



# Operations Bridge Reporter

Software Version: 10.22  
Windows® and Linux operating systems

## Secure Deployment Guide

Document Release Date: December 2017  
Software Release Date: December 2017

  
**Hewlett Packard**  
Enterprise

## Legal Notices

### Warranty

The only warranties for Seattle SpinCo, Inc and its subsidiaries ("Seattle") 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. Seattle 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. Except as specifically indicated, valid license from Seattle 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

© 2015 - 2017 EntIT Software LLC, a Micro Focus company

### 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.

## Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

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

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

## Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

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

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

**HPE Software Solutions Now** accesses the HPE SW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

# Contents

Operations Bridge Reporter Security Features .....	5
Security Updates Since the Previous Versions .....	5
Related Documents .....	6
Security Overview .....	6
Security Concepts .....	6
Common Security Concepts .....	7
OBR Terminology .....	7
Secure Implementation and Deployment .....	9
Default Security Settings .....	9
OBR Security Hardening .....	9
Physical Security .....	10
OBR in FIPS mode .....	10
Secure Installation Guidelines .....	12
Supported Operation Systems .....	12
Operating System Hardening Recommendations .....	12
Installation Permissions .....	12
Tomcat Hardening .....	13
Administration Interface Security .....	17
Accessing the Administration Interface .....	17
Securing the Administration Interface .....	17
User Management and Authentication .....	18
Authentication Model .....	18
Types of Users .....	18
Authentication, Administration and Configuration .....	19
User Authentication .....	20
Database Authentication .....	20
Authorization .....	21
Authorization Model .....	21
Authorization Administration .....	21
Backup .....	23
Encryption .....	24

Encryption Model .....	24
Encryption Administration .....	24
Digital Certificates .....	24
Log and Trace .....	26
Hardening the Operation Bridge Reporter .....	27
Security Hardening Recommendations .....	27
Configuring the TLS Protocol .....	27
Clickjacking Protection .....	28
Send documentation feedback .....	29

# Operations Bridge Reporter Security Features

This guide helps you to deploy and manage Operations Bridge Reporter (OBR) in a secure manner. The purpose of this guide is to help you make well informed decisions about various capabilities and features that OBR provides to meet modern enterprise security needs. Security requirements for the enterprise are constantly evolving and this guide provides you with best practices to meet those stringent requirements.

## Security Updates Since the Previous Versions

The following security updates were made between **SHR 9.x** and **OBR 10.00**:

- Changing password during first time log on is made mandatory.
- No default passwords are provided during post install configuration for Administration Console, SAP BusinessObjects, PostgreSQL database, or Vertica database users.
- Secure communication (HTTPS ) is enabled between browser and Administration Console/SAP BusinessObjects application.
- Self-signed certificate is deployed on the server. You must configure CA signed certificate by following the instructions. For information on instructions, see *Operations Bridge Reporter Interactive Installation Guide*.

The following security updates were made between **OBR 10.00 and 10.01**:

- Configure OBR to enable usage of FIPS certified libraries and FIPS compliant algorithms for encryption, signing and hashing. For information to enable FIPS, see *Configuring FIPS for OBR in Operations Bridge Reporter Configuration Guide*.
- The Administration console allows you to configure logon banner. The text that appears on logon banner is configurable. When you log on to Administration console or SAP BusinessObjects BI Launch Pad or CMC, the first screen warns you against unauthorized entry. For information to configure logon banner, see *Configuring Logon Banner for OBR in Operations Bridge Reporter Configuration Guide*.
- Secure Communication - You can configure JDBC or ODBC connections over TLS for the following:

- Vertica and OBR server/SAP BusinessObjects
- OBR collector and BSM/OMi Oracle database
- OBR collector and BSM/OMi RTSM

Using the Administration Console, you can enable TLS for OM and BSM/OMi to connect with Oracle database using ODBC or JDBC. For more information, see *Data Source Configuration* in *Operations Bridge Reporter Configuration Guide*.

Using the Administration Console, you can enable TLS for Vertica database. For more information, see *Enabling and Disabling TLS for Vertica* in *Operations Bridge Reporter Configuration Guide*.

The following security update is made in **OBR 10.22**:

- Enabling Tomcat Security for the Admin web server and Reporting Web server

## Related Documents

For more information about the security hardening of OBR, see the following documents:

- Operations Bridge Reporter Interactive Installation Guide
- Operations Bridge Reporter Configuration Guide
- Operations Bridge Reporter Administration Guide

## Security Overview

This document provides an overview of the security models and recommendations for a secure implementation of OBR. This includes subjects such as authentication, authorization, encryption, and more. Where relevant, there are references to other OBR documents, which describe how to complete security-related tasks.

## Security Concepts

This section provides information on common security concepts and terminologies.

# Common Security Concepts

## System Security

System Security is a process by which computer-based equipment, information, and services are protected from unintended or unauthorized access, change, or damage.

## Least Privilege

The practice of limiting access to the minimal level that will allow normal functioning. This means giving a user account only those privileges that are essential to that user's work.

## Authentication

The process of identifying an individual, usually based on a user name and password, or certificate.

## Authorization

Permission to access system objects, based on an individual's identity.

## Encryption

A way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right key to decode it. For example, the TLS protocol encrypts the communication data.

# OBR Terminology

Term	Description
<b>Permission</b>	A permission is a predefined authorization to perform a task. A set of permissions can be assigned to roles.
<b>Role</b>	A role is a collection of permissions.
<b>User</b>	A user is an object associated with a person (or application identity) representing the person and defining their authorization.  Roles are assigned to users, to define the actions they are authorized to perform.

It is possible to configure different kinds of users:

- **Internal users** - Log on to Administration Console using the user name and password that was set up locally.
- **LDAP users** - Define the user in the LDAP server and map LDAP groups to HPE OBR roles.



# Secure Implementation and Deployment

This section describes default and physical security settings.

## Default Security Settings

- **TLS Encryption** – The default SSL protocols for HTTPS communication with the OBR are TLSv1.0, TLSv1.1 and TLSv1.2. It is recommended to work with the latest version.
- **HTTPS enabled** - Secure communication (HTTPS ) is enabled between browser and Administration Console/SAP BusinessObjects application.
- **Certificate Authority (CA) signed certificate** - Self-signed certificate is deployed on the server. You must configure CA signed certificate by following the instructions. For information on instructions, see *Operations Bridge Reporter Interactive Installation Guide*.

**Note:** The certificates shipped with OBR are valid for three months.

- **Logon Banner** – You can enable a logon banner screen that appears and must be acknowledged before you can access the Administration Console, SAP BusinessObjects or CMC.

For information about enabling this functionality, see *Configuring Logon Banner for OBR* in *Operations Bridge Reporter Configuration Guide*.

- **Common Criteria (CC)** – By Default, OBR uses FIPS compliant algorithms and libraries.

## OBR Security Hardening

The Hardening section provides recommendations for safeguarding your OBR deployment from security risks or threats. Some of the most important reasons to secure an application include protecting the confidentiality, integrity, and availability of an organization's critical information.

To comprehensively protect your OBR system, it is necessary to secure both OBR and the computing environment (for example, the infrastructure and the operating system) upon which the application runs.

For more information, see "[Hardening the Operation Bridge Reporter](#)" on page 27.

## Physical Security

HPE Software recommends that OBR is protected by physical security controls defined by your organization. The OBR server components are installed in a physically secured environment, according to best practice. For example, the server must be in a closed room with access control.

## OBR in FIPS mode

When you configure OBR to run in FIPS mode, the following components are also configured to operate in FIPS mode:

- Tomcat server
- Java Runtime Environment
- SAP BusinessObjects
- Vertica

Secure communication - following are the communication channels that are secured:

- Browser to OBR Administration Console and SAP BusinessObjects - This communication is secured using HTTPS.
- OBR server to Vertica - OBR uses JDBC and ODBC to connect to Vertica. OBR provides steps/tools to achieve the JDBC and ODBC connections over TLS.
- SAP BusinessObject to Vertica - SAP BusinessObject uses JDBC over TLS to connect to Vertica.
- OBR server to OBR collector and OBR collector to agent - LCore BBC is used as the communication framework. OBR provides steps/tools to configure HTTPS for this communication.
- OBR collector to OMi Oracle database - OBR connects to OMi oracle database over JDBC to fetch events. OBR uses DataDirect JDBC driver for communication. OBR provides steps/tools to achieve the JDBC connection over TLS.
- OBR collector to OMi RtSM - OBR allows to configure HTTPS for this communication.

RSA BSAFE Crypto-J version 6.20 is used for Java crypto functions and OpenSSL 01.00.010 is used for 'C' crypto functions.

For more information on configuring OBR for FIPS, see *Configuring FIPS for OBR* section in *Operations Bridge Reporter Configuration Guide*.

## Secure Installation Guidelines

This section provides information on supported operating systems, operating system hardening recommendations, and installation permissions.

## Supported Operation Systems

For the types and versions of supported operating systems, see the *Operations Bridge Reporter Release Notes*.

## Operating System Hardening Recommendations

Contact your operating system vendor for recommended best practices for hardening your operating system.

For example:

- Latest patches should be installed
- Unnecessary services/software should be removed or disabled
- Minimal permissions should be assigned to users
- Auditing should be enabled

## Installation Permissions

The following permissions are required to install and run OBR:

Function	Operating System-Level Security
Installing and running OBR	<p><b>Linux:</b> Root user or equivalent root user or sudo user has permission to install and run the OBR.</p> <p>For information to create sudo user, see <i>Operations Bridge Reporter Interactive Installation Guide</i>.</p>

Function	Operating System-Level Security
	<b>Windows:</b> Administrator or equivalent to administrator has permission to install and run the OBR.

## Tomcat Hardening

When you install OBR, Tomcat is partially hardened by default. For more information, see the recommendations in the *CIS Apache Tomcat 7.0* document.

### Prerequisites

1. Install the OBR 10.22 patch.
2. Complete the OBR post installation configurations.

After the OBR 10.22 patch installation, the script `enableTomcatHardening.vbs` (For Windows) `enableTomcatHardening.sh` (For Linux) will be available in `{PMDB_HOME}/bin/` directory of the OBR server. Contact HPE Support for assistance.

### Enable Tomcat Hardening For Windows

Follow these steps to enable Tomcat Hardening:

1. Log on to the system and follow these steps to stop the `HPE_PMDB_Platform_Administrator` service:
  - a. From the Start, type **Run** in Search. The Run dialog box appears.
  - b. Type **services.msc** in the open field, and then press **ENTER**. The Services window appears.
  - c. Right-click the **HPE\_PMDB\_Platform\_Administrator** service and click **Stop**.
2. Run the following command on the command line console:
 

```
cscript EnableTomcatHardening.vbs -enable <Tomcat User Name> <Password>
```

where, `<Tomcat User Name>` – is the tomcat user to be created

`<Password>` - is the password for the tomcat user
3. Verify if the `HPE_PMDB_Platform_Administrator` is Running. If the service is not running, follow these steps to start the `HPE_PMDB_Platform_Administrator` service:
  - a. From the Start, type **Run** in Search. The Run dialog box appears.

- b. Type **services.msc** in the open field, and then press **ENTER**. The Services window appears.
- c. Right-click the **HPE\_PMDB\_Platform\_Administrator** service and click **Start**.

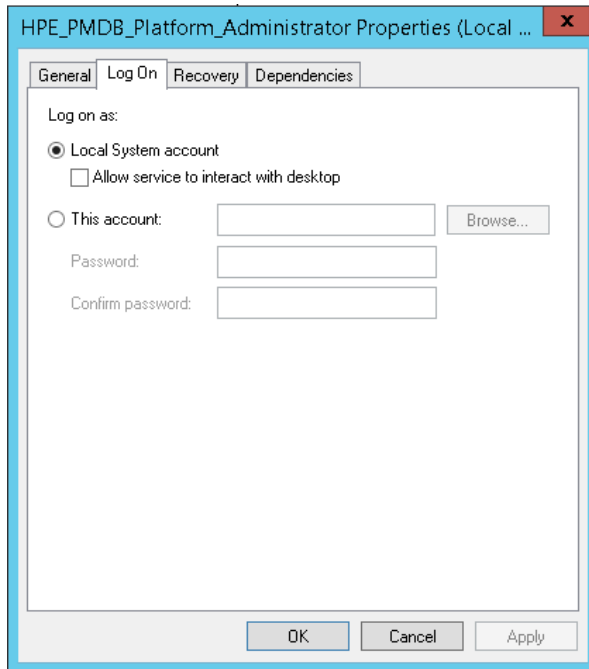
### Disable Tomcat Hardening For Windows

Follow these steps to disable Tomcat Hardening:

1. Log on to the system and follow these steps to stop the HPE\_PMDB\_Platform\_Administrator service:
  - a. From the Start, type **Run** in Search. The Run dialog box appears.
  - b. Type **services.msc** in the open field, and then press **ENTER**. The Services window appears.
  - c. Right-click the **HPE\_PMDB\_Platform\_Administrator** service and click **Stop**.
2. Run the following command on the command line console:  

```
cscript EnableTomcatHardening.vbs -disable <Tomcat User Name> <Password>
```

where, *<Tomcat User Name>* – is the tomcat user created while enabling the tomcat hardening  
*<Password>* - is the password for the tomcat user
3. Follow these steps to start the HPE\_PMDB\_Platform\_Administrator service:
  - a. From the Start, type **Run** in Search. The Run dialog box appears.
  - b. Type **services.msc** in the open field, and then press **ENTER**. The Services window appears.
  - c. Right-click the **HPE\_PMDB\_Platform\_Administrator** service and click **Properties**. The HPE\_PMDB\_Platform\_Administrator Properties pop-up appears.
  - d. Click **Log On** tab.



- e. Select **This account** option and type the user credentials. You must type the user credentials that was used before creating the Tomcat user.
- f. Click **Apply**.
- g. Right-click the **HPE\_PMDB\_Platform\_Administrator** service and click **Start**

### Enable Tomcat Hardening For Linux

Follow these steps to enable Tomcat Hardening:

1. Log on to the system and follow these steps to stop the HPE\_PMDB\_Platform\_Administrator service:
  - a. Go to the `/etc/init.d` directory
  - b. Run the following command:
 

**On RHEL 6.x/SUSE Linux Enterprise Server 11:** `service HPE_PMDB_Platform_Administrator stop`

**On RHEL 7.x:** `systemctl stop HPE_PMDB_Platform_Administrator.service`
2. Go to the `$PMDB_HOME/bin` directory and run the following command on the command line console:
 

```
./enableTomcatHardening.sh -enable <Tomcat User Name> <Password>
```

where, *<Tomcat User Name>* – is the user to be created

*<Password>* - is the password for the new user

3. Follow these steps to start the HPE\_PMDB\_Platform\_Administrator service:
  - a. Go to the `/etc/init.d` directory
  - b. Run the following command:

**On RHEL 6.x/SUSE Linux Enterprise Server 11:** `service HPE_PMDB_Platform_Administrator start`

**On RHEL 7.x:** `systemctl start HPE_PMDB_Platform_Administrator.service`

### Disable Tomcat Hardening For Linux

Follow these steps to disable Tomcat Hardening:

1. Log on to the system and follow these steps to stop the HPE\_PMDB\_Platform\_Administrator service:
  - a. Go to the `/etc/init.d` directory
  - b. Run the following command:

**On RHEL 6.x/SUSE Linux Enterprise Server 11:** `service HPE_PMDB_Platform_Administrator stop`

**On RHEL 7.x:** `systemctl stop HPE_PMDB_Platform_Administrator.service`

2. Go to the `$PMDB_HOME/bin` directory and run the following command on the command line console:

```
./enableTomcatHardening.sh -disable <Tomcat User Name> <Password>
```

where, *<Tomcat User Name>* – is the tomcat user created while enabling the tomcat hardening

*<Password>* - is the password for the tomcat user

3. Follow these steps to start the HPE\_PMDB\_Platform\_Administrator service:
  - a. Go to the `/etc/init.d` directory
  - b. Run the following command:

**On RHEL 6.x/SUSE Linux Enterprise Server 11:** `service HPE_PMDB_Platform_Administrator start`

**On RHEL 7.x:** `systemctl start HPE_PMDB_Platform_Administrator.service`



# Administration Interface Security

This section provides information on accessing and securing the administration interface. The Administration Console is the administration interface in OBR.

## Accessing the Administration Interface

There are several ways to control access to the administration interface:

- LDAP users (recommended)
- Internal users
- Client Certificate

## Securing the Administration Interface

The following are the recommendation for securing the administration interface:

- It is recommended to work with LDAP users, rather than internal users, because this is more secure. LDAP users should be defined with a strong password policy.
- For high security, it is recommended to set up authentication to access OBR Administrator Console and SAP BusinessObjects via Client Authentication certificates. This is more secure than user passwords.

For information to configure Client Authentication certificates, see Client Authentication Certificate for OBR section in *Operations Bridge Reporter Configuration Guide*.

# User Management and Authentication

This section provides information on authentication model, types of users, and database authentication.

## Authentication Model

The following are the methods to enable authentication in OBR:

- User name and password
- Client Authentication certificate
- LDAP users

**Note:** OBR authenticates using the SAP BusinessObjects authentication mechanism.

## Types of Users

OBR has user types based on the following:

- **Administration Console**

OBR Administration Console can be accessed by user belonging to Administrators group only. For example, **report user** and **report developer**.

- **SAP BusinessObject**

The following are the default user accounts in SAP BusinessObjects:

- **Administrator** - An administrator can perform all tasks in SAP BusinessObjects BI platform applications such as the CMC, CCM, Publishing Wizard, and BI launch pad. The administrator belongs to the Administrators and Everyone groups.
- **Guest** - The guest user is enabled by default and belongs to the Everyone group.
- **SMAAdmin** - The SMAAdmin is a read-only account used by SAP Solution Manager to access BI platform components.

The following are the default user groups in SAP BusinessObjects:

- Administrators
- Everyone
- QaaWS Group Designer
- Report Conversion Tool Users
- Translators
- Universe Designer Users

For more information on SAP BusinessObjects user types and groups, see *Business Intelligence Platform Administrator Guide*.

## Authentication, Administration and Configuration

You can set up internal users with passwords or define the user in the LDAP server and map LDAP groups to OBR roles. You can also configure OBR to work with Client Authentication certificate using smart card.

For information to configure Client Authentication Certificate for OBR, see Client Authentication Certificate for OBR section in *Operations Bridge Reporter Configuration Guide*.

OBR uses the SAP BusinessObjects authentication mechanism. The following are some of the authentication types available in SAP BusinessObjects:

- **Enterprise** - This is the default authentication type. Use this if you prefer to create distinct accounts and groups for use with BI platform, or if you have not already set up a hierarchy of users and groups in an LDAP directory server, or a Windows AD server.
- **LDAP** - This type of authentication, allows you to use existing LDAP user accounts and groups in the BI platform. When you map LDAP accounts to the BI platform, users can access BI platform applications with their LDAP user name and password. This eliminates the need to recreate individual user and group accounts within the BI platform.
- **Windows AD** - This type of authentication allows you to use existing Windows AD user accounts and groups in the BI platform. When you map AD accounts to the BI platform, users can log on to BI platform applications with their AD user name and password. This eliminates the need to recreate individual user and group accounts within the BI platform.

For more information on SAP BusinessObjects authentication, see *Business Intelligence Platform Administrator Guide*.

## User Authentication

Users can authenticate into the Administration console by using a local user account or by using one of several external authentication components. Each approach requires administrative setup.

## Database Authentication

OBR includes PostgreSQL and Vertica as database. The PostgreSQL database authentication is handled by allowing access only from within the OBR system.

OBR uses Vertica database for storing, processing, and managing the performance data of your IT environment. OBR uses SSL to communicate with Vertica database.

We recommend using a strong database password for database authentication and using a strong password policy.

For information on changing the database password, see *Changing Password* section in *Operations Bridge Reporter Online help for Administrators*.

# Authorization

This section provides information about authorization model, configure and administer the authorization.

## Authorization Model

User access to OBR resources is authorized based on the user's role, and the permissions.

OBR enforces resource access control on users/groups accessing resources. The resources include reports, folders, universe etc. The resource access control allows users or groups to gain access to the resources only if the user or group has the correct permission for the resource. OBR users and groups can have either Granted, Denied, View or Full access permissions.

### **Minimal Permissions Guidelines**

It is recommended to:

- Select appropriate permissions for the role.
- Use minimal permissions when creating new roles.
- Grant minimal permissions and extend the permissions only as needed to avoid unwanted privilege escalation.

## Authorization Administration

### **Authorizing Administration Console User Accounts**

An OBR administrator can set the following general behaviors that apply to all local user accounts of Administration Console:

- Minimum and maximum password length
- Password complexity

- Password expiration
- Password reuse

## **Authorizing SAP BusinessObjects User Accounts**

You can change the password settings for a specific user or for all users in the system. The various restrictions apply only to Enterprise accounts—that is, the restrictions do not apply to accounts that you have mapped to an external user database (LDAP or Windows AD). The following are the user and general password settings for user accounts of SAP BusinessObjects:

- User password settings:
  - Password never expires
  - User must change password at next log on
  - User cannot change password
- General password settings:
  - Enforce mixed-case passwords
  - Must contain at least N Characters
  - Must change password every N day(s)
  - Cannot reuse the N most recent password(s)
  - Must wait N minute(s) to change password
  - Disable account after N failed attempts to log on
  - Reset failed log on count after N minute(s)
  - Re-enable account after N minute(s)

## Backup

In order to prevent data loss, it is highly recommended to back up your data on the servers onto secure media on a regular basis. This is also helpful for disaster recovery and business continuity.

For more information on backup and recovery, see *Database Backup and Recovery* section in *Operations Bridge Reporter Configuration Guide*.

# Encryption

This section describes the encryption, encryption model and digital certificates.

## Encryption Model

Encryption is designed to prevent the exposure and modification of sensitive data, such as passwords, definitions, and so on, in the OBR system.

It is important to use well known, standard algorithms without known vulnerabilities, in order to prevent decryption by unauthorized persons.

### **Static Data**

All saved passwords are protected using well known algorithms and none are left in cleartext.

For example:

- The system account passwords are encrypted and protected.
- The database passwords are encrypted.

## Encryption Administration

In order to reach higher levels of security and cryptography, OBR uses FIPS compliant algorithms and libraries.

## Digital Certificates

A digital certificate is an electronic "passport" for a person, server, station, and so on.

- To use encryption between a browser and the OBR server, you need to install a digital certificate on the server side.



- To use Client Authentication certificate to authenticate the OBR server, you need to install a Client Authentication certificate on the client side.

### **Access Control to KeyStore and TrustStore**

It is recommended that the TrustStore and KeyStore are stored with read permissions only for the user that runs the Administration Console.

### **Replacing the OBR Self-signed Certificate**

It is recommended to replace the OBR self-signed certificate with CA signed certificate after a new installation of OBR or if your current certificate has expired.

For information to generate CA signed certificate, see *Operations Bridge Reporter Interactive Installation Guide*.

## Log and Trace

Logs let you trace errors, warnings, information, and debugging messages. The logs are saved in the file server, in the following locations:

- {PMDB\_HOME}\log - Contains log messages related to administrator services, database, OBR licensing, business objects, administration console, internal monitoring, collector, logger, mapper.
- {PMDB\_HOME}\adminServer\logs - Contains log messages related to Administration Console.
- {PMDB}\BOWebServer\logs - Contains log messages related to SAP BusinessObjects launch pad.
- {PMDB\_HOME}\log\VC\_collector\ - Contains log messages related to VC collector.
- <Postgres\_install\_directory>/data/pg\_log - Contains log messages related to PostgreSQL.

For more information on OBR log files, see *Introducing the OBR Log Files* section in *Operations Bridge Reporter Troubleshooting Guide*.

# Hardening the Operation Bridge Reporter

This section describes how to configure security hardening for Operations Bridge Reporter.

## Security Hardening Recommendations

1. Install the latest version and patch of Operations Bridge Reporter.
2. OBR uses FIPS compliant algorithms and libraries.
3. Configure OBR to use CA signed certificate. For more information, see *Operations Bridge Reporter Interactive Installation Guide*.
4. Secure communication (HTTPS ) is enabled between browser and Administration Console/SAP BusinessObjects application.

For information to disable the HTTPs, see *Operations Bridge Reporter Troubleshooting Guide*.

OBR strongly recommends the use of HTTPS, for security reasons, so that the only communication channel will be on TLS and encrypted.

5. Configure the OBR for TLS encryption and client certificate for strong authentication (mutual).
6. Configure the TLS protocol version.
7. Harden/secure the operating system and database.

## Configuring the TLS Protocol

You can configure OBR to define the supported TLS protocol version. By default, OBR allows TLS v1, TLS v1.1 and TLS v1.2, but you can narrow this down.

To configure TLS protocol, follow these steps:

1. Open the server.xml file located at %PMDB\_HOME%\BOWebServer\conf and %PMDB\_HOME%\adminServer\conf (**for Windows**) or \$PMDB\_HOME/BOWebServer/conf and \$PMDB\_HOME/adminServer/conf (**for Linux**).
2. Locate the SSL connector.

3. Edit the default value of `sslEnabledProtocols`. For example, change

```
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" to
```

```
sslEnabledProtocols="TLSv1.2"
```

4. Restart the server.

## Clickjacking Protection

The protection against clickjacking is handled in OBR by using the x-frame option. The preferred framing policy value `SAMEORIGIN` is used in the header to allow framing only by the specified site.

# 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 Secure Deployment Guide (Operations Bridge Reporter 10.22)**

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 [docfeedback@hpe.com](mailto:docfeedback@hpe.com).

We appreciate your feedback!

