LDAP Management or Single Sign-On in the *Administrator Guide*.

1. Connect Business Analytics to an LDAP server
2. Single Sign-On (in Perform Administration Tasks for Foundation)

Common Security Considerations

ITBA only supports deployment on the supported versions of Red Hat and CentOS. For details, see *Support Matrix*.

It is recommended to follow vendor-provided best practices and to consult security hardening guides for each of the third-party components used in support of your Business Analytics deployment, which includes Apache HTTP Server, Glassfish Server, PostgreSQL DB server and Vertica DB server. Below are some resources that can serve as a starting point for researching these recommended security considerations:

Apache HTTP Server Security Tips

https://httpd.apache.org/docs/current/misc/security_tips.html

Glassfish Server Security Tips

https://blogs.oracle.com/theaquarium/entry/glassfish_security_guide_hardening_and

PostgreSQL DB server Security Tips

<http://www.openscg.com/postgresql-security-guidelines/>

Vertica DB Server Security Tips

<http://my.vertica.com/docs/7.1.x/HTML/index.htm#Authoring/AdministratorsGuide/Security/ImplementingSecurity.htm>

Business Analytics Security Parameters

This section contains references to some of the Business Analytics parameters that are relevant to security.

This section includes the following topics:

Secure File Storage	8
Secure Debug Features	8

Secure File Storage

ITBA allows users to upload files (content packs, CAP, or personal files) to the ITBA Server. All files uploaded to the server must be validated, since they can contain viruses, malicious code, or Trojans.

As a result, it is strongly recommended to implement proper antivirus protection for the file storage. This is typically referred to as the scratch or ContentPacks directory of your ITBA server.

E.g. **<application_server_installation_path>/ContentPacks**

Example: /home/admin/HPEBA-10.10.00/ContentPacks

Secure Debug Features

ITBA runs on top of the Data Warehouse (DWH) server, it provides a set of tools for troubleshooting and to provide better supportability. These features, which can expose sensitive internal information about the system and about activities performed on the system, are disabled by default. It is recommended to disable them on time after using the debugger.

For details, see https://docs.oracle.com/cd/E18930_01/html/821-2418/beafc.html#scrolltoc

Installation Security

This section provides information on aspects of installation security.

This section includes the following topics:

Supported Operating Systems	9
Web Server Security Recommendations	9
Apache Web Server	9
Database Security Recommendations	10
PostgreSQL	10
Vertica	10
Application Server Security Recommendations	10
Best Practices	10

Supported Operating Systems

For the list of supported system environments, refer to the *Support Matrix*.

Note: The supported environment information in the Support Matrix is accurate for the Business Analytics 10.10 release, but there may be subsequent updates available in the Support Site (<https://softwaresupport.hp.com/group/softwaresupport/home>).

Web Server Security Recommendations

Apache Web Server

See http://httpd.apache.org/docs/current/ssl/ssl_howto.html for information on enabling SSL for all interactions with the web server and on enforcing strong security.

Database Security Recommendations

PostgreSQL

See <http://www.openscg.com/postgresql-security-guidelines/> for information about PostgreSQL database security solutions.

Vertica

See

<http://my.vertica.com/docs/7.1.x/HTML/index.htm#Authoring/AdministratorsGuide/Security/ImplementingSecurity.htm> for information about Vertica Server database security features.

Application Server Security Recommendations

When configuring TLS/SSL on the ITBA Server, keep your Java keystore file in a private directory with restricted access. The keystore is password protected. Although the Java keystore is password protected, it is vulnerable as long as the default value of `changeit` was not changed.

Note:

- Always change default passwords.
- Always use the minimal possible permissions when installing and running ITBA.

Action	Permissions Needed for User
Installing/Running ITBA	You can install and run with non-root permissions using the <code>sudo</code> command.
Database connection	The logon user permissions must be set properly according to the recommendations in the <i>Administrator Guide</i> . Do not use a higher level of permissions than required. Do not use the default password when creating the schema.

Best Practices

Refer to "Logs" on page 21 in this document for information on additional recommendations with regard to securing the log files generated by the various ITBA product components, and the third-party

software components such as Apache Tomcat, etc... Log files contain sensitive security information (especially when they contain debug or tracing data) and as such must be given careful consideration as to who may access them.

Network and Communication Security

This section provides information on network and communication security.

This section includes the following topics:

Secure Topology	12
FAQ	12

Secure Topology

ITBA is designed to be part of a secure architecture, and can meet the challenge of dealing with the security threats to which it could potentially be exposed.

Several measures are recommended to securely deploy ITBA:

- Use of the TLS/SSL communication protocol.
- Reverse proxy architecture:
ITBA uses Apache HTTP server as a reverse proxy, it's an intermediate server that is positioned between the browser and the application server.
- Separation between web servers, application servers, and database servers.

FAQ

Question

Are exceptions required to be added to the firewall policy?

Answer

It depends on what HTTP or HTTPS ports were specified, accordingly, the firewall exceptions for the incoming traffic are required.

Administration Interface

Business Analytics provides a separate administration tab in user interface. System administrators could perform administrative tasks there.

For details, see [Getting Started with Administration Tasks](#) in the *Administrator Guide*.

User Management and Authentication

This section provides information related to user management and authentication.

This section includes the following topics:

Authentication Model	14
Best Practices	14
User Management Model	16
Authentication Administration and Configurations	16

Authentication Model

ITBA supports the following authentication methods:

- **Username and password authentication**

In an out-of-the-box default installation, ITBA requires users to enter username and password credentials to gain access to the application.

- **LDAP authentication**

You can integrate ITBA with an LDAP directory service to share contact information across your network.

- **Lightweight Single Sign-On (LW-SSO)**

An optional but highly recommended model for some integrations such as Release Control. Enabling LW-SSO for integrations will bypass the login prompts when connecting two HPE products.

- **Common Access Card (CAC) Sign-On**

CAC sign-on enables users to log in to the web client directly with a smart card that stores a valid user certificate, and users only need to enter a card PIN, instead of a user name and password.

Best Practices

The following information provides guidance for increasing the security of HP product integrations using the previously described LW-SSO features of Business Analytics. They provide network configuration details regarding implementation of subdomains and information regarding cookie security specific to LW-SSO.

1. Ensure that the Business Analytics server components and the integrated HP product server components (PPM, SM, etc.) are deployed within appropriate subdomains. For example, if the ITBA server is currently named `ba-web.mycompany.com`, implement a subdomain with a name of your choosing under the **mycompany** domain and deploy ITBA within the new subdomain. In this example, the new subdomain is named after the region where the server resides: **americas**. Thus the resulting fully qualified domain name of the server would be: **ba-web.americas.mycompany.com**.

Repeat this process for each integrated HP product in your deployment; e.g.

releasecontrol.americas.mycompany.com

sm.americas.mycompany.com

Once the above is completed, you will need to change the LW-SSO configuration files for ITBA and the integrated products to point to the new subdomain. Modify the `<domain>` element's value in the `lwssofmconf.xml` file from:

```
<domain>mycompany.com</domain>
```

To:

```
<domain>americas.mycompany.com</domain>
```

lwssofmconf.xml is located in the ITBA deployed WAR file in the `WEB-INF/classes` subdirectory. For more information, see LW-SSO in the *Administrator Guide*.

Note: It will be necessary to change the LW-SSO configuration files of the integrated product (s) for the LW-SSO features to function properly. For information on changing the LW-SSO configuration for the integrated HP products, please refer to that product's installation and configuration documentation.

2. As stated throughout this guide, it is recommended that communications between integrated products, clients (browsers), and Business Analytics are secured using HTTPS. When this is completed, take the following additional steps to increase the security of the LW-SSO cookie.
 - Ensure that the parameter **secureHTTPCookie** in the `lwssofmconf.xml` is set to **true**.
 - Ensure that the parameter **useHTTPOnly** in the `lwssofmconf.xml` is set to **true**.

These parameters assure that the LW-SSO cookie is only sent over networks where HTTPS is enabled and not accessible via client-side scripting languages.
3. To further protect the LW-SSO session cookie, it is recommended to change the value of the parameter **expirationPeriod** in the `lwssofmconf.xml` file from:

<expirationPeriod>50</expirationPeriod>

To:

<expirationPeriod>8</expirationPeriod>

This file is located in the Business Analytics deployed WAR file in the WEB-INF/classes subdirectory. The expirationPeriod parameter controls how often the LW-SSO cookie is refreshed.

User Management Model

Each person (user) who logs onto Business Analytics must have a personal information record stored in the database. Without such a record, a user cannot log onto Business Analytics.

A Business Analytics administrator can control users in Business Analytics in the following ways:

- Setting individual users and their permissions.
- Setting groups and their permissions.

For details, see User Management in the *Administrator Guide*.

Authentication Administration and Configurations

For additional information on these options, refer to the following sections in the *Administrator Guide*:

1. LDAP Management
2. Single Sign-On

Authorization

This section provides information related to user authorization in Business Analytics.

This section includes the following topics:

Authorization Model	17
Authorization Configuration	17
FAQ	17

Authorization Model

Access to ITBA resources is authorized based on the user's following settings:

- User role
- Session & Inactivity timer timeouts

Authorization Configuration

For detailed information on authorization configuration, see Users, Roles, Resources, Permissions, LDAP, and Dimension Permissions in the *Administrator Guide*.

FAQ

Question

Can ITBA inherit users' information and authorization profiles from an external repository, such as LDAP?

Answer

No.

Question

Is Role Management (access to different views and access and edit permission to separate parts) supported?

Answer

Yes.

Question

Is Access Control supported at Field Level?

Answer

Yes. See Dimension Permissions in the *Administrator Guide*.

Data Integrity

The database server is used as a simple data store and is responsible for all persistent storage. While the database contains definitions describing business logic, no processing is actually performed in this tier, other than create, read, update, and delete (CRUD) operations in response to requests from the Business Analytics Server. Referential integrity is enforced by the application, thereby protecting transactions. In addition, the database captures a complete audit log of all changes to data.

The data backup procedure is also an integral part of data integrity and while ITBA does not provide native backup capabilities, the following guidelines should be considered:

- Database backup is especially important before critical actions such as upgrades.
- Backup files should be stored properly according to the industry best practices to avoid unauthorized access.
- Since database backup can be a resource intensive process, it is strongly recommended to avoid running backups during peak demand times.

Encryption

This chapter provides information on data encryption in Business Analytics.

This section includes the following topics:

TLS/SSL Data Transmission	20
Encryption of stored database fields	20

TLS/SSL Data Transmission

ITBA was configured to use TLS/SSL to transmit data between the server and browsers.

For detailed information, see Working with Secure Sockets Layer (SSL) in a Production Environment in the *Administrator Guide*.

Encryption of stored database fields

ITBA uses proprietary algorithms when encrypting data stored in the database. For example, passwords for operators are stored using SHA-256 a one-way encryption algorithm.

Logs

This section provides information related to logs.

This section includes the following topics:

Log and Trace Model	21
FAQ	21

Log and Trace Model

Recommendations:

- Pay attention to the log level and do not leave tracing or debug parameters enabled unnecessarily.
- Pay attention to log rotation/switching.
- Restrict user access to the log directory. Ensure only those user IDs that need access to the log files can do so and disallow other user IDs.
- If logs archiving is needed, create your own archiving policy as ITBA does not provide this feature.

For detailed information, see Logs and the LogTool in the *Administrator Guide*.

FAQ

Question

Does ITBA provide tools to prevent unauthorized access to log files generated by ITBA Server?

Answer

No. However, through the use of standard security and access control lists/permissions available through the operating system where ITBA resides, it is possible to restrict access to only those users that require access to view the log files.

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 Security Guide (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!

