HP IT Business Analytics

Software Version: 10.00
Linux ® operating system

Security Guide

Document Release Date: May 2015
Software Release Date: May 2015

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

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 sign in. To register for an HP Passport ID, go to: **https://hpp12.passport.hp.com/hppcf/createuser.do**

Or click the **the Register** link at the top of the HP Software Support 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 Online web site at: **https://softwaresupport.hp.com**

This web site 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 web site 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 sign in. Many also require a support contract. To register for an HP Passport ID, go to:

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. 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 Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Welcome to This Guide

Introduction

Welcome to the *HP Business Analytics Security Guide*.

This guide is intended for Business Analytics (BA) implementers and system administrators who need to implement their BA 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

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

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

Security in BA Configurations

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

1. **2 Servers Configuration** (1 server with BA, 1 server with DWH, and Vertica, 1 optional server with BOE)
2. **4 Servers Configuration** (1 server with BA 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 BA server by default.
2. BA requires users to enter username 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 BA 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*BA Administrator Guide*.

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

Common Security Considerations

BA 10.00 only supports deployment on on Red Hat 6.5 and CentOS 6.5. 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

BA allows users to upload files (content packs) to the BA 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 BA server.

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

Example: /home/admin/HPBA-10.00.00/ContentPacks

Secure Debug Features

BA 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

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

> **Note:** The supported environment information in the Support Matrix is accurate for the Business Analytics 10.00 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 BA 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 BA.

Action	**Permissions Needed for User**
Installing/Running BA	You can install and run with non-root permissions using the sudo command.
Database connection	The logon user permissions must be set properly according to the recommendations in the *BA Administrator Guide*. 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 18 in this document for information on additional recommendations with regard to securing the log files generated by the various BA 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

BA 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 BA:

- Use of the TLS/SSL communication protocol.
- Reverse proxy architecture:

  BA 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 *BA Administrator Guide*.

User Management and Authentication

This section provides information related to user management and authentication.

This section includes the following topics:

Authentication Model

BA supports the following authentication methods:

- **Username and password authentication**

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

- **LDAP authentication**

  You can integrate BA 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 HP products.

Authentication Administration and Configurations

For additional information on these options, refer to the following sections in the *BA 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

Access to BA 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 *BA Administrator Guide*.

FAQ

Question

Can BA 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 *BA 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 BA 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 inBusiness Analytics.

This section includes the following topics:

TLS/SSL Data Transmission

BA 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 *BA Administrator Guide*.

Encryption of stored database fields

BA 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

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 BA does not provide this feature.

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

FAQ

Question

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

Answer

No. However, through the use of standard security and access control lists/permissions available through the operating system where BA 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 10.00)

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@hp.com.

We appreciate your feedback!