Oracle® Hospitality Inventory Management

Security Guide

Release 8.5.1
E70931-03
May 2019

ORACLE

Oracle Hospitality Inventory Management 20TSecurity Guide, Release 8.5.1

E70931-03

Contents

Preface

This document provides security reference and guidance for Oracle Hospitality Inventory Management.

This document does not include information specific to other Oracle Hospitality Enterprise Back Office products.

Audience

This document is intended for administrators, developers, and system integrators who perform the following functions:

- Document specific security features and configuration details for the Oracle Hospitality Inventory Management, in order to facilitate and support the secure operation of the product and any external compliance standards.
- Guide administrators, developers, and system integrators on secure product implementation, integration, and administration.

It is assumed that the readers have general knowledge of administering the underlying technologies and the application.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL: https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Documentation

Product documentation is available on the Oracle Help Center at https://docs.oracle.com/en/industries/food-beverage/

Revision History

Date	Description of Change
July 2016	Initial publication.
April 2019	Improved encryption-related information.

1

Inventory Management Security Overview

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

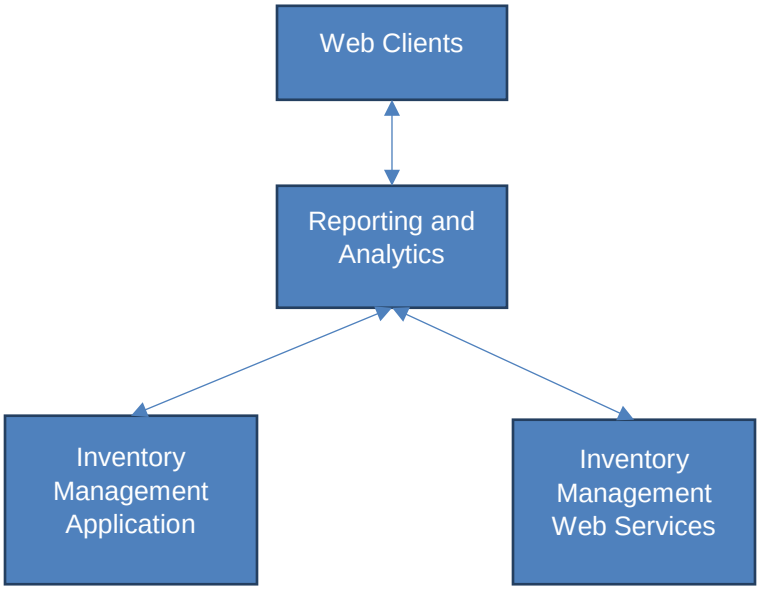
Basic Security Considerations

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 Inventory Management Installation for more information.
- Learn about and use the Inventory Management security features. See Implementing Inventory Management 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” website: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of Inventory Management Security

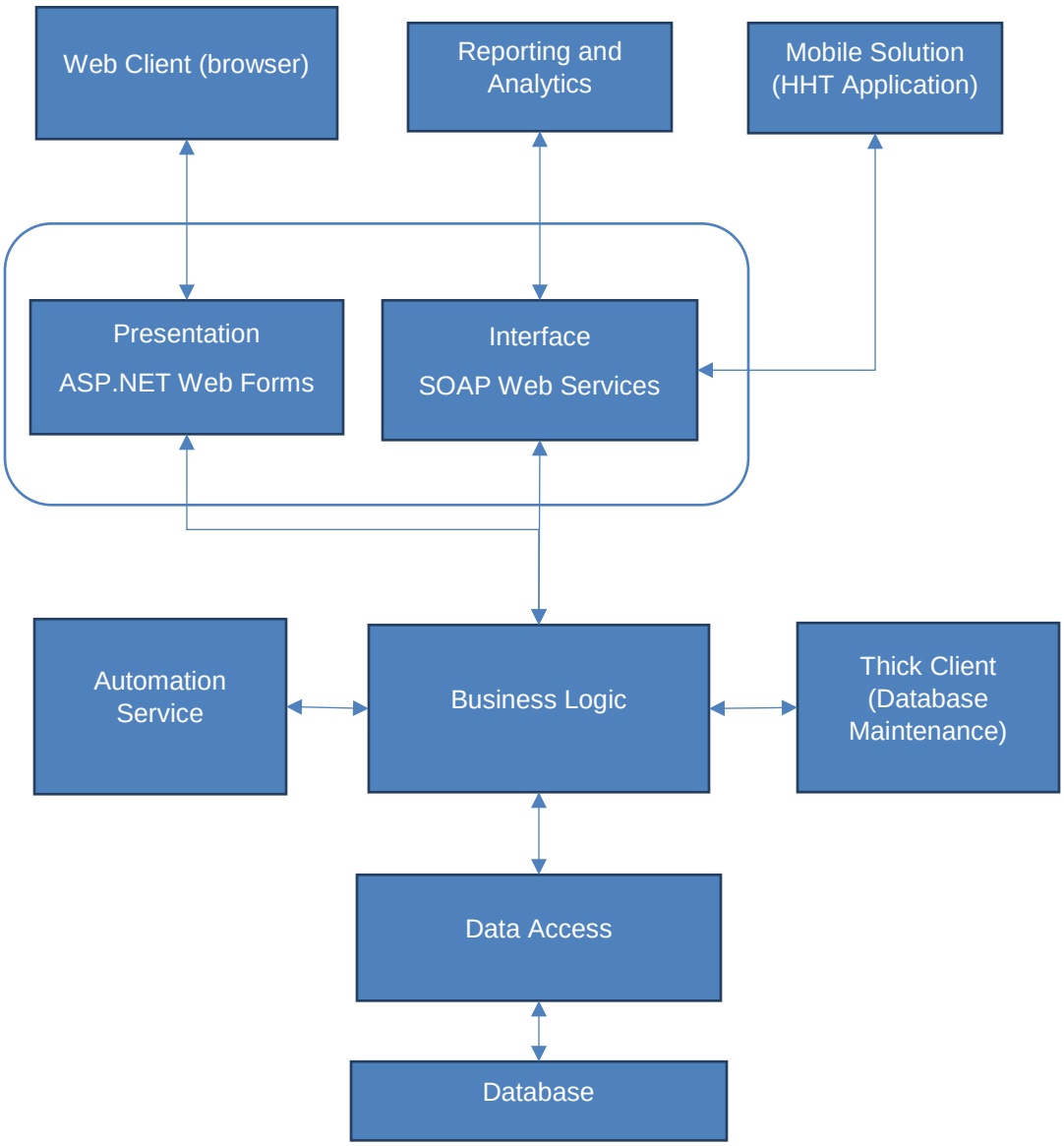
Figure 1-1 Web Application Architecture



Oracle Hospitality Inventory Management:

- Is a component of Enterprise Back Office.
- Exchanges information with Reporting and Analytics using SOAP services.
- Applies role-based access controls.

Figure 1-2 System Architecture



Inventory Management is dependent on Internet Information Services (IIS) and Oracle Database server. Consult the respective security guides regarding secured use of these tools.

Understanding the Inventory Management Environment

When planning your Inventory Management implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data, such as credit-card numbers.
  - You need to protect internal data, such as proprietary source code.

  - You need to protect system components from being disabled by external attacks or intentional system overloads.

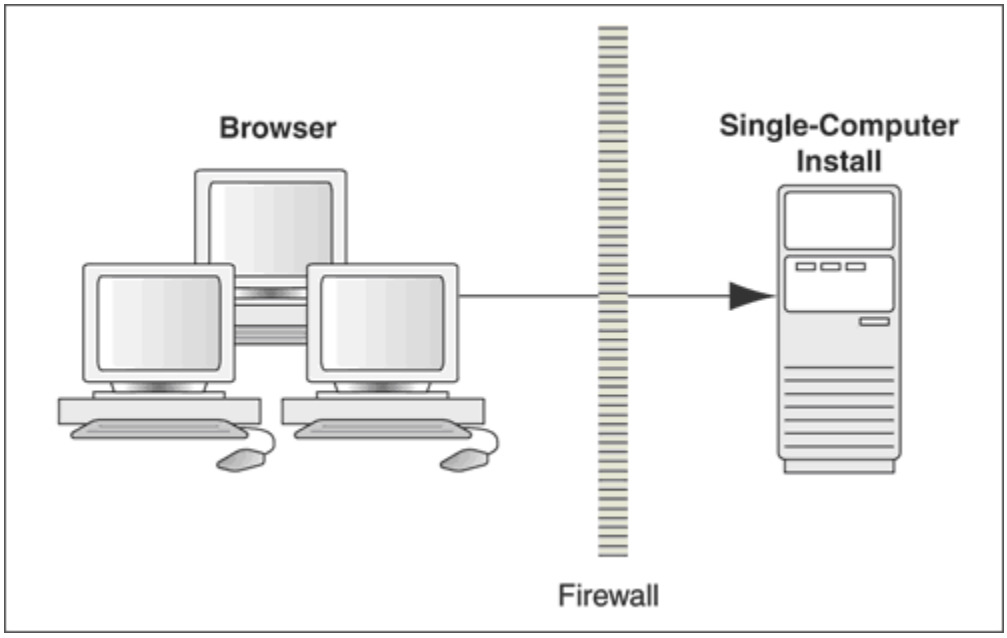
- **Who are you protecting data from?** For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- **What will happen if protections on strategic resources fail?** In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Recommended Deployment Configurations

Inventory Management can be deployed in hosting centers or on-premises (self-hosting, single computer).

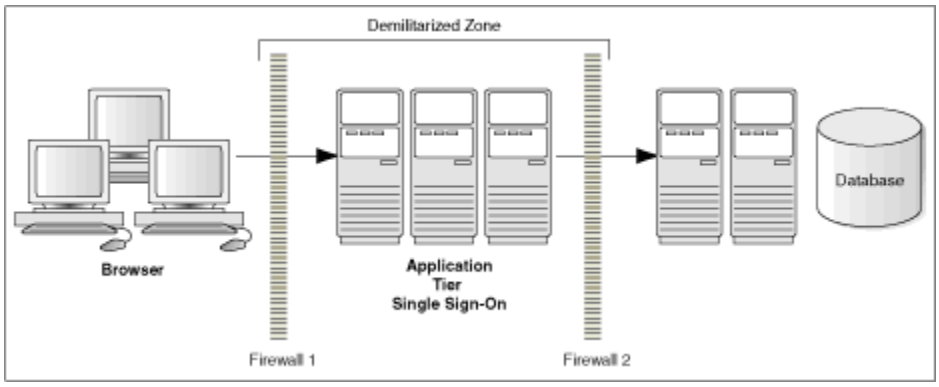
The simplest deployment architecture is the one shown in Figure 1-3. This single-computer deployment may be cost effective for small organizations; however it cannot provide high availability because all components are stored on the same computer.

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.

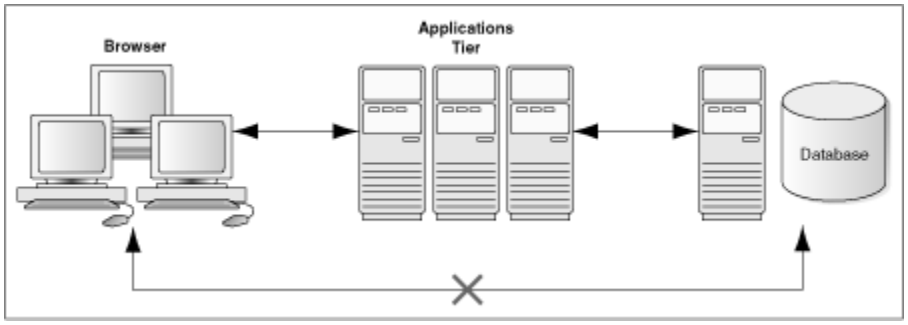
Figure 1-4 Traditional DMZ View



> **NOTE:**
>
> The term demilitarized zone (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

Small organizations that cannot invest huge amounts on firewalls can opt for the architecture in Figure 1-5.

Figure 1-5 Deployment Architecture for Small Organization



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:

- *Guide to Secure Windows Server 2008 R2* (https://technet.microsoft.com/en-us/library/dd548350%28v=ws.10%29.aspx)
- *Guide to Secure Windows Server 2012 R2 and 2012* (https://technet.microsoft.com/en-us/library/hh831360.aspx)
- *Guide to the Secure Configuration of Red Hat Enterprise Linux 5*
- *Hardening Tips for the Red Hat Enterprise Linux 5*

Oracle Database Security

See the *Oracle Database Security Guide*.

Internet Information Services (IIS) Security

See Security Best Practices for IIS (https://technet.microsoft.com/en-us/library/jj635855.aspx)

WebLogic Server Security

See the *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server* for more information.

2

Performing a Secure Inventory Management Installation

For information about installing Inventory Management, see the *Oracle Hospitality Inventory Management Deployment Guide*. Installation is a manual process (no installer program), and you cannot install Inventory Management as a standalone product.

Pre-Installation Configuration

Pre-installation configuration includes database schema set up. Use the standard guidelines provided in the *Oracle Database Security Guide* for setting up the database user name password strength.

Inventory Management Installation

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

See the *Oracle Hospitality Inventory Management Installation Guide* for more information and instructions.

Post-Installation Configuration

Starting from release 8.5.0, database password and encryption-key defining parameters will be stored in Protected Configuration (https://msdn.microsoft.com/en-us/library/53tyfkaw%28v=vs.100%29.aspx). Storing sensitive information in a non-readable format improves the security of our applications by making it difficult for an attacker to gain access to the sensitive information, even if an attacker gains access to the file, database, or other storage location. Inventory Management uses a RSA machine-level key container, which enables you to use a single machine-level key container for all our applications and simplifies the deployment on other PCs.

Encrypting Configuration Files

1. On the Inventory Management application server, extract `SecureConfig.exe` from `SecureConfig.zip` to the Inventory Management installation directory or to a temporary folder, right-click the executable, and then click **Run as administrator**.

> **NOTE:**
>
> - You must have administrator privileges to run **SecureConfig.exe**.

2. On the **Encryption Key Containers** tab, verify that the list includes the **myinventory** machine key container.
    a. If the key does not exist, click **Create new key container** to create a new container, or click **Import key container** to import an existing container at the site.
    b. Name the key `myinventory`.
3. Right-click **myinventory**, and then click **Show key file properties**.
4. On the **Security** tab:
    a. Verify that the **SYSTEM** group has **Full control** privileges.
    b. If you are using the application server for ASP.NET, give the **IIS_USRS** group **Read** privileges.
    c. Click **OK** to return to the SecureConfig tool.
5. On the **Files to Process** tab, click **Add** to add the configuration files that require encryption:

    Automation Service Activity Monitor: ASAMon.exe.config

    Automation Service: AutomationService.exe.config

    DGMIMIS: MobileSolutionsClient.exe.config

    MobileWebService: Web.config

    Inventory Management: web.config

    mymicrosWebService: web.config

    myOrganizations: web.config

    POSWebService: web.config

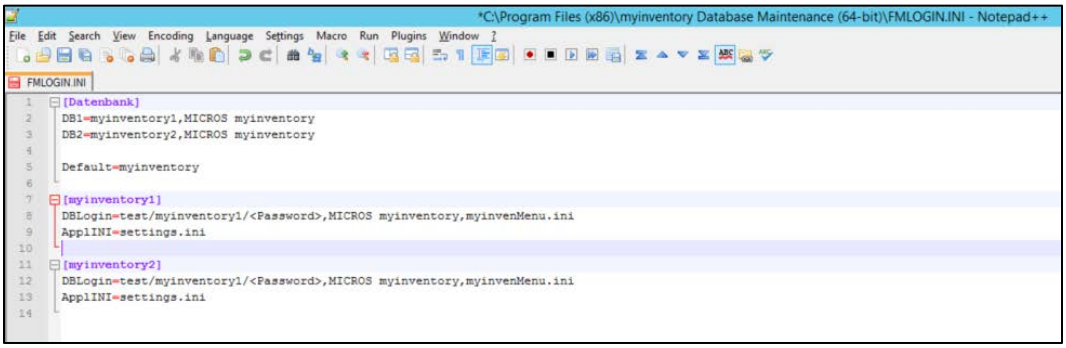
    DBMaintenance: DBMaintenance.config

    Thick Client: Encryption.config
6. Click **Encrypt Configuration Files**.
7. If you are deploying Inventory Management on more than one application server, right-click the **myinventory** key container, and then click **Export**. Import this key container using the SecureConfig tool on the other servers.

> **NOTE:**
>
> - .config files for ASAMon and DBMaintenance must be encrypted using the same parameters as other applications.
> - Unencrypted passwords in FMLOGIN.INI are automatically encrypted when opening the application.
> - When adding a new organization, you can enter the password in plain text. Plain text passwords are automatically encrypted when opening the application.

Configuring FMLOGIN.INI

This section describes the configuration of the login control file and features related to the login screen. The file FMLOGIN.INI controls access to the database files from the client application.



The FMLOGIN.INI file is divided into the following sections:

- Header Section
- Default DB Section
- Connection Details Section

Header Section
This section contains the list of databases available for selection in the login dialog.

[DATENBANK]

DB1=myinventory1,MICROS myinventory 1

DB2=myinventory2,MICROS myinventory 2

"DB1=" Sequence number of the database must be sequential.

- "myinventory1" Name of the database/unique identifier for the connection detail section below (-> link to SQL.config)
- "MICROS myinventory 1" Name of the database in the login dialog when selected.

Default DB Section

Here the default DB must be defined. The database defined here appears as the default when you click the **Options** button: DEFAULT=myinventory1

Connection Details Section

This section contains the connection settings per database.

[MYINVENTORY1]

DBLOGIN=test/myinventory1/<Password>,MICROS myinventory,myinvenMenu.ini

APPLINI=settings.ini

[MYINVENTORY2]

DBLOGIN=test/myinventory1/<Password>,MICROS myinventory,myinvenMenu.ini

APPLINI=settings.ini

[MYINVENTORY1]

The first line of each connection block refers to the selection in the database list. In this example [MYINVENTORY1] is linked to the entry for DB1 in the header section. If the user selects "MICROS myinventory 1" from the database list or does not select any database (default DB) the application will jump to this section.

DBLogin=[Server]/[USER]/[PASSWORD], myinventory,myinvenMenu.ini

This part above contains the following connection parameters:

- "[SERVER]" = Oracle instance as defined in TNSNAMES.ORA
- "[USER]" = Oracle DB user (organization name)
- "[PASSWORD]" represents the password for the Oracle User (without [ ])

> **NOTE:**
>
> - The username must be written without [ ] -> USER.
> - The password must be written without [ ] -> PASSWORD in clear text. It will be encrypted on first start of the application.

Change Default Passwords

Inventory Management is installed with default passwords. Change those passwords as soon as possible. Refer to the *Oracle Hospitality Enterprise Back Office Security Guide* for additional information regarding passwords and password security.

Changing the Default Administrator Password in an Environment with Inventory Management and Reporting and Analytics

1. Log in to Inventory Management directly (without using Reporting and Analytics) as user **Admin**.
2. Click **Main Menu**, click **Maintenance**, click **User Management**, and then select user **Admin**.
3. In the **New Password** field, enter a new Admin password.
4. Log in to MyOrganizations.
5. Select the organization you want to update, and then click **Edit.**
6. Change the password for both Web Services.
7. Log in to the Reporting and Analytics Micros Organization.
8. Go to **Organizations Setup**, and then select an organization to change.
9. Go to **Inventory Management Setup**, and then change the password.

3

Implementing Inventory Management Security

The security features differ depending on whether you are accessing Inventory Management as a standalone web application or with Reporting and Analytics.

- Authentication: Validating user logins (when Inventory Management is accessed as a standalone web application).
- Authorization: Validating access rights based on roles attached to the user.
- Audit: Inventory Management has audit-capability to track changes in commonly used Master Data and Inventory entry.

Encryption Key Parameters

You can configure encryption-related parameters in the following section in Inventory Management .config files:

```
<EncryptedAppSettingsGroup>
      <!--NOT YET ENCRYPTED!; wating for Key container management
      tool. This text SHOULD NOT BE VISIBLE!
      Do not store encrypted values here without specifying
      exported key container.
      -->
      <add key="passPhrase" value="any string value" />
      <add key="saltValue" value="any string value" />
      <add key="hashAlgorithm" value="SHA1 or MD5" />
      <add key="passwordIterations" value="any number" />
      <add key="initVector" value="any 16-byte string" />
      <add key="keySize" value="128, 192, or 256" />
      <add key="PASSWORD" value="any string value"/>
</EncryptedAppSettingsGroup>
```

You can also use the **Encrypted Section Definitions** tab of the Secure Config tool to set the encryption parameters and database password.

Enabling Transport Layer Security (TLS) 1.2

Oracle recommends enabling and using the Transport Layer Security (TLS) 1.2 protocol on your server.

1. Start the registry editor by clicking on **Start** and **Run**. Enter regedit, and then click **Run**.
2. Select **Computer** at the top of the registry tree. Backup the registry first by clicking **File** and then **Export**. Select a file location to save the registry file.

> **NOTE:**
>
> You will be editing the registry. This could have detrimental effects on your computer if done incorrectly, so it is strongly advised to make a backup.

3. Browse to the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
4. Right-click the **Protocols** folder, click **New**, and then select **Key** from the drop-down menu. Rename the new folder to **TLS 1.2**.
5. Right-click the **TLS 1.2** key and add two new keys underneath it.
6. Rename the two new keys as follows:
   - Client
   - Server
7. Right-click the **Client** key, click **New**, and then select **DWORD (32-bit) Value** from the drop-down list.
8. Rename the **DWORD** to **DisabledByDefault**.
9. Right-click **DisabledByDefault** and click **Modify** from the drop-down menu.
10. Ensure that the **Value** data field is set to `0` and the **Base** is `Hexadecimal`. Click **OK**.
11. Create another **DWORD** for the **Client** key.
12. Rename the new **DWORD** key to **Enabled**.
13. Right-click **Enabled** and click **Modify** from the drop-down menu.
14. Ensure that the **Value** data field is set to `1` and the **Base** is `Hexadecimal`. Click **OK**.
15. Repeat steps **7** to **14** for the **Server** key (by creating two DWORDs, **DisabledByDefault** and **Enabled**, and their values underneath the **Server** key).
16. Restart the server.

Appendix A
Secure Deployment Checklist

The following security guideline checklist to help you secure Inventory Management and its components:

- Make sure the operating system is secured according to the security recommendations of the operating system security guide.
- Follow the Oracle Database Security checklist for Oracle Database installation.
- Follow the Internet Information Services (IIS) Security checklist.