Oracle FLEXCUBE Direct Banking

Apache HTTP and Weblogic User Manual
Release 12.0.2.0.0

Part No. E50108-01

September 2013

ORACLE®

Apache HTTP and Weblogic User Manual
September 2013

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India
Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax:+91 22 6718 3001
www.oracle.com/financialservices/
Copyright © 2008, 2013, Oracle and/or its affiliates. All rights reserved.

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

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 failsafe, 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.

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.

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

1. Preface
1.1. Intended Audience 5
1.2. Documentation Accessibility 5
1.3. Access to OFSS Support 5
1.4. Structure 5
1.5. Related Information Sources 5
2. Abbreviations 5
3. Overview 9
3.1. Pre-requisites 10
4. Deployment Architecture Introduction 11
5. Configuring the communication between Apache HTTP server & Weblogic 13
5.1. Prerequisite: 14
5.2. Configuration: 15
6. Configuring SSL 17
6.1. Prerequisite: 18
6.2. Overview 19
6.3. Configure 1-way SSL from Browser to HTTP server 20
6.4. Configure SSL between Apache HTTP server & Weblogic Application server 21
7. Appendix 26
7.1. Keystore management 27
7.2. Sample file httpd.conf 28
7.3. Sample file httpd-ssl.conf 29
7.4. Sample file weblogic.conf 30
7.5. Configuration files used in the document 31

1. Preface

1.1. Intended Audience

This document is primarily targeted at

- Oracle FLEXCUBE Direct Banking Development Teams
- Oracle FLEXCUBE Direct Banking Implementation Teams
- Oracle FLEXCUBE Direct Banking Implementation Partners

1.2. Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

1.3. Access to OFSS Support

https://flexsupp.oracle.com/

1.4. Structure

This document consists of the following chapter

Chapter 4, "Deployment Architecture Introduction"

This chapter discusses the setup architecture.

Chapter 5, "Configure communication between Apache HTTP Server & Weblogic"

This chapter discusses configuration of insecure communication between Apache HTTP server and Weblogic 11g Application server/

Chapter 6, "Configuring SSL"

This chapter discusses how to configure secured (SSL) communication between browser/Apache HTTP server and Apache HTTP server/Weblogic 11g Application servers.

Chapter 7, "Appendix"

This chapter provides appendix information on key management & excerpt from sample config files.

1.5. Related Information Sources

For more information on Oracle FLEXCUBE Direct Banking Release 12.0.2.0.0, refer to the following documents:

- Oracle FLEXCUBE Direct Banking Licensing Guide

2.Abbreviations

FCDB	Oracle FLEXCUBE Direct Banking
HTTP	Hyper Text Transfer Protocol
SSL	Secure Socket Layer
HTTPS	HTTP Secure
J2EE	Java 2 Enterprise Edition
WL	Weblogic 11g

3.Overview

This document discusses following topics

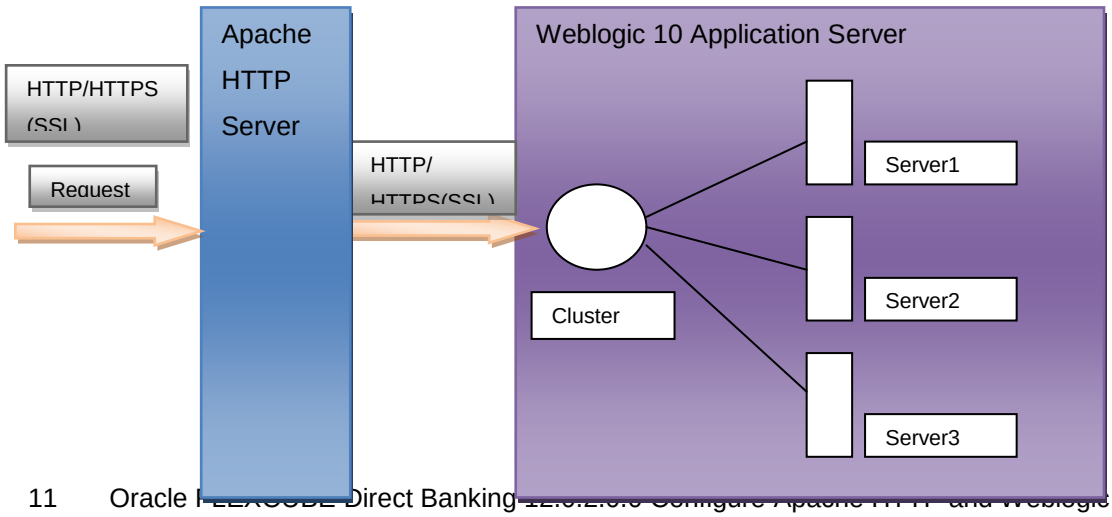
- Configuring the insecure communication between Apache HTTP server and Weblogic 11g Application server.
- Enabling SSL communication between browser & Apache HTTP server.
- Enabling SSL communication between Apache HTTP server & Weblogic 11g Application server.

3.1.Pre-requisites

1. Application should be successfully deployed on Weblogic11g Server/Cluster.
2. Apache HTTP Server 2.2 must be installed.
3. Oracle FLEXCUBE Direct Banking application is successfully installed using Oracle FCDB Installer.

4.Deployement Architecture Introduction

Using the Apache Web Server 2.2 to delegate the requests to the Weblogic cluster the architecture becomes similar to what is depicted in the following diagram.



Thus the changes done at the Managed Server does not affect the user requests. For example, multiple servers can be added / removed from the cluster or any particular server can be shut down for maintenance purposes without affecting the user request/response time.

5.Configuring the communication between Apache HTTP server & Weblogic

This chapter discusses about the configuration needed to enable communication between Apache HTTP server & Weblogic. After the communication is established you can secure the communication by enabling SSL on this path (this is discussed in '*Chapter 5, Configuring SSL*').

5.1.Prerequisite:

1. Required Web-Application is up & running on Weblogic. The link to the web-application (on Weblogic) has been tested.
2. Apache HTTP server is up & running.

5.2.Configuration:

Apache Web Server uses application-server vendor specific module/plug-in (provided by the vendor) to forward the request to the Application Server. This module/plug-in should be available to the Apache HTTP server & should be loaded. HTTP server should be configured on how to & where to forward the request. Following steps provides the said configurations:

1) Edit `httpd.conf` file. Update/add following configuration to update listen-port for http traffic.

```
Listen 80
```

Locate the module/plug-in provided by weblogic for your setup. The module is System/OS specific. Please refer to weblogic document to identify the appropriate module for your setup.

E.g.: `D:\bea\wlserver_10.0\server\plugin\win\32\mod_wl_22.so`

2) Copy the module from weblogic installed directory to apache web server's module directory:

From : `D:\bea\wlserver_10.0\server\plugin\win\32\mod_wl_22.so`

To : `D:\Program Files\ApacheHTTPServer\modules`

3) Once the module has been copied, direct the Apache HTTP server to load the module. To do this, add/uncomment following directive in the `httpd.conf` file :

```
LoadModule weblogic module modules/mod wl 22.so
```

4) Now that the module has been configured, HTTP server should be provided information on where to forward the request. All this information is generally put in a separate config file & this config file is included in Apache HTTP server's config file `httpd.conf`. To do this create a conf file '`weblogic.conf`' in conf/extra/ and add the include directive to `httpd.conf` file

```
<IfModule mod_weblogic.c>
       Include conf/extra/weblogic.conf
</IfModule>
```

5) Now edit conf file '`weblogic.conf`' to include following configuration

Property in 'weblogic.conf'	Value	Description
SetHandler weblogic-handler		Specifies the handle for the Apache HTTP Server plug-in module.
WeblogicHost		Specifies host of weblogic single server on which the web-app is available.
WeblogicPort		Specifies normal port of weblogic single server on which the web-app is available.
WebLogicCluster	App-serverHost1:port, App-serverHost2:port	Specifies weblogic cluster details
MatchExpression	Eg: /context/*	Specify the filename pattern while proxying by MIME type.
SecureProxy	OFF	Set this parameter to OFF Since this is not a secure communication setup. To configure secure communication read '*Chapter 5 Configuring SSL*'.
Debug	WARN,ERROR,ALL	Specifies debug level for WL plugin. Set to ALL during setup & set to ERROR once setup is verified.
WLLogFile		Location on file-system to log WL plugin debugs information.

Note: Above properties are minimal configurations needed to enable communication between Apache HTTP server & Weblogic application server. Please refer to Apache HTTP server/Weblogic documentation for additional properties.

6) Restart the HTTP Server & verify the communication by accessing the web application with new URL
http://<web-server host>: http-server listen port/context

6.Configuring SSL

6.1.Prerequisite:

1) Insecure communication between Apache HTTP server & Weblogic application server has been established as per *'Chapter 4 Configure communication between Apache HTTP server & Weblogic'*.
2) Private Key, server identity & server CA certificates for HTTP server are available.
3) Private Key, server identity & server CA certificates for application server are available.

6.2.Overview

SSL configuration can be enabled for two paths

1) Browser to HTTP server: This path can further be:
    a. 1 Way: This is when only server proves authenticity.
    b. 2 Way: Both server & client has to prove authenticity. This setup is not included in this document.
2) HTTP server to Appserver

6.3. Configure 1-way SSL from Browser to HTTP server

1) To enable SSL, apache web server should be directed to load SSL module. To load the SSL module add/uncomment following directive in `httpd.conf`:

```
LoadModule ssl_module modules/mod_ssl.so
```

2) Once SSL module is loaded, further SSL configuration is generally added to another config file '`conf/extra/httpd-ssl.conf`' & the file is included in `httpd.conf`. To do this edit `httpd.conf` and add/uncomment following include directive

```
Include conf/extra/httpd-ssl.conf
```

3) Now create/edit the file `conf/extra/httpd-ssl.conf` to add/uncomment following SSL configuration

Property	Value	Comment
`Listen`	`443`	HTTPS port
`SSLEngine`	`On`	Property to enable/disable SSL
`SSLVerifyClient`	`None`	This should be '`None`' since this is 1 Way SSL setup
`SSLCertificateFile`		Path on filesystem to locate HTTP server identity certificate.
`SSLCertificateKeyFile`		Path on filesystem to locate HTTP server private key.
`SSLCACertificateFile`		Path on filesystem to locate HTTP server CA certificate.

Note: Above properties are minimal configurations needed to enable 1 way SSL between browser & HTTP server. Please refer to Apache HTTP server documentation for additional properties.

4) ***Note**: Please set the file permissions for certificate and key file in such a way that only authorized users have access to it on the operating system.*

   One way SSL configuration is complete. Restart the HTTP Server & verify the same by using https://<host>:<SSL Listen port>/context

6.4 Configure SSL between Apache HTTP server & Weblogic Application server.

Before starting to configure SSL communication between Apache HTTP server & Weblogic application server, ensure following has been completed:

1) Insecure communication between Apache HTTP server & Weblogic application has been established. If not, please follow '*Chapter 4 Configure communication between apache HTTP server & Weblogic'*.
2) Secure (SSL) communication between browser & Apache HTTP server has been established. If not, please follow '*Chapter 5 SSL Configuration, Section 5.3*'.

SSL communication between Apache HTTP server & Weblogic application server will be configured in two phases:

Step 1: Configure SSL in Weblogic application server/cluster

Step 2: Configure SSL in Apache HTTP server

Step 1: Configure SSL in weblogic application server/cluster

This section gives detail about how to configure the BEA Weblogic 11g Server for SSL.

Perform following steps on Admin console of Weblogic Server for SSL configuration.

1. Go to the Admin console of Weblogic (*Figure 6.4.1*)

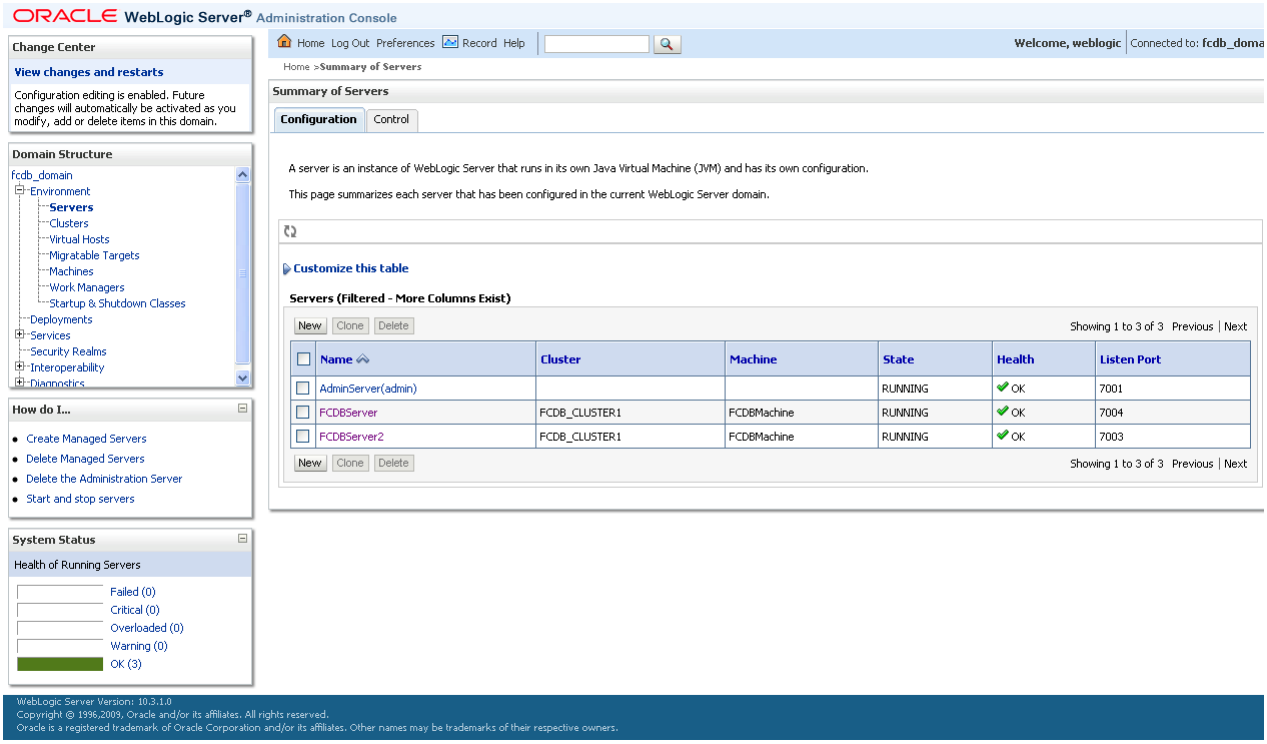


Figure 6.4.1

2. Click on ‘Environment’ -> ‘Servers’ from ‘Domain Structures’
3. Select one server from the list which is a part of the clustered deployment.
4. Go to `‘General Tab’` of that server
5. Click on `‘Lock & Edit’` to perform changes (*Figure 64.2*).

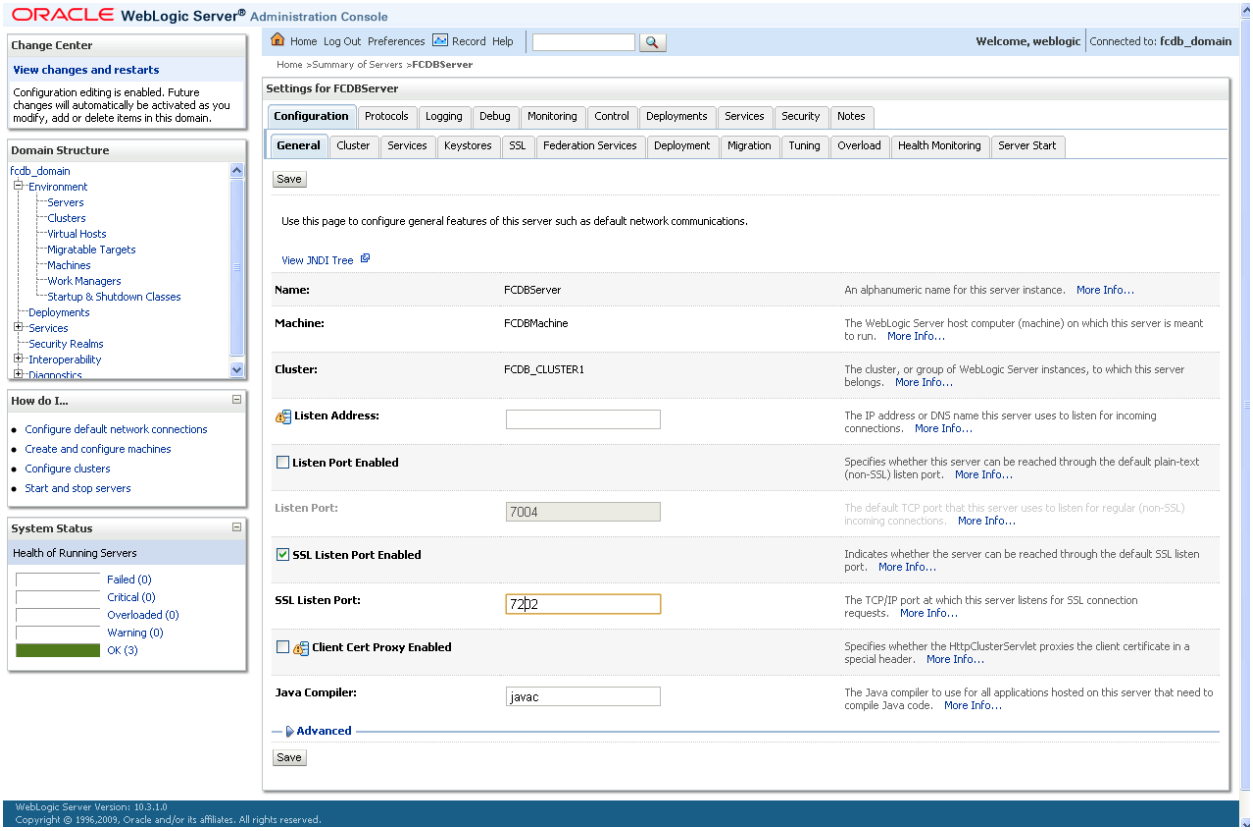


Figure 6.4.2

6. Select check box for – 'SSL Listen Port Enabled'.
7. Disable the check box for – 'Listen Port Enabled'. This ensures that the communication path to this server is only through SSL and normal HTTP listen port is disabled.
8. Provide the port number for SSL.
9. Click on 'Activate Changes' after saving it.
10. Click on 'Keystores' (*Figure 6.4.3*).

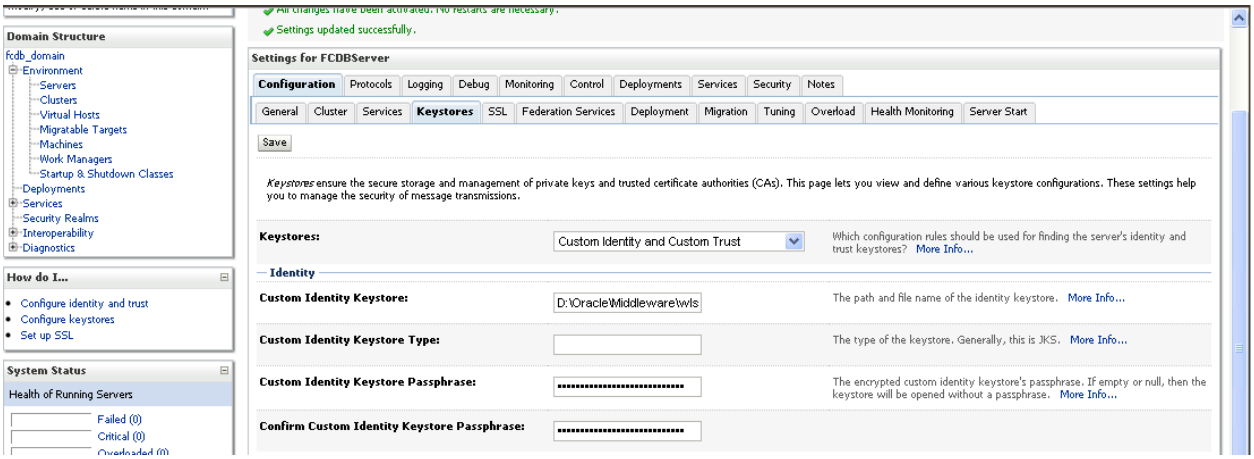


Figure 6.4.3

11. Select the 'Custom Identity and Custom Trust' for 'Keystore' from the drop down.
12. Specify the keystore location & passphrase for identity and trust.
13. Click on 'Save' and 'Activate Changes'.
14. Click on 'SSL' Tab (*Figure 6.4.4*).

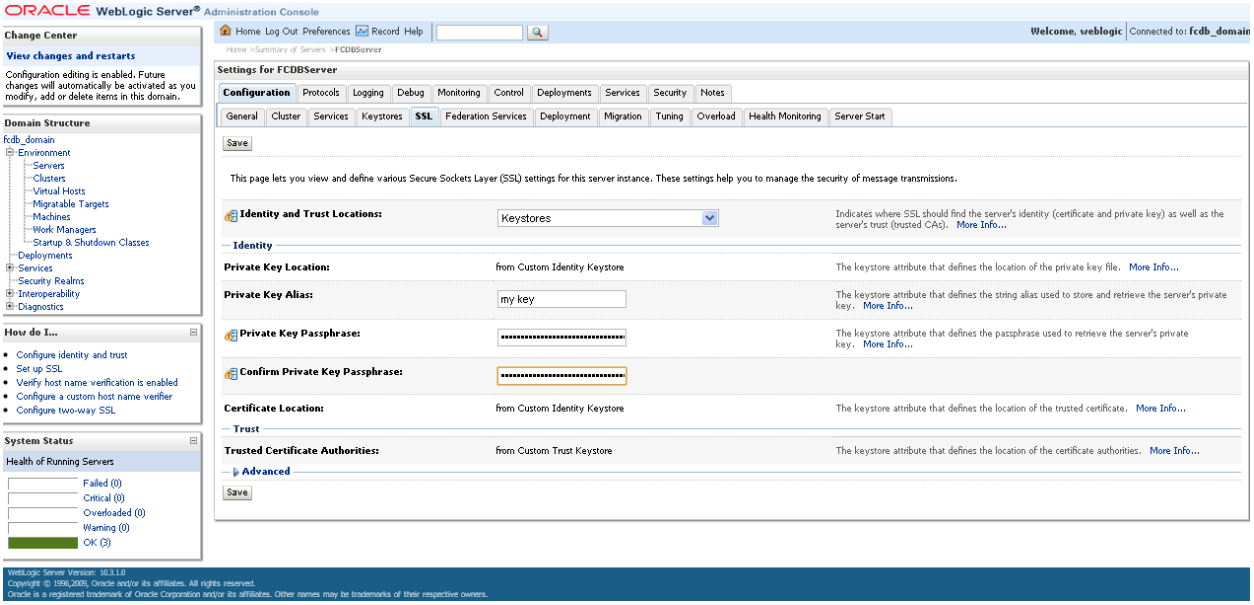


Figure 6.4.4

15. For 'Identity and Trust Locations' dropdown select 'KeyStores'
16. Enter value for 'Private Key alias' and 'Private Key Passphrase'.
17. Click on 'Save' and 'Activate Changes'.
18. If cluster perform the above steps for all managed server in the cluster.
19. Restart.

Step 2: Configure SSL in weblogic application server/cluster

The Weblogic application server has been configured for SSL. Now the Apache HTTP server should be configured for SSL between HTTP server & application server.

Please follow following steps:

1) Edit WL-plugin SSL config file `'conf/extra/weblogic.conf'` to update/add following properties:

Property in 'weblogic.conf'	**Value**	**Description**
`WeblogicPort`	SSL port number	Update the normal port with SSL port of the weblogic single server on which the web-app is available. This should be specified only if single server is available & not a cluster.
`WebLogicCluster`	App-serverHost1:SSLport, App-serverHost2:SSLport	Specifies weblogic cluster details
`SecureProxy`	`ON`	Set this parameter to `ON` since this is Secured communication.
`TrustedCAFile`		Path on filesystem to locate application server CA certificate.

Note: Above properties are minimal configurations needed to enable SSL communication between apache web server & weblogic application server. Please refer to apache/weblogic documentation for additional properties.

The SSL communication has been configured. Verify the same by accessing the web-application link.

7.Appendix

7.1 Keystore management

There are two key stores to be specified. One is identity keystore – which stores the private key of the server, the identity of the server.

The other keystore is Trust Keystore – which stores the Trusted CA Certificates from CA like Verisign. The digital certificate obtained from CA should be kept in this keystore.
These keystores can be managed using keytool utility.

The Certificate obtained from CA can be imported into Keystore using following command:

7.2 Sample file httpd.conf

Excerpt from sample `httpd.conf`

```
#http listen port
Listen 80

#config file containing SSL configuration.
Include conf/extra/httpd-ssl.conf

#Weblogic plugin/Module
LoadModule weblogic_module modules/mod_wl_22.so
```

7.3 Sample file httpd-ssl.conf

Excerpt from sample httpd-ssl.conf

```
# Port-number to listen for HTTPS protocol.
Listen 443

# This directive toggles the usage of the SSL/TLS Protocol Engine.
SSLEngine On

# HTTP server identity certificate to use
SSLCertificateFile "D:\FCDB\keys\serverSSLCertificate.cer"

# HTTP server private key to use.
SSLCertificateKeyFile "D:\FCDB\keys\unsec_priv_key.key"
```

***Note**: Please set the file permissions for certificate and key files in such a way that only authorized users have access to it on the operating system.*

7.4. Sample file weblogic.conf

Excerpt from sample httpd-ssl.conf

```
# Specifies the name of the handler for this module.
SetHandler weblogic-handler

#welogic cluster information with SSL port
WebLogicCluster IFLMUD5DLGV4G:7202,IFLMUD5DLGV4G:7303

MatchExpression /B001/*

# Set the debug level for the server logs
Debug ERROR

# Log file for the Weblogic plugin logs
WLLogFile "D:\FCDBLogs\WLLOGS.log"

# Set this parameter to ON to enable the use of the SSL protocol for all
```

7.5 Configuration files used in the document .

Apache HTTP Server configuration files used

Config File	Location w.r.t to Apache Install Dir	Description
`httpd.conf`	conf/	Main config file for Apache HTTP Server.
`httpd-ssl.conf`	conf/extra/	Config file to provide SSL properties. This file is included in `httpd.conf`
`Weblogic.conf`	conf/extra/	Config file to provide weblogic plug-in properties. This file is included in `httpd.conf`