Oracle® Collaboration Suite

SSL Configuration

Release 2 (9.0.4)

Part No. B15611-01

November 2004

ORACLE®

Oracle Collaboration Suite SSL Configuration, Release 2 (9.0.4)

Part No. B15611-01

Primary Author: Daria Hutchinson

Contributors: Richard J. Hall, Andrew Soutar, Lyju Vadassery, Meera Viswanathan

Contents

List of Figures

Send Us Your Comments

Oracle Collaboration Suite SSL Configuration, Release 2 (9.0.4)

Part No. B15611-01

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, please indicate the title and part number of the documentation and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: infodev_us@oracle.com
- FAX: (650) 506-7410. Attn: Oracle Collaboration Suite Documentation Manager
- Postal service:

  Oracle Corporation
  Server Technologies Documentation Manager
  500 Oracle Parkway, Mailstop 2op5
  Redwood Shores, CA 94065
  USA

If you would like a reply, please give your name, address, telephone number, and electronic mail address (optional).

If you have problems with the software, please contact your local Oracle Support Services.

Preface

This preface contains these topics:

Intended Audience

Oracle Collaboration Suite SSL Configuration provides concepts and procedures for configuring SSL to secure communications between Oracle9*i* Application Server Middle Tier and browser clients. The examples presented in this document apply to UNIX platforms.

This document is intended for system administrators responsible for the following tasks:

- Configuring Middle Tier security for Oracle Collaboration Suite
- Implementing security technologies

This document assumes that the reader has knowledge of enterprise network topologies, UNIX operating systems, Internet protocols, and Web server administration concepts.

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. 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 additional information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

JAWS, a Windows screen reader, 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, JAWS 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.

Structure

This book has the following structure:

Chapter 1, "Overview of SSL in Oracle Collaboration Suite"

This chapter provides some high-level information about SSL and the associated connections and ports involved in configuring SSL for Oracle Collaboration Suite components.

Chapter 2, "Before You Begin"

This chapter provides information for validating your current Oracle Collaboration Suite installation before you begin configuring SSL.

Chapter 3, "Creating Wallets"

This chapter provides information about using Oracle Wallet Manager to create wallets that contain your SSL certificates to use in your SSL configuration.

Chapter 4, "Configuring Web Cache for SSL"

This chapter provides information about configuring Web Cache for SSL.

Chapter 5, "Configuring SSL for Oracle9iAS Single Sign-On Administration"

This chapter provides instructions for configuring SSL to the Single Sign-On Administration interface.

Chapter 6, "Configuring SSL for the Infrastructure"

This chapter provides instructions for configuring the Infrastructure tier of Oracle Collaboration Suite to recognize SSL connections.

Chapter 7, "Configuring SSL for the Middle Tier Applications"

This chapter provides instructions for configuring the Middle Tier of Oracle Collaboration Suite to recognize SSL connections.

Chapter 8, "Configuring Oracle Web Conferencing for SSL"

This chapter provides instructions for enabling Oracle Web Conferencing to work over SSL.

Chapter 9, "Configuring Oracle Calendar for SSL"

This chapter provides instructions for configuring Calendar for SSL if the standard ports are being used. This only applies to a distributed installation.

Appendix A, "Troubleshooting"

This appendix provides troubleshooting information for problems you may encounter while configuring Oracle Collaboration Suite for SSL.

Related Documents

For more information, see these Oracle resources:

- *Oracle9i* Application Server Administrator's Guide *Release 2 (9.0.2)*
- *Oracle9i* Application Server Security Guide *Release 2 (9.0.2)*
- *Oracle9i* Application Server Single Sign-On Administrator's Guide *Release 2 (9.0.2)*
- *Oracle9i*AS Web Cache Administration and Deployment Guide *Release 2 (9.0.2)*
- *Oracle Collaboration Suite Installation and Configuration Guide for Solaris*
- *Oracle Web Conferencing Administration Guide*

Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- Conventions in Text
- Conventions in Code Examples

Conventions in Text

We use various conventions in text to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an **index-organized table**.
Italics	Italic typeface indicates book titles or emphasis.	*Oracle Database Concepts* Ensure that the recovery catalog and target database do *not* reside on the same disk.
`UPPERCASE monospace (fixed-width) font`	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, usernames, and roles.	You can specify this clause only for a `NUMBER` column. You can back up the database by using the `BACKUP` command. Query the `TABLE_NAME` column in the `USER_TABLES` data dictionary view. Use the `DBMS_STATS.GENERATE_STATS` procedure.

Convention	Meaning	Example
lowercase monospace (fixed-width) font	Lowercase monospace typeface indicates executables, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, usernames and roles, program units, and parameter values. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter `sqlplus` to open SQL*Plus. The password is specified in the `orapwd` file. Back up the datafiles and control files in the `/disk1/oracle/dbs` directory. The `department_id`, `department_name`, and `location_id` columns are in the `hr.departments` table. Set the `QUERY_REWRITE_ENABLED` initialization parameter to `true`. Connect as `oe` user. The `JRepUtil` class implements these methods.
lowercase italic monospace (fixed-width) font	Lowercase italic monospace font represents placeholders or variables.	You can specify the *`parallel_clause`*. Run `U`*`old_release`*`.SQL` where *`old_release`* refers to the release you installed prior to upgrading.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
`[ ]`	Brackets enclose one or more optional items. Do not enter the brackets.	`DECIMAL (`*`digits`*` [ , `*`precision`*` ])`
`{ }`	Braces enclose two or more items, one of which is required. Do not enter the braces.	`{ENABLE | DISABLE}`
`|`	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options. Do not enter the vertical bar.	`{ENABLE | DISABLE}` `[COMPRESS | NOCOMPRESS]`
`...`	Horizontal ellipsis points indicate either: ■ That we have omitted parts of the code that are not directly related to the example ■ That you can repeat a portion of the code	`CREATE TABLE ... AS `*`subquery`*`;` `SELECT `*`col1`*`, `*`col2`*`, ... , `*`coln`*` FROM employees;`

Convention	Meaning	Example
. . .	Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.	SQL> SELECT NAME FROM V$DATAFILE; NAME ---------- /fsl/dbs/tbs_01.dbf /fs1/dbs/tbs_02.dbf . . . /fsl/dbs/tbs_09.dbf 9 rows selected.
Other notation	You must enter symbols other than brackets, braces, vertical bars, and ellipsis points as shown.	acctbal NUMBER(11,2); acct CONSTANT NUMBER(4) := 3;
Italics	Italicized text indicates placeholders or variables for which you must supply particular values.	CONNECT SYSTEM/*system_password* DB_NAME = *database_name*
UPPERCASE	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. However, because these terms are not case sensitive, you can enter them in lowercase.	SELECT last_name, employee_id FROM employees; SELECT * FROM USER_TABLES; DROP TABLE hr.employees;
lowercase	Lowercase typeface indicates programmatic elements that you supply. For example, lowercase indicates names of tables, columns, or files. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	SELECT last_name, employee_id FROM employees; sqlplus hr/hr CREATE USER mjones IDENTIFIED BY ty3MU9;

1

Overview of SSL in Oracle Collaboration Suite

Oracle Collaboration Suite relies on the Infrastructure of Oracle9*i* Application Server to host and serve its applications. Enabling Secure Sockets Layer (SSL) for Oracle Collaboration Suite involves configuring the following components:

- Oracle9*i* Application Server Web Cache
- Oracle9*i* Application Server Single Sign-On
- Oracle Delegated Administration Services
- Oracle Collaboration Suite applications
- Oracle HTTP Server (on the Middle Tier and the Infrastructure tier)

This document explains how to configure SSL for these components only, and provides instructions for both a single-box installation and a distributed installation of Oracle Collaboration Suite.

This document refers to the **Infrastructure tier** and the **Middle Tier** of Oracle Collaboration Suite. The following clarifies which components reside on each tier:

- Infrastructure tier refers to the Oracle9*i*AS Single Sign-On, Oracle HTTP Server for Oracle9*i*AS Single Sign-On, and Oracle Delegated Administration Services.
- Middle Tier refers to the Oracle Collaboration Suite applications, Oracle HTTP Server for Oracle Collaboration Suite applications, and Web Cache.
- For a single-box installation, a Web Cache reverse proxy sits in front of the Middle Tier and accepts and redirects incoming HTTP/HTTPS requests. Web Cache in the Middle Tier is disabled.
- For a distributed installation, Web Cache is running on the Middle Tier and accepts incoming HTTP/HTTPS requests to the Middle Tier. Requests to the Infrastructure tier bypass Web Cache in a distributed installation.

This chapter contains the following topics:

1.1 Overview of SSL Configuration

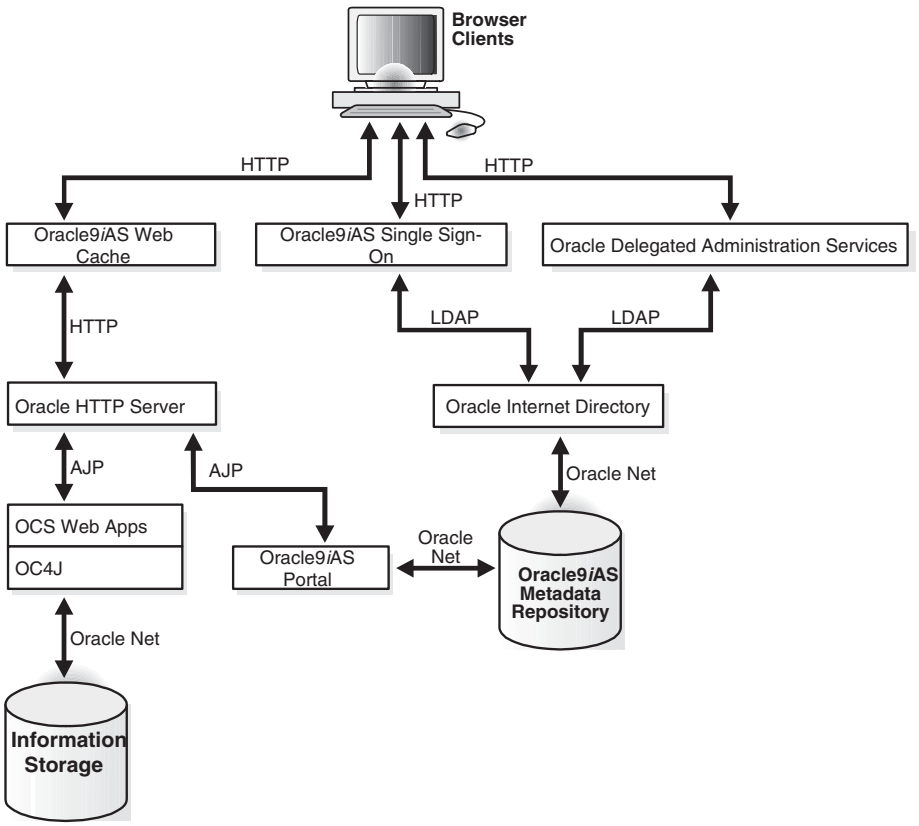
You enable components in Oracle9*i* Application Server to use SSL using the Enterprise Manager Web site. In some cases, you need to manually edit configuration files.

SSL secures communication between two parties: a client and a server. If three or more parties are involved, for example, client browser, Web Cache, Oracle HTTP Server, and OC4J, then you may have to configure all components to use SSL.

Figure 1–1 shows typical communication paths between Oracle9*i* Application Server components and the protocols that they use. For example, browsers use HTTP to communicate with Web Cache, and Oracle HTTP Server uses Apache Java Protocol (AJP) to communicate with OC4J. All these protocols can work with SSL.

When you enable SSL for Oracle Collaboration Suite, the HTTP communications depicted in Figure 1–1 will then use the HTTPS protocol for secure connections. URLs that require an SSL connection begin with `https` rather that `http`.

Figure 1–1 Communication Paths Between Components in Oracle9i Application Server



1.1.1 Default SSL Configuration

If you select the default options in the Oracle Collaboration Suite Infrastructure installation, none of the components are configured for SSL.

1.1.2 Partial SSL Configuration

Oracle9*i* Application Server enables you to selectively configure SSL for the paths that you want to secure. There are many paths used by components, as illustrated in Figure 1–1. You might not want to secure all the paths for the following reasons:

- SSL is resource-intensive. If you have heavy SSL traffic, then you should consider offloading SSL processing to an SSL accelerator.
- If your computers are behind firewalls, then you might want to secure only those paths that are accessed by the public. For example, you might choose to secure only Web Cache and Oracle HTTP Server if the public can access only these components. This document only provides instructions for this scenario.

1.2 Understanding the SSL Port Configuration

Configuring SSL involves changing the default HTTP and HTTPS ports for Web Cache and Oracle HTTP Server. Note that the `Port` and `Listen` directives in the `httpd.conf` configuration file of Oracle HTTP Server can be set to different values depending on your environment.

Default Port Layout for Oracle9*i* Application Server

In the basic port layout for a default Oracle9*i* Application Server installation, Web Cache runs on HTTP port 7777 (or HTTPS port 4443) and dispatches requests to Oracle HTTP Server HTTP port 7778 (or HTTPS port 4444). This means that the entry point for a browser to reach something on the HTTP Server is 7777 and not 7778. Browser requests are directed to the Web Cache port 7777. The HTTP Server ports are configured with the following directives in the `httpd.conf` file:

`Listen:` This directive defines the port on which the HTTP Server listens for incoming connections and receives them. This is the *physical* HTTP Server port.

`Port:` This directive defines the port through which the HTTP Server must be accessed. This value is used when the HTTP Server creates redirections to itself, and it is also passed to Web applications so that applications can create links and redirections to themselves by using it. This is the *advertising* port.

In links and redirections, a browser will never see the port of the HTTP Server. Instead, they are able to access only the port under which the HTTP Server is advertised.

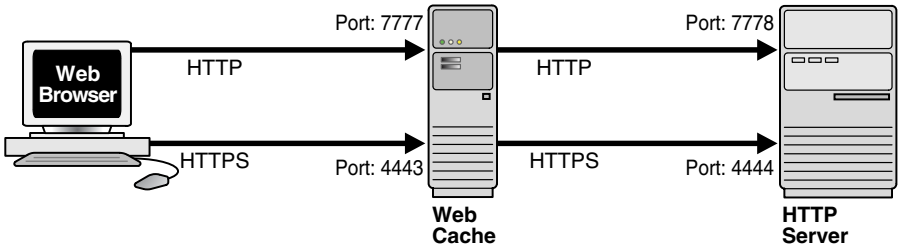
In addition to connecting to port 7777 through HTTP, the browser can also connect to port 4443 through HTTPS. In the latter case, Web Cache dispatches the request to the HTTPS port 4444 of the HTTP Server.

> **Note:** SSL is used both between the browser and Web Cache and between Web Cache and the HTTP Server.

A `VirtualHost` declaration in the `httpd.conf` file is used to specify the ports for HTTPS connections. The default configuration is as follows:

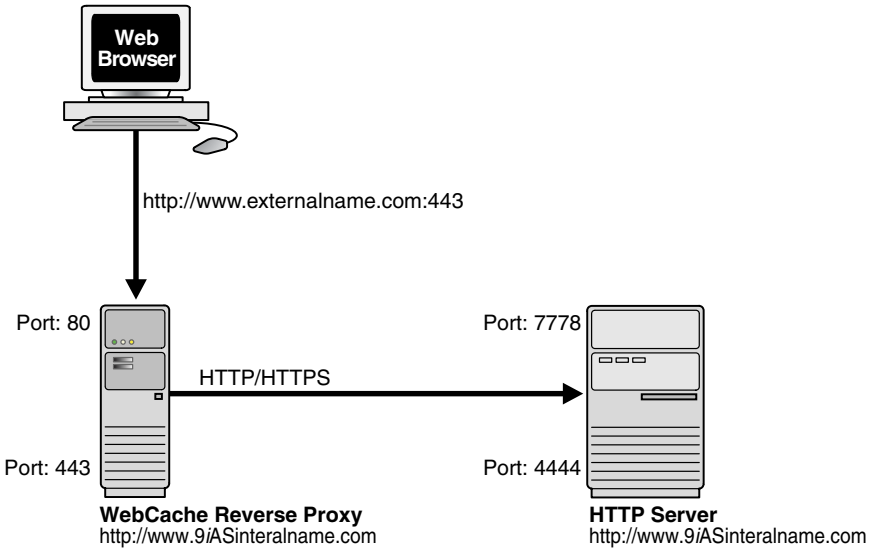
```
<VirtualHost _default_:4444>
    Port 4443
    Listen 4444
    SSLEngine on
</VirtualHost>
```

The second line, `Port 4443,` signifies that this port (4444) in the HTTP Server should be accessed through the front-end port of 4443. The HTTP Server generates redirections to itself by naming the Web Cache SSL port. Therefore, in redirections, a browser will not see the SSL port of the HTTP Server, but rather the SSL port under which the HTTP Server is advertised. This is illustrated in the following figure.



For a distributed installation, you must configure the Middle Tier and the Infrastructure tier to use the standard HTTP and HTTPS ports (80 and 443).

For a single-box installation of Oracle Collaboration Suite, a Web Cache reverse proxy can accept all incoming requests directed to the standard HTTP and HTTPS ports (80 and 443), and redirect them to the internal Oracle Collaboration Suite components running on the nonstandard ports. This is illustrated in the following figure.



1.3 High-Level Tasks to Enable SSL in Oracle Collaboration Suite

To enable SSL communications in Oracle Collaboration Suite, follow these high-level steps:

1. Ensure that you have a working installation of Oracle Collaboration Suite. For instructions, refer to *Oracle Collaboration Suite Installation and Configuration Guide*, for your platform. To verify that you have a valid Oracle Collaboration Suite installation, check the list of prerequisites for Oracle Collaboration Suite SSL. See Chapter 2, "Before You Begin".
2. Obtain certificates for your Oracle Collaboration Suite components, and create a wallet on each computer in your Oracle Collaboration Suite installation that will accept SSL connections. See Chapter 3, "Creating Wallets".

3. Configure SSL to Oracle9*i* Application Server Web Cache. See Chapter 4, "Configuring Web Cache for SSL".
4. Configure SSL to Oracle9*i*AS Single Sign-On Administration. See Chapter 5, "Configuring SSL for Oracle9iAS Single Sign-On Administration".
5. Configure the Infrastructure for SSL. See Chapter 6, "Configuring SSL for the Infrastructure".
6. Configure Oracle HTTP Server and Oracle9*i*AS Single Sign-On for the Middle Tier Oracle Collaboration Suite components. See Chapter 7, "Configuring SSL for the Middle Tier Applications".
7. Make configuration changes for Oracle Web Conferencing to work with SSL. See Chapter 8, "Configuring Oracle Web Conferencing for SSL".
8. Make configuration changes for Oracle Calendar to work with SSL. See Chapter 9, "Configuring Oracle Calendar for SSL".
9. Troubleshoot your Oracle Collaboration Suite SSL set up. Refer to Appendix A, "Troubleshooting" for solutions to some common problems that you may encounter.

2

Before You Begin

Before you begin configuring the Oracle Collaboration Suite components for SSL, you must have a valid, working installation of Oracle Collaboration Suite. For detailed instructions, refer to *Oracle Collaboration Suite Installation and Configuration Guide* specific to your platform. This chapter provides information to help you confirm that your Oracle Collaboration Suite installation is installed correctly before you begin the SSL configurations.

Special Considerations for a Single-Box Installation

The challenge with enabling SSL on a single-box installation is that both the Infrastructure Tier and the Middle Tier have Oracle HTTP Server processes that need to share ports. This prevents you from using the standard HTTP and HTTPS ports (80 and 443) for accepting incoming requests from the browser. One way to work around this port conflict is to set up Web Cache as a reverse proxy to listen for incoming requests on the standard ports, preferably in the DMZ. Web Cache listens on ports 80 and 443 and translates the requests to the listening ports of the Infrastructure and Middle Tier components.

> **Note:** In a single-box installation, Web Cache is disabled on the Middle Tier in the example described in this document. Any references to Web Cache in a single-box installation are actually references to the Web Cache reverse proxy.

This chapter contains the following topics:

2.1 Naming Conventions

The following naming conventions are used in this document to represent information that is specific to your environment:

- *`midtierhostname`* represents the fully qualified host name of your Middle Tier computer, for example, `myhost.company.com`. In a single-box installation, you must use the Web Cache host name, which may or may not be the same as the Middle Tier host name.
- *`infratierhostname`* represents the fully qualified host name of your Infrastructure tier server, for example, `myhost.company.com`. In a single-box

installation, you must use the IP address of the Infrastructure server instead of the host name to differentiate it from the Middle Tier installation.

- *$ORACLE_HOME* is the location where your Oracle Collaboration Suite installation resides on either the Infrastructure or Middle Tier.
- `webcachehostname` represents the host name of your Web Cache reverse proxy server. For a single-box installation, all requests to `webcachehostname` will be forwarded to the Middle Tier applications.
- `webcacheipaddress` represents the IP address of your Web Cache reverse proxy server. The IP address should resolve to the `webcachehostname` when using `nslookup`. This will only be used in a single-box installation where all requests to `webcacheipaddress` will be forwarded to the Infrastructure (Oracle9*i*AS Single Sign-On).

2.2 System Requirements

The requirements described in this section assume that your Oracle Collaboration Suite installation meets the following system requirements:

- Oracle Collaboration Suite release 9.0.4.1 or 9.0.4.2.
- Update your `PATH` environment variable to include the *$ORACLE_HOME*`/bin` directory and *$ORACLE_HOME*`/opmn/bin` directory. You should update your `PATH` on both the Infrastructure and Middle Tier.

2.2.1 System Requirements for a Single-Box Installation

If you have installed all the Oracle Collaboration Suite components on a single box, then the following system requirements apply to your environment:

- Single-box installation (Infrastructure tier, Middle Tier, and data store all on the same server.)
- Web Cache (reverse proxy) running in the DMZ (or on the Middle Tier).
- Middle Tier listens on HTTP port 7778 and HTTPS port 4444.
- Infrastructure tier listens on HTTP port 7777 and HTTPS port 4443.
- Web Cache (reverse proxy) listens on the standard HTTP port 80 and HTTPS port 443.
- Oracle Internet Directory listens on the LDAP port 389.

2.2.2 System Requirements for a Multiple Box Installation

If you have installed the Oracle Collaboration Suite components on multiple boxes (Middle Tier on one server and Infrastructure tier on a different server), the following system requirements apply to your environment:

- Multiple box installation (Infrastructure tier and Middle Tier on different servers)
- Web Cache listens on HTTP port 80 and HTTPS port 443 on `midtierhostname`
- Middle Tier Oracle HTTP Server listens on HTTP port 7778 and HTTPS port 4444
- Infrastructure tier Oracle HTTP Server listens on HTTP port 80 and HTTPS port 443
- Oracle Internet Directory listens on the LDAP port 389 on `infratierhostname`

2.3 Validating Your Installation

Before you begin configuring your Oracle Collaboration Suite installation for SSL, you must first ensure that you have a valid, working installation. It is important that you complete the original installation process without errors. Otherwise, you may not be able to complete the reregistration process necessary for SSL. This section provides some instructions for testing your current Oracle Collaboration Suite installation before beginning the SSL configurations.

> **Note:** If you are not sure about the ports that were assigned at installation time, then you will find the port assignments for your initial installation in:
>
> `$ORACLE_HOME/install/portlist.ini`

To validate your Oracle Collaboration Suite installation, run the following tests:

1. Verify that you can log in to Oracle9*i*AS Single Sign-On Server Administration as the `orcladmin` user at the following URL:

   `http://`*`infratierhostname:port`*`/pls/orasso`

2. Verify that you can log in to Oracle Internet Directory Delegated Administration Services (OIDDAS) as the `orcladmin` user at the following URL:

   `http://`*`infratierhostname:port`*`/oiddas`

   Ensure that you are able to add a new user and log out.

3. Verify that you can access all configured Oracle Collaboration Suite applications that require Oracle9*i*AS Single Sign-On at the following URLs:

   Oracle Email URL = `http://`*`midtierhostname:port`*`/um/traffic_cop`

   Oracle9*i*AS Portal URL = `http://`*`midtierhostname:port`*`/pls/portal`

   Oracle Calendar URL =
   `http://`*`midtierhostname:port`*`/ocas-bin/ocas.fcgi?sub=web`

   Oracle Files URL = `http://`*`midtierhostname:port`*`/files/app`

   Oracle Web Conferencing URL =
   `http://`*`midtierhostname:port`*`/imtapp/app/home.uix`

   Oracle Ultra Search URL =
   `http://`*`midtierhostname:port`*`/files/app/FederatedSearch`

4. The Distributed Configuration Management (DCM) utility, `dcmctl`, provides a command-line alternative to using Oracle Enterprise Manager. Ensure that you can run the `dcmctl updateConfig` command. Before running `dcmctl` you must first shut down Oracle Enterprise Manager (`emctl`). Run the following commands:

   ```
   $ORACLE_HOME/bin/emctl stop
   $ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
   ```

5. Correct any problems with your installation before proceeding. After you have confirmed that there are no errors, shut down everything and perform a cold backup.

> **See Also:** For information about troubleshooting your installation, refer to *Oracle Collaboration Suite Installation and Configuration Guide*

3

Creating Wallets

To configure SSL communications for Oracle Collaboration Suite components, you will need to create a wallet for each computer in your installation. A wallet contains the certificates needed for SSL authentication of a server. You can use Oracle Wallet Manager to create wallets for use with Oracle Collaboration Suite components.

This chapter contains the following topics:

3.1 Obtaining a Certificate and Creating a Wallet

To obtain a digital certificate from the relevant certificate authority (CA), you must submit a certificate request (CR) to the CA that uniquely identifies your server. The CA validates your CR and sends you a user certificate for your site. You need to create a wallet in Oracle Wallet Manager that contains your user certificate as well as the trusted certificate of the CA.

3.1.1 Creating and Submitting a Certificate Request

To generate a certificate request using Oracle Wallet Manager:

1. Open Oracle Wallet Manager on the Middle Tier. On UNIX, this can be done by running `owm` at the command prompt.
2. Create a new wallet.

   Click **Wallet**, click **New**, and enter a password when prompted. On UNIX, the wallet is stored by default at `/etc/ORACLE/WALLETS/`*`creator_accountname`*
3. Click **Yes** when prompted to create a certificate request. Specify the required information in the **Certificate Request** dialog box. For **Common Name**, provide the name or alias of your site, for example, `www.abc.com`.
4. Click **OK** to create the CR. A message is displayed stating that the CR was created successfully. The **Certificate** node in the Wallet Navigator changes to **Requested**.
5. Save the wallet in a directory that can be accessed by all components that will be using the wallet.

3.1.2 Submitting the Certificate Request to the CA

Depending on the CA, you may need to copy the CR onto a form on the Web site of the CA or export the CR to a file.

To submit a certificate by copying the CR:

1. Select the **Certificate** node in the Wallet Navigator.
2. Highlight the CR text in the **Certificate Request** field. You must include the `BEGIN NEW CERTIFICATE REQUEST` and `END NEW CERTIFICATE REQUEST` lines.
3. Copy the text onto the Certificate Request form on the Web site of the CA.

To export the CR as a file:

1. Select **Operations,** and then **Export Certificate Request.**
2. Specify the name and location to save the exported CR file. A status line message confirms that the CR was successfully exported.
3. After the CR is exported, you can upload the file to the Web site of the CA.

3.1.3 Importing Certificates Into Your Wallet

After the CA has validated your CR, they will send you a user certificate for your site, either as simple text within an e-mail message or as a file. You must then import this user certificate into your wallet.

If you are using a trial Root Certificate or have chosen a CA that does not have a trusted CA certificate already installed in Oracle Wallet Manager, then you must first import the trusted CA certificate before importing your site-specific user certificate.

Importing the Trusted Certificate (if required)

To import the trusted certificate:

1. Click**Operations**, and then **Import Trusted Certificate**.
2. Based on the format that was supplied by the CA, select either **Paste the Certificate** or **Select** the file that contains the certificate.
3. Select the certificate file or paste in the trusted certificate text supplied by the CA in an e-mail message.

   Oracle Wallet Manager expects base-64 encoded Root Certificates. If you do not have a base-64 encoded Root Certificate, you must convert the certificate to the supported format. This is explained in the following section.
4. Click **OK**.

Changing the Trusted Certificate Format (If Necessary)

If the import of the trusted certificate fails, then it is possible that the certificate is in a format that Oracle Wallet Manager does not support. In this case, you need to convert the certificate to a supported format before importing. The easiest way to do this is through the certificate Import/Export Wizards within a browser. The following steps are for the Microsoft Internet Explorer browser.

1. In Microsoft Internet Explorer, select **Tools** and then **Internet Options**.
2. Click the **Content** tab.
3. Click **Certificates...**.
4. Click the **Trusted Root Certification Authorities** tab.
5. Select **Import...**, and follow the steps in the wizard to import the certificate.
6. Highlight the newly imported certificate in the list.

7. Click **Export...**, and follow the steps of the wizard. On the **Export File Format** page of the wizard, select **Base-64 encoded X.509**.
8. Click **Next,** and give the certificate file a name.
9. Click **Next**.
10. Click **Finish**.

Importing the User Certificate of the Server

To import the user certificate:

1. Click **Operations,** and then **Import User Certificate**.
2. Based on the format that was supplied by the CA, either **Paste the Certificate** or **Select** the file that contains the certificate.
3. Select the certificate file or paste in the user certificate text supplied by the CA in an e-mail message.
4. Click **OK**. A status line message is displayed indicating the that the user certificate has been successfully imported.

3.2 Saving Wallet with AutoLogin Enabled

After importing your certificates into your wallet, you must save the wallet with the AutoLogin functionality enabled. This step is required because Web Cache needs to access the wallet without supplying a wallet password. If AutoLogin is not set, then Web Cache cannot run in SSL mode.

To save the wallet with the AutoLogin functionality enabled:

1. In Oracle Wallet Manager, select the newly imported Trusted Certificate from the list.
2. Select **Wallet,** and then **AutoLogin** (if it is not already selected).
3. Click **Wallet,** and then **Save.**

4

Configuring Web Cache for SSL

To configure SSL in Web Cache, you will be using the Web Cache Manager administration interface.

> **See Also:** For more information about the Web Cache Manager, refer to *Oracle9i*AS Web Cache Administration and Deployment Guide

For a Single-Box Installation

In a single-box installation, Web Cache is configured as a reverse proxy. Web Cache receives incoming requests on the standard HTTP port 80 or HTTPS port 443. It then redirects these requests to the configured nonstandard ports on the Middle Tier and Infrastructure components. Because the Middle Tier and Infrastructure are on the same server, all requests received at `webcacheipaddress` are directed to the Infrastructure and all requests received at `webcachehostname` are redirected to the Middle Tier. Even though both resolve to the same server, Web Cache handles them differently.

For a Distributed Installation

For a distributed installation, Web Cache runs on the Middle Tier and receives requests from the browser on the standard HTTP and HTTPS ports (80 and 443). The Middle Tier Oracle HTTP Server listens for requests from Web Cache on 7778 and 4444. The Infrastructure tier HTTP server is configured to use the standard HTTP and HTTPS ports (80 and 443). Requests to the Infrastructure bypass the Web Cache.

This chapter contains the following topics:

4.1 Starting Web Cache Manager

To start Web Cache Manager:

1. Start the admin server process with the `webcachectl start` or `webcachectl startadm` commands.
2. Point your browser to the following URL:

   `http://`*`webcachehostname`*`:4000`
3. When prompted for the administrator user ID and password, enter `administrator` for the user name, and then enter the appropriate password. The first time you log in, the password is `administrator`.

4.2 Configuring Web Cache Listening Ports

By default, Web Cache listens with the HTTP protocol on port 7777 and HTTPS on port 4443. You must change these to listen on HTTP port 80 and HTTPS port 443 on the *`webcachehostname`* or the *`midtierhostname`*.

> **Note:** The IP addresses for the default HTTP and HTTPS ports are set to ANY. On startup, Web Cache attempts to bind the ports to all IP addresses. If multiple instances of Web Cache are running on a multihomed host with multiple IP addresses, then change ANY to a specific IP address to avoid port conflicts.

To change the listening ports in Web Cache Manager:

1. In the navigator pane, select **Cache-Specific Configuration,** and then select **Listening Ports.** The Listening Ports page appears.
2. In the Listening Ports page, select **Add**. The Edit Listening Ports page dialog box appears.
3. Select the cache from the list to modify. For example, *`hostname-Webcache`*.
4. Complete the fields as follows for non-SSL connections:
   - **IP Address** = `Any`
   - **Port**=`80`
   - **Protocol**=`HTTP`
5. Complete the fields as follows for SSL connections:
   - **IP Address** = `Any`
   - **Port**=`443`
   - **Protocol**=`HTTPS`
   - **Wallet**=*`path_to_wallet`*

   On UNIX, wallets are stored by default in `/etc/ORACLE/WALLETS/`*`user_name`*.
6. Clisk **Submit.**

4.3 Configuring Site Definitions

Web Cache uses site settings to determine the appropriate site for the requests. The default site definition established during installation uses the host name and listening port of the computer on which the Oracle Application Web Server was installed, typically `midtierhostname:7777`. For SSL, you must replace this site definition with the ones described in this section.

For a single-box installation, you need two site definitions: one that maps to the host name (`webcachehostname:443`) and one that maps to the IP address (`webcacheipaddress:443`) of the Web Cache server. This allows Web Cache to redirect requests to the appropriate Middle Tier or Infrastructure components even though they reside on the same server. You must also create an alias for the `webcachehostname` site with the port set to 80. This alias redirects all HTTP requests to use a secure HTTPS connection.

For a distributed installation, you only need one site definition, defined as `midtierhostname` with the port set to 443. You must also create an alias for the site that is `midtierhostname` with the port set to 80. This alias redirects all HTTP requests to use a secure HTTPS connection.

To configure site definitions in Web Cache Manager:

1. In the navigator pane, select **General Configuration** and then select **Sites.** The Site Definitions page appears.
2. In the Site Definitions page, select **Add Site**. The Add Site dialog box appears.
3. For single-box installations, create the following site definitions:

   Site Definition 1

   - **Host Name** = `webcachehostname`
   - **Port**=`443`
   - **Default**=`Yes`
   - **Alias**=*`webcachehostname`*`:80`

   Site Definition 2

   - **Host Name** = `webcacheipaddress`
   - **Port**=`443`
   - **Default**=`No`
   - **Alias**=`webcacheipaddress:80`

   For distributed installations, create the following site definition:

   - **Host Name** = `midtierhostname`
   - **Port**=`443`
   - **Default**=`Yes`
   - **Alias**=`midtierhostname:80`
4. Click **Submit**.

4.4 Configuring Application Web Server

Configure Web Cache with the application Web servers for which it sends cache misses. Typically, Web Cache uses application Web servers for internal sites.

By default, the listening port and host name of the Oracle HTTP Server are configured. When Web Cache is installed, Oracle HTTP Server has a default listening HTTP port of 7778 and an HTTPS port of 4444.

For a single-box installation, you must create two Application Web Server entries. One entry directs traffic to the Listen HTTPS port (4444 in this example) of the Middle Tier

Oracle HTTP Server. The other entry directs traffic to the HTTPS port (4443) on the Infrastructure tier Oracle HTTP Server.

For a distributed installation, you must create one Application Web Server entry for the Middle Tier that directs traffic to the Listen HTTPS port (4444) of the Middle Tier Oracle HTTP Server.

To configure the application Web server in Web Cache Manager:

1. In the navigator pane, select **General Configuration,** and then select **Application Web Server.** The Application Web Server page appears.
2. On the Application Web Server page, select **Add Site.** The Create Application Web Server dialog box appears.
3. For single-box installations, create the following Application Web Server entries:

   Entry 1

   - **Host Name** = `infratierhostname`
   - **Port**=`4443`
   - **Capacity**=`50`
   - **Failover Threshold**=`25`
   - **Ping URL** = `/`
   - **Ping Interval**=`10`
   - **Protocol**=`HTTPS`

   Entry 2

   - **Host Name** = `midtierhostname`
   - **Port**=`4444`
   - **Capacity**=`50`
   - **Failover Threshold**=`25`
   - **Ping URL** = `/`
   - **Ping Interval**=`10`
   - **Protocol**=`HTTPS`

   For **distributed installations**, create the following Application Web Server entry:

   - **Host Name** = `midtierhostname`
   - **Port**=`4444`
   - **Capacity**=`50`
   - **Failover Threshold**=`25`
   - **Ping URL** = `/`
   - **Ping Interval**=`10`
   - **Protocol**=`HTTPS`
4. Select **Submit**.

When using HTTPS as the listening protocol, you must also specify the location of the wallet for Web Cache communication to the application Web server. By default, wallets are stored in the following location on UNIX:

`/etc/ORACLE/WALLETS/user_name`

To specify the wallet location:

1. In the navigator pane, select **Cache-Specific Configuration** and then select **Origin Server Wallet.** The Origin Server Wallet page appears.
2. On the Origin Server Wallet page, select the cache for which to modify wallet settings, and then click **Edit**. The Edit Origin Server Wallet dialog box appears.
3. In the **Wallet Directory** field, enter the location of the wallet in the Wallet field.
4. Click **Submit**.

4.5 Configuring Site to Server Mappings

In this step, you will map the sites you have defined to the physical servers in your installation.

In a single-box installation there will be two mappings: one that maps the *webcachehostname* to the Middle Tier components and one that maps the *webcacheipaddress* to the Infrastructure tier components.

In a distributed installation there will be one mapping. This will map requests received by Web Cache to the Middle Tier components HTTP Server listening port.

To configure site to server mappings:

1. In the navigator pane, select **General Configuration** and then select **Site to Server Mapping.** The Site to Server Mapping page appears.
2. On the Site to Server Mapping page, select **Create** if no mappings exist. If mappings already exist, select a mapping, and then select **Insert Above** or **Insert Below**. The Create Site to Server Mapping or Edit/Add Site to Server Mapping dialog box appears.
3. Select from **Site Definitions** to select a site definition created in the Site Definitions page.
4. On the **Select Origins Servers to which this Site is mapped** page, select **Select Application Web Servers** to select application Web servers specified in the Application Web Servers page.
5. Your site to server mappings should be as follows:

   For a single-box installation

   Mapping 1

   - **Site Host Name**=*webcachehostname*
   - **Site Port**=443
   - **Site Exclude**=NONE
   - **Origin Server Host Name**=midtierhostname
   - **Origin Server Port**=4444
   - **Origin Server Proxy**=No

   Mapping 2

- **Site Host Name**=*webcacheipaddress*
- **Site Port**=443
- **Site Exclude**=NONE
- **Origin Server Host Name**=infratierhostname
- **Origin Server Port**=4443
- **Origin Server Proxy**=No

For a distributed installation

- **Site Host Name**=*midtierhostname*
- **Site Port**=443
- **Site Exclude**=NONE
- **Origin Server Host Name**=midtierhostname
- **Origin Server Port**=4444
- **Origin Server Proxy**=No

6. Click **Submit**.

4.6 SSL Configurations for Web Cache Clusters

In a distributed installation that involves a Web Cache cluster, you must perform all of the SSL configuration steps explained in Section 4.2 through Section 4.5 on each Web Cache server in the cluster. After completing the SSL configuration changes, you must propagate your changes across the cluster.

> **See Also:** *Oracle9i*AS Web Cache Administration and Deployment Guide

4.7 Verifying Your Web Cache SSL Configuration

If you have configured Web Cache correctly for SSL, then you should be able to access the Middle Tier and Infrastructure tier default page by using the following URLs:

For a single-box install:
https://*webcachehostname*

https://*webcacheipaddress*

For a distributed install:
https://*midtierhostname*

If this test fails, go back and correct your Web Cache SSL configuration before proceeding.

5

Configuring SSL for Oracle9*i*AS Single Sign-On Administration

This chapter explains how to configure SSL connections to the Application Server Single Sign-On Server Administration interface, which resides in the Infrastructure tier.

This involves the following high-level steps:

- Section 5.1, "Enabling SSL for the Oracle9iAS Single Sign-On HTTP Server"
- Section 5.2, "Updating the Database Access Descriptor"
- Section 5.3, "Configuring the Oracle9iAS Single Sign-On URLs for HTTPS"

5.1 Enabling SSL for the Oracle9*i*AS Single Sign-On HTTP Server

The file `$ORACLE_HOME/Apache/Apache/conf/httpd.conf` on the Infrastructure tier is used to configure the HTTP Server for SSL, where `$ORACLE_HOME` is the directory where the Oracle Collaboration Suite Infrastructure is installed.

To enable SSL on the Oracle9*i*AS Single Sign-On HTTP Server:

1. Open the `$ORACLE_HOME/Apache/Apache/conf/httpd.conf` on the Infrastructure tier.
2. Within this file, the SSL parameters reside within a `VirtualHost` definition. You must change the `Port` directive from 4443 to `443` and the `ServerName` directive to *`webcacheipaddress`* (for a single-box installation) or *`infratierhostname`* (for a distributed installation). See the following example:

```
<VirtualHost _default_:443>
ServerName webcacheipaddress|ifratierhostname
Port 443
SSLEngine on
SSLVerifyClient none
</VirtualHost>
```

3. After making these changes in the `httpd.conf` file, run the Distributed Configuration Management (DCM) utility to update your configurations and then restart the server. Run the following commands on the Infrastructure server:

```
dcmctl updateconfig -d -v
dcmctl stop -ct ohs
dcmctl start -ct ohs -v
```

5.2 Updating the Database Access Descriptor

To configure the `plsql` module for SSL, environment variables need to be added to the database access descriptor (DAD) of the Single Sign-On server. Navigate to the `dads.conf` file located in the `$ORACLE_HOME/Apache/modplsql/conf/dads.conf` directory on your Infrastructure server.

Add the following parameters to the end of the `<Location /pls/orasso>` container, using *`webcacheipaddress`* for a single-box installation or *`infratierhostname`* for a distributed installation:

```
PlsqlCGIEnvironmentList SERVER_NAME=webcacheipaddress|infratierhostname
PlsqlCGIEnvironmentList SERVER_PORT=443
PlsqlCGIEnvironmentList REQUEST_PROTOCOL=https
PlsqlCGIEnvironmentList HTTP_HOST=webcacheipaddress|infratierhostname:443
</Location> #Do not insert this line. It already exists, shown for reference only
```

5.3 Configuring the Oracle9*i*AS Single Sign-On URLs for HTTPS

To enable the Oracle9*i*AS Single Sign-On server for SSL, all references to HTTP in the Oracle9*i*AS Single Sign-On URLs must be changed to HTTPS. The script `ssocfg.sh` is provided for this purpose. Run this script on your Infrastructure tier as follows:

1. Ensure that your `LD_LIBRARY_PATH` environment variable is updated as follows:

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/jlib
   export LD_LIBRARY_PATH
   ```

2. Run the `ssocfg.sh` script as follows, supplying either *`webcacheipaddress`* (for a single-box installation) or *`infratierhostname`* (for a distributed installation):

   ```
   $ORACLE_HOME/sso/bin/ssocfg.sh https webcacheipaddress|infratierhostname 443
   ```

3. Restart the server for the changes to take effect by running the following commands:

   ```
   opmnctl stopall
   opmnctl startall
   ```

4. Access the following URL to ensure that you can access the Oracle9*i*AS Single Sign-On Administration over SSL:

   For a single-box installation:

   ```
   https://webcacheipaddress/pls/orasso
   ```

   For a distributed installation:

   ```
   https://infratierhostname/pls/orasso
   ```

6

Configuring SSL for the Infrastructure

This chapter explains how to configure SSL connections to the Oracle Collaboration Suite Infrastructure, which includes the Oracle9*i*AS Single Sign-On server and Oracle Delegated Administration Services. This involves the following steps:

- Section 6.1, "Reregistering HTTP Server with Oracle9iAS Single Sign-On Server"
- Section 6.2, "Changing the Oracle Delegated Administration Services URL"

6.1 Reregistering HTTP Server with Oracle9*i*AS Single Sign-On Server

The Oracle9*i*AS Single Sign-On module for the Oracle HTTP Server, `mod_osso`, is registered automatically with the Oracle9*i*AS Single Sign-On server when Oracle9*i* Application Server is installed. However, when SSL is enabled on the Oracle9*i*AS Single Sign-On server after installation, the `mod_osso` component must be registered again manually with the Oracle9*i*AS Single Sign-On server. This ensures that the Oracle9*i*AS Single Sign-On server listens for all requests on the SSL port. If this registration is not done, then the user will be redirected to the Oracle9*i*AS Single Sign-On page using HTTP rather than HTTPS.

Running the Oracle9*i*AS Single Sign-On registration tool updates the `mod_osso` registration record in the `osso.conf` file to reflect SSL settings on the Oracle9*i*AS Single Sign-On server. The Oracle9*i*AS Single Sign-On registration tool generates this file whenever it is run.

Before running this tool, you must remove all partner applications from the Oracle9*i*AS Single Sign-On server *except* the Oracle9*i*AS Single Sign-On server and Wireless. You will be re-creating these partner applications later on.

To remove the partner applications:

1. Log in to the Oracle9*i*AS Single Sign-On Administration as `orcladmin` at:

   For a single-box installation at:

   `https://`*`webcacheipaddress`*`/pls/orasso`

   For a distributed installation at:

   `https://`*`infratierhostname`*`/pls/orasso`

2. Click **SSO Server Administration,** and then click **Administer Partner Applications.**
3. Delete all partner applications *except* the Oracle9*i*AS Single Sign-On server and Wireless.

To run the Oracle9*i*AS Single Sign-On registration tool, perform the following steps on your Infrastructure tier:

1. Update your `LD_LIBRARY_PATH` environment variable as follows:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/jlib
export LD_LIBRARY_PATH
```

2. Run the Oracle9*i*AS Single Sign-On registration tool by running the following command.

> **Note:** Replace the placeholder information (denoted by text in italic font) with the correct information for your environment. For example, for a single-box installation use *webcacheipaddress*. For a distributed installation, use *infratierhostname*.

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path infrastructure $ORACLE_HOME
-host infrastructure_hostname \
-port 1521 \
-sid iasdb \
-site_name infra_webcacheipaddress|infratierhostname \
-success_url https://webcacheipaddress|infratierhostname/osso_login_success \
-logout_url https://webcacheipaddress|infratierhostname/osso_logout_success \
-cancel_url https://webcacheipaddress|infratierhostname/ \
-home_url https://webcacheipaddress|infratierhostname/ \
-config_mod_osso TRUE \
-u root \
-sso_server_version v1.2
```

3. After the script is run, you should see the "SSO Registration Successful" message.
4. Restart the HTTP server for the Infrastructure tier by running the following commands:

```
dcmctl stop -ct ohs
dcmctl start -ct ohs -v
```

6.2 Changing the Oracle Delegated Administration Services URL

To access the Oracle Delegated Administration Services interface over SSL, you must change the DAS URL within Oracle Internet Directory to use the HTTPS protocol rather than HTTP.

> **See Also:** *Oracle Internet Directory Administrator's Guide*

The high-level steps are as follows:

1. Change the Oracle Delegated Administration Services URL in the `ldapserver (OIDADMIN)` for the attribute `orcldasurlbase` in the context `cn=OperationURLs, cn=DAS, cn=Products, cn=OracleContext`
2. Update the `orclbase` entry to reflect the HTTPS URL used for the Infrastructure. For a single-box installation use `https://`*webcacheipaddress*. For a distributed installation use `https://`*infratierhostname*. For example:

```
https://123.44.555.66
https://infratier_host.company.com
```

3. After changing the Oracle Delegated Administration Services URL in Oracle Internet Directory, stop and restart OC4J_DAS by running the following commands:

```
dcmctl stop -co OC4J_DAS
dcmctl start -co OC4J_DAS -v
```

4. Your Infrastructure tier should now be configured to listen for requests on port 443 (SSL). Check the following URLs to confirm that you can access them without errors:

   For a single-box installation:

```
https://webcacheipaddress/pls/orasso
https://webcacheipaddress/oiddas
https://webcacheipaddress:443
```

   For a distributed installation:

```
https://infratierhostname/pls/orasso
https://infratierhostname/oiddas
https://infratierhostname:443
```

7

Configuring SSL for the Middle Tier Applications

This chapter explains how to configure SSL connections to the Middle Tier applications. This involves the following steps:

- Section 7.1, "Enabling SSL for HTTP Server"
- Section 7.2, "Configuring the Portal Parallel Page Engine"
- Section 7.3, "Reregistering HTTP Server with the Oracle9iAS Single Sign-On Server"
- Section 7.4, "Configuring Portal for SSL"

7.1 Enabling SSL for HTTP Server

In this step, you will configure the advertising port of the Middle Tier Oracle HTTP Server (the `Port` directive only). The advertising port should always be the same as the front-end port by which the Oracle HTTP Server is accessed. In this case, the front-end port is the Web Cache port, which we have already set to 80 for HTTP and 443 for HTTPS. See Section 1.2 for more information about the default ports of Oracle HTTP Server.

The file `$ORACLE_HOME/Apache/Apache/conf/httpd.conf` on the Middle Tier is used to configure the HTTP Server for SSL, where `$ORACLE_HOME` is the directory where the Oracle Collaboration Suite Middle Tier applications are installed.

To enable SSL on the Middle Tier HTTP Server:

1. Open the `$ORACLE_HOME/Apache/Apache/conf/httpd.conf` file on the Middle Tier.
2. In this file, the SSL parameters reside within a `VirtualHost` definition. You must change the `Port` directive from 4443 to `443` and the `ServerName` directive to *`webcachehostname`* (for a single-box installation) or *`midtierhostname`* (for a distributed installation). Do not change the `Listen` directive, because Web Cache will still point to this port on the Middle Tier. For example:

```
<VirtualHost _default_:4444> #do not change this line
ServerName webcachehostname|midtierhostname
Port 443
SSLEngine on
SSLVerifyClient none
</VirtualHost>
```

3. Change the nonsecure HTTP `Port` directive from 7777 to 80. Do *not* change the `Listen` directive. Web Cache will still direct requests to the Middle Tier on this port. For example:

```
Port 80
Listen 7777
```

4. After making these changes in the `httpd.conf` file, run the Distributed Configuration Management (DCM) utility to update your configurations and then restart the server. At the command line of your Middle Tier server, run the following commands:

```
dcmctl updateconfig -d -v
dcmctl stop -ct ohs
dcmctl start -ct ohs -v
```

7.2 Configuring the Portal Parallel Page Engine

The Portal Parallel Page Engine obtains the page metadata from the Portal repository and is responsible for assembling the portlets on a page. To secure the Portal Parallel Page Engine, you must edit its `web.xml` file and add some initialization parameters for SSL.

To configure the Portal Parallel Page Engine for SSL:

1. Open the following file in your Middle Tier installation:

```
$ORACLE_HOME/j2ee/OC4J_Portal/applications/portal/portal/WEB-INF/web.xml
```

2. Add the following lines just under the `<servlet-class>` section of this file. The lines to be added are displayed in boldface font in the following example:

```
<servlet>
   <servlet-name>page</servlet-name>
   <servlet-class>oracle.webdb.page.ParallelServlet</servlet-class>
   <init-param>
      <param-name>httpsports</param-name>
      <param-value>443</param-value>
   </init-param>
```

7.3 Reregistering HTTP Server with the Oracle9*i*AS Single Sign-On Server

The Oracle9*i*AS Single Sign-On module for the Oracle HTTP Server, `mod_osso`, is registered automatically with the Oracle9*i*AS Single Sign-On server when Oracle9*i*AS is installed. However, when SSL is enabled on the Oracle9*i*AS Single Sign-On server after installation, the `mod_osso` component should be registered again manually with the Oracle9*i*AS Single Sign-On server. This ensures that the Oracle9*i*AS Single Sign-On server listens for all authentication requests on the SSL port. If this registration is not done, then the user will be redirected to the single sign-on page using HTTP rather than HTTPS.

Running the Oracle9*i*AS Single Sign-On registration tool updates the `mod_osso` registration record in the `osso.conf` file to reflect the SSL settings of the Oracle9*i*AS Single Sign-On server. The Single Sign-On registration tool generates this file whenever it is run.

To run the Oracle9*i*AS Single Sign-On registration tool, complete the following steps on your Middle Tier installation:

1. Update your `LD_LIBRARY_PATH` environment variable as follows:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/jlib
export LD_LIBRARY_PATH
```

2. Run the Oracle9*i*AS Single Sign-On registration tool by running the following command:

> **Note:** Replace the placeholder information (denoted by text in italic font) with the correct information for your environment. For example, for a single-box installation use *webcachehostname*. For a distributed installation, use *midtierhostname*.

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path middle tier $ORACLE_HOME
-host infrastructure_hostname \
-port 1521 \
-sid iasdb \
-site_name middleTier.webcachehostname|midtierhostname \
-success_url https://webcachehostname|midtierhostname/osso_login_success \
-logout_url https://webcachehostname|midtierhostname/osso_logout_success \
-cancel_url https://webcacheihostname|midtierhostname/ \
-home_url https://webcachehostname|midtierhostname/ \
-config_mod_osso TRUE \
-u root \
-sso_server_version v1.2
```

3. After the script is run, you should see the "SSO Registration Successful" message.
4. Restart the HTTP server for the Middle Tier by running the following commands:

```
dcmctl stop -ct ohs
dcmctl start -ct ohs -v
```

7.4 Configuring Portal for SSL

This section discusses the steps involved in configuring Portal for SSL. It contains the following topics:

Section 7.4.1, "Before You Begin"

Section 7.4.2, "Running the Portal Configuration Script"

Section 7.4.3, "Changing the Default Portal Page"

7.4.1 Before You Begin

Before you run the Portal configuration script, ensure that a NET8 client like SQL*Plus can connect to the Portal Repository and Infrastructure on the `infratierhostname` from the `midtierhostname`. This requires a valid TNS alias defined in the `$ORACLE_HOME/network/admin/tnsnames.ora` file on the Middle Tier host.

Before you can run the Portal configuration script, you will also need the passwords for the following database users:

- `portal`
- `orasso`
- `orasso_ps`

- orasso_pa

To obtain these passwords:

1. Run the following from the command line. You must provide the correct information for *orcladmin_password*, *infratierhostname*, *ldap_port* (which is typically 389). For OrclresourceName, enter the password you want to retrieve (orasso, orasso_ps, orasso, portal). Substitute *orclpasswordattribute* for the password value that is retrieved from Oracle Internet Directory:

```
ldapsearch -D cn=orcladmin -w orcladmin_password -p ldap_port -h
infratierhostname -b "cn=IAS,cn=Products,cn=OracleContext" -s sub -v
OrclresourceName=orasso | grep orclpasswordattribute
```

2. You can also get these passwords by using the administrator interface of Oracle Internet Directory. After signing on to oidadmin as orcladmin follow this path:

```
cn=orclcontext
cn=Products
cn=IAS
cn=IAS Infrastructure databases
cn=oracleReferenceName=iasdb.host.domain
cn=OrclresourceName=orasso, orasso_ps, orasso, portal
```

7.4.2 Running the Portal Configuration Script

To run the Portal configuration script:

1. Run the following script from $ORACLE_HOME/assistants/opca on the Middle Tier:

> **Note:** Replace the placeholder information (denoted by text in italic font) with the correct information for your environment. For example, for a single-box installation use *webcachehostname*. For a distributed installation, use *midtierhostname*.
>
> The ptlasst.csh script must be run on one line.

```
ptlasst.csh
-i custom
-mode MIDTIER
-s portal
-sp portal_password
-c infrahostname:1521:iasdb
-sdad portal
-o orasso
-op orasso_password
-odad orasso
-host webcachehostname | midtierhostname
-port 443
-silent
-verbose
-ldap_d "cn=orcladmin"
-ldap_h infratierhostname
-ldap_p ldap_port
-ldap_w oid_admin_password
-pwd initial_password_for_oid_seeded_users
-sso_c infrastructure:1521:iasdb
-mc false
```

```
-mi true
-chost webcachehostname | midtierhostname
-cport_i cache_port_for_webcache_invalidation
-cport_a cache_port_for_webcache_administration
-wc_i_pwd invalidator
-wc on
-pa orasso_pa
-pap orasso_pa password
-ps orasso_ps
-pp orasso_ps password
-sso_h webcacheipaddress | infratierhostname
-sso_p 443
-oh $ORACLE_HOME on the Middle Tier
-emhost midtierhostname
-emport 1810
-p_tns iasdb.hostname.domain
-s_tns iasdb.hostname.domain
-iasname middle.middletierhostname
-ssl
```

2. After the script is run, stop all the Middle Tier components:

```
opmnctl stopall
```

3. Clear the cache by removing the directories `$ORACLE_HOME/Apache/modplsql/cache/plsql` and `$ORACLE_HOME/Apache/modplsql/cache/sessions`. These directories will be re-created.

4. Restart all the Middle Tier components:

```
opmnctl startall
```

7.4.3 Changing the Default Portal Page

To finish the configuration for Portal, you must change all of the URLs on the default Portal page to use the HTTPS protocol rather than HTTP.

To edit the default Portal page:

1. Open the following file in your Middle Tier installation:

```
$ORACLE_
HOME/webclient/classes/oracle/collabsuite/webclient/resources
/webclient.properites
```

2. Change the following URLs from `http://` to `https://` and enter the correct host name according to the following example. For a single-box installation, you must use `webcachehostname`. For a distributed installation, you must use `midtierhostname` in place of `hostname`.

```
quicktour.url = https://hostname/quicktutorial/index.htm
tools.url = https://hostname/download/index.html

#Do not change this line.
mail.help.url = http://collabtng11.us.oracle.com:7778/um/help/_MAIL_LOCALE_
TOKEN_/The_All_Messages_Subtab.htm
files.help.url = https://hostname/files/app/WelcomeHelp
# The entry point to the Calendar online help system:
# Note: Do not change the value for _CAL_LOCALE_TOKEN_.
# This value is replaced dynamically by application.
calendar.help.url = http://hostname:port/ocas/ocwc/_CAL_LOCALE_TOKEN_
```

```
/help/helptoc.htm
#Do not need to change this url
imeeting.help.url = http://hostname:port/imthelp/help
search.help.url = https://hostname/files/app/FederatedSearchHelp
wireless.help.url = https://hostname/marconi/help
mail=https://hostname/um/traffic_cop
calendar=https://hostname/ocas-bin/ocas.fcgi?sub=web
files=https://hostname/files/app
search=https://hostname/files/app/FederatedSearch
wireless=https://hostname/marconi/welcome.uix
portal=https://hostname/pls/portal/PORTAL.wwsec_app_priv.login
imeeting=https://hostname/imtapp/app/home.uix
mail.provider=https://hostname/um/servlet/soaprouter
files.provider=https://hostname/files/Portlet
search.provider=https://hostname/files/Portlet/search
wireless.provider=https://hostname/marconi/servlet/soaprouter
webclient.provider=https://hostname/webclient-common/servlet/soaprouter
imeeting.provider=https://hostname/webclient-imeeting/servlet/soaprouter
calendar.provider=https://hostname/webclient-calendar/servlet/soaprouter
```

3. After editing this file, run the following script to update the Portal Repository with the correct URLs:

```
$ORACLE_HOME/webclient/bin/webclient_Installer.sh
```

4. Stop and restart all Middle Tier components:

```
opmnctl stopall
opmnctl startall
```

8

Configuring Oracle Web Conferencing for SSL

This chapter explains how to configure Oracle Web Conferencing for SSL. The setup is different depending on whether you have a single-box installation or a distributed installation. Refer to one of the following sections depending on your environment:

- Section 8.1, "Single-Box Installation Instructions"
- Section 8.2, "Distributed Installation Instructions"

8.1 Single-Box Installation Instructions

For iMeeting to work properly, you may require a second dedicated IP address.

See Also: *Oracle Web Conferencing Administrator's Guide*

This is required only if you use ports 443 and 80 on the Middle Tier setup. Because in the example described in this document, port 443 has been used on the Middle Tier for Oracle9*i*AS Single Sign-On, this port cannot be used. There, a virtual host must be created and the IP address on the virtual host must be externally resolvable.

8.1.1 Setting Up MOD_IMEETING

To set up `MOD_IMEETING`:

1. Set up an alias with a new DNS-registered IP address.
2. Log in as `root`, and enter the following commands as illustrated in the following example. Note that this example is specific to a Linux environment:

```
$>su root Password : your password
/sbin/ifconfig eth0:0 ip_address
/sbin/route add -host ip_address hostname eth0:0
```

If you type `/sbin/ifconfig` on the command prompt, then the following is displayed:

```
eth0 Link encap:Ethernet HWaddr 00:06:5B:F8:06:32
inet addr:144.20.172.61 Bcast:144.20.173.255 Mask:255.255.254.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:117495 errors:0 dropped:0 overruns:0 frame:0
TX packets:104768 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:16888694 (16.1 Mb) TX bytes:25845123 (24.6 Mb)
Interrupt:28
eth0:0 Link encap:Ethernet HWaddr 00:06:5B:F8:06:32
```

```
inet addr:144.20.172.172 Bcast:144.20.255.255 Mask:255.255.0.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
Interrupt:28 RX packets:0 errors:0 dropped:0 overruns:0
TX packets:0 errors:0 dropped:0 overruns:0
```

3. Configure the Oracle HTTP Server on the Middle Tier home to include the virtual host settings.
4. Add another virtual host in the `<IfModule mod_ossl.c>` section for the second IP address, as illustrated in the following example:

```
<VirtualHost second-ip-address:443>
ServerName <if a hostname alias is created for second-ip-address (optional)>
Port 443
SSLEngine on
SSLCipherSuite SSL_RSA_WITH_RC4_128_MD5:SSL_RSA_WITH_RC4_128_SHA:SSL_RSA_WITH_
3DES_EDE_CBC_SHA:SSL_RSA_WITH_DES_CBC_SHA:SSL_RSA_EXPORT_WITH_RC4_40_MD5:SSL_
RSA_EXPORT_WITH_DES40_CBC_SHA
SSLWallet <wallet file location: You can set it for the same wallet as the
wallet used for ssl on primary IP-address>
Listen second-ip-address:443
</VirtualHost>
```

   Ensure that the virtual-host enabled for SSL on `primary IP-address` is listening on `primary-ip-address`:443 (and *not* 443 only).
5. Also set the Infrastructure `httpd.conf` file to only listen on the main address of the Middle Tier, `middletierhostname`. By default, the Infrastructure listens on all addresses.
6. Restart Oracle HTTP Server by running the following command:

```
dcmctl restart -ct ohs
```

7. Create a script in the `$Midtier_ORACLE_HOME/imeeting/bin/scripts` directory with the following entries:

```
vi $Midtier_ORACLE_HOME/imeeting/bin/scripts/mysetup.imt
setproperty -pname ApacheProtocolSecure -pvalue false
setproperty -pname ApacheTunnelHost -pvalue WebcacheHOSTNAME
setproperty -pname ApacheTunnelPort -pvalue 443
setproperty -pname ApacheWebHost -pvalue WebcacheHOSTNAME
setproperty -pname ApacheWebPort -pvalue 80
setproperty -pname ApacheWebSecurePort -pvalue 443
setproperty -pname GlobalWebHost -pvalue WebcacheHOSTNAME
setproperty -pname GlobalWebPort -pvalue 80
setproperty -pname MxWalletLocation -pvalue
/u02/mtier/Apache/Apache/conf/ssl.wlt/default
setProperty -ct mxcomm -pname SrvNumProcs -pvalue 1
setProperty -ct clbsvr -pname SrvNumProcs -pvalue 4
setProperty -ct mxcomm -pname MxListenPort -pvalue "[\"2400\"]"
setProperty -ct mxcomm -pname MxRedirectPort -pvalue "[\"2420\"]"
```

   After you create the script, run it by using the following command:

```
$ORACLE_HOME/imeeting/bin/scripts> ../imtctl <../scripts/mysetup.imt
```

8. Test the setup.

   Run tests should look like this for basic setup.

```
imtctl>runtests
Instance - mtier.WebcacheHOSTNAME:
```

```
TEST NAME SUCCESS
mtgtest true
voiceconvtest false
docconvtest false
dbtest true
apptest true
mxmodtest true
proxytest false
emailtest false
```

8.1.2 Updating Component E-mail

Besides SSL, you must change the following for the Web client application:

```
Update the file $ORACLE_HOME/j2ee/OC4J_UM/config/oc4j.properties
oracle.mail.Portlet.httpsToWebmail=true
```

You must stop and restart the Middle Tier processes after you complete the procedure.

```
$ORACLE_HOME/opmn/bin/opmnctl stopall
$ORACLE_HOME/opmn/bin/opmnctl startall
```

8.2 Distributed Installation Instructions

For Oracle Web Conferencing to work properly with SSL and standard ports, make the following changes:

1. On the Middle Tier host, change to the `$ORACLE_HOME/imeeting/bin/` directory and run the following commands:

   ```
   setproperty -pname ApacheProtocolSecure -pvalue true
   setproperty -pname ApacheWebPort -pname 80
   setproperty -pname ApacheWebSecurePort -pname 443
   setproperty -pname ApacheWebHost -pvalue MidtierHostname

   setproperty -pname MxWalletLocation -pvalue $ORACLE_
   HOME/Apache/Apache/conf/ssl.wlt/default
   ```

   `MxWalletLocation` should reflect the location of your certificate.

   After this is completed, stop and start Oracle Web Conferencing:

   ```
   $ORACLE_HOME/imeeting/bin/imtctl stop
   $ORACLE_HOME/imeeting/bin/imtctl start
   ```

   Stop and restart the Middle Tier processes:

   ```
   $ORACLE_HOME/opmn/bin/opmnctl stopall
   $ORACLE_HOME/opmn/bin/opmnctl startall
   ```

2. Test the setup.

   Run tests should look like this for basic setup.

   ```
   imtctl> runtests
   Instance - MidtierHostname.DomainName:
   TEST NAME SUCCESS
   mtgtest true
   voiceconvtest false
   docconvtest false
   dbtest true
   apptest true
   ```

```
mxmodtest true
proxytest false
emailtest false
```

9

Configuring Oracle Calendar for SSL

This chapter explains how to configure Oracle Calendar for SSL when using the standard ports. This configuration is only required for a distributed installation.

9.1 Configuring Oracle Calendar

For Oracle Calendar to work properly with SSL and standard ports, make the following changes:

1. Update the `$ORACLE_HOME/ocal/misc/unison.ini` file.
2. In the `unison.ini` file, change all occurrences of 7777 to 80 and all occurrences of 4443 to 443.
3. Stop and restart Oracle Calendar by running the following commands:

```
$ORACLE_HOME/ocal/bin/unistop -y
$ORACLE_HOME/ocal/bin/unistart
```

4. Stop and restart the OPMN processes by running the following commands:

```
$ORACLE_HOME/opmn/bin/opmnctl stopall
$ORACLE_HOME/opmn/bin/opmnctl startall
```

A

Troubleshooting

This appendix provides solutions to some problems and errors that you may encounter with your SSL configuration on Oracle Collaboration Suite. This appendix contains the following sections:

A.1 Oracle9*i*AS Portal

This section lists the common errors that occur when accessing Oracle9*i*AS Portal using the standard SSL port.

Problem1

WWC-41439 error when trying to access Portal using the 443 SSL port with URL: `https://`*`midtierhostname`*`/pls/portal`. This is a known issue with the `ptlasst.sh` script inserting SSL port 443 into ENABLER tables.

Solution1

Update the tables manually.

For example, login to SQL*Plus as the `portal` schema:

```
SQL> SELECT LSNR_TOKEN,site_id FROM wwsec_enabler_config_info$;
LSNR_TOKEN SIT E_ID xyz.us.oracle.com:7777 1324 xyz.us.oracle.com:443 1329
SQL> UPDATE wwsec_enabler_config_info$ SET LSNR_TOKEN = 'midtierhost.domain.com'
WHERE site_id = 1329;
SQL> commit;
```

You should now be able to log in to the Middle Tier by using the following URL

`https://midtierhostname`

Problem 2

The Portlet could not be contacted. SSL Handshake Failed NZERROR=28858

Note: You may encounter this error while attempting to get to `https://midtierhostname/pls/portal`

Solution 2

Check `$ORACLE_HOME/Webcache/logs/event_log` on the Middle Tier. Then check the accuracy of the entry that you created in the `web.xml` file as described in Section 7.2.

Problem 3

The Portlet could not be contacted. SSL Handshake Failed NZERROR=28874

Note: You may still receive the following error while attempting to get to `https://midtierhostname/pls/portal`

Solution 3

Check `$ORACLE_HOME/Webcache/logs/event_log` on the Middle Tier. This is a known issue with the `http_client.jar` file.

You can fix this by following Metalink note: 225502.1. This will require downloading and applying a patch.

Problem 4

The address from which this authentication request was made does not match your IP address. Notify your administrator if you believe this message to be in error. (WWC-41452)

Note: Users encounter this error when attempting to log in to Portal only.

Solution 4

You can turn off the IP Check feature by running the following SQL commands:

```
sqlplus portal schema/portal password
SQL>SELECT url_cookie_ip_check FROM wwsec_enabler_config_info$;
```

If it is not set to N, then run the following:

```
SQL>UPDATE wwsec_enabler_config_info$ SET url_cookie_ip_check='N';
SQL>commit;
SQL>exit
```

Problem 5

The style sheet was the only component on the Portal page that could not be secured.

Solution 5

This style sheet issue is corrected by the 9.0.4.2.0 patch set.

Problem 6

Incorrect rendering while connecting to `http://midtierhostname.domain.com:443`

The header link in the e-mail portlet will open the following URL:

http://*hostname.domain*.com:443

The URL does not display properly. The first time you access the URL it may display properly, but subsequent accesses will not display properly.

Solution 6

Modify the `$ORACLE_HOME/j2ee/OC4J_UM/config/oc4j.properties` file on the Middle Tier. Set `oracle.mail.client.portlet.HTTPStowebmail=TRUE`. Then stop and restart the Middle Tier by running the following commands:

```
opmnctl stopall
opmnctl startall
```

A.2 Oracle Webmail

This section lists the common errors that occur when accessing Oracle Webmail using the standard SSL port.

Problem 7

In `Traffic_cop`, if you login as `orcladmin` or as an administrative user you have the option to create new users in Oracle WebMail. If the user is not already created in Oracle Internet Directory, then the Web client will prompt you to create the user first and supply you with a link to Oracle Internet Directory Delegated Administration Services. This link is incorrect.

Solution 7

Ensure that the URL for Delegated Administration Services (DAS) is configured correctly as explained in Section 6.2. Clear the Portal cache and Oracle Internet Directory cache as follows:.

To clear Portal cache:

1. Shut down the Middle Tier.

   ```
   opmnctl stopall
   ```

2. Delete the `plsql` and `session` directories in `$ORACLE_HOME/Apache/modplsql/cache` on the Middle Tier.

3. Restart the Middle Tier.

   ```
   opmnctl stopall
   ```

To clear Oracle Internet Directory cache:

1. Log in to Portal as a portal user.
2. Click **Builder,** click **Admin,** click **Global Settings,** and then click the **SSO/OID** tab.
3. Select the **Refresh Cache for OID Parameters** option.
4. Click **Apply**.

Problem 8

Browse buttons have Oracle9*i*AS Single Sign-On warnings.

Solution 8

See Solution 7.

A.3 Oracle Web Conferencing

This section lists the common errors that occur when accessing Oracle Web Conferencing using the standard SSL port.

Problem 9

The Oracle Web Conferencing portlet does not work properly.

When you attempt to access a conference from the main portal site, you are directed to an HTTP error page that displays the message: "Page cannot be found".

Solution 9

This can be fixed by editing the `$ORACLE_HOME/j2ee/OC4J_UM/config/oc4j.properties` file on the Middle Tier. Change the `oracle.mail.Portlet.httpsToWebmail` parameter to `TRUE` to correct the problem. You may need to restart `OC4J_IMEETING`.

A.4 Oracle Files

This section lists the common errors that occur when accessing Oracle Files using the standard SSL port.

Problem 10

The files Portlet is not rendering in HTTPS. If you hover over the links they display as: `http://`*`midtierhostname`*`:443/files/app/FileBrowsePage?event=ChangeDir&FBP=Private`

This URL should begin with `https`, not `http`.

Solution 10

Using the Enterprise Manager, ensure that the following server properties in `FilesBaseServerConfiguration`: `ApplicationHost`, `ApplicationPort` and `ApplicationUseHttps` are correct. If these correctly point to the reverse proxy URL and port, then the images should be generated correctly.

Navigate to

`http://`*`midtierhost`*`:1810`

Select the Middle Tier `middle.`*`midtierhostname`*

`iFS_`*`infrahostname`*`:1521:store.`*`infrahostname`*`:FILES`

Server Configurations

FilesBaseServerConfiguration

Confirm the following parameters:

```
IFS.SERVER.APPLICATION.UIX.ApplicationPort = 443
IFS.SERVER.APPLICATION.UIX.ApplicationHost = midtierhostname
IFS.SERVER.APPLICATION.UIX.ApplicationUseHttps = true
```

This also fixes the Oracle Ultra Search portlet because Oracle Files and Oracle Ultra Search are closely linked together.

Problem 11

Logging in when two Oracle HTTP Servers are on the same host and using Microsoft Internet Explorer and SSL Configuration (from Metalink note: 235112.1).

When two Oracle9iAS HTTP Servers are running on a single computer, such as when the Infrastructure and Middle Tier are both installed on a single server, logging in to Portal is not possible when using a Microsoft Internet Explorer (MSIE) Browser. This has been verified with versions 5.5 and 6.0 of MSIE. The problem occurs when a browser redirect is issued from one port used by the Oracle9*i*AS Single Sign-On server, to the port used by Web Cache which is fronting the Oracle9iAS Portal. When MSIE receives the redirect it erroneously sets the Host: header with the first port rather than the destination port. This behavior is not exhibited by Netscape Navigator (versions 4.6, 4.7, 7.0). When this error occurs with MSIE, one of the following error messages may be displayed after an attempt to log in:

```
Error: Unexpected error encountered in wwsec_app_priv.process_signon (ORA-6502:
PL/SQL: numeric or value error: character string buffer too small) (WWC-41417)
```

Refresh the page to bypass this error

Solution 11

Oracle cannot recommend a solution to this problem because it is internal to Microsoft Internet Explorer. The Oracle Collaboration Suite setup as described in Metalink note 235112.1 will bypass this issue.

Problem 12

Redirecting to the wrong port.

Attempting to access `https://`*`midtierhostname`*`:4444/um/traffic_cop`

directs to:

```
https://collabtng11.us.oracle.com/pls/orasso
```

to log in and then redirects back to:

```
https://midtierhostname>/um/traffic_cop
```

This fails with 404 because it is the wrong port. The redirect should be: `https://collabtng11.us.oracle.com:4444/um/traffic_cop`

This problem is not reproducible in Netscape. 7.1 /4.7 or Mozilla 1.6.

The problem is reproducible in Microsoft Internet Explorer only.

Solution 12

If using Web Cache as described in Chapter 4, "Configuring Web Cache for SSL" you will not encounter this problem.

A.5 Oracle Calendar

This section lists the common errors that occur when accessing Calendar using the standard SSL port.

Problem 13

Referencing the old Oracle9*i*AS Single Sign-On site ID.

Solution 13

The Calendar issue may be corrected by changing the `httpd.conf` file on the Middle Tier.

Comment out the `include` line as shown in this example:

```
# General setup for the virtual host
# include "midtier_install_path/.../Apache/Apache/conf/modosso_https.conf"
```

Problem 14

Out of the box, the calendar Portlet does not work with HTTPS. You receive the error message: "This service is currently unavailable, please try later".

Solution 14

Apply the following patch:

```
3458344 Calendar: Patch Oracle Calendar Application System 9.0.4.1.6
```

Read the install instructions for the patch. To apply the patch:

1. Before you apply the patch, add the following lines in the file `$ORACLE_HOME/config/jazn-data.xml`

   ```
   = = = = add to jazn-data.xml = = = =
   <jazn-policy> #Do not enter this line as it is just to show where to insert the
   text.
   <grant>
   <grantee>
   <codesource>
   <url>file:$ORACLE_HOME/webclient/lib/webclient_common.jar</url>
   </codesource>
   </grantee>
   <permission>
   <class>oracle.ias.repository.schemaimpl.CheckRepositoryPermission</class>
   <name>connectAs</name>
   </permission>
   </permissions>
   </grant>
   ```

2. After the 3458344 patch is applied, edit `$ORACLE_HOME/j2ee/OC4J_Portal/applications/webclient-calendar/webclient-calendar-web/Portlets/Calendar.jsp`.

   Remove the following line because we are not using authentication:

   ```
   System.setProperty("javax.net.ssl.KeyStorePassword", "Oracle_Wallet_
   Password");
   ```

   Edit the following line:

   ```
   System.setProperty("javax.net.ssl.KeyStore",
   "Oracle_Wallet_Client_Certificate_Path");
   ```

   Replace the `Oracle_Wallet_Client_Certificate_Path` with the path to Oracle Wallet, for example:

   ```
   System.setProperty("javax.net.ssl.KeyStore",
   "/u02/mtier/Apache/Apache/conf/ssl.wlt/default");
   $ORACLE_HOME/jlib/javax-ssl-1_1.jar
   $ORACLE_HOME/jlib/jssl-1_1.jar
   ```

Include the following Java Archive (JAR) files in the Oracle Containers for J2EE (OC4J) instance CLASSPATH.

For example, you could include JAR files in

$ORACLE_HOME/j2ee/OC4J_Portal/config/application.xml

by using the following lines:

```
<library path="$ORACLE_HOME/jlib/javax-ssl-1_1.jar"/>
<library path="$ORACLE_HOME/jlib/jssl-1_1.jar"/>
```

On AIX, Solaris, and Linux systems, ensure that `libnjssl9.so` is in the directory specified in the LD_LIBRARY_PATH environment variable. On HP-UX systems, ensure that `libnjssl9.sl` is in the directory specified in the `SHLIB_PATH` environment variable.

A.6 References

The following notes are available on the Metalink Web site, which you can access at

http://www.metalink.oracle.com

On this Web site, you can search for a particular note by using the note number.

- **235112.1:** *How to Configure Portal 9.0.2.x to enable access via HTTPS (SSL)*
- **254790.1:** *Securing your Oracle Collaboration Suite installation*
- **230164.1:** *Configuring Reverse Proxy in front of 9ias v2 SSO (Single Sign-On) server on UNIX*
- **225502.1:** *HTTPClient.HTTPConnection.initDefaultSSLCredential and SSL Handshake Failed NZERROR=28874 when configuring SSL with Portal 9.0.2.x*
- **251789.1:** *Configuring Middle Tier mod_osso Protected Applications for Both HTTP and HTTPS Access*
- **205119.1:** *Unable to Login to Portal: ERROR WWC-41452*

Index