Oracle® MICROS Enterprise Back Office

Security Guide
Release 9.0.0
E81081-09

September 2023

ORACLE

Contents

Preface

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

- Reporting and Analytics
- Gift and Loyalty
- Labor Management
- Forecasting and Budget
- InMotion Mobile (server-side security)

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

Customer Support

To contact Oracle Customer Support, access the Support Portal at the following URL: https://iccp.custhelp.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 MICROS product documentation is available on the Oracle Help Center at https://docs.oracle.com/en/industries/food-beverage/

Revision History

Date	Description of Change
March 2017	• Initial publication.
May 2017	• Clarified scope of document in preface.
July 2017	• Added step to Appendix D for importing certificates.

October 2017	• Added clarification regarding hardcoded alias name for Gift and Loyalty security certificates.
March 2018	• Added instructions for requiring a PIN to log into myiCard.net. • Added information regarding approved Transport Layer Security 1.2 ciphers.
September 2023	• Updated guide title.

1 Enterprise Back Office Security Overview

This chapter provides an overview of Oracle MICROS Enterprise Back Office 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 Enterprise Back Office Installation for more information.
- **Learn about and use the Enterprise Back Office security features.** See Implementing Enterprise Back Office 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 Enterprise Back Office Security

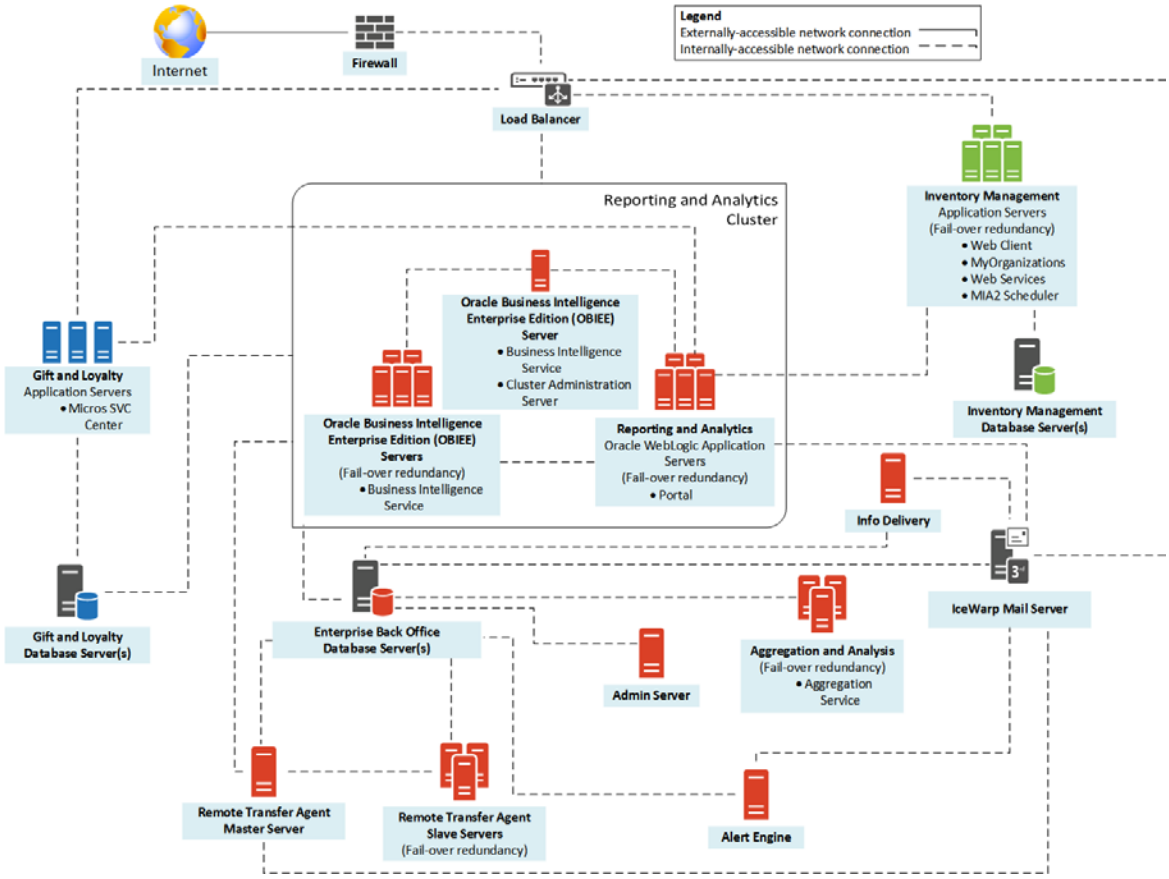


Figure 1 – System Architecture of Enterprise Back Office

Reporting and Analytics and Gift and Loyalty are hosted on Oracle WebLogic 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.

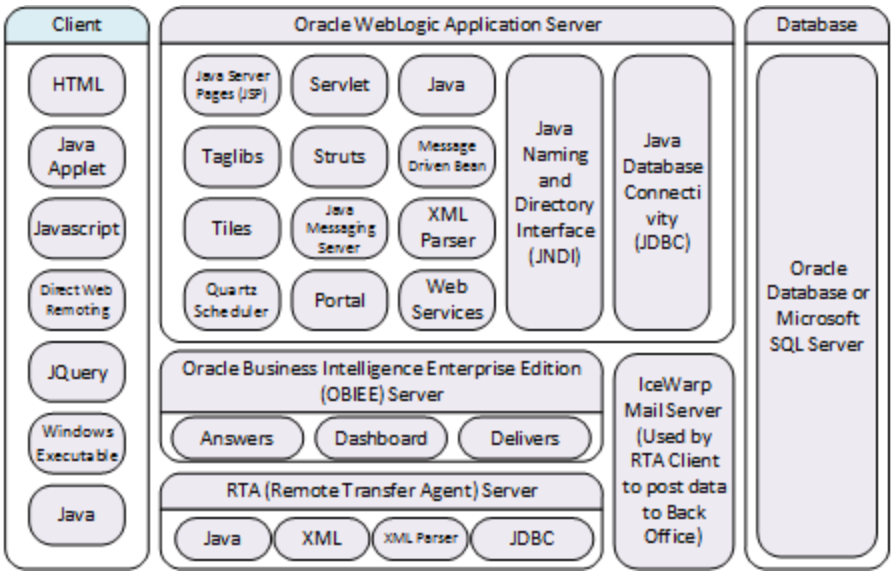


Figure 2 - Technology stack of Reporting and Analytics and Gift and Loyalty

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 Oracle WebLogic 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 Oracle WebLogic 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* MICROS *Inventory Management Security Guide* contains more information to security pertaining to the Inventory Management architecture.

Understanding Load Balancer Impact

This document is intended for environments that do not use a Load Balancer to implement or enforce security.

Understanding the Enterprise Back Office Environment

Enterprise Back Office 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. HTTPS Redirect and Enforcing Minimum SSL Protocol contain information and instructions.
- Certificate signed by an authorized Certificate Authority (CA). Appendix D contains instructions for requesting a signed certificate. The installer for Gift and Loyalty expects the security certificate to have an alias of `Server` because this is hardcoded in the installer.

The My Oracle Support knowledge base article 1557737.1 contains more information about support entitlements for obtaining and updating to the required Java version.

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. HTTPS Redirect and Enforcing Minimum SSL Protocol contain information and instructions.
- Certificate signed by an authorized Certificate Authority (CA). Appendix D contains instructions for requesting a signed certificate.

The My Oracle Support knowledge base article 1557737.1 contains more information about support entitlements for obtaining and updating to the required Java version.

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 1-3 or in a cluster of servers as shown in Figure 1-4.

- In 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.

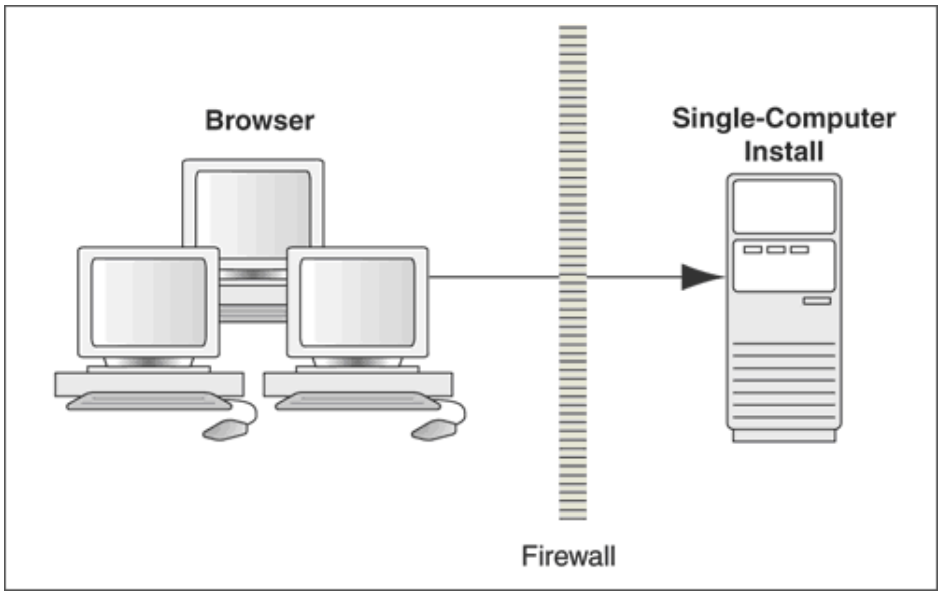


Figure 1-3 Single-Computer Deployment Architecture

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 1-4.

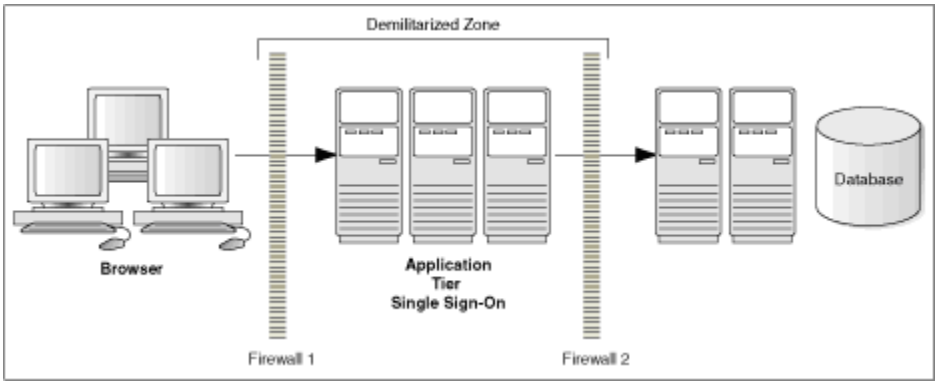


Figure 1-4 Traditional DMZ View

Network Port Requirements

Make sure to open the following ports.

- 24
- 25
- 80
- 110
- 443
- 465
- 995
- 1433
- 1521
- 9443

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.

2 Performing a Secure Enterprise Back Office Installation

The *Oracle* MICROS *Enterprise Back Office Installation Guide* contains information and instructions for installing the application.

Pre-Installation Configuration

The *Oracle* MICROS *Enterprise Back Office Release Notes* contains information about new functionality and technology changes. Make sure your installation environment adheres to the supportability and requirements information for your release.

Secure Certificate

The Enterprise Back Office installation requires a Secure Socket Layer (SSL) certificate for each server. Appendix D contains instructions for requesting an SSL certificate from a Certificate Signing Authority.

Microsoft Windows User Group

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.

Installing Enterprise Back Office

Database Passwords

For all database passwords, you must follow the password security guidelines outlined for the respective databases:

- Oracle Database: *Oracle Database Security Guide*
- Microsoft SQL Server: *Security Center for SQL Server Database Engine*

HTTPS Redirect

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.

To disable the HTTPS redirect, open `microsConfig.properties` in a text editor and uncomment the following line: `forceProtocol=https`

Secure Socket Layer (SSL)

Enterprise Back Office now requests the SSL certificate and passwords during the installation. You can configure SSL after the installation using the Oracle WebLogic Console.

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 MICROS Simphony-only installations.

Appendix B contains information about SSL for RMI.

Enforcing Minimum Required SSL Protocol

You can configure the minimum required SSL protocol accepted by Enterprise Back Office by setting the `-Dweblogic.security.SSL.minimumProtocolVersion` parameter in the WebLogic startup script.

For example, if you want to set TLS 1.2 as the earliest supported protocol:
`-Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.2`

Service Installation Requirements

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)

File-Based Encryption

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

Entering the Organization Passwords

After successful installation, the system administrator must log into the `m` organization and enter the following passwords to enable the respective functionality:

- External Application
- Forecasting Messaging Queue (for Forecasting and Budget)
- ExactTarget FTP (for Gift and Loyalty)

- Urban Airship (for Alert Engine)
- Bounce eMail (for Gift and Loyalty CRM)
- iCare Messaging Queue (for Gift and Loyalty)
- WLST (for Reporting and Analytics WebLogic AdminServer)
- SOAP (for Reporting and Analytics WebLogic AdminServer)
- myInventory DB (for Inventory Management)
- Simphony DB (for Simphony Point-of-Sale)

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.

Enabling Secure Socket Layer (SSL)

If you installed Enterprise Back Office without enabling SSL, perform the following instructions to enable SSL:

1. Log in to the Oracle WebLogic console, and then upload the security certificate and enable SSL. Refer to the Oracle WebLogic help for information and instructions.
2. Change the Published URL to comply with SSL requirements.

   WARNING: If you do not enable TSL 1.2, your deployment will not be compliant with security standards.

Reporting and Analytics supported TLS and Ciphers

TLS protocol

Before RNA 8.5.1 Patch 126 and 9.0 Patch 8

- TCA client\TCA server(component of RNA Server) support TLSv1, TLSv1.1
- RTA client\RTA Server support TLSv1 and TLSv1.1

From RNA 8.5.1 Patch 126 and 9.0 Patch 8

- TCA client\TCA server(component of RNA Server) support TLSv1, TLSv1.1, and TLSv1.2
- RTA client\RTA Server support TLSv1 and TLSv1.1, and TLSv1.2

List of Ciphers

RTA client, RTA Server and TCA server (a component of RNA Server) support Ciphers are below:

- 8.5.1 support Cipher Suites is in link https://docs.oracle.com/javase/6/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider and scroll down a little to go to “Cipher Suites” section.
- 9.0 support Cipher Suites is in link https://docs.oracle.com/javase/7/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider and scroll down a little to go to “Cipher Suites” section.

TCA client support Cipher is below:

Before RNA 8.5.1 Patch 126 and 9.0 Patch 8

- 8.5.1 and 9.0 support Cipher Suites are in link https://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx

From RNA 8.5.1 Patch 126 and 9.0 Patch 8 Client Side ciphers list as below:
//Priority 1 - TLSv1.2
CipherSuite.TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
CipherSuite.TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
CipherSuite.TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
CipherSuite.TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
CipherSuite.TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
CipherSuite.TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
CipherSuite.TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,
CipherSuite.TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,
CipherSuite.TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
CipherSuite.TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
//Priority 2 - TLSv1.2
CipherSuite.TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_RSA_WITH_AES_128_GCM_SHA256,
CipherSuite.TLS_DH_DSS_WITH_AES_128_GCM_SHA256,
CipherSuite.TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
CipherSuite.TLS_RSA_WITH_AES_256_GCM_SHA384,
CipherSuite.TLS_DH_DSS_WITH_AES_256_GCM_SHA384,
CipherSuite.TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,
CipherSuite.TLS_RSA_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_DH_DSS_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_RSA_WITH_AES_256_CBC_SHA256,
CipherSuite.TLS_DH_DSS_WITH_AES_256_CBC_SHA256,
CipherSuite.TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
CipherSuite.TLS_RSA_WITH_AES_128_CBC_SHA, (Mandatory per RFC5246 TLSv1.2)
CipherSuite.TLS_DH_DSS_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_RSA_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_DH_DSS_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
//Approved CipherSuite
//TLSv1.2
CipherSuite.TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, (MSFT implementation is reported as weak)
CipherSuite.TLS_DH_RSA_WITH_AES_128_GCM_SHA256,

CipherSuite.TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,
CipherSuite.TLS_DH_RSA_WITH_AES_256_GCM_SHA384,
CipherSuite.TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
CipherSuite.TLS_DH_RSA_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,
CipherSuite.TLS_DH_RSA_WITH_AES_256_CBC_SHA256,
CipherSuite.TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,
//TLSv1.1
CipherSuite.TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_DH_DSS_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_RSA_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_DH_DSS_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
// TLSv1.2, TLSv1.1
CipherSuite.TLS_DH_RSA_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,
CipherSuite.TLS_DH_RSA_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,
CipherSuite.TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,
CipherSuite.TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,
CipherSuite.TLS_RSA_WITH_3DES_EDE_CBC_SHA,

Configuring HTTPS Ports for Gift and Loyalty

You can enable other ports for HTTPS in Gift and Loyalty, such as 443:

1. Log in to the Gift and Loyalty Oracle WebLogic console.
2. In the Domain Structure, click **iCare_Domain**, click **Environment**, click **Servers**, and then in the table of servers, click **icare_server**.
3. Click the **Protocol** tab, click the **Channels** tab, click **Lock & Edit**, and then click **New**.
4. Fill out the **Create a New Network Channel** form:
    a. Enter a name, and then select `https` from the **Protocol** drop-down list.
    b. Enter `443` (or another open and unused port) in **Listen Port** and **External Listen Port**. Do not enter 7001 or 9443.
    c. Select **Enabled** and **HTTP Enabled for This Protocol**.
    d. If you installed a security for 9443 during the Gift and Loyalty installation, select **Use Server's SSL Identity** from the **Channel Identity** drop-down list. Select **Customize Identity** if you want to enter a new SSL certificate.
5. Click **Finish** and activate the changes.

Securing the Mail Server

Appendix A contains information and instructions.

3 Implementing Enterprise Back Office Security

Password Strength and Maintenance

Make sure passwords in the Enterprise Back Office application 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.

Database Passwords

For database passwords, refer to your database security standards for strength requirements and guidelines.

Appendix E contains instructions for setting up the environment to allow database password changes.

Appendix C contains instructions for using the Database Password Change Utility to update the password used by Enterprise Back Office to access the databases.

Operating System Passwords

Refer to the secure configuration guide for your operating system:

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

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.

Changing the Forecasting Messaging Queue Password

1. Log in to the Oracle WebLogic console.
2. Under the **bifoundation_domain** domain structure, click **Security Realms**, click **myrealm**, click **Users and Groups**, and then click **Users**.
3. Search for the messaging user, and then change the password.
4. Log in to Reporting and Analytics using the M organization and system administrator credentials.
5. Navigate to the MICROS organization and enter the new **Forecasting Messaging Queue Password**.

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.

Enabling Secure Socket Layer (SSL) Certificates

If you install Enterprise Back Office in an unsecure state, follow these instructions to enable SSL, enter or update security certificate information, update the WebLogic Node Manager, and to enable SAML.

Enabling SSL and Certificates for WebLogic Admin Server and Managed Servers

Enable SSL using a security certificate on the WebLogic Admin Server, or on managed OBIEE or Reporting and Analytics application servers:

1. In the WebLogic Server Administration Console, click **Environment** from the **Domain Structure**, click **Servers**, and then click **AdminServer(admin)** or a managed server, such as **appServ1**.
2. Click **Lock & Edit.**
3. On the **Configuration** tab, click the **General** tab, deselect **Listen Port Enabled** , select **SSL Listen Port Enabled**, and then click **Save**.
4. Click the **Keystores** tab, and then click **Change** next to the **Keystores** field.
5. Select **Custom Identity and Java Standard Trust**, and then click **Save**.
   To verify that your certificate is from an approved certificate authority, open a command prompt, and then enter the following command:
   ```
   keytool -list -v -keystore
   C:\Java\JDK17~1.0_7\jre\lib\security\cacerts -storepass
   changeit
   ```
6. Enter the certificate identity details:
   a. For the **Custom Identity Keystore**, enter *`PATH_TO_ID`*`/identity.jks`
   b. Enter `JKS` in the **Custom Identity Keystore Type**. This is typically the default setting.
   c. Enter and confirm the **Custom Identity Keystore Passphrase**.
7. For the trust details, change the **Java Standard Trust Keystore Passphrase** if you changed the Java cacerts.
8. Click **Save**, and then click the **SSL** tab.

9. Enter the identity details:
    a. Enter the server alias in **Private Key Alias**.
    b. Enter and confirm the keystore passphrase in **Private Key Passphrase**.
10. Click **Advanced**, select **Use JSSE SSL**, and then click **Save**.
11. Click **Activate Changes**, and then restart the managed server.

Configuring Node Manager for SSL

Update Node Manager properties for each managed server after enabling SSL and entering certificate details in the Oracle WebLogic Administration Console.

Navigate to `$WL_HOME/common/nodemanager/` and open `nodemanager.properties` in a text editor, and then add or edit the following entries:

```
KeyStores=CustomIdentityAndJavaStandardTrust
CustomIdentityKeyStoreFileName=PATH_TO_ID\\identity.jks
CustomIdentityKeyStorePassPhrase=KEYPASS
CustomIdentityPrivateKeyPassPhrase=PRIVATEPASS
CustomIdentityAlias=SERVER_ALIAS
CustomTrustKeyStorePassPhrase=STOREPASS
```

When entering the path, you must escape colons (:) and slashes (\). For example:
`C\:\\myMicros\\Oracle\\MIDDLE~1\\WLSERV~1.3\\common\\NODEMA~1\\`

Restart Node Manager after saving the changes to the properties file.

Enabling or Updating Security Assertion Markup Language (SAML)

Update SAML settings after making changes to SSL or certificate configurations for OBIEE or Reporting and Analytics managed servers.

1. In the WebLogic Server Administration Console, click **Environment** from the **Domain Structure**, click **Servers**, and then click a managed server, such as **appServ1**.
2. Click **Lock & Edit.**
3. On the **Configuration** tab, click the **Federation Services** tab, and then click the **SAML 2.0 General** tab.
4. In the **Single Sign-On** section, enter the keystore details:
    a. Enter the server alias in **Single Sign-on Signing Key Alias**.
    b. Enter and confirm the keystore passphrase in **Single Sign-on Signing Key Pass Phrase**.
5. Click **Save**, and then click **Activate Changes**.

Changing the Published Site URL for Oracle Business Intelligence Enterprise Edition

1. In the Oracle WebLogic console, navigate to the **Summary of Servers** page, click OBI server name (typically **bi_server*number***), click **Configuration**, click **Federation Services**, click **SAML 2.0 General**, and then change the **Published Site URL**.

   The **Published Site URL** is case sensitive in server cluster deployments.

2. Publish the metadata to the following location:
   `*INSTALLATION_DIR*\Oracle\Middleware\user_projects\domains\bifoundation_domain\obiee_metadata.xml`
3. Navigate to **Security Realms**, click **myrealm**, click **Providers**, click **Credential Mapper**, click the **saml2CMP** credential mapping provider, and then click **Management**.
   a. Delete and then re-create the **obiee** service provider partner.
   b. Use the metadata file you created for the new published site URL.
   c. Select **Enabled**, select **Key Info Included**, and then select **Only Accept Signed Artifact Requests**.
4. Change the value for **OBIEE.PUBLISH_URL** in `microsConfig.properties`.
5. Change the values for **OBIEE.SOAPWSDLURL** and **OBIEE.URL** in `obieeConfig.properties`.
6. Redeploy `portal.ear` and `obieeWebService.war`.

Changing the Published Site URL for Reporting and Analytics

1. In the Oracle WebLogic console, navigate to the **Summary of Servers** page, click the application server name (typically **appServ*number***), click **Configuration**, click **Federation Services**, click **SAML 2.0 General**, and then change the **Published Site URL**.

   The **Published Site URL** is case sensitive in server cluster deployments.

2. Publish the metadata to the following location:
   `*INSTALLATION_DIR*\Oracle\Middleware\user_projects\domains\bifoundation_domain\app_metadata.xml`
3. In a two-box or cluster installation, the WebLogic console creates the metadata file on the Reporting and Analytics application server. You must copy the file to the OBI server running the Oracle WebLogic Administration Server.
4. Navigate to **Security Realms**, click **myrealm**, click **Providers**, click **Authentication**, click the **saml2AP** identity assertion provider, and then click **Management**.
   a. Delete and then re-create the **app_data** service provider partner.
   b. Use the metadata file you created for the new published site URL.
   c. Select **Enabled**, enter `/analytics/*` in the **Redirect URIs** field, and then select **Only Accept Signed Artifact Requests**.
5. Change the value for **portalDomainURL** in `microsConfig.properties`.
6. If you are not changing the OBIEE published URL, redeploy `portal.ear`.

Requiring PIN for Gift and Loyalty myiCard.net

1. Log in to Gift and Loyalty organization.
2. From Gift and Loyalty side menu, navigate to **Gift and Loyalty GPL** | **Programs, Cards, Coupons and Rules** | **Programs**.
3. Select **Loyalty** or **Gift or Debit card** program, and then click **Edit**.
4. On **General** tab, select **Prompt for PIN on myicard.net**.
5. Select **Pin Type**.
    a. If you select **Final 4 Digits of Account Number** then you should be able to use last 4 digit of account number to log in to myiCard.net. For example: If your card number is `11110001`, then your PIN will be `0001`.
    b. If you select **Birthdate Month and Day** then you should be able use birthday month and day to log in to myiCard.net.

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

1. Create the Certificate Signing Request (CSR) and Private Key.
    a. Start the IceWarp Server Administration console.
    b. From the menu, click **System** and click **Certificates**.
    c. On the **Server Certificates** tab, click **Create CSR/Server Certificate**.
    d. Fill out the **Create CSR/Server Certificate** form, click **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.k
    ey + SignedCertificate.pem nameCert.pem
    ```
4. Import the merged certificate into the IceWarp Mail Server:
    a. In the IceWarp Server Administration console, click the **Server Certificates** tab and then click **Add**.
    b. Enter the IP address of the Mail Server, browse to the merged certificate, and then click OK.
5. Enable SSL/TSL for SMTP messaging:
    a. From the menu, click **System** and click **Advanced**.
    b. On the **Protocol** tab, click **Enable SSL/TLS**, and then click **Apply**.
    c. On the **Advanced** tab, click **Use TLS/SSL (Secured Delivery)**, and then click **Apply**.
6. Restart all modules:
    a. From the menu, click **System** and then click **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 = 995
```

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) directory.

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 Requesting a Secure Socket Layer (SSL) Certificate

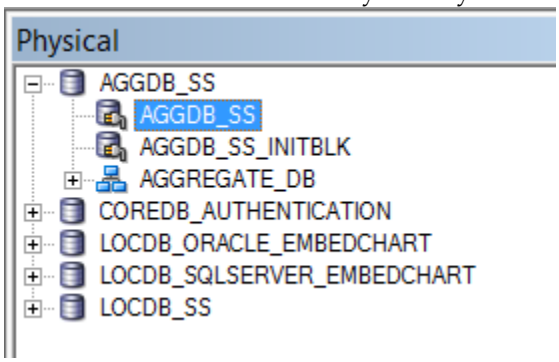
You must create a Java keystore containing a Secure Socket Layer (SSL) certificate to be used when enabling SSL during Enterprise Back Office installation. The installer for Gift and Loyalty expects the security certificate to have an alias of `Server` because this is hardcoded in the installer.

1. 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 server –storepass yourStorePassword
         -keypass yourStoreKeypass –keyalg RSA
         -keysize 2048 –keystore keystoreName.keystore
         –dname "CN=domain,O=company,L=city/locality,
               ST=state,C=countrycode"
   ```
3. Run the following command to create the CSR:
   ```
   keytool -certreq –v –alias server –file filename.csr
         –keystore keystoreName.keystore
         -storepass yourStorePassword
         –sigalg SHA256withRSA
   ```
   Make sure the `-keystore` and `-storepass` 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:
   ```
   keytool –v import –alias server –file signedFilename
         –keystore keystoreName.keystore
   ```
   Make sure the `-keystore` value is the same as the one used to create the keystore in Step 2.

Appendix E Setting Up Database Password Changes

You must perform the following steps to enable changing database passwords:

1. Run the password change utility to change the Reporting and Analytics jdbc xml.
2. Use the WebLogic console to change the data source:
3. In the Oracle WebLogic console, navigate to the **Summary of JDBC Data Sources** page, and then for each data source:
    a. Click the data source name, click **Connection Pool**, verify the user name in the **Properties** field, and then change the password.
    b. Click **Lock & Edit**, and then click **Save**.
4. Click **Activate Changes**.
5. Change the OBIEE Repository file (RPD) password:
    a. In the Oracle BI Administration tool, click **File**, and then click **Open RPD in Online mode**.
    b. Enter the Oracle WebLogic credentials and the RPD password created during installation.
    c. Click the data source in the Physical layer.



    d. Change the login credentials for database connections. You must update all connection pools for each physical database.
    e. Click the **Check in your changes** button, and then click **Save**.
6. Restart all managed servers.