Oracle® Hyperion Enterprise Performance Management System

SSL Configuration Guide

RELEASE 11.1.1.3

ORACLE®

ENTERPRISE PERFORMANCE
MANAGEMENT SYSTEM

EPM System SSL Configuration Guide, 11.1.1.3

Authors: EPM Information Development Team

Contents

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support for Hearing-Impaired Customers

Oracle customers have access to electronic support through My Oracle Support or by calling Oracle Support at 1.800.223.1711. Hearing-impaired customers in the U.S. who wish to speak to an Oracle Support representative may use a telecommunications relay service (TRS). Information about the TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html/, and a list of telephone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html. International hearing-impaired customers should use the TRS at +1.605.224.1837. An Oracle Support engineer will respond to technical issues according to the standard service request process.

1

Assumptions and Information Sources

In This Chapter

Overview

This document describes how to deploy Oracle Hyperion Enterprise Performance Management System in Secure Sockets Layer (SSL)-enabled environments. SSL is a cryptographic protocol used to secure data exchange over the network.

The procedures in this document are designed for users who intend to use SSL in their Web environments to secure communication with EPM System products.

Assumptions

- You know how to SSL-enable the following:
  - Application servers: Oracle Application Server, WebLogic, Apache Tomcat, and IBM WebSphere
  - Web Servers: Oracle HTTP Server, Apache, IBM HTTP Server (IHS), Microsoft Internet Information Services (IIS)
  - User directories: Oracle Internet Directory, Microsoft Active Directory (MSAD) Sun ONE Directory Server, and Novell eDirectory.

    In addition to external user directories, EPM System applications use either Oracle Internet Directory or OpenLDAP as the Native Directory. Oracle Internet Directory and OpenLDAP can be SSL-enabled.

  See "Information Sources" on page 8 for a list of reference documents that you can use to SSL-enable your deployment environment.
- You have determined the deployment topology and identified the communication links that are to be secured using SSL. Note that if you SSL-enable the Web server, you must also SSL-enable the application server. EPM System products do not support SSL offloading.

- You have obtained the required certificates from a Certificate Authority (CA), either a well-known CA or your own, or created self-signed certificates. See "Required Certificates" on page 18. You must obtain certificates for Web server, application server, and user directories. Each server that hosts EPM System products requires a separate certificate.

Information Sources

- "Application Servers" on page 8
- "Web Servers" on page 8
- "User Directories" on page 9

Application Servers

Information on configuring your application server for SSL is available in your application server vendor's documentation. The following resources provide a starting point for SSL-enabling the application server.

- **Oracle Application Server:** See "Part IV, Secure Socket Layer" in the *Oracle Application Server Administrator's Guide*.
- **WebLogic 9.2:** See "Configuring SSL" in the *Securing WebLogic Server Guide*.
- **WebSphere 6.1.x:** See "Configuring SSL for WebSphere Application Server" in the *Installing the Solution Guide*.
- **Tomcat:** See "SSL Configuration HOW-TO" in the *Apache Tomcat 5.5 Servlet/JSP Container User Guide*.

Web Servers

For detailed information on configuring your Web server for SSL, see your Web server vendor's documentation.

- **Oracle HTTP Server:** See the following topics in the Oracle HTTP Server Administrator's Guide:
  - Managing Security
  - Enabling SSL for Oracle HTTP Server

  If you are using a Web server other than Oracle HTTP Server with Oracle Application Server (for example, Apache, IIS, and Sun ONE), see "Using Oracle Containers for J2EE Plug-in" in the *Oracle HTTP Server Administrator's Guide*.

Note: Oracle's IIS proxy DLL, which is used when using IIS as a reverse proxy for Oracle Application Server, does not support SSL, leaving the communication between IIS Web server and other Web servers unencrypted. See "Configuring IIS Listener to Use OracleAS Proxy Plug-in" in the *Oracle HTTP Server Administrator's Guide*. For instance, assume that Oracle Enterprise Performance Management Workspace, Fusion Edition, is deployed on Oracle Application Server with an IIS HTTP server and Oracle Hyperion Financial Management, Fusion Edition, is deployed on a different IIS instance. In this scenario, the communication between the two IIS instances cannot be SSL-enabled. This issue can be resolved by using one IIS instance to host all EPM System products.

- For information on configuring IIS for SSL, go to http://support.microsoft.com/kb/299875/.
- For information on configuring Apache HTTP Server for SSL, go to http://httpd.apache.org/docs/2.0/ssl/.
- IHS provides out-of-the-box support for SSL. Use the key management utility (iKeyman) to self-sign certificates.
  - IHS 1.3: go to http://www-306.ibm.com/software/webservers/httpservers/doc/v1326/manual/ibm/9atikeyu.htm.
  - IHS 6.0: go to http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/tsec_keytu.html.

User Directories

For detailed information, see the documentation from the user directory vendor. Useful links:

- **Oracle Internet Directory:** See Oracle Internet Directory Administrator's Guide
- **Oracle Virtual Directory:** See Oracle Virtual Directory Product Manual
- **Sun ONE Directory Server:** See "Implementing Security" in the *Sun ONE Directory Server Administration Guide*
- **Microsoft Active Directory:** See Microsoft Windows Server 2003 Active Directory documentation
- **Novell eDirectory:** Novell eDirectory documentation

2

SSL and EPM System Products

In This Chapter

About SSL-Enabling Oracle's EPM System Products

The EPM System deployment process automatically deploys Oracle's EPM System products in both SSL and non-SSL modes. For example, a default deployment deploys Oracle's Hyperion® Shared Services to port 28080 (non-SSL mode) and 28443 (SSL mode).

While deploying Shared Services, you must specify whether to use SSL for the entire EPM System.

Caution! If you choose to SSL-enable Shared Services, SSL mode is automatically selected for all products that share the Oracle's Hyperion Shared Services Registry.

Selecting the “Enable SSL for Communications” check box in the Oracle's Hyperion Enterprise Performance Management System Configurator to enable SSL does not configure your environment to use SSL. It only sets a flag in the Shared Services Registry to indicate that all EPM System products that use the repository must use the secure protocol (HTTPS) for communication. You must complete additional procedures to SSL-enable your environment. These procedures are discussed in this document.

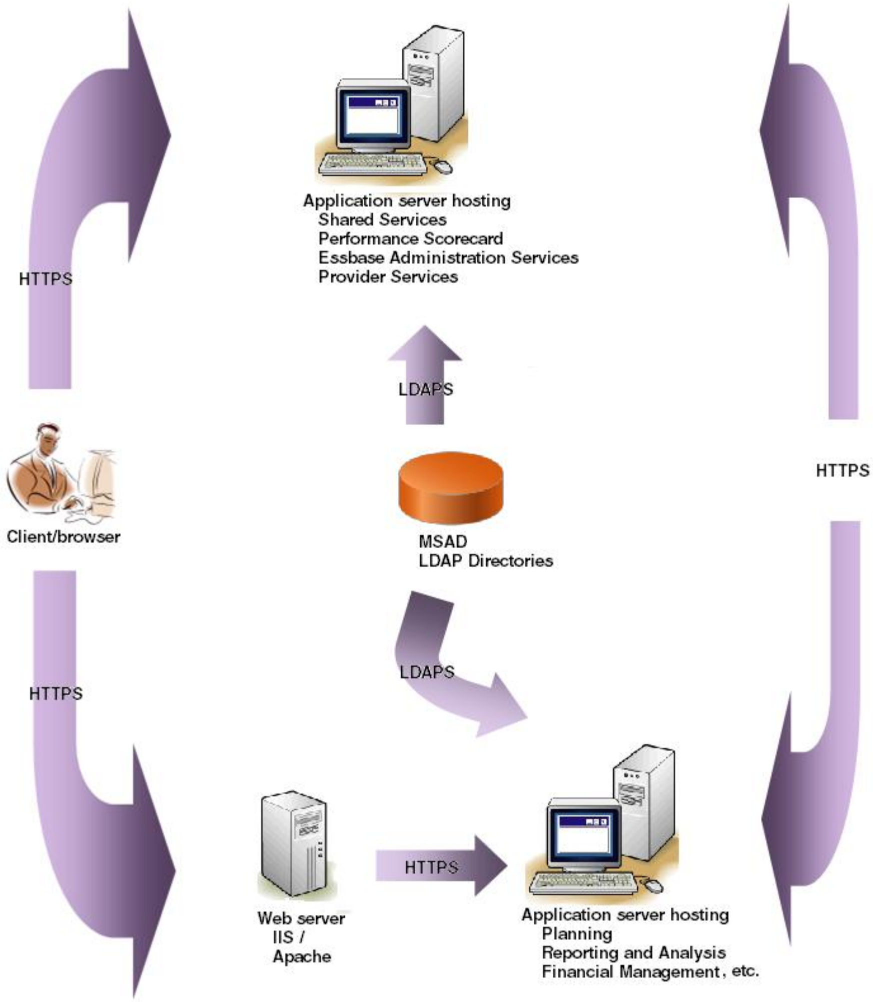
Identifying SSL Points

This section provides diagrams that indicate the secure connections that can be established for Oracle's EPM System products. Non-SSL communication links are not depicted in these diagrams. Oracle's EPM System products that do not support SSL communication are not included in these diagrams.

A Sample Secure Deployment Topology

This section presents a sample deployment topology that illustrates the SSL communication links that can be established among EPM System products.

Caution! The illustrated topology is for information only and is not a suggested deployment topology.



Note: Requests sent to applications deployed to an Oracle Application Server instance are received by a Web server. By default, the Oracle HTTP Server is configured when you install Oracle Application Server. You can configure this Web server to receive secure HTTP requests.

Connections to LDAP-enabled user directories, such as Oracle Internet Directory, MSAD, and Sun ONE Directory Server, can be secured using LDAPS.

Securable EPM System Connections

This section lists the EPM System connections that can be secured. This is not a complete listing of all EPM System connections.

Table 1 Foundation Services Connections That Can Be SSL-Enabled

Source	Destination	Protocol	Server to Server[1]
Shared Services			
Browser	Shared Services Web application	HTTP/HTTPS	No
Browser	Web server	HTTP/HTTPS	No
Web server	Shared Services Web application	HTTP/HTTPS or AJP[2]	Yes
Shared Services Web application	Applications Registered with Shared Services	HTTP/HTTPS	Yes
Shared Services Web application	User directories (Native Directory and external user directories)	LDAP/LDAPS	Yes
Oracle Enterprise Performance Management System Lifecycle Management Utility	Shared Services Web application	HTTP/HTTPS	No
Oracle Enterprise Performance Management System Lifecycle Management Utility	User directories (Native Directory and external user directories)	LDAP/LDAPS	No
Oracle Enterprise Performance Management System Lifecycle Management Utility	EPM System product Web applications and Web servers	HTTP/HTTPS	No
EPM Workspace			
Browser	Web server	HTTP/HTTPS	No
EPM Workspace Web server	EPM Workspace Web application	HTTP/HTTPS	Yes
EPM Workspace Web application	User directories (Native Directory and external user directories)[3]	LDAP/LDAPS	Yes
EPM Workspace Services	User directories (Native Directory and external user directories)	LDAP/LDAPS	Yes
EPM Workspace Services	Shared Services Web application	HTTP/HTTPS	Yes
Oracle Hyperion Smart View for Office, Fusion Edition			
Smart View Client	Financial Management provider	HTTP/HTTPS	No
Smart View client	Oracle Hyperion Provider Services	HTTP/HTTPS	No
Smart View client	Oracle Hyperion Planning, Fusion Edition provider	HTTP/HTTPS	No
Smart View client	Oracle's Hyperion Reporting and Analysis	HTTP/HTTPS	No

Source	Destination	Protocol	Server to Server[1]
Smart View client	Shared Services Web application	HTTP/HTTPS	No
Smart View client	Oracle's Hyperion® Enterprise®	HTTP/HTTPS	No
Oracle Hyperion EPM Architect, Fusion Edition			
Performance Management Architect Web server	Dimension Server Web services	HTTP/HTTPS	Yes
Performance Management Architect Web server	Data Sync Web services	HTTP/HTTPS	Yes
Browser	Performance Management Architect Web server	HTTP/HTTPS	No
Performance Management Architect Web server	Shared Services Web application	HTTP/HTTPS	Yes
Performance Management Architect Web server	User directories (Native Directory and external user directories).	LDAP/LDAPS	Yes
Performance Management Architect Web server	Planning Web application	HTTP/HTTPS	Yes
Performance Management Architect Web server	Financial Management Web application	HTTP/HTTPS	Yes
Performance Management Architect Web server	Oracle Hyperion Profitability and Cost Management, Fusion Edition Web application	HTTP/HTTPS	Yes
Performance Management Architect Web server	Oracle Essbase Administration Services	HTTP/HTTPS	Yes
Performance Management Architect Web server	Oracle Essbase Studio	HTTP/HTTPS	Yes
Batch client	EPM Workspace Web application	HTTP/HTTPS	No
File export tool	Financial Management Web application	HTTP/HTTPS	No
Data Sync server	Performance Management Architect Web server	HTTP/HTTPS	Yes
Data Sync server	Planning Web application	HTTP/HTTPS	Yes
Performance Management Architect Dimension Server	Shared Services Web application	HTTP/HTTPS	Yes
Performance Management Architect Dimension Server	User directories (Native Directory and external user directories)	LDAP/LDAPS	Yes
Batch client	Performance Management Architect Web server	HTTP/HTTPS	No
Batch client	Performance Management Architect Dimension Server Web services	HTTP/HTTPS	No
File export tool	Planning Web application	HTTP/HTTPS	No

Source	Destination	Protocol	Server to Server[1]
File export tool	Performance Management Architect Dimension Server Web services	HTTP/HTTPS	No
Hyperion Calculation Manager			
Browser	Hyperion Calculation Manager server	HTTP/HTTPS	No
Oracle Smart Space, Fusion Edition Client			
Smart Space client	Oracle Business Intelligence Enterprise Edition Analytics	HTTP/HTTPS	Yes
Smart Space client	Oracle Business Intelligence Publisher	HTTP/HTTPS	Yes
Smart Space client	Reporting and Analysis Web service	HTTP/HTTPS	No
Smart Space client	Smart Space server	HTTP/HTTPS	No
Smart Space client	Collaborator Administration Console	HTTP/HTTPS	No
Smart Space Server			
Authentication Web service	User Directories (Native Directory and external user directories)	LDAP/LDAPS	Yes
Authentication Web service	Shared Services Web application	HTTP/HTTPS	Yes
Analytics Web service	Provider Services	HTTP/HTTPS	Yes

[1] If you are not using a trusted third-party CA for server-to-server communication, you must import the CA cert into the originating server keystore.

[2] AJP implementation is platform-specific.

[3] Used only if using portlets. If not using portlets, EPM Workspace process does not connect directly to user directories.

Table 2 Essbase Connections That Can Be SSL-Enabled

Source	Destination	Protocol	Server to Server[1]
Provider Services Web application	BPM Server	HTTP/HTTPS	Yes
Provider Services client	Provider Services Web application	HTTP/HTTPS	No
Essbase Studio Excel Add-in	Essbase Studio server	HTTP/HTTPS	No
Administration Services	Performance Management Architect Web server	HTTP/HTTPS	Yes
Oracle Essbase Studio	Performance Management Architect Web server	HTTP/HTTPS	Yes

[1] If you are not using a trusted third-party CA for server-to-server communication, you must import the CA cert into the originating server keystore.

Table 3 Reporting and Analysis Connections That Can Be SSL-Enabled

Source	Destination	Protocol	Server to Server[1]
Oracle Hyperion Financial Reporting, Fusion Edition, Server	Provider Services	HTTP/HTTPS/TCPIP	Yes

Source	Destination	Protocol	Server to Server[1]
Financial Reporting Studio	Provider Services	HTTP/HTTPS/TCPIP	No
Financial Reporting Studio	Related Content Providers[2]	HTTP/HTTPS	No
Financial Reporting Studio	EPM Workspace Web server[3]	HTTP/HTTPS	No
Financial Reporting Studio	Shared Services Web application	HTTP/HTTPS	No
EPM Workspace Web server	Financial Reporting Web application	HTTP/HTTPS/AJP[4]	Yes
Financial Reporting Web application	EPM Workspace Web server	HTTP/HTTPS	Yes
Financial Reporting Web application	Provider Services	HTTP/HTTPS/TCPIP	Yes
Financial Reporting Web application	Related content providers	HTTP/HTTPS	Yes
Financial Reporting Web application	Shared Services Web application	HTTP/HTTPS	Yes
Financial Reporting Web application	Provider Services Web server	HTTP/HTTPS	Yes
Financial Reporting Scheduler	Web server (for EPM Workspace and Financial Reporting)	HTTP/HTTPS	Yes
Financial Reporting Scheduler	Provider Services Web server	HTTP/TCPIP	Yes
Oracle's Hyperion® Web Analysis Studio	EPM Workspace Web server	HTTP/HTTPS	No
Oracle's Hyperion® Web Analysis Studio	Shared Services Web application	HTTP/HTTPS	Yes
EPM Workspace Web server	Oracle's Hyperion® Web Analysis Web application	HTTP/HTTPS or AJP[5]	No
Web Analysis Web application	Shared Services Web application[6]	HTTP/HTTPS	Yes
Web Analysis Web application	User directories (Native Directory and external user directories)	LDAP/LDAPS	Yes
Web Analysis Web application	Provider Services	HTTP/HTTPS	Yes
Web Analysis Web application	EPM Workspace Web server[7]	HTTP/HTTPS	Yes

[1] If you are not using a trusted third-party CA for server-to-server communication, you must import the CA cert into the originating server keystore.

[2] Related content providers are applications such as Planning and EPM Workspace.

[3] For HTML export.

[4] AJP implementation is platform-specific.

[5] AJP implementation is platform-specific.

[6] For related content

[7] For related content

Note: If you are using Financial Reporting server machines with multiple IP addresses or server names, you can determine the server name that is returned to Financial Reporting. In all report services, add the `JVMOptionx ----> -Djava.rmi.server.hostname=` and `JVMOptiony ----> -Djava.rmi.server.useLocalHostname=false` registry keys and increment `jvmoptioncount`.

Table 4 Planning Connections That Can Be SSL-Enabled

Source	Destination	Protocol	Server to Server[1]
Browser	EPM Workspace Web server[2]	HTTP/HTTPS	No
Planning Web application	Shared Services Web application	HTTP/HTTPS	Yes
Planning Web application	User Directories (Native Directory and external user directories)	LDAP/LDAPS	Yes
Planning Web application	Performance Management Architect Web server	HTTP/HTTPS	Yes
Administration Services Console (for Oracle's Hyperion® Business Rules)[3]	Administration Services Web application	HTTP/HTTPS	Yes

[1] If you are not using a trusted third-party CA for server-to-server communication, you must import the CA cert into the originating server keystore.

[2] Planning is accessed through EPM Workspace Web server

[3] Business rules are designed in Administration Services Console

Table 5 Financial Management Connections That Can Be SSL-Enabled

Source	Destination	Protocol	Server to Server[1]
Browser	EPM Workspace Web server [2]	HTTP/HTTPS	No
EPM Workspace Web server	IIS (Financial Management Web server)[3]	HTTP/HTTPS	Yes
Financial Management application server	Performance Management Architect Web server	HTTP/HTTPS	Yes
Financial Management application server	Shared Services Web application	HTTP/HTTPS	Yes
Financial Management application server	User Directories (Native Directory and external user directories)	LDAP/LDAPS	Yes

[1] If you are not using a trusted third-party CA for server-to-server communication, you must import the CA cert into the originating server keystore.

[2] Financial Management is accessed through EPM Workspace Web server.

[3] Proxy redirection to the IIS used by Financial Management.

Table 6 Profitability and Cost Management Connections That Can Be SSL-Enabled

Source	Destination	Protocol	Server to Server[1]
Oracle Hyperion Profitability and Cost Management, Fusion Edition Web application	Performance Management Architect Web server	HTTP/HTTPS	Yes

[1] If you are not using a trusted third-party CA for server-to-server communication, you must import the CA cert into the originating server keystore.

Table 7 Performance Scorecard Connections That Can Be SSL-Enabled

Source	Destination	Protocol	Server to Server[1]
Browser	EPM Workspace Web server	HTTP/HTTPS	No
EPM Workspace Web server	Provider Services Web application	HTTP/HTTPS	Yes

Source	Destination	Protocol	Server to Server[1]
Oracle's Hyperion® Application Link	Oracle Hyperion Performance Scorecard, Fusion Edition application server	HTTP/HTTPS	No
Provider Services PowerConnect	Oracle Hyperion Performance Scorecard, Fusion Edition application server	HTTP/HTTPS	Yes

[1] If you are not using a trusted third-party CA for server-to-server communication, you must import the CA cert into the originating server keystore.

Required Certificates

EPM System supports one-way SSL communication. One-way SSL communication occurs when an SSL-enabled server component presents a certificate to its clients, but the clients do not present certificates to the server.

To establish an SSL connection, the clients must trust the CA that issued the server's certificate. Most popular third-party CAs are trusted by modern SSL capable applications, including Java.

If you use a CA unknown to the applications that establish SSL connectivity (as in the case of self-signed certificates), you must import the CA's public key certificate to the keystore of each application and into the Web server as needed. For example, if you are using self-signed certificates, you must import the public key certificate you used to sign all the certificate requests to each SSL client. In EPM System, SSL clients may include Web browsers and Java Virtual Machines (JVMs) such as server JVMs or thick clients.

Common Activities

This section discusses the common tasks that you should complete to enable SSL communication for EPM System products. They should be completed regardless of your operating system, application server, and Web server.

Required Certificates

You must use a valid certificate for each component that implements SSL. The following components can be SSL-enabled:

- User directories (MSAD and other LDAP-enabled directories)
- Application servers
- Web servers

See vendor documentation for detailed procedures on SSL-enabling these components.

Note: Each SSL-enabled component/server machine requires its own certificate. Using default or self-signed certificates is not recommended.

Obtaining and Using Certificates from a CA

Obtaining a certificate from a CA typically involves the following actions:

- Generating a certificate request and sending it to the CA for processing.
- Receiving the digitally signed certificate from the CA.

If the JRE is configured to use your own trusted keystore (and not the default trusted store `cacerts`), you must load the CA root certificate into your trusted keystore and not into the default trusted store `cacerts`. To determine whether your JRE is using your own trusted keystore, ensure that the `javax.net.ssl.trustStore` Java start parameter points to trusted keystore; for example, – `Djavax.net.ssl.trustStore=`*`Absolute_path_to_Trusted_keystore`*.

Location References

This book refers to the following installation locations:

- *`HYPERION_HOME`* denotes the root directory where Oracle's EPM System products are installed. The location of this directory is specified during installation. For example, `C:/Hyperion` (Windows) `/vol1/Hyperion` (UNIX).
- *`HSS_HOME`* denotes the Shared Services root directory; for example, `C:/Hyperion/deployments/`*`App_Server_Name`*`/SharedServices9` (Windows) and `/vol1/Hyperion/deployments/`*`App_Server_Name`*`/SharedServices9` (UNIX).
- *`ESSBASE_HOME`* denotes the Oracle Essbase root directory; for example, `C:/Hyperion/products/Essbase` (Windows) and `/vol1/Hyperion/deployments/`*`App_Server_Name`*`/SharedServices9` (UNIX).
- *`ORACLE_AS_HOME`* denotes the root directory where Oracle_AS is installed; for example, `C:/product/10.1.3.x/OracleAS_1` (Windows) and `/vol1/product/10.1.3.x/OracleAS_1` (UNIX).
- *`BIPLUS_HOME`* denotes the Reporting and Analysis root directory; for example, `C:/Hyperion/deployments/`*`App_Server_Name`*`/BIPLUS` (Windows) and `/vol1/Hyperion/deployments/`*`App_Server_Name`*`/BIPLUS` (UNIX).
- *`EAS_HOME`* denotes the Administration Services root directory; for example, `C:/Hyperion/products/Essbase/EAS` (Windows) and `/vol1/Hyperion/deployments/`*`App_Server_Name`*`/AAS` (UNIX).
- *`BEA_HOME`* denotes the root directory where WebLogic is installed; for example, `C:/bea` (Windows) and `/vol1/bea` (UNIX).
- *`TOMCAT_HOME`* denotes the installation location of Embedded Java Container. By default, Shared Services uses the Embedded Java Container installed in *`HYPERION_HOME`*`/deployments/Tomcat5`. Other EPM System products use similar *`TOMCAT_HOME`* locations.
- *`APACHE_HOME`* indicates the installation location of Apache Web server. By default, Reporting and Analysis installs Apache to *`HYPERION_HOME`*`/common/httpServers/`

`Apache/`*`apache_version`*; for example, `Hyperion/common/httpServers/Apache/2.0.52`.

- *`WEBSPHERE_HOME`* denotes the root directory where WebSphere application server is installed; for example, `C:/WebSphere/AppServer` (Windows) and `/vol1/WebSphere/AppServer` (UNIX).

Installing and Deploying EPM System Products

You must install and SSL-enable Shared Services before installing and SSL-enabling other EPM System products. See the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

While configuring Shared Services, you must select the “Enable SSL for Communications” check box in the EPM System Configurator to enable SSL communication for all EPM System products that share the Shared Services Registry.

Selecting the “Enable SSL for Communications” check box does not configure your environment to use SSL. You must complete additional procedures to SSL-enable your environment. These procedures are discussed in this document.

3 Configuring EPM System for SSL

In This Chapter

Shared Services

The instructions in this section assume that you have installed and deployed Shared Services for SSL by selecting “Enable SSL for Communications” in the EPM System Configurator. See the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

Note: See “Location References” on page 19 for a list of locations referenced in this document.

The default Shared Services SSL port is 28443. Use the following URL to access SSL-enabled Shared Services on the application server.

`https://`*`Host_Name`*`:`*`SSL_Port`*`/interop/index.jsp`; for example, `https://myServer:28443/interop/index.jsp`

Note: SSL-enabling Shared Services does not SSL-enable Workflow. To SSL-enable Workflow, add `sslEnabled=true` in `Hub.properties`.

➤ To SSL-enable Shared Services:

1 **Optional: If the CA root certificate you are using is not from a default trusted third-party CA, import the CA root certificate into the `cacerts` of the JVM. `cacerts` is in the `/lib/security` directory within the JRE install directory.**

   Ensure that you load the CA root certificate into all JREs used by EPM System (application server, EPM System applications, HTTP servers, LDAP servers, etc.). The typical location of the JVM:

   - Oracle Application Server: *`ORACLE_AS_HOME`*`/jdk/jre/lib/security`
   - WebLogic (you must import CA root certificate into both jRockit and SUN JVMs):
     - jRockit: *`BEA_HOME`*`/jrockit`*`version_number`*`/jre/lib/security/cacerts`
     - SUN: *`BEA_HOME`*`/jdk`*`version_number`*`/jre/lib/security/cacerts`

where *version_number* identifies the JRE version.

- WebSphere: *WEBSPHERE_HOME*/java/jre/lib/security//cacerts
- Tomcat (if using the Embedded Java Container installed by Oracle Hyperion Enterprise Performance Management System Installer, Fusion Edition): *HYPERION_HOME*/common/JRE/Sun/1.5.0/lib/security/cacerts

2 **Configure Shared Services on the application server using the appropriate procedures for the application server:**

- "SSL-Enabling Shared Services on Oracle Application Server" on page 23
- "SSL-Enabling Shared Services on WebLogic" on page 23
- "SSL-Enabling Shared Services on WebSphere" on page 24
- "SSL-Enabling Shared Services on Tomcat" on page 24

3 **If the CA root certificate you are using is not from a default trusted third-party CA, import the CA root certificate into** *HYPERION_HOME*/common/JRE/Sun/1.5.0/lib/security/cacerts.

4 **Optional: If EPM System products are deployed on a 64–bit operating system, import the CA certificate into** *HYPERION_HOME*/common/JRE-64/Sun/1.5.0/lib/Security/cacerts.

5 **SSL-enable user directory connections.**

a. Obtain the CA root certificate for your LDAP-enabled user directory.

b. If the CA root certificate you are using is not from a default trusted third-party CA, import the CA root certificate into the cacerts of the JVM. cacerts is in the /lib/security directory within the JRE install directory.

You can use different keystores for inbound and outbound requests. LDAPS is an outbound request from the application server; HTTPS is an inbound request.

Caution! When Oracle's EPM System applications are installed and deployed on multiple servers, if the root CA certificate is not from a trusted third-party CA, you must load the CA root certificate into all of the JREs that are used by EPM System products.

Note: All servers must be set up to open SSL connections when they are acting as SSL clients. For example, Planning Web application should open SSL connection to the user directory server.

6 **Restart Shared Services.**

7 **Log on to Oracle's Hyperion® Shared Services Console as Shared Services Administrator. Connect using the secure URL** https://*host*:*SSL-port*/interop/index.jsp; **for example,** https://myServer:28443/interop/index.jsp.

8 **SSL-enable the configurations of LDAP-enabled user directories.**

For detailed information on configuring user directories, see the *Oracle Enterprise Performance Management System Security Administration Guide*. On the User Directory Configuration screen:

- Verify that the value in the **Port** field identifies the SSL port of the user directory.

- Verify that **SSL Enabled** is selected.

SSL-Enabling Shared Services on Oracle Application Server

Requests sent to applications deployed to an Oracle Application Server instance are received by Oracle HTTP Server, which is, by default, configured as a part of Oracle Application Server.

Oracle recommends that you SSL-enable the communication between the Oracle HTTP Server and clients to secure Oracle's EPM System applications. If required, you can enhance security by using secure AJP instead of AJP for communication between the HTTP server and the OC4J instance that hosts Shared Services.

For detailed information on SSL-enabling Oracle HTTP Server, see "Enabling SSL for Oracle HTTP Server" in the *Oracle HTTP Server Administrator's Guide*. The procedures for SSL-enabling the Oracle HTTP Server include:

- Creating a wallet to store your credentials (certificate requests, certificates, and private keys). The default wallet installed with Oracle HTTP Server is primarily for testing.
- Editing `opmn.xml` (the primary configuration file for Oracle Process Manager and Notification Server) and changing the value of the start-mode property to `ssl-enabled`.

Note: Oracle HTTP Server based on Apache 1.3 does not support the `SSLProxyEngine` directive that is required for reverse-proxying requests to SSL protected targets. For example, you cannot proxy requests to an SSL protected Financial Management Web server using Oracle HTTP Server based on Apache 1.3. If SSL communication is required between Oracle HTTP Server and the applications for which it is acting as a reverse-proxy, you must use Oracle HTTP Server 2 (based on Apache 2), available on the Oracle 10gR3 Companion (10.1.3.x) CD. See Application Server 10g Release 3 (10.1.3.x) Downloads.

If you are using an HTTP server other than Oracle HTTP Server, see "Using Oracle Containers for J2EE Plug-in" in the *Oracle HTTP Server Administrator's Guide*.

SSL-Enabling Shared Services on WebLogic

➤ To SSL-enable Shared Services on WebLogic:

1. Log on to WebLogic Administration Console.
2. Select **Servers > Shared Services (admin)**.
3. From **General**, select **SSL Listen Port Enabled**.
4. Specify the port (for example, 28443) on which Shared Services listens for SSL communication.
5. From **Keystore**, set up the identity and trust keystore.

   If you are not using a root certificate from a trusted third-party CA, verify that your root CA certificate is loaded into the trust keystore and that the server certificate is loaded into your identity keystore.

6 From **SSL**, set up the key alias, certificate location, and pass phrase.

7 **Optional:** Click **Advanced** and set **Hostname Verification** value to `None`.

> **Note:** Disabling host name verification is not secure and is not recommended. If you do not disable host name verification, ensure that the host name that the client sees matches the host name specified in the certificate.

8 Save the configuration.

SSL-Enabling Shared Services on WebSphere

On WebSphere, Shared Services is deployed automatically to the SSL port. The SSL port number is the non-SSL port number plus 3. For example, Shared Services deployed to port 28080 also is deployed to SSL port 28443. This port is, by default, configured to use the built-in (default) certificates. You must modify the SSL settings to use the certificates you generated or obtained from a CA.

Note: If you are using Windows services to manage and monitor SSL-enabled EPM System products deployed on WebSphere, you must update the secure port number of the products in the Windows Registry keys to correctly reflect the applications' status. In general, the value data of the JVMOption parameter that indicates the HTTP listen port of the SSL-enabled application must be changed to reflect the secure (HTTPS) port. For example, assume that the SSL-enabled Shared Services port is 28443, and that `JVMOption2` parameter contains the Shared Services HTTP listen port value. You must update the value data of `JVMOption2` with the value of the secure listen port as shown in the example `HKEY_LOCAL_MACHINE\SOFTWARE\Hyperion Solutions \SharedServices9\HyS9SharedServices\JVMOption2="-Dwas.port=28443`.

➤ To SSL-enable Shared Services on WebSphere:

1 Log on to WebSphere Administrative Console.

2 Select **Security**, then **SSL**, and then **SharedServices9/DefaultSSLSettings**.

   a. In **Key file** section, identify the key file, key file password, and key file format.

   b. In the **Trust file** section, identify the trust file, trust file password, and trust file format.

   c. Click **Apply**.

   You can use different keystores for inbound and outbound requests. LDAPS is an outbound request; HTTPS is an inbound request. See WebSphere documentation for details.

SSL-Enabling Shared Services on Tomcat

➤ To SSL-enable Shared Services on Tomcat:

1 Create the certificate keystore and import certificates into the keystore.

2 **If you are not using a trusted third-party root CA certificate, import the certificates into the `cacerts` file.**

3 **Stop Shared Services.**

4 **Edit `server.xml`.**

a. Using a text editor, open *`TOMCAT_HOME`*`/SharedServices9/conf/server.xml`; for example, `C:/Hyperion/deployments/Tomcat5/SharedServices9/conf/server.xml`.

b. Comment out the following lines in `<Service name="Catalina">` to disable HTTP connectors:

```
<Connector port="28080" useBodyEncodingForURI="false" URIEncoding="UTF-8" />
```

c. Insert or update the `Connector` definition to enable HTTPS connector:

```
<Connector port="28443" minProcessors="5" maxProcessors="75"
enableLookups="true"
disableUploadTimeout="true"
acceptCount="100"
debug="1" scheme="https"
clientAuth="false"
sslProtocol="TLS"
keystoreFile="keystore_file" keystorePass="keystore_password" />
```

where *`keystore_file`* identifies the path to the signed certificate that you imported; for example, `C:/Hyperion/common/ssl/keystore/mykeystore.jks` and *`keystore_password`* indicates the keystore password.

The following attributes must be specified:

- `keystoreFile:` The location of a custom keystore file. Add this attribute if the keystore you created is not in the default location where Tomcat expects the keystore file (this file is named `.keystore` and generally is stored in the user's home directory). You can specify an absolute path or a path relative to the `$CATALINA_BASE` environment variable.
- `keystorePass:` The keystore password. You must add this attribute if you use a custom keystore. If you are using the default keystore, you must update the `keystorePass` if you use a password other than the default password (`changeit`).

Note: Specify the `keystoreType` element if you are using a PKCS12 keystore.

Note: The `Connector port` value (default - 28443) in `server.xml` must match the SSL port number recorded in the Shared Services Registry.

d. **Optional:** Set these additional attributes in the connector definition:

- `algorithm:` The certificate encoding algorithm to be used. If not specified, `SunX509`, the default value, is used. If you are configuring Shared Services on Tomcat running on an AIX server machine, you must set the value of the `algorithm` attribute in `SSL HTTP/1.1 Connector` definition to `ibmX509`.

- `useBodyEncodingForURI`: Indicates whether to use body encoding for URI. You must set this attribute to `false` if using Tomcat as the HTTP server for the Korean language version of Shared Services.
- `URIEncoding`: Indicates the character set for URI encoding. You must set this attribute to `UTF-8` if using Tomcat as the HTTP server for the Korean language version of Shared Services.

e. Save and close `server.xml`.

5 Restart Shared Services.

6 Configure other EPM System products for SSL.

WebSphere with LDAPS-Enabled User Directories

If you are using WebSphere 6.x with SSL-enabled user directories, you must import signer certificate from SSL-enabled user directories, and port signer certificate to Shared Services environment.

Importing Signer Certificates

Signer certificates must be imported from each LDAPS-enabled user directories configured in Shared Services.

➤ To import a signer certificate:

1 From WebSphere Administrative Console, select **Security** > **SSL certificate and key management** > **Manage endpoint security configurations.**

2 From **Local Topology**, select **nodes** from **Inbound**, and then select the node where Shared Services is installed.

3 On the Configuration screen, from **Additional Properties**, select **Signer certificates.**

4 Select **Retrieve from port.**

5 On the Configuration screen, enter the required information (host name, SSL port number, and alias) about the user directory from which signer certificate is to be imported.

6 Click **Retrieve signer information.**

7 Click **OK.**

Porting Signer Certificate Keystore to Shared Services

Port the keystore to Shared Services environment only after importing signer certificates from all configured SSL-enabled user directories.

➤ To port signer certificates to Shared Services environment:

1 Copy *`WEBSPHERE_HOME`*`/profiles/`*`profile_name`*`/config/cells/`*`cell_name`*`/nodes/`*`node_name`*`/trust.p12`.

2 Paste `trust.p12` into *HYPERION_HOME*`/deployments/WebSphere6/profile/config/cells/hyslCell/nodes/hyslNode` to overwrite the current file.

Note: If the root CA certificate is not from a trusted third-party CA, thick Java clients must import the root CA certificate into the client JRE `cacert`.

SSL-Enabling EPM System Web Applications

- “General Procedures” on page 27
- “Foundation Services” on page 28
- “Essbase” on page 29
- “Planning” on page 32
- “Financial Management” on page 32
- “Reporting and Analysis” on page 33

General Procedures

The process for SSL-enabling EPM System Web applications is identical across applications. See “Shared Services” on page 21 for a detailed procedure that uses Shared Services as an example. Any deviation from the procedure is documented in the following sections.

In a deployment scenario, EPM System Web applications are installed into *HYPERION_HOME*. During deployment, you specify the Oracle's Hyperion Shared Services Registry that the applications must use.

Most EPM System Web application users are managed in the user directories configured in Shared Services. If Shared Services is configured to access the user directories over secure connection, you must import the CA root certificate of the LDAP user directory into the JVM of the application server that hosts the Web application.

Note: If you get a host name mismatch error during a session, ensure that the host name that the client sees matches the host name (common name) in the certificate.

➤ To configure an EPM System Web application:

1 Install and deploy the EPM System component as instructed in the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

2 Configure the SSL port on the application server. For detailed instructions, see one of the following topics that describe how to SSL-enable Shared Services. Adapt the procedures to use the secure port used by the application.

   - “SSL-Enabling Shared Services on Oracle Application Server” on page 23
   - “SSL-Enabling Shared Services on WebLogic” on page 23
   - “SSL-Enabling Shared Services on WebSphere” on page 24

- "SSL-Enabling Shared Services on Tomcat" on page 24

Note: The `server.xml` file that you must edit to SSL-enable EPM System applications on the Embedded Java Container (Tomcat) is available in *`HYPERION_HOME`*`/deployments/ Tomcat5/PRODUCT_CODE/conf` directory. For example, this file for Administration Services is available in `C:/Hyperion/deployments/Tomcat5/eas`.

3 **Perform the required application-specific steps.**

- "Foundation Services" on page 28
- "Essbase" on page 29
- "Planning" on page 32
- "Financial Management" on page 32
- "Reporting and Analysis" on page 33

4 **If you are using a Web server, configure it.**

- "Configuring the EPM System with Oracle HTTP Server" on page 35
- "Configuring EPM System with Apache" on page 35
- "Configuring EPM System with IIS" on page 38

5 **Restart your environment (Web server, application server, and Web application).**

6 **Configure the client. If you are configuring a thick Java client that opens an SSL connection using a root certificate that is not from a trusted third-party CA, you must import the root CA certificate into the client JRE `cacert`.**

Foundation Services

The following Oracle's Hyperion® Foundation Services components use the general deployment procedures. See "General Procedures" on page 27.

- EPM Workspace
- Performance Management Architect
- Calculation Manager
- Smart Space

Smart View can connect to the following SSL-enabled data sources:

- Essbase, Planning, and Oracle Business Intelligence Enterprise Edition using Provider Services
- Financial Management, Planning, and Reporting and Analysis using independent providers

If an SSL-enabled Web server is used as a front-end for the data source provider, Smart View Client can use HTTPS to connect to the Web server.

After SSL-enabling EPM Workspace, verify that the value of `ConfigurationManager.hubUseSSL` in the `v8_prop_value` table in the repository is set to `true`.

Note: SSL-enabling EPM Workspace SSL-enables Oracle's Hyperion® Interactive Reporting.

Configuring EPM Workspace Services

You must manually configure EPM Workspace services for SSL by editing *`HYPERION_HOME`*`/common/workspacecert/9.5.0.0/common/config/task.xml`.

➤ To configure EPM Workspace services:

1. **Stop the EPM Workspace agent.**
2. **Using a text editor, open** `task.xml`**.**
3. **Append the following directives to EPM Workspace task type definition** `(<task type=”workspace”>):`

   ```
   <system property="javax.net.ssl.trustStore">${HYPERION_HOME}${/}common${/}ssl$
   {/}keystore</system>
   ```

   ```
   <system property="javax.net.ssl.password">password</system>
   ```

   `trustStore` specifies the trust store where the CA certificate is stored and *`password`* indicates the CA certificate password. You do not need to specify the *`password`* directive is you are using the default password.
4. **Save and close** `task.xml`**.**
5. **Start EPM Workspace agent.**

Smart Space on Tomcat

Add the following JVM option in `setCustomParamsSmartSpaceWebServices.bat` to disable certificate checking for Oracle Smart Space, Fusion Edition, service-to-service communications. This file is available in `C:/Hyperion/deployments/Tomcat5/bin`.

```
-Daxis.socketSecureFactory= org.apache.axis.components.net.SunFakeTrustSocketFactory
```

Performance Management Architect

Performance Management Architect server requires an SSL certificate for IIS even if you are using an Apache Web server. Without this certificate, Performance Management Architect cannot connect to the Apache Web server.

Essbase

The following Essbase components use the general deployment procedures. See “General Procedures” on page 27.

- Oracle Hyperion Provider Services
- Oracle Hyperion Smart Search Command Line Utility
- HAB.Net

Essbase Server

Essbase Server cannot be SSL-enabled. It can, however, communicate with a Shared Services instance that is SSL-enabled.

After SSL-enabling Shared Services, verify that you can successfully start the Oracle Essbase Server and communicate with Shared Services.

Administration Services

The default Administration Services Client SSL port is 10083. Use the following URL to access SSL-enabled Administration Services Server on the application server.

Note: If the root CA certificate is not from a trusted third-party CA, you must import the CA root certificate into the JVM `cacert`. The JVM location can be identified from `essbase.cfg`.

Note: When you access an SSL-enabled Administration Services Console from a browser for the first time, the Administration Services Console presents its certificate, which you must accept and import into the browser's JVM. If you do not accept the certificate, a “404–NotFound” message is displayed.

➤ To configure Administration Services:

1 **Edit** *`EAS_HOME`*`/server/HUB.properties`**.**

   a. Using a text editor, open `Hub.properties`; for example, `C:/Hyperion/products/Essbase/eas/server/HUB.properties`.

   b. Update the port number to reflect the SSL-enabled port of Shared Services.

   c. Set `HubUseSecure` to `true`. If the `HubUseSecure` property is not present in the file, add it.

   d. Save and close `HUB.properties`

2 **Update** `setCustomParamseas.bat`**.**

   a. Using a text editor, open `setCustomParamseas.bat`; for example, `C:/Hyperion/deployments/Tomcat5/bin/setCustomParamseas.bat`.

   b. **WebSphere, WebLogic, and Oracle Application Server:** Append the `JAVA_OPTIONS` directive with the following:

   Note: **Embedded Java Container only:** Append the `SET JAVA_OPTS` directive.

keystore_file `-Djavax.net.ssl.password =`*keystore_password* here *keystore_file* identifies the path to the signed certificate that you imported; for example, `C:/Hyperion/common/ssl/keystore/mykeystore.jks` and *keystore_password* indicates the keystore password.

c. Save and close `setCustomParamseas.bat`.

3 **Optional**: If you plan to start Administration Services as a Windows service, add these options in the Windows Registry key for Administration Services:

- `JVMOptionX`
- `JVMOPTIONSCOUNT`

4 Restart Administration Services.

WebSphere Information

You must add generic JVM arguments for Administration Services web application to support SSL.

➤ To add generic JVM arguments for Administration Services web application:

1 Stop Administration Services web application if it is running. Select **Start** then **Programs** then **Oracle EPM System** then **Essbase** then **Administration Services**, and then **Stop Administration Services (WebSphere).**

2 Log in to WebSphere Administrative Console.

3 Expand the **Servers** node and select **Application Servers.**

Application servers page, which lists the application servers in the cell, opens.

4 Select **eas.**

5 In **Server Infrastructure**, expand **Java and Process Management**, and select **Process Definition.**

6 From **Additional Properties**, select **Java Virtual Machine**

7 In **Generic JVM arguments**, enter the following JVM arguments.

Note: Update the JVM arguments to reflect the values for your deployment. The following JVM arguments assume that your *HYPERION_HOME* is `C:\Hyperion`, SSL trust store is `C:\Hyperion\common\ssl\keystore`, and trusted JKS keystore password is `password`.

```
-DcomponentId=a9500b0d98e652a9735493ff11f80e5d0d47a98 -Dsun.net.inetaddr.ttl=0
-DHYPERION_HOME=C:\Hyperion -Dhyperion.home=C:\Hyperion -DEAS_LOG_LOCATION=C:
\Hyperion\logs\eas\easserver.log -DEAS_LOG_LEVEL=5000 -Djavax.net.ssl.trustStore=C:
\Hyperion\common\ssl\keystore -Djavax.net.ssl.trustStorePassword=password
```

8 Click **OK** repeatedly until **Application servers** page is displayed.

9 After all SSL-related tasks have been completed, start Administration Services web application. Select **Start** then **Programs** then **Oracle EPM System** then **Essbase** then **Administration Services**, and then **Start Administration Services (WebSphere).**

Tomcat Information

Because Administration Services Web console cannot be loaded through HTTPS, do not disable HTTP connector for Administration Services. You must always load Oracle Essbase Administration Services Web console using the nonsecure URL.

Administration Services Client

➤ To SSL-enable the Administration Services client:

1 **Using a text editor, open** `admincon.lax`**; for example,** `C:/Hyperion/products/Essbase/eas/console/bin/admincon.lax`**.**

2 **Locate the line that starts with** `lax.nl.java.option.additional`**.**

3 **Append the following parameters to the value of** `lax.nl.java.option.additional=` **property:**

```
-Djavax.net.ssl.trustStore=keystore_file
-Djavax.net.ssl.password= keystore_password
```

where *`keystore_file`* identifies the name and absolute location of the signed CA root certificate that you imported, for example, `C:/Hyperion/common/JRE/Sun/1.5.0/lib/security/cacerts` and *`keystore_password`* indicates the keystore password. See "Importing Signer Certificates" on page 26.

4 **Save and close** `admincon.lax`**.**

Planning

Oracle Hyperion Planning, Fusion Edition Web application uses the general deployment procedures. See "General Procedures" on page 27.

Financial Management

If you are setting up SSL using a root CA certificate that is not from a trusted third-party CA, you must import the root CA certificate into the Windows certificate trusted store on the machine where the Win 32 Client is running. Use Microsoft Management Console to import the certificate. If you are using Microsoft certificate server, see Microsoft documentation at http://support.microsoft.com/kb/218445/ for detailed procedures to install the root CA certificate on the client.

These applications use standard procedures:

- Financial Management
- Financial Management Oracle Hyperion Smart View for Office, Fusion Edition Provider

Financial Management Web application is hosted on IIS application server, which you must SSL-enable. See "Web Servers" on page 8.

Reporting and Analysis

The following Reporting and Analysis components use the general deployment procedures. See "General Procedures" on page 27.

- Web Analysis
- Financial Reporting

Communication with Reporting and Analysis components are always routed through a Web server, which must be SSL-enabled.

Note: If you are using Oracle Access Manager WebGate, Financial Reporting may not stream PDF content to Internet Explorer if SSL is enabled between the Internet Explorer and the Web server. This is because, WebGate, by default, sets the values of `CachePragmaHeader` and `CacheControlHeader` to `no-cache`. Oracle recommends that you set the value of these parameters to `public`.

Web Analysis

If Web Analysis is SSL-enabled using a root CA certificate that is not issued by a trusted third-party CA, you must load the root CA into the JRE keystore used by the browser so that the Web Analysis client (Java applet) can connect successfully to the SSL-enabled server.

Encrypting RMI Communication Among Financial Reporting Components

Communication among Financial Reporting's stand-alone Java components (Studio, Report Server, and Print Server) uses Remote Method Invocation (RMI) and can be encrypted.

➤ To encrypt RMI communication among Financial Reporting components:

1. **Open the `fr_repserver.properties` file on the server that hosts the Financial Reporting Report Server.**
2. **Uncomment the following line:**

   `RMI_Encryptor=com.hyperion.reporting.security.impl.HsRMICryptor`.
3. **Save `fr_repserver.properties`.**

FDM

If the certification authority is not from a trusted third party, you must import the public certificate of the CA that is used for signing Shared Services certificate into the trusted keystore that is used by *HYPERION_HOME*`/common/JRE`. This should be done on each server where Oracle Hyperion Financial Data Quality Management, Fusion Edition components are installed.

4 Configuring Web Servers for EPM System

In This Chapter

Configuring the EPM System with Oracle HTTP Server

By default, EPM System products deployed to Oracle Application Server use the built-in Oracle HTTP Server. The deployment process configures the Oracle HTTP Server, which you must SSL-enable.

For information on configuring Oracle HTTP Server for SSL, see "Enabling SSL for Oracle HTTP Server" in the *Oracle HTTP Server Administrator's Guide*.

Configuring EPM System with Apache

The Apache Web server that is installed when you install and deploy Reporting and Analysisis not SSL-compatible. Oracle recommends that you obtain an SSL-compatible Apache Web server (2.0.59) to support EPM System products.

Note: Oracle recommends that you back up the existing Apache installation in `HYPERION_HOME/common/httpServers/Apache/apache_version` and then install Apache so that it overwrites the existing Apache installation.

See your Web server documentation (see "Web Servers" on page 8) for instructions on SSL-enabling the Web server.

Apache with Oracle Application Server

For instructions to use Apache with Oracle Application Server see "Integrating Generic Apache with Oracle Application Server" in the *Oracle HTTP Server Administrator's Guide*.

Apache with WebLogic

This discussion assumes that you have SSL-enabled the Apache Web server.

The Web server plug-in (`HYSL-WebLogic.conf`) required to establish a connection between Apache and WebLogic is generated in `*HYPERION_HOME*/common/httpServers/Apache/2.0.59/conf`. You must modify `HYSL-WebLogic.conf` to specify SSL ports for EPM System products; for example, Web Analysis and Financial Reporting.

➤ To update the Web server configuration file:

1 **Using a text editor, open** *HYPERION_HOME*`/common/httpServers/Apache/2.0.59/conf/HYSL-WebLogic.conf`**.**

2 **In each** `LocationMatch` **definition, update the** `WeblogicCluster` **property to reflect the application server SSL ports used by EPM System products.**

`HYSL-WebLogic.conf` contains numerous `LocationMatch` definitions. For example, Web Analysis-related definitions are indicated by `/WebAnalysis` (for example, `<LocationMatch /WebAnalysis/..`), and Financial Reporting definitions are indicated by `/hr` (for example, `<LocationMatch /hr`).

A sample `LocationMatch` definition for EPM Workspace UI Services:

```
<LocationMatch /workspace/cdsrpc$>
      SetHandler weblogic-handler
      PathTrim /
          KeepAliveEnabled ON
      KeepAliveSecs 20
      WeblogicCluster host.example.com:45003
</LocationMatch>
```

3 **In** `HYSL-WebLogic.conf` **turn on the secure proxy and identify the absolute path where the trusted CA file is stored. You can do so by including the following parameters:**

```
SecureProxy ON
TrustedCAFile location_of_certificate
```

`location_of_certificate` must be expressed as the absolute path to the certificate file; for example, `C:/certificates/ssl-keys/CA.crt`.

Note: If you get a host name mismatch error during a session, you can either turn off SSL host matching by including the parameter `RequireSSLHostMatch=false`, or ensure that the host name that the client sees matches the host name in the certificate.

4 **Save and close** `HYSL-WebLogic.conf`**.**

5 **Restart the Apache Web server.**

6 **Connect to Reporting and Analysis applications by accessing the SSL-enabled Web URL.**

Apache with Tomcat

Communication between the Apache Web server and Tomcat application server uses the binary Apache JServ Protocol (AJP), which cannot be SSL-enabled.

SSL-enabling the Apache Web server establishes secure communication between the Apache server and the browser.

Note: If this Apache server installation is used as a Web server for other EPM System components, you must perform additional configuration steps as described in the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

Note: Performance Management Architect server requires an SSL certificate for IIS even when you are using an Apache Web server. Without this certificate, Oracle Hyperion EPM Architect, Fusion Edition cannot connect to the Apache Web server.

Apache with WebSphere

If you plan to enable SSL communication between a Web server and a WebSphere application server, you must install the Global Security Kit (GSKit) on the machine hosting the Web server. See IBM documentation for detailed instructions on installing GSKit.

The `plugin-cfg.xml` that is required to establish communication between the Apache Web server and the WebSphere application server that hosts Reporting and Analysis applications is autogenerated in *`APACHE_HOME`*`/conf` when you deploy the application using the EPM System Configurator. This file must be updated with appropriate transport information from `plugin-cfg.xml` generated by the SSL-enabled application server.

The automated deployment process deploys Oracle's Hyperion Reporting and Analysis applications to separate profiles on the application server. You must generate `plugin-cfg.xml` for each application.

➤ To configure Reporting and Analysis for an SSL-enabled Apache Web server:

1 **Generate `plugin-cfg.xml` for EPM System products.**

   a. Open a command prompt window.

   b. Navigate to *`HYPERION_HOME`*`/deployments/WebSphere6/profile/bin`.

   c. Execute `GenPluginCfg.bat` (Windows) or `GenPluginCfg.sh` (UNIX).

   WebSphere generates `plugin-cfg.xml` in *`HYPERION_HOME`*`/deployments/WebSphere6/profile/config/cells`.

2 **Copy the transport definition from `plugin-cfg.xml`, which you generated in step 1.**

   a. Using a text editor, open *`HYPERION_HOME`*`/deployments/WebSphere6/profile/config/cells/plugin-cfg.xml`. This file contains a transport definition for each Web application.

   b. Copy the `Transport` definition, a sample of which is presented below:

```
<Transport Hostname="myServer.example.com" Port="45000" Protocol="http" />
<Transport Hostname="myServer.example.com" Port="45002" Protocol="https" >
   <Property Name="keyring" Value="c:\Program Files\IBM\WebSphere\Plugins\etc
\plugin-key.kdb" />
   <Property Name="stashfile" Value="c:\Program Files\IBM\WebSphere\Plugins\etc
\plugin-key.sth" />
</Transport>
```

Note: You may remove the HTTP transport definition if the application server is SSL-enabled.

3 **Update Apache's `plugin-cfg.xml`.**

a. Using a text editor, open Apache's `plugin-cfg.xml`, in *`APACHE_HOME`*`/conf`; for example, `C:/Hyperion/common/httpServers/Apache/`*`2.0.59`*`/conf`

b. Paste the `Transport` definition you copied from the WebSphere-generated plug-in file to replace the existing `Transport` definition.

Caution! `plugin-cfg.xml` contains a `Transport` definition for each Web application. Ensure that you paste the `transport` definition to the correct location.

c. Verify that the `keyring` and `stashfile` properties in the `Transport` definition are accurate.

d. In the `<VirtualHostGroup>` definition, insert a virtual host definition, which identifies the SSL port used by the application; for example, you may insert the following definition for Web Analysis:

```
<VirtualHost Name="*:16002" />
```

e. Save and close `plugin-cfg.xml`.

4 **Restart the Apache Web server.**

Configuring EPM System with IIS

- "IIS with Oracle Application Server" on page 38
- "IIS with WebLogic" on page 39
- "IIS with Tomcat" on page 40
- "IIS with WebSphere" on page 40

IIS with Oracle Application Server

If you are using IIS to front-end Oracle HTTP Server, you must configure the Oracle_AS Proxy Plug-in. See "Using Oracle Application Server Proxy Plug-in" in the *Oracle HTTP Server Administrator's Guide*.

If you are configuring IIS to access the Oracle Containers for J2EE (OC4J), you must configure the OC4J Plug-in. See "Using Oracle Containers for J2EE Plug-in" in the *Oracle HTTP Server Administrator's Guide*.

Note: Oracle's IIS proxy DLL, which is used when using IIS as a reverse proxy for Oracle Application Server, does not support SSL, leaving the communication between the IIS Web server and other Web servers unencrypted. For instance, assume that EPM Workspace is deployed on Oracle Application Server with an IIS HTTP server and Oracle Hyperion Financial Management, Fusion Edition, is deployed on a different IIS instance. In this scenario, the communication between the two IIS instances cannot be SSL-enabled. This issue can be resolved by using a single IIS instance to host all EPM System products.

IIS with WebLogic

The `iisproxy.ini` file is generated during the deployment of EPM System products to the application server. This file is created only for EPM System that require the use of an HTTP server. `iisproxy.ini` contains `name=value` pairs that define configuration parameters for the IIS plug-in (`iisproxy.dll`). The locations of `iisproxy.ini`:

- **Oracle Enterprise Performance Management Workspace, Fusion Edition:** *`HYPERION_HOME`*`/deployments/WebLogic9/workspace`
- **Web Analysis:** *`HYPERION_HOME`*`/deployments/WebLogic9/WebAnalysis`
- **Oracle Hyperion Financial Reporting, Fusion Edition:** *`HYPERION_HOME`*`/deployments/WebLogic9/hr`

A sample `iisproxy.ini`:

```
WebLogicCluster=myserver.example.com:port
ConnectTimeoutSecs=20
ConnectRetrySecs=2
WlForwardPath=/workspace
DynamicServerList=ON
SecureProxy=ON
TrustedCAFile=location_of_certificate
```

`location_of_certificate` must be expressed as the absolute path to the certificate file; for example, `C:/certificates/ssl-keys/CA.crt`.

Note: If you get a host name mismatch error during a session, you can either turn off SSL host matching by including the parameter `RequireSSLHostMatch=false`, or ensure that the host name that the client sees matches the host name in the certificate.

➤ To configure IIS redirection to Reporting and Analysis running on the WebLogic server:

1. **Using a text editor, open `iisproxy.ini` for the application; for example, Web Analysis, for which you want to configure IIS redirection.**
2. **Verify that the following directives are set correctly:**

```
SecureProxy=ON
TrustedCAFile=location_of_certificate
```

location_of_certificate must be expressed as the absolute path to the certificate file; for example, `C:/certificates/ssl-keys/CA.crt`.

Note: If you get a host name mismatch error during a session, you can either turn off SSL host matching by including the parameter `RequireSSLHostMatch=false`, or ensure that the host name that the client sees matches the host name specified in the certificate.

3 **Save and close** `iisproxy.ini`**.**

4 **Repeat the procedure for other applications.**

IIS with Tomcat

Communication between the IIS and Tomcat servers uses AJP. SSL-enabling the IIS server is sufficient to establish secure communication between the IIS server and the browser.

Note: If this IIS server installation is used as the Web server for other products, you must perform additional configuration steps as described in the *Oracle Enterprise Performance Management System Installation and Configuration Guide*.

IIS with WebSphere

If you plan to enable SSL communication between a Web server and the WebSphere application server, you must install GSKit on the machine hosting the Web server. See IBM documentation for detailed instructions on installing GSKit.

The `plugin-cfg.xml` file that is required to establish communication between the IIS server and the WebSphere application server that hosts EPM System applications is autogenerated when you deploy the application using the EPM System Configurator. The default location of `plugin-cfg.xml` file is *`HYPERION_HOME`*`/deployments/WebSphere6/`*`EPM_APP`*`/profile/config/cells`. For example, for Oracle's Hyperion® Web Analysis, `plugin-cfg.xml` is generated in `C:/Hyperion/deployments/WebSphere6/WebAnalysis/profile/config/cells`.

EPM System Configurator deploys EPM System applications into a WebSphere profile, allowing you to generate the `plugin-cfg.xml` for the entire profile.

`plugin-cfg.xml` must be updated with transport information from the SSL-enabled WebSphere server. Transport information can be extracted from `plugin-cfg.xml` generated by the application server.

➤ To generate `plugin-cfg.xml` for EPM System products:

1 **Open a command prompt window.**

2 **Navigate to** *`HYPERION_HOME`*`/deployments/WebSphere6/profile/bin` **directory.**

3 **Execute** GenPluginCfg.cmd **(Windows) or** GenPluginCfg.sh **(UNIX).**

The WebSphere server generates plugin-cfg.xml for all the EPM System servers in the hys1Cell. This file is generated in *HYPERION_HOME*/deployments/WebSphere6/profile/config/cells.

4 **Restart IIS.**

Registering IIS Proxy URLs with Shared Services

The Oracle's Hyperion Enterprise Performance Management System Configurator does not register IIS proxy URLs directly in Oracle's Hyperion® Shared Services. You must complete the following manual steps if the Oracle Hyperion Enterprise Performance Management System Web application uses IIS as the Web server. These procedures are not applicable if an Apache Web server is used.

➤ To register IIS proxy URLS with Shared Services:

1 **Open Microsoft Word.**

2 **Select File > Open.**

3 **In File name, enter the following URL:**

http://*hss_server_name*:*port_no*/interop/content; for example, http://myServer:28080/interop/content.

4 **Log in as** admin **user.**

5 **Browse to** files/Products/*product_name*/Published/

6 **Open every instance file that is present.**

7 **Right-click every context node, and select Attributes.**

8 **Change the URL, port number, and logical Web application name as needed.**

9 **Save the document.**

Index