Oracle® Hospitality Enterprise Back Office

Reporting and Analytics, Gift and Loyalty, and Labor Management

Security Guide

8.5.0

E66671-02

December 2016

ORACLE®

Oracle® Hospitality Enterprise Back Office Security Guide, Release 8.5.0

Contents

Preface

This document provides security reference and guidance for the following Oracle Hospitality Enterprise Back Office products:

- Reporting and Analytics Advanced
- Gift and Loyalty Advanced
- Labor Management

This document does not include information specific to Inventory Management.

Audience

This document is intended for the following audience:

- Datacenter administrators
- Database administrators
- Professional services

Related Documentation

Please refer to following documents:-

- Oracle Hospitality Enterprise Back Office Deployment Guide
- Oracle Hospitality Inventory Management Security Guide

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com).

Revision History

Date	Description of Change
September 2015	Initial publication.
March 2016	Added Appendix D: Installing Secure Socket Layer (SSL) Certificate in JBOSS Server.
November 2016	Added Understanding the InMotion Mobile Security Requirements.
December 2016	Added Understanding the Gift and Loyalty Security Requirements and Appendix E: Java 1.6 Prerequisite for Transport Layer Security (TLS) 1.2.

Chapter 1: Oracle Hospitality Reporting and Analytics Security Overview

This chapter provides an overview of Oracle Hospitality Enterprise Back Office Reporting and Analytics 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 Oracle Hospitality Reporting and Analytics Installation" for more information.
- **Learn about and use the Enterprise Back Office security features.** See "Implementing Oracle Hospitality Reporting and Analytics 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:

  http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of Oracle Hospitality Reporting and Analytics Security

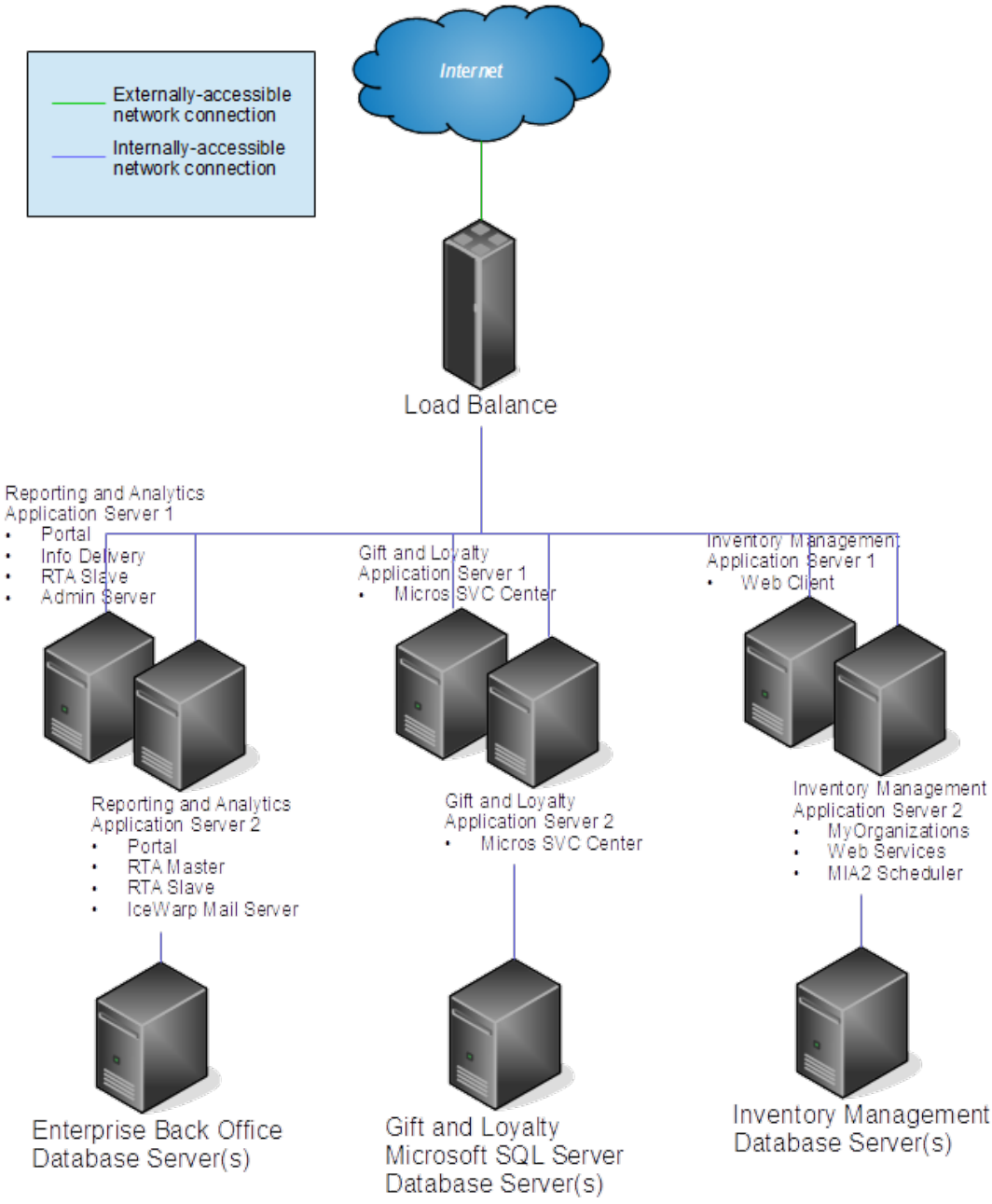


Figure 1 - Typical deployment topography of Reporting and Analytics and Gift and Loyalty.

Reporting and Analytics and Gift and Loyalty are hosted on JBoss 5.1.0 application servers. Reporting and Analytics is compatible with both Oracle RDBMS and Microsoft SQL database servers. Gift and Loyalty is certified only with Microsoft SQL database server.

The application servers and database servers are hosted inside a De-Militarized Zone (DMZ) within two firewalls. A DMZ refers to a server that is isolated by firewalls from both the Internet and the intranet, thus forming a buffer between the two. Firewalls separating DMZ zones provide two essential functions:

- Blocking any traffic types that are known to be illegal
- Providing intrusion containment, should successful intrusions take over processes or processors

Users access Enterprise Back Office applications over the HTTP protocol on a TLS-secured network. Clients typically use web browsers as their user agents, but Enterprise Back Office also supports clients who require access to the RESTful and SOAP web services that are deployed on these servers. Access to the web services is secured by basic authentication requiring a username, password, and a tenant identifier for our multi-tenant hosting centers.

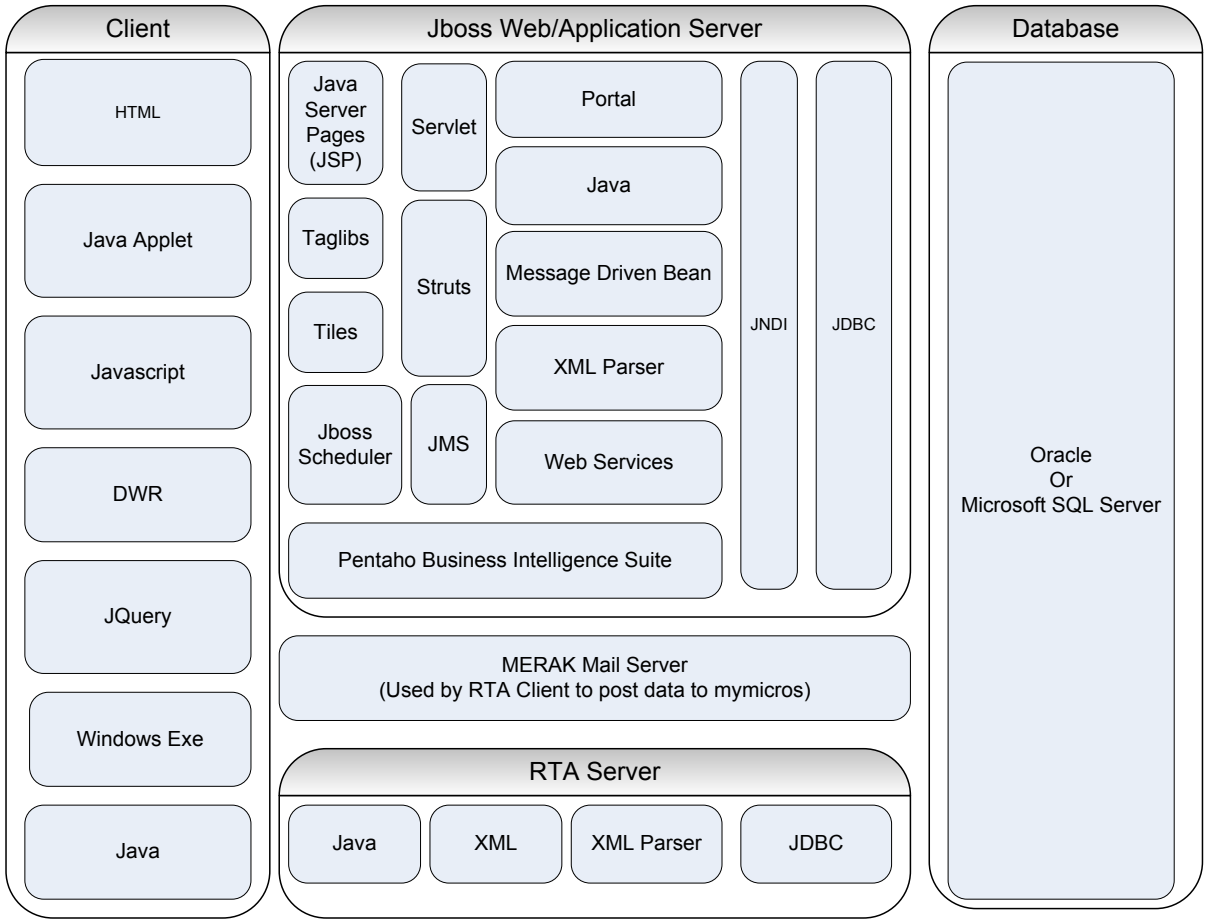


Figure 2 - Technology stack of Reporting and Analytics and Gift and Loyalty.

The figure shows the technology that is used within the browser, but does not include non-browser-based technology such as the RTA (Remote Transfer Agent) client and standalone executables such as the Timeclock application and the Advanced Scheduler that is used to communicate with the server.

The JBoss Application and web servers render the presentation layer to web based clients, provide business logic, host some scheduled jobs, and communicate with the persistent storage in either Oracle RDBMS or Microsoft SQL server.

The IceWarp Mail Server runs outside of JBoss and is responsible for holding data to be sent by the RTA client as email messages. The RTA Server is responsible for processing those messages and storing them in our database.

Users can download the RTA client agent program from the Enterprise Back Office web application and install it in the restaurant POS IT infrastructure. Each property is assigned a username and password at the point of provisioning, which is used by the RTA Client as authentication when sending messages to the SMTP server and when it attempts to consume Enterprise Back Office web service calls. The RTA Client encrypts and stores the password with the corresponding username in a locally-managed properties file.

The Oracle Hospitality Inventory Management Security Guide contains more information to security pertaining to the Inventory Management architecture.

Understanding the Reporting and Analytics Environment

Reporting and Analytics is designed to host data for multiple tenants, or organizations, within the same database. Users for a tenant are restricted to viewing data for their organization. Provisioning a new organization or tenant involves a super administrator who has view access across multiple tenants for configuring organization-wide parameters.

In a multitenant hosting center, a super administrator is a system administrator account that belongs to the “Micros” organization.

Users with the "portal" portlet can add/edit/revoke privileges for other users within the organization. Care must be taken when assigning administration privileges for the portlet.

Understanding the Gift and Loyalty Security Requirements

Gift and Loyalty must comply with the following security requirements:

- HTTPS using Transport Layer Security (TLS) 1.2.
- Certificate signed by an authorized Certificate Authority (CA).

Servers must update to Java JDK 1.6 update 121 or later to support TLS 1.2. The My Oracle Support knowledge base article 1557737.1 contains more information about support entitlements for obtaining and updating to the required Java version.

Appendix D: Installing Secure Socket Layer (SSL) Certificate in JBOSS Server contains instructions for setting up server compliance.

Appendix E: Java 1.6 Prerequisite for Transport Layer Security (TLS) 1.2 contains instructions for setting up Java JDK 1.6 for TLS 1.2.

Understanding the InMotion Mobile Security Requirements

To allow users to install and use Oracle MICROS InMotion Mobile versions made available after January 2017, application and server connections must comply with the following security requirements:

- HTTPS using Transport Layer Security (TLS) 1.2.
- Certificate signed by an authorized Certificate Authority (CA).

Servers must update to Java JDK 1.6 update 121 or later to support TLS 1.2. If your software includes a Java JDK distribution, you can update to the required JDK version. If your software does not include Java JDK, contact your Oracle representative.

Appendix D: Installing Secure Socket Layer (SSL) Certificate in JBOSS Server contains instructions for setting up server compliance.

Appendix E: Java 1.6 Prerequisite for Transport Layer Security (TLS) 1.2 contains instructions for setting up Java JDK 1.6 for TLS 1.2.

Recommended Deployment Configurations

This section describes recommended deployment configurations for Enterprise Back Office.

The product can be deployed on a single server as shown in Figure 3 or in a cluster of servers as shown in Figure 4.

- On a single server environment such as the typical installation when bundled with Simphony, the server should be protected behind a firewall.
- In a clustered mode, the application should reside in a DMZ. Sticky sessions that can be configured in a hardware load balancer should govern the requests to the application servers.

Make sure to open the following ports:

- 80
- 81
- 443
- 8080
- 9443

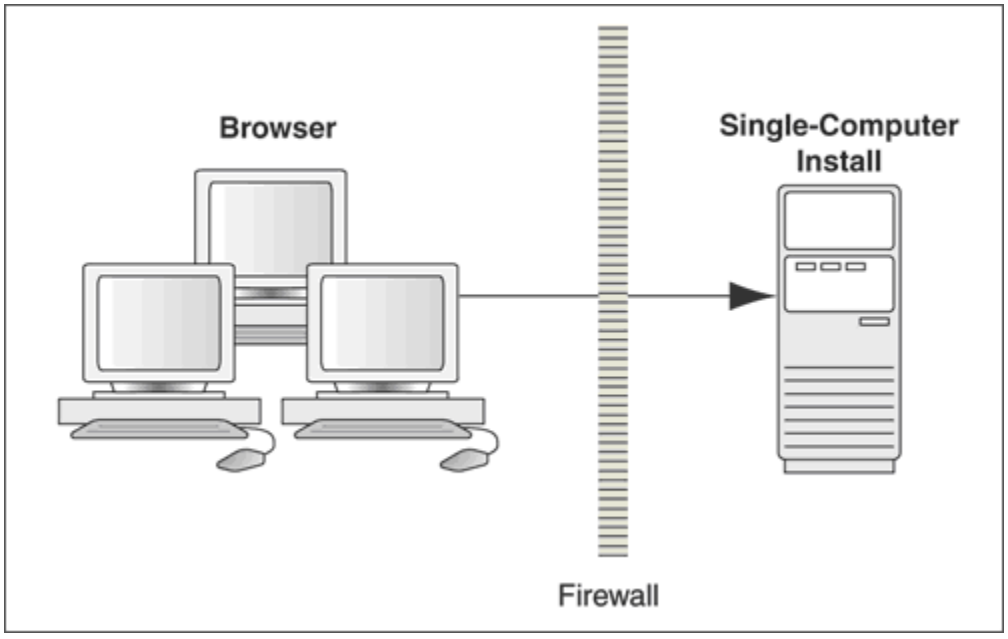


Figure 3 - Single-Computer Deployment Architecture

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 4.

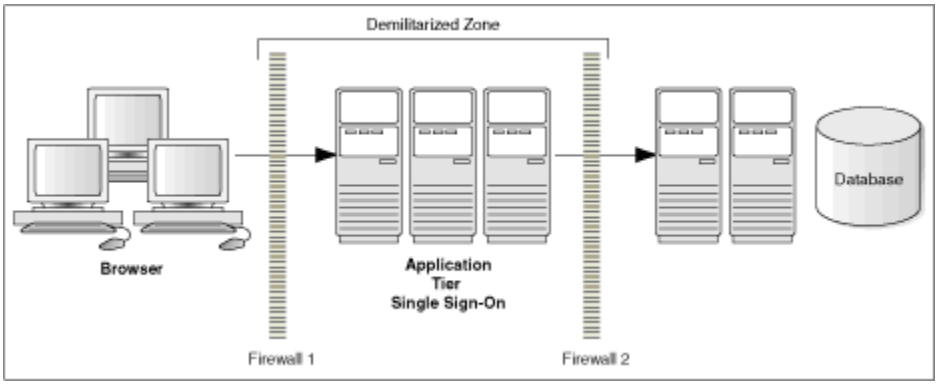


Figure 4 - Traditional DMZ View

Component Security

- The product relies on SSL (TLS) to be enabled on port 443 to enable https.
- The product relies on secure SMTP (SMTPs).
- The product relies on sFTP.

Operating System Security

See the following documents:

- Secure configuration guide for Microsoft Windows
- Secure configuration guide for Oracle Linux

Oracle Database Security

See *Oracle Database Security Guide*.

Chapter 2: Performing a Secure Enterprise Back Office Installation

For installation information, see the Oracle Hospitality Reporting and Analytics Deployment Guide.

Pre-Installation Configuration

Oracle or Microsoft SQL server database must be installed.

Installing Reporting and Analytics securely

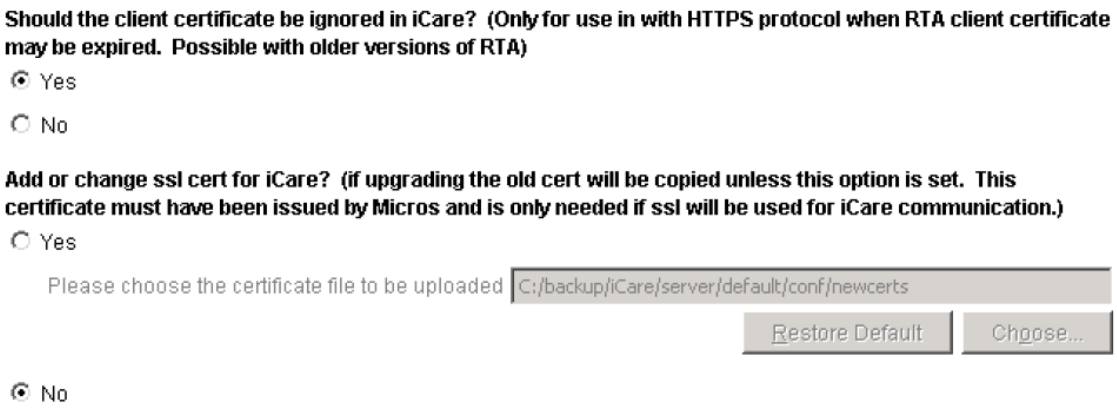
The installation requires the creation of the Microsoft Windows user group 'OHGBU_ADMIN,' which is given privileges for browsing the installation directory, editing configuration files, and reading log files. As a result, the user running the installation must have permissions for creating groups and assigning file permissions. All other users will not have access to the installation directory.

When installing the portal service, the option to force an https redirect is enabled by default. You should leave the option enabled and configure a signed certificate from a trusted authority prior to load balancing.

You can enable SSL for Java Remote Method Invocation (RMI) when installing the portal service, the master service, and the slave service. Enterprise Back Office only uses the RMI when the master service is installed. You do not need RMI for Oracle Hospitality Simphony-only installations.

For more information about SSL for RMI and required certificates reference, see Appendix B: Secure Socket Layer (SSL) in Java Remote Method Invocation (RMI).

You must upload a certificate when installing Gift and Loyalty with SSL. You can upload the certificate during installation:



When creating a new database, enter a complex password that adheres to the database hardening guide for all users.

The following services are required for a Simphony-only installation:

- Portal
- Aggregation Adjustment Service
- Simphony Mobile Aggregation
- infoDelivery (report mail)
- Alert Engine

These services are required to support non-Simphony POS systems

- Master (one instance only)
- Posting
- Optional Services include:
- Admin Server (used for scheduled exports/imports)
- Weather (allows weather information to be recorded with daily sales)
- iCare (must be installed on a separate server from portal, used for Gift and Loyalty)
- Analysis Aggregation (Used for Segmentation and Exports)

A unique encryption key is generated during installation for areas requiring file-based encryption. This key is unique to the machine installed and is re-generated and replaced on upgrade or reinstallation.

Post-Installation Configuration

Changing the Default Passwords

Reporting and Analytics is installed with a default password for the Sys Admin user account for Micros organization. Change the password as soon as possible.

Configuring the OHGBU_ADMIN User Group

After successful installation, add users that will administer the product to the OHGBU_ADMIN group. Users must log out before the change takes effect.

Securing the Mail Server

See Appendix A: Secure Socket Layer (SSL)/Transport Layer Security (TLS) on the Mail Server for more information and instructions.

Chapter 3: Implementing Oracle Hospitality Reporting and Analytics Security

Maintaining Strong Passwords

Make sure passwords adhere to the following strength requirements:

1. The password must be at least 8 characters long and maximum 20 characters.
2. The password must contain letter(s), number(s), and punctuation character(s):
   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
3. Client may not choose a password equal to the last 4 passwords used.

Maintaining the User Group for System File Access

Members of the OHGBU_ADMIN group have been granted permissions to traverse the folder structure. This will give users who are both administrator users and OHGBU_ADMIN users the ability to traverse the folder structure to areas where additional permissions are required and to make any necessary changes.

For example, if it is necessary to add additional files to the Pentaho custom folders, the administrator or OHGBU_ADMIN user can navigate to myportal\pentaho-solutions\myMicros folder and modify the permissions on the containing folder to allow the OHGUB_ADMIN group to insert files.

Encryption Key Rotation

Enterprise Back Office automatically rotates the encryption key after upgrades and after 180-day intervals in which no upgrade takes place.

You can view the date of the last rotation in the cedb.ce_rotation_schedule table. Make sure only cedb users have view access to the table. Do not allow other users, such as support2, to view the table.

Chapter 4: Security Considerations for Developers

Adding additional datasources

1. In myPortal/microsConfig.properties, add the datasource name to the list on the variable db.dsNames. The name chosen here will be used as the reference in any report accessing this datasource.
2. Add the database name to the list on the variable db.dbNames. This should be the name of the database or schema being added.
3. Add the additional properties in myPortal/microsConfig.properties, replacing 'YourDSName' with the datasource name entered in db.dsNames

   db.vendor.YourDSName=oracle-9i

   (oracle-9i will work for all versions of oracle)

   db.server.YourDSName=<ServerName>

   db.user.YourDSName=<DatabaseUserName>

   db.password.YourDSName=

   db.port.YourDSName=<PortNumber>

4. After these fields have been added and saved, run passwordChangeUtility/ChangePassword.vbs. Use this utility to set passwords for new database users.

Appendix A: Secure Socket Layer (SSL)/Transport Layer Security (TLS) on the Mail Server

Setting up SSL/TLS on an IceWarp Mail Server (Merak)

1. Create the Certificate Signing Request (CSR) and Private Key.
    a. Start the IceWarp Server Administration console.
    b. From the menu, expand **System** and select **Certificates**.
    c. On the Server Certificates tab, click **Create CSR/Server Certificate**.
    d. Fill out the Create CSR/Server Certificate form, select **Create Certificate Signature Request (CSR)**, and click **OK** to create and save the CSR file.
    The mail server uses the information you entered in the **Common Name** field as the mail server hostname.
2. Send the CSR to a Certification Authority (CA) for signing.
3. Run the following command to merge the signed certificate with the private key generated by the IceWarp Server Administration console:
    `copy` *`IceWarpInstallationPath`*`\config\_certs\csr\`*`name`*`_private.key +` *`SignedCertificate`*`.pem` *`name`*`Cert.pem`
4. Import the merged certificate into the IceWarp Mail Server:
    a. In the IceWarp Server Administration console, on the Server Certificates tab, click **Add**.
    b. Enter the IP address of the Mail Server and browse to the merged certificate, then click **OK**.
5. Enable SSL/TSL for SMTP messaging:
    a. From the menu, expand **System** and select **Advanced**.
    b. On the Protocol tab, select **Enable SSL/TLS**, and then click **Apply**.
    c. On the Advanced tab, select **Use TLS/SSL (Secured Delivery)**, and then click **Apply**.
6. Restart all modules:
    a. From the menu, expand **System** and select **Services**.
    b. Click **Restart All Modules**.

Setting up SSL/TSL on RTA Master E-mails

Configure the following properties in the MasterServer.properties file:

```
#enable SSL on emails
mail.smtp.ssl.enable      = true
mail.smtp.starttls.enable = true
```

If the properties do not exist in the file, define them as shown.

Setting up SSL/TLS on RTA Client E-mails

Configure the following properties in the serverInfo.properties file:

```
#enable SSL on emails
smtpSslPort = 465
pop3SslPort = 99
```

If the properties do not exist in the file, define them as shown.

Appendix B: Secure Socket Layer (SSL) in Java Remote Method Invocation (RMI)

You must create a single keystore with a certificate signed by a Certification Authority (CA) to support Secure Socket Layer (SSL) in Java Remote Method Invocation (RMI) communication between Remote Transfer Agent (RTA) Master and Clients (RTA Slave, Portal, EMS). Deploy the keystore during installation to all RTA-related modules (Master, Slave, Portal and EMS) directories.

1. Make sure Java is installed on the machine. The following commands use the Java keytool command to create the keystore, to generate the Certificate Signing Request (CSR) file, and to import a certificate signed by a CA.
2. Create the keystore:
    a. Run the following command:
    ```
    keytool -genkey –v –storepass yourStorePassword
            –keypass yourKeyPassword –alias rta –keyalg RSA
            -keystore rta.keystore
    ```
    b. Enter the following required information:
    ```
    What is your first and last name?
    [Unknown]: RTA
    What is the name of your organizational unit?
    [Unknown]: HGBU
    What is the name of your organization?
    [Unknown]: Oracle
    What is the name of your City or Locality?
    [Unknown]: Columbia
    What is the name of your State or Province?
    [Unknown]: Maryland
    What is the two-letter country code for this unit?
     [Unknown]: US
    Is<CN=RTA Master, OU=HGBU, O=Oracle, L=Columbia, ST=Maryland,
    C=US> correct?
    [no]: yes
    ```
3. Run the following command to create the CSR:
    ```
    keytool -certreq –v –storepass yourStorePassword
            –keypass yourKeyPassword -alias rta
            –keystore rta.keystore -file rta.csr
    ```
    Make sure the -storepass, -keypass, -alias, and -keystore values are the same as the ones used to create the keystore in Step 2.
4. Send the CSR to a Certification Authority (CA) for signing.

5. Run the following command to import the signed certificate to the keystore:

```
keytool -import –v –storepass yourStorePassword
        –keypass yourKeyPassword -alias rta
        -keystore rta.keystore -file rta.cer
```

6. Run the following command to verify the keystore entries:

```
keytool -list –v –storepass yourStorePassword
        –keystore rta.keystore
```

Appendix C: Database Password Changes

Use the Password Change Utility to update passwords within Enterprise Back Office to align with database password changes. Refer to the Security Guidelines in your Point-of-Sales application for information about database password maintenance.

Warning: The Password Change Utility updates the new passwords for the Enterprise Back Office configuration files and does not change the passwords in the database. If you do not change the passwords in the database or enter the passwords incorrectly in the utility, the database connections will fail.

1. Navigate to *InstallationPath*\PasswordChangeUtility\ and double-click ChangePassword.cmd
2. For each database user account that you want to change, select the checkbox next to the account name and enter the new password. You can select **Show Passwords** to unmask the passwords being entered.
3. Click **Apply Changes** to update the new passwords. The utility creates a backup of the .properties files in the same folder.

Appendix D: Installing Secure Socket Layer (SSL) Certificate in JBOSS Server

You must create the keystore, the Secure Socket Layer (SSL) certificate request using the Certificate Signing Request (CSR), move the keystore to the correct location in the JBOSS server, and then configure Enterprise Back Office to use SSL.

1. Make sure Java is installed on the machine. The following commands use the Java keytool command to create the keystore, to generate the Certificate Signing Request (CSR) file, and to import a certificate signed by a Certification Authority (CA).
2. Run the following command to create the keystore:
   ```
   keytool -genkey -alias name -storepass yourStorePassword
           -dname "CN=domain,O=company,L=city/locality,
                   ST=state,C=counrycode"
           -alias rta -keyalg RSA -keysize 2048
           -keystore domain.keystore
   ```
3. Run the following command to create the CSR:
   ```
   keytool -certreq -v -alias name -file name.csr
           -keystore domain.keystore -sigalg SHA256withRSA
   ```
   Make sure the -alias and -keystore values are the same as the ones used to create the keystore in Step 2.
4. Send the CSR to a Certification Authority (CA) for signing.
   If you are using an Oracle SSL certificate, submit the request at http://my.oracle.com/site/git/2727/11529/index.html
5. Run the following command to import the signed certificate:
   ```
   keytool -v import -alias name -file signedFilename
           -keystore domain.keystore
   ```
   Make sure the -alias and -keystore values are the same as the ones used to create the keystore in Step 2.
   a. If the certificate is part of a chain, import the root and intermediate certificates before the machine certificate. If you do not import the root and intermediate certificates, the system shows the following error:
      ```
      keytool error: java.lang.Exception: Failed to establish chain
      from reply
      ```
   b. If you are using a certificate issued by Oracle SSL, obtain the root and intermediate certificates from http://my.oracle.com/site/git/2727/11529/index.html
6. Copy the keystore file from the Java installation directory to the configuration directory. If you used standard file paths during installation, these are:

```
c:\program files\java\jdkversion\bin
d:\micros\mymicros\myportal\server\default\conf\
```

7. Open \server\default\deploy\jbossweb.sar\server.xml in a text editor.
   a. Add the following section:

```
<!-- Secure web service traffic: HTTPS Connector on port 443 -->
<Connector protocol="HTTP/1.1" SSLEnabled="true" port="443"
address="${jboss.bind.address}" maxThreads="100" strategy="ms"
maxHttpHeaderSize="8192" emptySessionPath="true"
scheme="https" secure="true" clientAuth="want"
keystoreFile="${jboss.server.home.dir}/conf/{DOMAIN}.keystore"
keystorePass="{KEYSTORE PASSWORD}"
truststoreFile="${jboss.server.home.dir}/conf/{DOMAIN}.keystore"
truststorePass="{TRUSTSTORE PASSWORD}"
ciphers="SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_RS
A_WITH_AES_128_CBC_SHA" sslProtocols = "TLSv1,TLSv1.1" />
```

   b. Change all ports in server.xml from 8443 to 443.
8. Open \server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml in a text editor.
   a. Find and remove the following lines:

```
<xsl:when test="(name() = 'redirectPort')">
<xsl:attribute name="redirectPort"><xsl:value-of
select="$portHttps" /></xsl:attribute>
</xsl:when>
```

   b. Change all ports in bindings-jboss-beans.xml from 8443 to 443.
   c. Find and set the following line:

```
<xsl:variable name="portHttps" select="$port - 7637"/>
```

9. Open microsConfig.properties in a text editor and uncomment the following line:
   `forceProtocol=https`
10. Restart the Portal service.

Appendix E: Java 1.6 Prerequisite for Transport Layer Security (TLS) 1.2

1. Upgrade to Oracle Java 1.6 Update 121.
2. Add the Oracle Java Cryptography Extension (JCE) Provider:
   a. Copy *INSTALLATION_DIR*\server\default\deploy\portal.ear\employeeManagement.war\WEB-INF\lib\bcprov-jdk.16-1.46.jar to *JAVA_INSTALLATION_DIR*\jre\lib\ext\
   b. Add the following line in the *JAVA_INSTALLATION_DIR*\jre\lib\java.security configuration file to add providers, where *X* is the next number in the list:
      security.provider.*X*=*PROVIDER_INFO*
      For example,
      security.provider.2=org.bouncycastle.jce.provider.BouncyCastleProvider
3. Download and then follow the instructions to add the Oracle JCE Unlimited Strength Jurisdiction Policy Files 6.