

Oracle® Insurance Policy Administration

Security Guide

Version 9.4.1.0

Documentation Part Number: E23637_01

October 2011

Copyright © 2009, 2011, 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, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software 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.

Where an Oracle offering includes third party content or software, we may be required to include related notices. For information on third party notices and the software and related documentation in connection with which they need to be included, please contact the attorney from the Development and Strategic Initiatives Legal Group that supports the development team for the Oracle offering. Contact information can be found on the Attorney Contact Chart.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Software License and Service Agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Table of Contents

Overview	4
System Deployment	5
Network Security in OIPA environment	5
OIPA use of Coherence	6
Configuring SSL	7
SSL in <i>WebLogic</i>	7
SSL in Apache Web Server 2	7
SSL in JBoss 4.2	8
SSL in JBoss 4.2 – Alternate Procedure	8
SSL in WebSphere	9
User Authentication	10
User Management	12
User Registration	12
User Privileges and Group-Based Access Control	12
Using Cookies in OIPA application	14
Additional Sources of Security Information	15

OVERVIEW

Security planning is a critical step to help protect your company's valuable data and ensure that information is not compromised. Established security policies and goals should guide the security plan your organization executes to secure its systems.

The Oracle Insurance Policy Administration (OIPA) system stores sensitive data and requires security measures to be taken. Security policies should align with those already established at your organization, or new ones should be established if they are not already defined.

This document provides guidelines for securing an OIPA installation, including the configuration and installation steps needed to meet security goals. Details on the on the types of security features and services that are available to detect and prevent a potential security breach are provided. This encompasses secure system deployment, protection of sensitive data, reliability and availability of the application, authentication and authorization mechanisms.

You may use this document to develop your organization's security policies and practices in the context of OIPA. It is critical that an organization set security standards and properly implement them. The development and review of security documentation, an evaluation of business requirements, and the configuration and validation of available security measures and services should all be performed.

SYSTEM DEPLOYMENT

NETWORK SECURITY IN OIPA ENVIRONMENT

When deploying OIPA onto a network there are many security issues to take into consideration, especially the use of firewall and VPN technologies. A firewall will permit or deny network permissions based on configured rules, to protect the internal network from unauthorized access while permitting legitimate communications.

Firewalls perform the following functions in a typical OIPA environment:

- Guard the company Intranet from unauthorized outside access.
- Separate Intranet users accessing the OIPA system from internal subnetworks where critical corporate information and services reside.
- Protect from IP spoofing and routing threats.
- Prohibit unauthorized users from accessing protected networks and control access to restricted services.

The OIPA user interface is browser-based and allows home-office users to access the application services. It is recommended that the users access the application from within the company network, secured behind the outside firewall. Virtual Private Network (VPN) technology should be used to allow employees working remotely to access the OIPA application. A VPN tunnels outside traffic through the firewall, placing outside clients virtually inside the firewall.

It may be required to provide access to the OIPA web services for external clients that are not allowed inside the company firewall. In that case, the web services must be accessed only through HTTP secured with SSL. OIPA web services support WS-Security standards, enabling web service user authentication using OIPA user accounts.

Please make sure that the firewalls used to secure an OIPA environment support the HTTP 1.1 protocol; it enables browser cookies and inline data compression for improved performance.

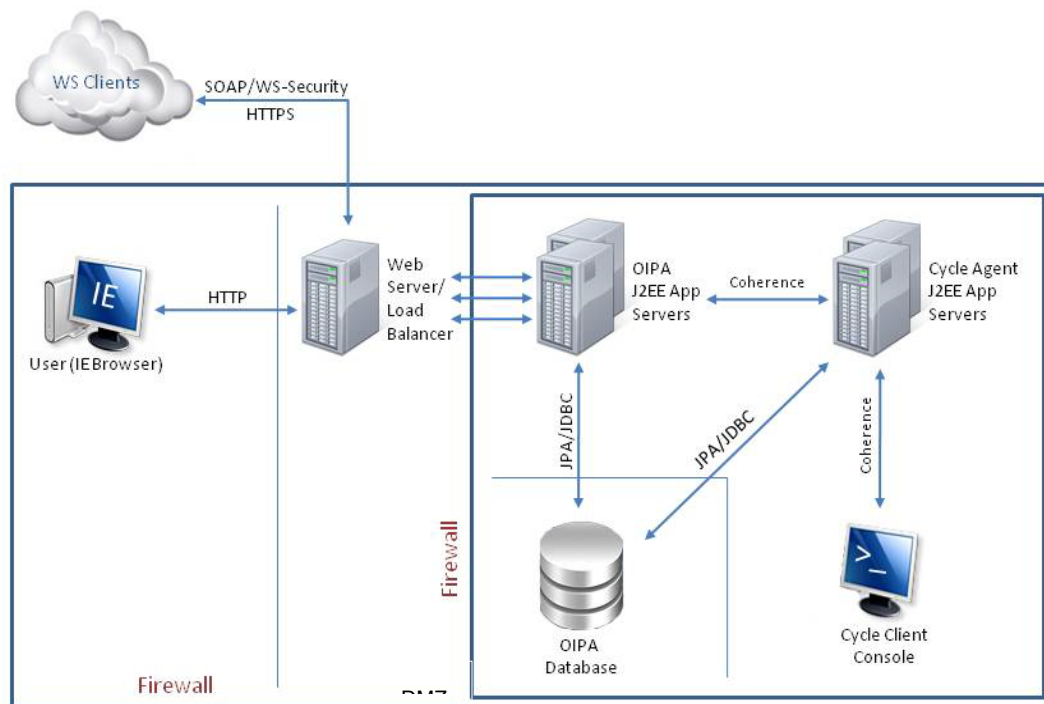


Figure 1. Firewalls in the OIPA environment

A typical OIPA environment usually has the following security zones:

- **Internet** - External web service clients may come from outside of the company network.
- **Intranet** - A company network separated by the external firewall that gives home users access to the OIPA user interface. This is also where OIPA web servers and load balancers may be placed. Alternatively, for additional protection, web and load balancing servers may be placed in a separate demilitarized zone (DMZ) where external and internal clients first interact with the OIPA environment.
- **OIPA application server and database zone** - OIPA application servers, including Cycle Agent servers, database servers and possibly authentication servers (for example, if a customer chooses to implement a single sign-on using LDAP servers) reside in this zone. Also, access to the database that holds critical client information must be secured, with access restricted to system and database administrators only.

OIPA USE OF COHERENCE

The OIPA application uses the Oracle Coherence distributed cache solution to minimize database traffic. In addition to using the cache, OIPA Cycle uses the Coherence Processing Pattern as a computing grid to allow task distribution among all OIPA Cycle Agents. Batch processing on the grid is initiated through the Coherence communication protocol by the Cycle Client. Even though all parties involved in Coherence communications are

located behind the firewall in the OIPA application server and database zone, it is important nevertheless to secure Coherence according to the Coherence User guide.

Oracle Coherence also provides workload management to distribute tasks across a computer cluster or other resources. This enables Cycle to achieve optimal resource utilization, maximize throughput, minimize response time and avoid overload, and also to avoid having a single point of failure for tasks processed in the grid. Along with the security provided by the firewalls, Coherence workload management provides these additional security features:

- TCP port exposure is limited to a single port that allows easier port security and firewall configuration.
- A virtual IP address hides actual physical IP addresses of the OIPA application servers.
- The suspect protocol protects against Denial of Service (DoS) attacks by detecting and barring “rogue” clients that attempt to overuse server resources.

Configuring SSL

The Secure Sockets Layer (SSL) protocol provides communication security by encrypting traffic across a network in a way designed to prevent eavesdropping and tampering. It uses asymmetric cryptography for privacy and a keyed message authentication code for message reliability. Setting up an SSL-secured connection requires a digital certificate issued by a trusted certificate authority. Self-signed digital certificates should only be used for internal testing.

Any entry points for OIPA web services that are consumed by external third party clients should be secured with SSL. Also, organization standards may require securing communication between browser-based clients and web servers in the demilitarized zone that host the front end of the OIPA system.

Setting up a web server to use SSL-secured HTTP protocol (HTTPS) instead of unsecure HTTP is server-specific. The information below should help locate information to navigate through the configuration process.

SSL in WebLogic

WebLogic Application Server supports SSL 3.0 and Transport Layer Security (TLS) 1.0 specifications. WebLogic does not support SSL version 2.0 and below.

For information on how to configure SSL in WebLogic please visit the following URLs:

http://download.oracle.com/docs/cd/E17904_01/web.1111/e13707/ssl.htm#SECMG384

<http://download.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html>

http://download.oracle.com/docs/cd/E17904_01/apirefs.1111/e13952/taskhelp/security/ConfigureKeystoresAndSSL.html

SSL in Apache Web Server 2

An option is to deploy Apache Web Server in front of the application servers. It helps with security and performance and may also perform load balancing. Please visit the following URL for information on how to configure Apache Web Server 2 with SSL

<http://httpd.apache.org/docs/2.0/ssl/>

<http://wiki.apache.org/tomcat/FAQ/Connectors>

SSL in JBoss 4.2

The following steps cover the SSL configuration process for the JBoss application server. It is assumed that JBoss Admin Console is not used for administration.

1. Create a certificate keystore:

1. Go to the bin directory of the JDK.
2. Run this command:

```
keytool -genkey -alias tomcat -keyalg RSA
```

(Note: this will create a .keystore certificate in the user profile).

3. Enter all input details and save it in notepad.
2. Enable the SSL setting for port number 8443 in server.xml in the default directory in JBoss.

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" />
```

3. Disable unsecure HTTP port number (8080 or 80) in server.xml by commenting out its Connector entry (for example):

```
<!--
<Connector port="8080" address="{jboss.bind.address}"
    maxThreads="250" maxHttpHeaderSize="8192"
    emptySessionPath="true" protocol="HTTP/1.1"
    enableLookups="false" redirectPort="8443" acceptCount="100"
    connectionTimeout="20000" disableUploadTimeout="true" />
-->
```

4. Start the server instance.
5. Make sure that the URL to access the OIPA application specifies the HTTPS protocol and correct port number:

<https://machinename:8443/PASJava>

SSL in JBoss 4.2 – Alternate Procedure

1. Generate the keystore with the following command (specifying NAME_OF_KEYSTORE and NUMBER_OF_DAYS according to local requirements).

```
keytool -genkey -alias tomcat -keyalg RSA -keystore NAME_OF_KEYSTORE -
    validity NUMBER_OF_DAYS
```

2. Copy the keystore file into the directory: jboss/server/<NAME>/conf/
3. Edit server.xml in jboss/server/<NAME>/deploy/jboss-web.deployer/. The SSL-connector should be configured like this:

```
<!--
SSL/TLS Connector configuration using the admin dev1 guide keystore
```


-->

```
<Connector port="THE_PORT_YOU_LIKE" address="${jboss.bind.address}"
    maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
    emptySessionPath="true"
    scheme="https" secure="true" clientAuth="false"
    keystoreFile="${jboss.server.home.dir}/conf/THE_KEYSTORE_NAME"
    keystorePass="PASSWORD_FOR_THE_KEYSTORE" sslProtocol = "TLS" />

<Connector port="THE_PORT_YOU_LIKE" protocol="HTTP/1.1"
    SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true" clientAuth="false"
    strategy="ms" address="${jboss.bind.address}"
    keystoreFile="${jboss.server.home.dir}/conf/THE_KEYSTORE_NAME"
    keystorePass="PASSWORD_FOR_THE_KEYSTORE"
    truststoreFile="${jboss.server.home.dir}/conf/THE_KEYSTORE_NAME"
    truststorePass="PASSWORD_FOR_THE_KEYSTORE" sslProtocol="TLS"/>
```

4. Disable unsecure HTTP port number (8080 or 80) in `server.xml` by commenting out its Connector entry.
5. Start the server instance.
6. Make sure that the URL to access the OIPA application specifies the HTTPS protocol and correct port number.

For more information please visit the following URL:

<http://docs.jboss.org/jbossweb/3.0.x/ssl-howto.html>

SSL in WebSphere

Starting with version 6 of WebSphere Application Server everything is done from the admin console that includes a complete overview of the SSL management capabilities.

For more information about managing SSL in WebSphere please visit the following URL

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/cs_ec_sslconfigs.html

USER AUTHENTICATION

The OIPA application provides an out-of-the box user authentication mechanism as well as an ability to implement alternative authentication models like a Single Sign-On (SSO) authentication through the OIPA extensions. If the system is implemented with SSO, additional measures need to be taken to properly secure the authentication infrastructure. Depending on the implementation chosen, either an authentication server should be placed within the OIPA application server and database zone, or the call to an authentication service needs to be made via a secure connection.

Out-of-the box OIPA user authentication is performed both for interactive users using Internet browsers to access the system, and for incoming web service calls. Interactive users are prompted on the application's login page to provide a username and password to authenticate to the server. Web services are protected with WS-Security, which requires incoming web service calls (which must be transmitted on a secure (SSL) connection) to carry a security header with a user name and password.

Both web service and interactive user authentication are implemented through the same authentication service provided by the business logic tier of the OIPA application. The authentication service retrieves a matching user record from the OIPA database that contains basic user information and a secure digest of a password. The password digest is then compared to the digest of the incoming password and an authentication decision is made based on the result of the comparison.

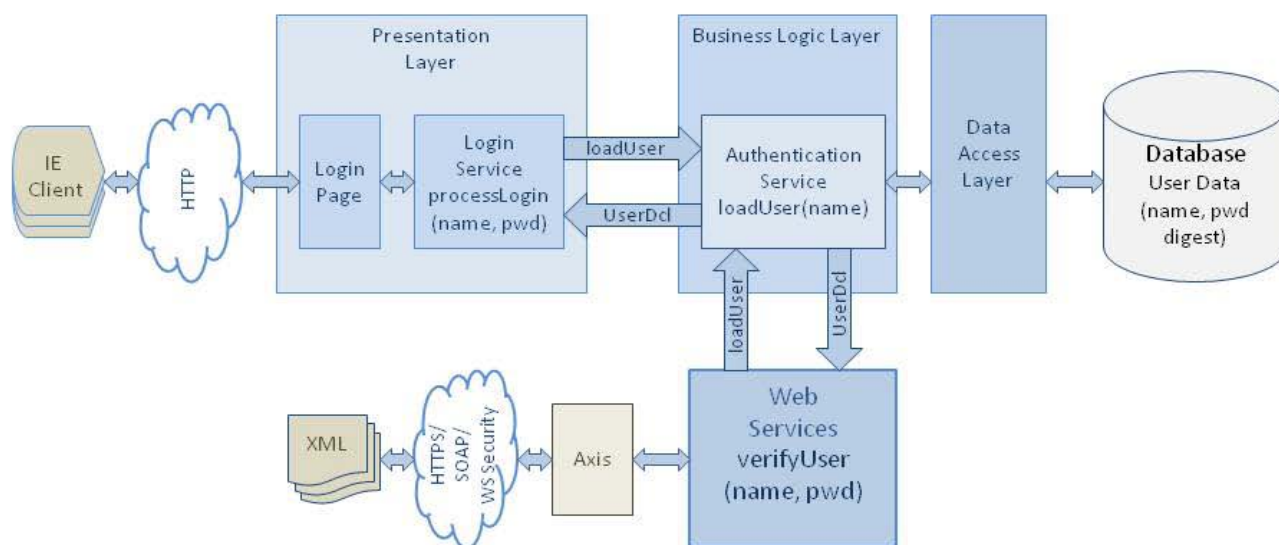


Figure 2. OIPA User Authentication

The encrypted password digest is created by the Rules Palette when a user is created. The Rules Palette allows configuring of the encryption parameters used by the encryption algorithm. The settings include the particular encryption algorithm (from the list of the supported algorithms below), and the number of iterations of the algorithm.

- SHA-256
- SHA-384
- SHA-512

The number of encryption iterations is a value between 1000 and 9999. A higher number of iterations makes the password more secure, but also requires more computation to encrypt. For more information, please refer to the associated version of the Rules Palette Help System that is located on the Oracle Technology Network.

USER MANAGEMENT

USER REGISTRATION

A user must have an existing OIPA user account identified by username and password to log into the OIPA application. An OIPA administrator uses the Rules Palette to create a new OIPA user account. The OIPA administrator's Rules Palette credentials must be associated with a security group that allows for the management of security. With the proper security rights, the administrator may use the Rules Palette to add, edit and delete OIPA user accounts. When creating a new user account, an administrator enters the following information:

- User's login name and password
- Basic information about user – first and last name, email, gender, etc.
- User's primary company
- Locale
- Security groups that user belongs to

This information is persisted in the OIPA database, with the encrypted password digest stored as discussed in the User Authentication section of this document. The user security groups determine what features of the system are available to the user.

There are no pre-existing or default user accounts in the OIPA application that need to be disabled after the system is deployed. The OIPA application user interface may be accessed only after at least one user account is created through the Rules Palette.

USER PRIVILEGES AND GROUP-BASED ACCESS CONTROL

The OIPA user privileges and access restrictions implementation is based on the role-based access control (RBAC) model. According to the model, user permissions are assigned to specific groups or roles that are created for various job functions. A user who is assigned to particular groups gains permissions through those groups to perform particular system functions. If a user is assigned to multiple groups, the user will have access to all resources authorized for all of those groups.

For example, users that are assigned to the CSR group (or role) may not be able to execute such activities as issuing a policy or paying a death benefit. A user in an Underwriter group should be able to issue a policy. A user in an administrator group is usually allowed access to all resources.

The following picture shows what application resources are protected by the OIPA security.

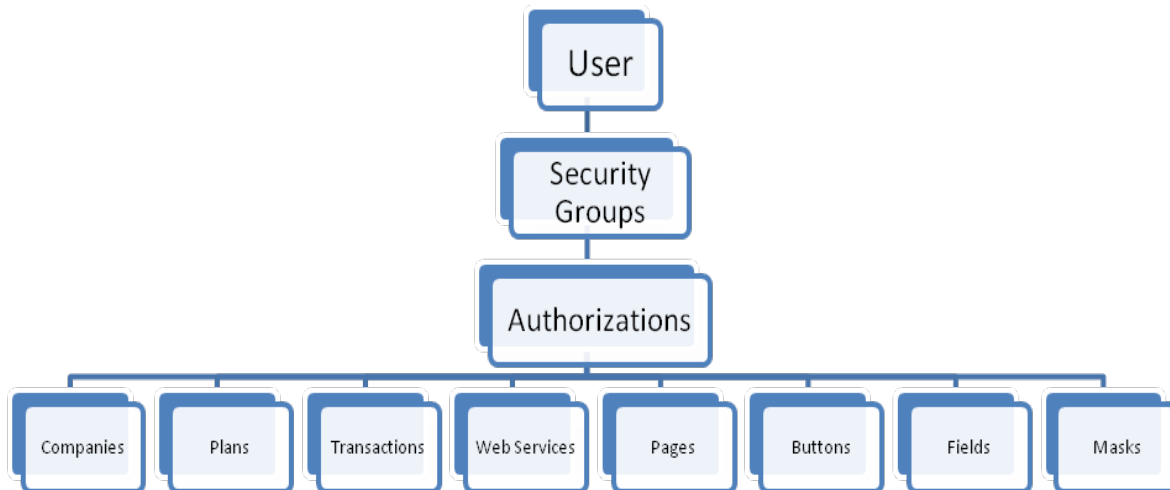


Figure 3. Hierarchy of User Authorizations

By default, a newly created user account does not have authorizations to access any of the application restricted resources. Authorizations have to be explicitly granted by an OIPA security administrator. In setting up the user groups, an administrator needs to be careful to include only the minimum set of permissions that allow users of a particular group to perform their job functions.

For more information on how to create security groups and manage user accounts please refer to the Rules Palette User guide.

USING COOKIES IN OIPA APPLICATION

The OIPA application is accessed by users through Internet Explorer. Because OIPA uses session cookies to manage user sessions, cookies must be enabled in the Internet Explorer browser. To allow using cookies in Internet Explorer, open the Privacy tab of the Internet Options dialog, then choose the Sites popup dialog and add the OIPA server address to the list of Allowed sites.

The *JSESSIONID* session cookie contains session ID generated for a user to manage data associated with the user's session. A unique session ID is generated when a user successfully logs into the OIPA application. The session ID is generated by the J2EE web server and passed to a browser as a non-persistent cookie. The browser retains it for the duration of the session, and deletes it when the user logs out or the session times out. During a session, when a browser issues a request back to the application server, it sends the session cookie in the HTTP header of the request. Requests that do not contain valid session IDs are not processed by the server.

The *ice.sessions* cookie is generated by the IceFaces library used by OIPA to implement the user interface. The cookie is a session-scope cookie and used by IceFaces to maintain IceFaces user session.

ADDITIONAL SOURCES OF SECURITY INFORMATION

In addition to securing the OIPA application, all infrastructure resources –Linux/Windows servers, J2EE application and database servers – that comprise an OIPA environment must be secured. The following list of links should be helpful while planning how to lockdown the OIPA environment.

Coherence 3.5 User Guide

<http://coherence.oracle.com/display/COH35UG/Coherence+3.5+Home>

Oracle 11g Database

http://download.oracle.com/docs/cd/E11882_01/network.112/e16543/toc.htm

http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/toc.htm

http://download.oracle.com/docs/cd/E11882_01/network.112/e10744/toc.htm

Microsoft SQL Server 2005 Database

<http://www.microsoft.com/sqlserver/2005/en/us/Security.aspx>

Microsoft SQL Server 2008 Database

<http://www.microsoft.com/sqlserver/2008/en/us/Security.aspx>

IBM DB2 9.7 Database

http://public.dhe.ibm.com/ps/products/db2/info/vr97/pdf/en_US/DB2Security-db2sece971.pdf

Microsoft Windows 2003 Server

<http://www.microsoft.com/download/en/details.aspx?id=8222>

Microsoft Windows 2008 Server

<http://www.microsoft.com/download/en/details.aspx?id=17606>

Red Hat Enterprise Linux 6

http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/

JBoss 4.2 J2EE Application Server

http://docs.jboss.org/jbossas/docs/Server_Configuration_Guide/4/html/index.html

Oracle WebLogic 10.3 J2EE Application Server

http://download.oracle.com/docs/cd/E12840_01/wls/docs103/security.html

IBM WebSphere 6.1 J2EE Application Server

http://www.ibm.com/developerworks/websphere/library/techarticles/0606_botzum/0606_botzum.html