

**Oracle® Hospitality Bellavita**  
Security Guide  
Release 2.7.2.4

July 2017

Copyright © 2014, 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

---

---

# Contents

<b>Preface</b> .....	<b>4</b>
Audience.....	4
Customer Support .....	4
Documentation .....	4
Revision History.....	4
<b>1 Bellavita Security Overview</b> .....	<b>5</b>
Basic Security Considerations.....	5
Overview of Bellavita Security .....	6
Understanding the Bellavita Environment .....	7
Recommended Deployment Configurations.....	8
Component Security .....	9
Operating System Security .....	9
Oracle Database Security .....	9
<b>2 Performing a Secure Bellavita Installation</b> .....	<b>10</b>
Specific Secure Configuration Rules .....	10
Specific Secure Configuration Rules .....	10
Pre-Installation Configuration .....	10
Installing Bellavita Securely.....	11
Installing Spa and Leisure Subcomponent Securely.....	11
Installing Online Booking Subcomponent Securely.....	11
Post-Installation Configuration.....	11
Change Default Passwords .....	11
<b>3 Implementing Bellavita Security</b> .....	<b>12</b>
<b>4 Installation of the Web Services via SSL</b> .....	<b>14</b>
Accessing the webservice in a browser .....	14
Missing Certificate .....	14
What a security certificate is .....	14
Self-signed certificate.....	15
Authorized certificate.....	15
<b>Appendix A Secure Deployment Checklist</b> .....	<b>17</b>

---

---

# Preface

## Audience

This installation guide is intended for system administrators and support familiar with Bellavita.

## Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

## Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at

<http://docs.oracle.com>

## Revision History

Date	Description of Change
July 2017	<ul style="list-style-type: none"><li>• Initial publication.</li></ul>

---

---

# 1 Bellavita Security Overview

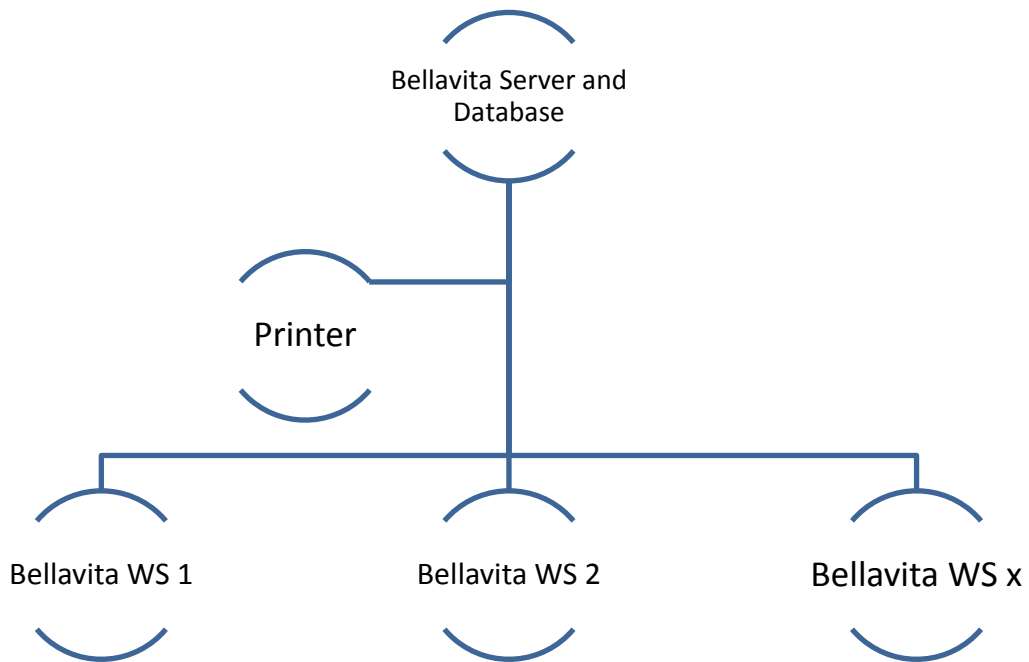
This chapter provides an overview of Oracle Hospitality Bellavita security and explains the general principles of application security.

## Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See “Performing a Secure Bellavita Installation” for more information.
- **Learn about and use the Bellavita security features.** See “Implementing Bellavita Security” for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See “Security Considerations for Developers” for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the [Critical Patch Updates and Security Alerts](#) Web site:

## Overview of Bellavita Security



**Figure 1 Bellavita Network Diagram for typical installation**

In accordance with the PA DSS Data Security Standard, Oracle strongly recommends that every site installs and maintains a firewall configuration to protect data. Configure your network so that databases and client PCs always reside behind a firewall and have no direct access to the Internet. Oracle strongly recommends that each site ensures that servers, databases, client PCs, and any medium containing sensitive data reside behind a firewall.

Firewalls are computer devices that control the computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

---

## Understanding the Bellavita Environment

When planning your Bellavita implementation, consider the following:

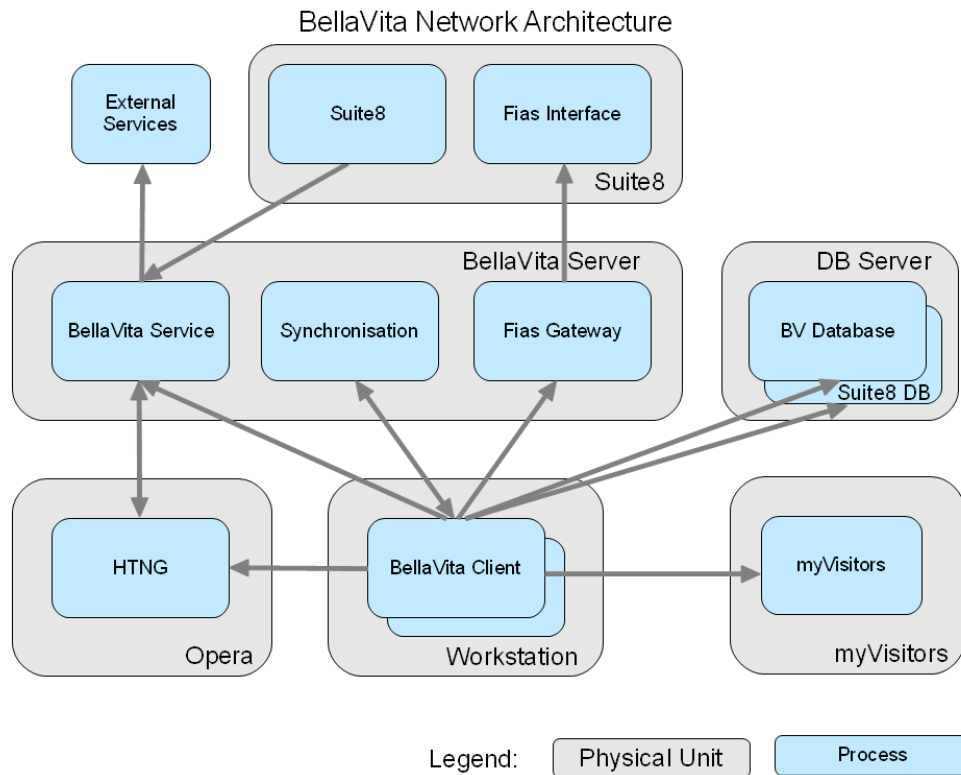
- **Which resources need to be protected?**
  - You need to protect customer data, such as passwords
  - You need to protect internal data, such as proprietary source code.
  - You need to protect access data to third party interfaces from misuse.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?** For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- **What will happen if protections on strategic resources fail?** In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

**Oracle provides functionality within the Bellavita Application for Personal Information (for example, name, date of birth, home address). Placing this information in any fields other than the designated areas, i.e., Notes or Comments fields, is open for PCI review and is not compliant with PA-DSS rules and regulations.**

## Recommended Deployment Configurations

This section describes recommended deployment configurations for Bellavita.

There are different deployment scenarios possible depending on the used dataflow and installed interfaces.



**Figure 2 Bellavita Network Architecture**

As from release 2.5, the application code is kept in %allusersprofile%/bellavita on the workstation. Report files are read on demand from the server.

### List of Port Numbers

BellaVita Version 2.6 upwards

<i>Usage</i>	<i>Node</i>	<i>Default value</i>	<i>Remark</i>
Oracle DB	Server	1521	
BV Service	Server	9090	
Synchronisation	Server	50122	
Synchronisation	Workstation	Random	
Fias Gateway	Server	5001	Not for Opera/HTNG/Leisure
Suite 8 XML Interface	Server	80	

**Figure 3 Port list for network**



---

As Bellavita provides no interfaces to the internet the internet zone security directions are not applicable.

Bellavita is only intranet client - / server – architecture.

In hosted environment generally, the user access the Bellavita application via citrix client. Therefore only the citrix client needs to be secured, not the application itself.

## **Component Security**

### **Operating System Security**

See the [Network Security Checklists](#).

### **Oracle Database Security**

See the [Oracle Database Security Guide for 11.2](#).

---

---

## 2 Performing a Secure Bellavita Installation

This chapter presents planning information for your Bellavita installation. For information about installing Bellavita, see the Bellavita Installation Guide.

### Specific Secure Configuration Rules

The table below lists all the secure configuration rules. Each row in the table contains a rule, a link to a page which describes the rule in detail, and a priority for that rule.

<b>Specific Secure Configuration Rules</b>		
The table below lists all the secure configuration rules. Each row in the table contains a rule, a link to a page which describes the rule in detail, and a priority for that rule.		
<a href="#">SCO30-ORCL</a>	Do not create default accounts with default passwords.	Critical
<a href="#">SCO37-ORCL</a>	Protect 'Debug Tools' appropriately	Critical
<a href="#">SCO32-ORCL</a>	Access control must be restrictive by default	Critical
<a href="#">SCO39-ORCL</a>	Clean up sensitive information after the installation	Critical
<a href="#">SCO31-ORCL</a>	Enable a password policy by default	High
<a href="#">SCO33-ORCL</a>	Disable Weak Protocols and Weak Cryptographic Algorithms by Default	High
<a href="#">SCO34-ORCL</a>	Samples or Other Demonstration Material Must Not Be Installed by Default	High
<a href="#">SCO41-ORCL</a>	Enable Security Audit Logging by Default	High
<a href="#">SCO43-ORCL</a>	Enable secure protocols by default	High
<a href="#">SCO36-ORCL</a>	Ensure processes run at the lowest required privilege	Medium
<a href="#">SCO40-ORCL</a>	Minimize the Attack Surface	Medium
<a href="#">SCO38-ORCL</a>	No Oracle Internal Information Should be Leaked in Oracle Products	See Rule Specific Table

7

### Pre-Installation Configuration

Install and maintain a firewall configuration to protect data.

Do not use vendor-supplied defaults for system passwords and other security parameters.

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

Bellavita does not provide default accounts.

---

## Installing Bellavita Securely

The following guides are a pre-requisite before installing Bellavita:

- Bellavita 2.7.2.1 and Patch 2.7.2.4

These Guides and Best Practices can be found on the Oracle Help Center.

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation.

When installing the DB, you are obliged to create secure DB passwords. Do not use default or well-known passwords and rotate passwords frequently.

See the “Oracle Hospitality Bellavita Installation Guide” for more information and instructions.

## Installing Spa and Leisure Subcomponent Securely

The following guides are a pre-requisite before installing Suite8 Spa and Leisure

- Suite8 Spa and Leisure Install Shield\_8100  
(Installation Guide for Suite8 Leisure\_8.10.0.0)
- Installation of the Web Services via SSL (see Chapter 4 )

## Installing Online Booking Subcomponent Securely

The following guides are a pre-requisite before installing Suite8 Spa and Leisure

- Bellavita Install Shield\_2721  
(Installation Guide for Bellavita Leisure\_2721)
- Installation of the Web Services via SSL (see Chapter 4 )

## Post-Installation Configuration

- Remove or disable components that are not needed in a given type of deployment.
- Configure communications security. In case WebConnect or XML Interface is used SSL must be installed on the IIS server. See “How to Install SSL” document for more details. Weak or plain-text protocols, such as FTP, must be disabled. It is still possible to enable them for backward compatibility (or communication with third parties which still don't support secure protocols), however this might be insecure. It is planned for the future versions to completely disable insecure protocols.
- Enable User Access Control.
- Change the User Access Rights for the Oracle Client/Bellavita Client files to be restrictive (See Bellavita Install Shield\_2721 for the details).
- Enable User Log for all sensitive data.
- When possible, access to XML Interface has to be restricted using firewall rules to allow requests only from the trusted IP addresses. For example when only WebConnect is used, firewall has to be configured to allow only the traffic from the know WebConnect Web Server.

## Change Default Passwords

Bellavita is not installed with any default passwords.

When defining the passwords, use Complex Passwords and change them frequently.

**Supervisor or members of the Supervisor Group are not to be used by regular users and must only be used by authorized Administrators.**

---

---

## 3 Implementing Bellavita Security

This chapter explains the Bellavita security features. Bellavita provides 2 options for user authentication:

- **Bellavita native authentication**  
In this case all user management and password control mechanisms are implemented by Bellavita. Access Controls definition and password rules are done in Bellavita.  
In order to comply with PA DSS rules, you must set:
  - Password requirements to have a minimum of 7 characters and include both numeric and alphabetic characters
  - Password change requirements to be at least every 90 days
  - Password history management to require new passwords to not repeat the previous four passwords.
  - Repeated access attempts to lock out the user account after a maximum of six logon attempts
  - Lockout duration to a minimum of 30 minutes or until an administrator enables the user ID (configurable)
  - Re-authentication requirements to re-activate the session if the application session has been idle for more than 15 minutes
- **LDAP authentication.** The property can decide to use existing LDAP server (e.g. Microsoft Exchange server). In this case user configuration and password management is managed by the LDAP Server.

Disable all logging by copying the original bellavitaLog4j configuration file into the application directory:

```
xcopy <cid>\deployment\templates\bellaVitaLog4j.properties  
<cid>\bellavita\ini
```

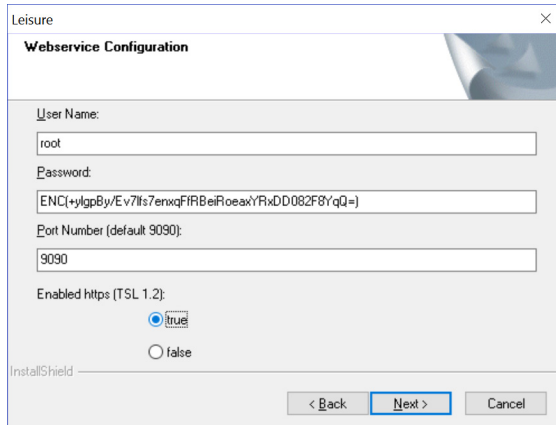


---

---

# 4 Installation of the Web Services via SSL

1. The Web service can be installed via InstallShield (upgrade, change password)
2. Web service is configured as follows:



## Accessing the webservice in a browser

After the webservice was installed with SSL enabled, enter url <https://lg00ejk:9090/bvserver/services/> in a webbrowser. If a valid certificate was installed on that server for that hostname,



a padlock closed is visible near to the url.

Otherwise an open padlock symbol appear or an error shows up.

If the latter is the case, a certificate is missing ( see section below Missing Certificate).

The page content looks like this:

Available Services:

- ActivityExtService [\[wsdl\]](#)
- BVServer [\[wsdl\]](#)
- BVServerReservations [\[wsdl\]](#)
- BVServerUserInterface [\[wsdl\]](#)
- IBookings [\[wsdl\]](#)
- NameProvider [\[wsdl\]](#)
- OLBooking [\[wsdl\]](#)

## Missing Certificate

### What a security certificate is

When you go to a site that uses HTTPS (connection security), the website's server uses a certificate to prove the website's identity to browsers, like Chrome. Anyone can create a certificate claiming to be whatever website they want.

To help you stay on safe on the web, a webbrowser requires websites to use certificates from trusted organizations.

---

## Self-signed certificate

For testing purposes the developer can create his own certificate:

Open Leisure Console in deployment directory of:

- <Bellavita\_ROOT>\ (in casse of a bellavita env.)

Run the following commands:

```
keytool -genkeypair -alias signatureKey22 -keyalg "RSA" -keysize 2048 -keystore ..\leisure\ini\bellavita.keystore -storepass VBellavIta_1909506874670161525 -dname "CN=%COMPUTERNAME%, OU=Suite 8 Web Services, O=Oracle Corporation, L=Redwood City, ST=California, C=US"
```

```
keytool -genkeypair -alias signatureKey22 -keyalg "RSA" -keysize 2048 -keystore ..\bv-service\ini\bellavita.keystore -storepass VBellavIta_1909506874670161525 -dname "CN=%COMPUTERNAME%, OU=Suite 8 Web Services, O=Oracle Corporation, L=Redwood City, ST=California, C=US"
```

Restart the service.

## Authorized certificate

A authorized certificate can be created by an official vendor (Thawte, Symantec, etc.). Pls. follow the instructions after receiving the certificate on how to install.

The certificate needs to be imported in the bellavita.keystore.

Open Bellavita Console in deployment directory of:

- <Bellavita\_ROOT>\ (in casse of a bellavita env.)

Run the following commands:

Assume you received certificate for root and ca and cn itself:

```
cert.cer.txt, Symantec_Private_SSL_SHA256_CA.txt,  
Symantec_Private_SSL_SHA256_Root.txt
```

Run the following commands:

```
keytool -importcert -alias signatureKey2 -trustcacerts -file ..\tools\certs\cert.cer.txt -keystore ..\bv-service\ini\bellavita.keystore -storepass VBellavIta_1909506874670161525
```

```
keytool -import -trustcacerts -alias signatureKey2_CA -keystore ..\bv-service\ini\bellavita.keystore -file ..\tools\certs\Symantec_Private_SSL_SHA256_CA.txt -storepass VBellavIta_19095068746701615
```

```
keytool -import -trustcacerts -alias signatureKey2_ROOT -keystore ..\leisure\ini\bellavita.keystore -file
```

---

```
.\tools\certs\Symantec_Private_SSL_SHA256_Root.txt -storepass  
VBellavita_1909506874670161525
```



---

---

# Appendix A Secure Deployment Checklist

The following security checklist includes guidelines that help secure your database:

- Install only what is required.
- Lock and expire default user accounts.
- Enforce password management.
- Enable data dictionary protection.
- Practice the principle of least privilege.
  - Grant necessary privileges only.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
- Enforce access controls effectively and authenticate clients stringently.
- Restrict network access.
- Apply all security patches and workarounds.
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Protect the Oracle listener.
  - Monitor listener activity.
  - Monitor who accesses your systems.
  - Check network IP addresses.
  - Encrypt network traffic.
  - Harden the operating system.