Oracle® Enterprise Manager

Installation and Configuration Guide for CA Service Desk Connector

Release 1.0.5.1.0

E16519-02

June 2011

ORACLE®

Oracle Enterprise Manager Installation and Configuration Guide for CA Service Desk Connector, Release 1.0.5.1.0

E16519-02

Primary Author: Michael Zampiceni

Contents

Preface

This *Connector Installation and Configuration* guide provides the information that you require to install and configure Management Connectors that integrate Enterprise Manager with other management tools and help desk systems.

Audience

This guide is written for Oracle Database system administrators who want to install and configure Management Connectors to enable integration between Enterprise Manager and other systems.

You should already be familiar with Oracle Enterprise Manager.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website 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.

TTY Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711.

Related Documents

For more information, see the following books in the Oracle Enterprise Manager documentation set:

- *Oracle Enterprise Manager Integration Guide*

- *Oracle Database 2 Day DBA*
- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Quick Installation Guide*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Advanced Configuration*
- *Oracle Enterprise Manager Metric Reference Manual*
- *Oracle Enterprise Manager Command Line Interface*
- *Extending Oracle Enterprise Manager*

The latest versions of this and other Oracle Enterprise Manager documentation can be found at:

http://www.oracle.com/technology/documentation/oem.html

Oracle Enterprise Manager also provides extensive online help. Click **Help** on any Oracle Enterprise Manager page to display the online Help system.

Printed documentation is available for sale in the Oracle Store at

http://oraclestore.oracle.com/

To download free release notes, installation documentation, white papers, or other collateral, please visit the Oracle Technology Network (OTN). You must register online before using OTN; registration is free and can be done at

http://otn.oracle.com/membership/

If you already have a user name and password for OTN, then you can go directly to the documentation section of the OTN Web site at

http://otn.oracle.com/documentation/

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction to the Connector

The Oracle Management Connector for CA Service Desk (CASD) integrates CA Service Desk 11 or 12 with Enterprise Manager through either an HTTP or HTTPS connection. Using this connector, you can create, update, close, or reopen a ticket based on the following types of alerts in Enterprise Manager.

- Metric alerts
- Availability alerts (includes alerts for Up, Down, Blackout Started, Blackout Ended, Agent Unreachable, and Agent Unreachable Resolved)

The connector also supports job availability events (that is, job failed and job suspended).

Note that the term ticket refers to a CA Service Desk incident.

The following sections explain various CA Service Desk Connector concepts that you must understand before you start using the CA Service Desk Connector.

1.1 Auto Ticketing

Whenever an alert is triggered or changes in state in Enterprise Manager, the CA Service Desk Connector can automatically open or update a ticket. You can specify the set of alerts for which tickets must be opened.

You can do this in Notification Rules, the user-defined rules that define the criteria by which notifications should be sent for alerts.

> **See Also:** "Configuring Notifications" in the *Oracle Enterprise Manager Administration*.

After the ticket is opened, any subsequent update of the alert, such as a change in alert severity, updates the ticket. After the alert is cleared (severity is set to Clear), you can optionally close the ticket.

See Also: "Section 4.1, "Automatically Creating a Ticket".

For Job alerts, this release of the connector for CA Service Desk supports creating, updating, or closing tickets for Jobs executed by Oracle Enterprise Manager. Tickets are created/updated and closed, for jobs with various Status changes like Error, Failed, Suspended, Succeeded.

1.2 Manual Ticketing

From the Enterprise Manager console, you can manually open a CASD ticket based on an open alert in Enterprise Manager. The CA Service Desk Connector populates the ticket with details based on the alert and the ticket template selected.

See Also: "Section 4.2, "Manually Creating a Ticket".

1.3 Ticket Templates

Ticket templates are XML transformation style sheets that transform Enterprise Manager alerts to a ticket format before the requests are sent to CA Service Desk. A ticket template specifies how Enterprise Manager alert attributes can populate the fields of a CASD ticket.

In Auto Ticketing, a notification method is created for each registered ticket template. The selected notification method determines which ticket template is used when a notification is sent out to the Connector. In the case of manual ticketing, you have to select a ticket template before submitting a request to create the ticket.

The CA Service Desk Connector includes some out-of-box default ticket templates. You may want to customize the templates to suit your needs.

See Also: Chapter 5, "Using Default Templates"

1.4 Grace Period

The grace period provides you with a configuration to prevent the creation of a large number of tickets for frequently reoccurring alerts. For alerts that occur frequently within a relatively short time interval, it is often desirable to open and maintain a ticket that tracks each occurrence of the alert instead of separate tickets each time.

For recurring alerts, the grace period is a time period during which reoccurrences of the same alert update (or re-open) an existing ticket for the alert, rather than create a new ticket.

For example, an alert triggers and a ticket is opened for it. If the grace period is one hour and the alert is cleared at 10:00 a.m., and if the same alert retriggers before 11:00 a.m. (one-hour grace period), the original ticket will be updated/reopened.

1.5 Versions Supported

The base Enterprise Manager version number for the *CA Service Desk Connector Release 1.0.5.1.0* is *Enterprise Manager 10g Release 5*.

2

Installing and Uninstalling the Connector

The CA Service Desk (CASD) ticketing connector is comprised of two components. The first component is the CASD adapter. The CASD adapter provides a web service interface for manipulating incidents in CA Service Desk. The *casd_adapter.jar* file contains the installation files for the CASD adapter. The second component is the CASD connector. The *casd_connector.jar* file contains the CASD connector and is deployed via the Enterprise Manager *emctl* command.

You can download the connector bundle jar file and extract it by using the following command:

```
jar -xvf casd_connector_bundle.jar
```

You will see the two components mentioned above, *casd_connector.jar* and *casd_adapter.jar*.

This chapter provides the following information for installing or uninstalling the CASD Connector, as well as switching from one console to the other:

2.1 Prerequisites

As a prerequisite before using CA Service Desk Connector, ensure that CA Service Desk 11 or 12 is installed and configured. As a prerequisite to installing the CASD Adapter, Java JRE 6.0 update 15 or higher must be installed on the system where the CASD Adapter will be installed.

There can be only one ticketing connector in Oracle Enterprise Manager. Before proceeding to the next section, follow these steps to remove any existing ticketing connector:

1. Click the **Setup** link in the upper right corner of the Oracle Enterprise Manager console.
2. Click the **Management Connectors** link in the left column of the Overview of Setup page.

3. Remove any ticketing connector you may have.

2.2 Installing the Adapter

The CASD Adapter acts as a front-end for all incidents flowing into and out of CASD. Oracle Enterprise Manager posts calls to the web service whenever it needs to create or update an incident, or get an incident from CASD.

You can install the CASD Adapter on any Unix or Windows system that has connectivity to the CASD server and the Oracle Enterprise Manager server.

2.2.1 Security Recommendations

Because the CASD Adapter stores sensitive information for accessing CA Service Desk, access to the adapter files should be limited. Oracle recommends setting up a separate group (hereafter referred to as "the adapter group") that has permission to configure and run the CASD Adapter. Access to the adapter should not be allowed for anyone that is not a member of the adapter group.

2.2.2 Installing and Running the CASD Adapter on Unix

The following sections explain how to install and then subsequently run the Adapter.

2.2.2.1 Installing the Adapter on Unix

To install the adapter on a Unix platform, perform the following steps:

1. Log in as a user that is a member of the adapter group. See the Security Recommendations sections for more information regarding the adapter group.
2. Create a directory where you want to install the adapter.
3. Open a terminal and change the working directory to the installation directory.
4. Download the *casd_adapter.jar* file from the Oracle Technology Network (OTN) to the installation directory.
5. Make sure the *JAVA_HOME* environment variable is set to the directory where Java 1.6 is installed.
6. Enter the following command to unzip and extract the jar file:

   ```
   $JAVA_HOME/bin/jar xvf casd_adapter.jar
   ```

   This creates the adapters directory that contains the installation files.

   Note: If the system where the CASD adapter is being installed does not have the JDK installed, you cannot extract the jar file contents. You must copy the jar file to a system that has the JDK installed and transfer the files after they have been extracted.

7. Enter the following command to change the working directory:

   ```
   cd adapters/endpoints/ca-usd
   ```

8. Enter the following command to run the installation script:

   ```
   sh ./install.sh
   ```

9. When the script prompts whether you want to use HTTPS, answer Y (yes) or N (no):

- If you specify Y, the adapter is set up to use HTTPS port number 8443.
- If you specify N, the adapter is set up to use HTTP port number 8082.

10. When the script prompts for the user name of the web service, enter the user name that must be provided to access the CASD adapter web service.

    Note: This user name is not associated with any CASD or system account. It can be any value that you choose. This user name will be used to restrict access to the adapter web service interface.

11. When the script prompts for the password of the web service, enter the password that must be provided to access the CASD adapter web service.

    Note: This password is not associated with any CASD or system account. It can be any value that you choose. This password will be used to restrict access to the adapter web service interface.

12. When the script prompts for the hostname/IP address of the CASD server, enter the hostname or IP address of the machine where the CASD server is deployed. The hostname will default to *localhost* if no value is provided.
13. When the script prompts for the port number of the CASD server, enter the port number used by the CASD web server (Tomcat or IIS). The port number will default to 8080 if no value is provided.
14. When the script prompts for the user name to use when accessing CASD, enter the user name of the CASD account that the adapter should use when accessing CASD.

    Note: The account must have permission to create, update, and retrieve incident information.

15. When the script prompts for the password to use when accessing CASD, enter the password of the CASD account that the adapter should use when accessing CASD.

    Note: The account must have permission to create, update, and retrieve incident information.

16. After the script displays the message *CASD Adapter Install Complete*, press **Enter** to complete the installation.
17. Enter the following command to change the working directory to the *conf* directory.

    ```
    cd ../../conf
    ```

18. Change the permissions on the *framework.properties* file to allow read, write, and execute permissions for the owner and the adapter group and no access for any other users.
19. If the adapter was configured to run using the HTTPS protocol, you must install a SSL certificate. You can install a self-signed certificate, or you can acquire a certificate from a Certificate Authority (CA).

- To generate and install a self-signed SSL certificate, enter the following commands and replace <*hostname*> with the system host name or the IP address that the CASD adapter will use:

```
$JAVA_HOME/bin/keytool -delete -alias iwave -keypass iwavepw -storepass
iwavepw -keystore keystore.jks

$JAVA_HOME/bin/keytool -genkey -alias iwave -keyalg RSA -keysize 1024
-dname "CN=<hostname>, OU=Development, O=iWave Software, L=Frisco, ST=TX,
C=US" -keypass iwavepw -storepass iwavepw -keystore keystore.jks
```

- To install a certificate that the Certificate Authority issues:
  - Request a certificate from a Certificate Authority, such as VeriSign.

    In the certificate request, make sure to specify the host name or IP address that the CASD adapter will use. The host name in the certificate must match the host name configured for the adapter. If they do not match, the adapter cannot function.
  - After you obtain the certificate from the Certificate Authority, enter the following command to install the certificate, where <*certificateFile*> is the full path name of the file provided by the Certificate Authority:

```
$JAVA_HOME/bin/keytool -export -alias iwave -file <certificateFile>
-keypass iwavepw -storepass iwavepw -keystore keystore.jks
```

The adapter framework is now installed and ready to start.

To add signed certificates to Wallet Manager, see Section 2.7, "Adding Signed Certificates to Wallet Manager".

2.2.2.2 Running the Adapter on Unix

To run the CASD Adapter framework commands listed with the following tasks, first change the working directory in the installation directory to:

adapters/bin

Run the following four commands:

- Start - `./service.sh start`
- Shut Down - `./service.sh stop`
- Restart - `./service.sh restart`
- Check Status - `./service.sh status`

2.2.2.3 Testing the Adapter on Unix

Perform the following steps to verify that the CASD Adapter is functional.

1. Open a terminal and change the working directory to the *adapters/bin* directory in the installation directory.
2. Enter the following command to run the test script:

   `./testAdapter.sh`
3. The test script will prompt for the password information. At the prompt, enter the password that was configured for accessing the Adapter web service in step 11 of Section 2.2.2.1, "Installing the Adapter on Unix".

4. If the test completes successfully, the last line the utility displays is *Test completed successfully.*

2.2.3 Installing and Running the CASD Adapter on Windows

The following sections explain how to install and then subsequently run the Adapter.

2.2.3.1 Installing the Adapter on Windows

To install the adapter on a Windows platform, perform the following steps:

1. Log in as a user that is a member of the adapter group. See the Security Recommendations sections for more information regarding the adapter group.
2. Create a directory where you want to install the adapter.
3. Open a terminal and change the working directory to the installation directory.
4. Download the *casd_adapter.jar* file from the Oracle Technology Network (OTN) to the installation directory.
5. Make sure the *JAVA_HOME* environment variable is set to the directory where Java 1.6 is installed.
6. Enter the following command to unzip and extract the jar file:

   ```
   "%JAVA_HOME%\bin\jar" xvf casd_adapter.jar
   ```

   This creates the adapters directory that contains the installation files.

   Note: If the system where the CASD adapter is being installed does not have the JDK installed, you cannot extract the jar file contents. You must copy the jar file to a system that has the JDK installed and transfer the files after they have been extracted.

7. Enter the following command to change the working directory:

   ```
   cd adapters\endpoints\ca-usd
   ```

8. Enter the following command to run the installation script:

   ```
   .\install.bat
   ```

9. When the script prompts whether you want to use HTTPS, choose Y (yes) or N (no):
   - If you specify Y, the adapter is set up to use HTTPS port number 8443.
   - If you specify N, the adapter is set up to use HTTP port number 8082.
10. When the script prompts for the user name of the web service, enter the user name that must be provided to access the CASD adapter web service.

    Note: This user name is not associated with any CASD or system account. It can be any value that you choose. This user name will be used to restrict access to the adapter web service interface.

11. When the script prompts for the password of the web service, enter the password that must be provided to access the CASD adapter web service.

> **Note:** This password is not associated with any CASD or system account. It can be any value that you choose. This password will be used to restrict access to the adapter web service interface.

12. When the script prompts for the hostname/IP address of the CASD server, enter the hostname or IP address of the machine where the CASD server is deployed. The hostname will default to *localhost* if no value is provided.
13. When the script prompts for the port number of the CASD server, enter the port number used by the CASD web server (Tomcat or IIS). The port number will default to 8080 if no value is provided.
14. When the script prompts for the user name to use when accessing CASD, enter the user name of the CASD account that the adapter should use when accessing CASD.

> **Note:** The account must have permission to create, update, and retrieve incident information.

15. When the script prompts for the password to use when accessing CASD, enter the password of the CASD account that the adapter should use when accessing CASD.

> **Note:** The account must have permission to create, update, and retrieve incident information.

16. Enter the following command to change the working directory to the *conf* directory.

```
cd ..\..\conf
```

17. Change the permissions on the framework.properties file to allow read, write, and execute permissions for the adapter group and no access for any other users.
18. After the script displays the message *CASD Adapter Install Complete*, press **Enter** to complete the installation.
19. If the adapter was configured to run using the HTTPS protocol, you must install a SSL certificate. You can install a self-signed certificate, or you can acquire a certificate from a Certificate Authority (CA).
    - To generate and install a self-signed SSL certificate, enter the following commands, and replace <*hostname*> with the system host name or IP address that the CASD adapter will use:

```
"%JAVA_HOME%\bin\keytool" -delete -alias iwave -keypass iwavepw -storepass
iwavepw -keystore keystore.jks

"%JAVA_HOME%\bin\keytool" -genkey -alias iwave -keyalg RSA -keysize 1024
-dname "CN=<hostname>, OU=Development, O=iWave Software, L=Frisco, ST=TX,
C=US" -keypass iwavepw -storepass iwavepw -keystore keystore.jks
```

    - To install a certificate that the Certificate Authority issues:
      – Request a certificate from a Certificate Authority, such as VeriSign.

        In the certificate request, make sure to specify the host name or IP address that the CASD adapter will use. The host name in the certificate must

match the host name configured for the adapter. If they do not match, the adapter cannot function.

– After you obtain the certificate from the Certificate Authority, enter the following command to install the certificate, where <*certificateFile*> is the full path name of the file provided by the Certificate Authority:

```
"%JAVA_HOME%\bin\keytool" -export -alias iwave -file <certificateFile>
-keypass iwavepw -storepass iwavepw -keystore keystore.jks
```

The following steps are optional. If you want the adapter to run as a Windows service, perform the following steps.

1. Log into an account that has permission to add a windows service.

> **Note:** On most systems, the account must be a member of the Administrators group to add a windows service.

2. Make sure the account has read and execute permissions for the *adapters\bin* directory.
3. Change the working directory to the *adapters\bin* directory in the installation directory.
4. Enter the following command to install the adapter as a Windows service:

```
service.bat install
```

5. Make sure the designated login account for the windows service has Full Control for the adapter directory and read and execute permissions on the *conf\framework.properties* file.

The adapter framework is now installed and ready to start.

To add signed certificates to Wallet Manager, see Section 2.7, "Adding Signed Certificates to Wallet Manager".

2.2.3.2 Running the Adapter on Windows

There are two ways you can run the adapter on Windows: *Standalone Service* and *Windows Service*.

2.2.3.2.1 Standalone Service

To start the CASD adapter framework when set up as a standalone application (not set up to run as a Windows service):

1. Change the working directory to the *adapters\bin* directory in the installation directory.
2. Run the following command:

```
startAdapters.bat
```

To shut down the CASD adapter framework, close the window where you started the adapter.

2.2.3.2.2 Windows Service

To start the CASD adapter framework when set up to run as a Windows service, run the following command:

```
net start iWaveAdapters
```

To shut down the CASD adapter framework, run the following command:

```
net stop iWaveAdapters
```

2.2.3.3 Testing the Adapter on Windows

Perform the following steps to verify that the CASD Adapter is functional.

1. Open a terminal and change the working directory to the *adapters\bin* directory in the installation directory.
2. Enter the following command to run the test script:

   ```
   .\testAdapter.bat
   ```

3. The test script will prompt for the password information. At the prompt, enter the password that was configured for accessing the Adapter web service in step 11 of Section 2.2.3.1, "Installing the Adapter on Windows".
4. If the test completes successfully, the last line the utility displays is *Test completed successfully*.

2.3 Installing the Connector

Perform the following steps to install the connector:

1. Copy *casd_connector.jar* to *$ORACLE_HOME/sysman/connector* on the server hosting your OMS. For multiple OMSes, you need to copy the jar file for all OMSes.
2. Run the following *emctl* command on all OMSes if you have a multi-OMS environment:

   ```
   $ORACLE_HOME/bin/emctl extract_jar connector -jar <jarfile>
   -cname <connector_name>
   ```

   This extracts the jar file to this folder:

   $ORACLE_HOME/sysman/connector/CASD_Connector/

   For example:

   ```
   emctl extract_jar connector -jar casd_connector.jar
   -cname "CASD Connector"
   ```

3. Deploy the connector by running the following *emctl* command. You only need to run this step on one OMS.

   ```
   $ORACLE_HOME/bin/emctl register_connector connector -dd
   <connectorType.xml>
   ```

   ```
   -cs //<server>:<port>/<dbSID> -repos_user <username> -repos_
   pwd <password>
   ```

   For example:

   ```
   emctl register_connector connector -dd $ORACLE_HOME/sysman/connector/
   CA_Service_Desk_Connector/CADeploy.xml
   -cs  //$emhost:$dbport/$dbSID -repos_user sysman -repos_pwd $repospwd
   ```

The CASD Connector should now appear in the Management Connector page with version 1.0.5.1.0.

2.3.1 Registering the Ticket Templates

There are two default templates located in the *$ORACLE_HOME/sysman/connector/CASD_Connector/templates* directory:

- *CASD_Default_Incident.xsl*
- *CASD_Default_Incident_AutoClose.xsl*

> **Note:** See Section 5.1, "Template Process" for detailed information about these templates.

Perform the following steps to register these templates as well as others:

1. For each template above, run the following *emctl register_ticket_template* connector command as a user with execute privilege on emctl and the ability to read the ticket template:

   ```
   $ORACLE_HOME/bin/emctl register_ticket_template connector -t
   <ticketTemplate.xsl> -cs //<server>:<port>/<dbsid/service name for RAC DB>
   -repos_user <username> -repos_pwd <password> -ctname <connectorTypeName> -cname
   <connectorName> -iname <internalName> -tname <templateName> -ttype 2 -d
   <description>
   ```

   See Table 2–1, " emctl Parameters" for descriptions of the command parameters.

2. Run the same command for each of the following templates:

   - *createTicketResponse.xsl* - Specify ttype 1, iname createTicket
   - *getTicket_response.xsl* - Specify ttype 1, iname getTicket
   - *getTicket_request.xsl* - Specify ttype 2, iname getTicket
   - *updateTicketResponse.xsl* - Specify ttype 1, iname updateTicket

   These templates are located in the following directory:

   $ORACLE_HOME/sysman/connector/CASD_Connector

   For templates *CASD_Default_Incident.xsl* and *CASD_Default_Incident_AutoClose.xsl*, the internal name can be the file names. For the other templates, the inames are fixed.

   For multiple OMS installations, you must run the *emctl* command only once for each template from any of the OMSes.

   Table 2–1, " emctl Parameters" provides descriptions for the parameters shown in the *emctl* command above.

Table 2–1 emctl Parameters

Parameter	Description
cs	Connect string. Specify as "*//$emHost:$dbPort/$dbSID*", where, *$emHost* is the server, *$dbPort* is the port, and *$dbSID* is the database session identifier.
server	Host name of the Enterprise Manager repository
port	Listener port of the repository.
database sid / Service Name for RAC DB	Repository database instance ID or service name if you are using RAC database as the repository
repos_user	Specify SYSMAN

Table 2–1 (Cont.) emctl Parameters

Parameter	Description
repos_pwd	Password for SYSMAN
ctname	Connector type name - Specify "CA Service Desk Connector". The double quotes ("") are mandatory.
cnameConnector name	Specify "CA Service Desk Connector". The double quotes ("") are mandatory
inameInternal name	Depending on the template, the values can be *CASD_Default_Incident_AutoResolve.xsl*, *CASD_Default_Incident_AutoClose.xsl*, or createTicket, getTicket
tnameTemplate name	Depending on the template, the values can be Create Ticket Response, Get Ticket Request, Get Ticket Response, Update Ticket Response, or a value defined by the user
ttypeTemplate type	Specify 1 for inbound transformation and 2 for outbound transformation
description	Short description for the ticket template. This description is also displayed in Enterprise Manager

Example 2–1, "Registration Example" shows template registration for the *CASD_Default_Incident_AutoClose.xsl* template.

Example 2–1 Registration Example

```
emctl register_template connector -t "$ORACLE_HOME/sysman/connector/CASD _
Connector/templates/CASD_Default_Incident_AutoClose.xsl" -cs
"//$emHost:$dbPort/$dbSID" -repos_user sysman -ctname "CASD Connector" -cname
"CASD Connector" -tname "CASD_Default_Incident_AutoClose.xsl" -iname "CASD_
Default_Incident_AutoClose.xsl" -ttype 2 -d "Template creates a ticket with
priority based on event severity. It sets the ticket to 'Closed' if the event
severity clears" -repos_pwd $repos_pwd
```

The following table lists the properties of each template for the CASD Connector.

Table 2–2 Template Properties

Template	Template Name	Internal Name	Template Type
CASD_Default_Incident_AutoClose.xsl	<Defined by the users>	CASD_Default_Incident_AutoClose.xsl	2
CASD_Default_Incident.xsl	<Defined by the users>	CASD_Default_Incident_.xsl	2
createTicketResponse.xsl	Create Ticket Response	createTicket	1
getTicket_request.xsl	Get Ticket Request	getTicket	2
getTicket_response.xsl	Get Ticket Response	getTicket	1
updateTicketResponse.xsl	Update Ticket Response	updateTicket	1

2.4 Uninstalling the Connector

To uninstall the connector, follow these steps:

1. Click the **Setup** link in the upper right corner of the Oracle Enterprise Manager console.

2. Click the **Management Connectors** link in the left column of the Overview of Setup page.
3. Select the connector, then click **Delete**.
4. On the Confirmation page, click **Yes**.

2.5 Uninstalling the Adapter

This section describes the procedures for uninstalling the adapter on Unix and on Windows.

2.5.1 Uninstalling the Adapter on Unix

To uninstall the adapter on a Unix platform, perform the following steps:

1. Stop the adapter as specified in Section 2.2.2.2, "Running the Adapter on Unix".
2. Delete the adapters folder from the adapter installation directory.

2.5.2 Uninstalling the Adapter on Windows

To uninstall the adapter on a Windows platform, perform the following steps:

1. Stop the adapter as specified in Section 2.2.3.2, "Running the Adapter on Windows".
2. If the adapter is installed as a Window service, perform the following steps to uninstall the adapter as a service:
   - Open a command window and change the working directory to the *adapters**bin* directory in the adapter install directory.
   - Issue the command `.\service uninstall`
3. Delete the adapters folder from the adapter installation directory.

2.6 Navigating Between CASD and Enterprise Manager

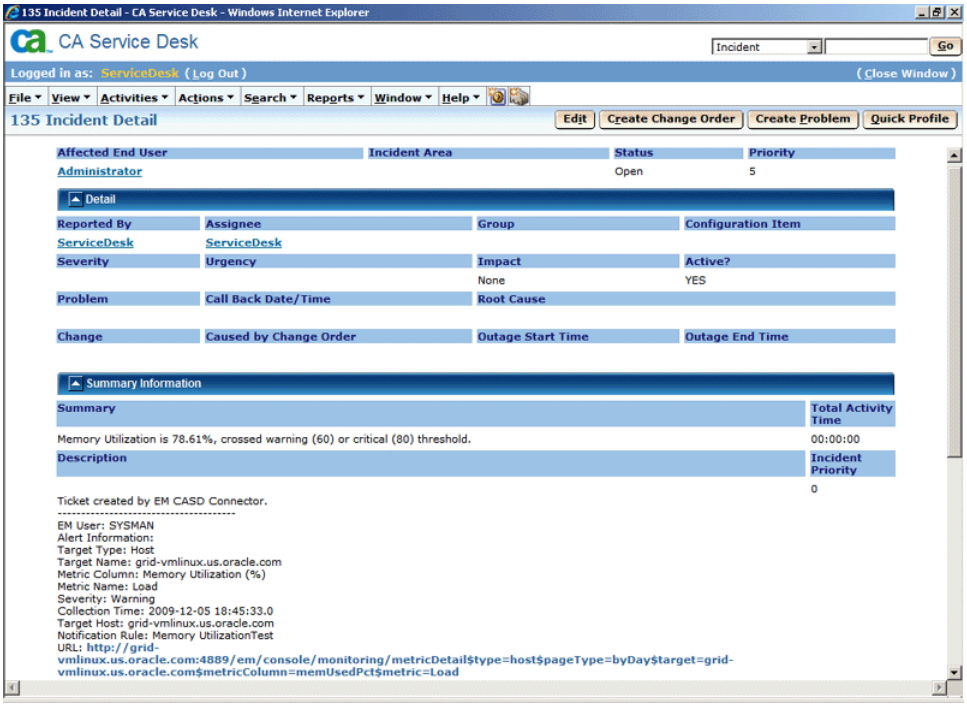
The following sections explain how to switch from one console to the other.

2.6.1 Navigating from CASD to Enterprise Manager

From the Incident Detail page, click the link to the URL label in the Description field, as shown in Figure 2–1. This action takes you to the Enterprise Manager console login page. After you provide the Enterprise Manager user name and password, you are forwarded to the alert related to this incident.

Note: The Enterprise Manager user whose name you specify should at least have View privileges on the target on which the alert was raised.

Figure 2–1 Incident Detail in CASD Console



2.6.2 Navigating from Enterprise Manager to CASD

Follow these steps to navigate from Enterprise Manager to CASD:

1. In the Enterprise Manager console, click the alert message to go to the Metric Details page for the alert.
2. In the Alert History table, locate the ticket ID link in the Last Comment column.

> **Note:** The ticket id that is displayed is comprised of two identifiers used by CASD. The first ID is the external identifier and is a numeric value. This is the incident identifier that is displayed at the CASD web console. The second ID is the internal identifier and is listed in parentheses. The internal identifier is comprised of *cr:* followed by a numeric value. This identifier is used when the connector submits update, reopen, or close requests to the CASD Adapter.

3. (If not found) Click the icon in the Details column to get more information about the alert.
4. On the page that appears, locate the ticket ID in the Alert Details table.
5. Click the ticket ID link. You are forwarded to the CASD Web console login page.
6. Provide valid CASD account details.

The incident details associated with this alert are displayed.

2.7 Adding Signed Certificates to Wallet Manager

To add signed certificates to Wallet Manager, follow these steps on Enterprise Manager:

Note: Oracle Wallet Manager is available at *$ORACLE_HOME/bin* on OMS. See the *Oracle Application Server Administrator's Guide* for details.

1. Do the following to obtain a copy of the certificate that the CASD Adapter is using:
   a. Open a command prompt window and change the working directory to the adapters/comf directory in the adapter install directory:

      <ADAPTER_INSTALL>/adapters/conf

   b. Issue the following command to extract the certificate:
      – Unix platforms:

        ```
        $JAVA_HOME/bin/keytool -exportcert -alias iwave -file
        CASDws.cer -keystore keystore.jks -storepass iwavepw
        ```

      – Windows platforms:

        ```
        "%JAVA_HOME%\bin\keytool" -exportcert -alias iwave
        -file CASDws.cer -keystore keystore.jks -storepass
        iwavepw
        ```

   c. Transfer the certificate file *CASDws.cer* to the system where Enterprise Manager is installed.
2. As Super Administrator, create a wallet using the following *orapki* utility command at the OMS host:

   ```
   orapki wallet create -wallet client -auto_login
   ```

   Note: *orapki* is available at *$ORACLE_HOME/bin* on OMS.

3. Add the trusted certificate to the wallet by entering the following command:

   ```
   orapki wallet add -wallet client -trusted_cert -cert
   CASDws.cer
   ```

4. To view the content of the wallet, enter the following command:

   ```
   orapki wallet display -wallet client
   ```

   Ensure that the information for the CASDws.cer certificate is displayed.
5. In Oracle Wallet Manager, open the client wallet.
6. Go to *Select Trusted Certificates* and select **Operations** on the main menu.
7. Select **Export All Trusted Certificates**.
8. Save the file as *certdb.txt*.
9. Place the file *certdb.txt* in the connector home root directory (*$OMS_HOME/sysman/connector*).

   If the file *certdb.txt* already exists in the root directory, open the file and add the contents of your *certdb.txt* to the existing content.

Now Java SSL can use this file for communication between Enterprise Manager and the CASD Adapter in HTTPS mode.

Note: For information on creating a wallet, see "Creating and Viewing Oracle Wallets with orapki" in the *Oracle Database Advanced Security Administrator's Guide, 10g Release 2 (10.2)*.

3

Configuring the Connector

This chapter provides the following information for setting up and configuring the CA Service Desk Connector and related tasks:

- Configuring the Connector
- Providing General Settings
- Working with Ticket Templates

3.1 Configuring the Connector

Perform the following steps for basic configuration:

1. As Super Administrator, from the Enterprise Manager console, click **Setup**.

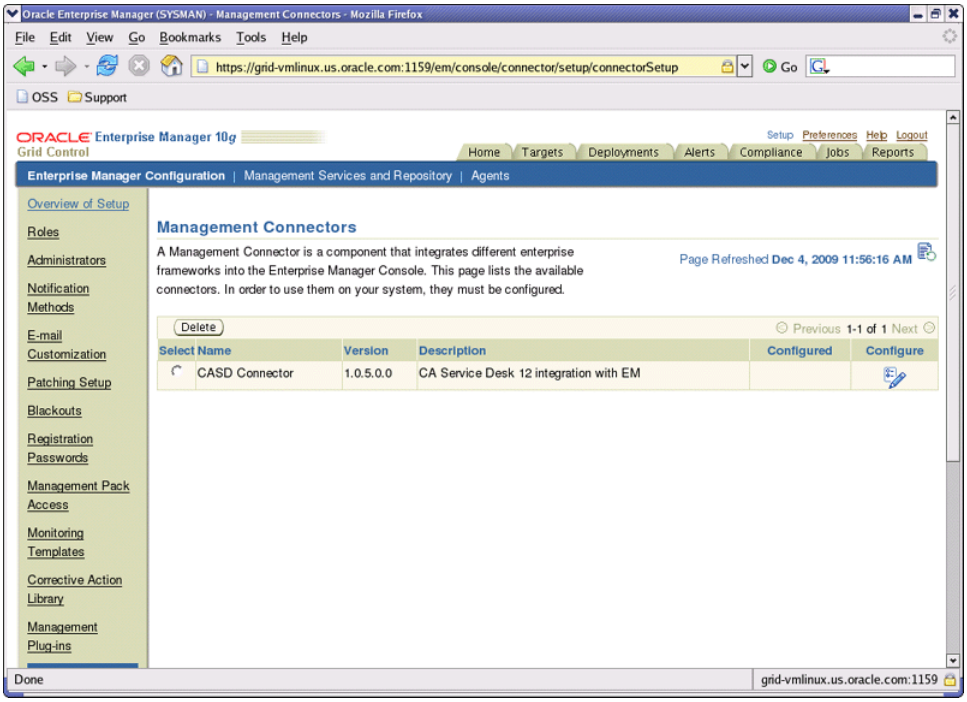
   The Overview of Setup page appears.

2. Click **Management Connectors** in the left pane.

   The Management Connectors page appears. For the CA Service Desk Connector row, the Configured column should be blank, as shown in Figure 3–1.

> **Note:** A check mark instead indicates that the Connector is already configured.

Figure 3–1 Management Connectors Page



3. Click the Configure icon for the CA Service Desk Connector.

   The General tab of the Configure Management Connector page appears, as shown in Figure 3–2.

4. Provide the required settings. See Section 3.2, "Providing General Settings" for details.

5. Click **OK**.

   The Management Connectors page reappears. The row for the CA Service Desk Connector should have a check mark in the Configured column.

6. Optionally you can click the configure icon again to check for the available ticket templates.

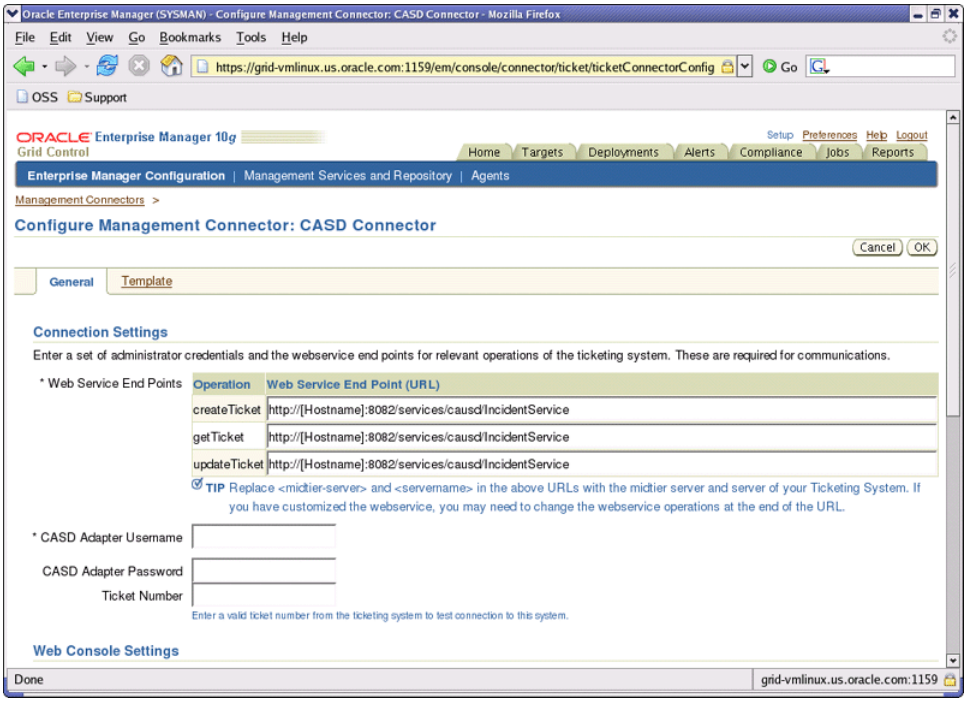
7. Click the **Ticket Templates** tab.

   All out-of-box ticket templates should appear in the table.

   If any of the ticket templates are missing, you can register them using the *emctl* command from the *ORACLE_HOME/bin* directory, where *ORACLE_HOME* is the Oracle home directory of OMS.

   If you choose HTTPS as the protocol to establish a connection between CASD and Enterprise Manager, see Section 2.7, "Adding Signed Certificates to Wallet Manager".

Figure 3–2 Configure Management Connector Page



3.2 Providing General Settings

The following sections explain how to provide various configuration details.

3.2.1 Connection Settings

The CA Service Desk Connector communicates with the Service Desk through a web service provided by the CASD Adapter. Mandatory fields are indicated by an asterisk (*).

- Web Service End Points - End points to *createTicket*, *updateTicket*, and *getTicket* web services exposed by the CASD Adapter. See "Using the Correct URL for CASD Adapter Operations" in Appendix A for additional information.
- CASD Adapter Username - User name that was configured for accessing the Adapter web service in step 10 of the appropriate adapter installation section (Section 2.2.2.1 for Unix and Section 2.2.3.1 for Windows).
- CASD Adapter Password - Password that was configured for accessing the Adapter web service in step 11 of the appropriate adapter installation section (Section 2.2.2.1 for Unix and Section 2.2.3.1 for Windows).
- Ticket Number - Enter a valid ticket number if you want to test the connection when you save the configuration.
  - If you do not enter a ticket number, no message appears on the Management Connectors page after you click OK and the configuration is saved.
  - If you specify the correct Web service end points and enter a valid ticket number, the following message appears on the Management Connectors page after you click OK:

    Connection test succeeded. The configuration was saved.

- If you have not previously saved the connector configuration and entered an invalid ticket number, the following message appears on the Management Connectors page after you click OK:

  Connection test failed. The configuration was saved.

- If you have saved the connector configuration before, specify incorrect Web service end points, and specify either a valid or invalid ticket number, the following message appears on the Management Connectors page after you click OK:

  Connection test failed. The configuration was not saved.

3.2.2 Web Console Settings

Web Console settings are required if you want the Connector to provide links to CA Service Desk tickets created by Enterprise Manager in the context of an alert.

To enable this functionality, provide the following Web console settings.

- Enable web console - Check this box to enable launching of the CASD ticket page within context from Enterprise Manager.
- CASD Server Port - Port number used by the CASD server for the web console.
- CASD Server Host - Host name or IP address of the CASD server that hosts the web console.

3.2.3 Grace Period

You can enable and disable the grace period and configure its value. By default, the grace period is disabled. See Section 1.4, "Grace Period" for details. This setting applies to all alerts the CA Service Desk Connector processes.

3.3 Working with Ticket Templates

The following sections provide information about registering, removing, replacing, and adding ticket templates.

3.3.1 Registering Ticket Templates

You need to register ticket templates before they are recognized in Enterprise Manager. For Auto Ticketing, a notification method is created for each registered ticket template and a ticket is created and updated based on the ticket template associated with the selected notification method. For manual ticketing, registered ticket templates are available for selection.

All registered ticket templates are displayed in the Configure Management Connector Ticket Templates page. To register additional ticket templates that you create, see Section 2.3, "Installing the Connector".

See Also: Table 2–1, " emctl Parameters"

3.3.2 Viewing Template Code

Click a template name to view the XSLT code for the template.

The ticket templates are in XSLT format. A basic knowledge of XSLT is required to understand the code.

3.3.3 Removing a Template

To remove a template, do the following:

> **Important:** If the template you delete has a notification rule associated with it, ticketing will not work for this particular notification rule after the deletion.

1. Select the template and click **Remove**.
2. At the prompt, confirm the removal.
3. Before you exit the page, click **OK** for the deletion to take effect.

> **Note:** Unless you click OK before you exit, the template is not deleted. The next time you go to the Ticket Template page, the templates reappear.

Though the ticket template is removed from the Enterprise Manager repository, it is still available on OMS in the Connector home directory. You can re-register the ticket template later if required.

3.3.4 Replacing Templates

To replace an existing ticket template, complete these steps:

1. Delete the ticket template.
2. Register the new template using *emctl*.

3.3.5 Adding New Templates

To add templates other than the out-of-box templates Oracle provides, you should define new templates and register them using emctl.

> **See Also:** Section 5.3, "Customizing Ticket Templates"

4

Creating Service Desk Tickets

You can create tickets automatically or manually. The following sections explain how to create both types:

- Automatically Creating a Ticket
- Manually Creating a Ticket

4.1 Automatically Creating a Ticket

Complete the following steps to automatically create a ticket:

1. Review Chapter 5, "Using Default Templates".
2. Select an appropriate ticket template with the desired mapping of Enterprise Manager alert fields to the Service Desk ticket fields.
3. If you do not have a ticket template that satisfies your requirement, create one and register it. For more information, see Section 5.3, "Customizing Ticket Templates".
4. Create a notification rule using the following steps:

   Important: Do not select more than one ticket template for this notification rule.

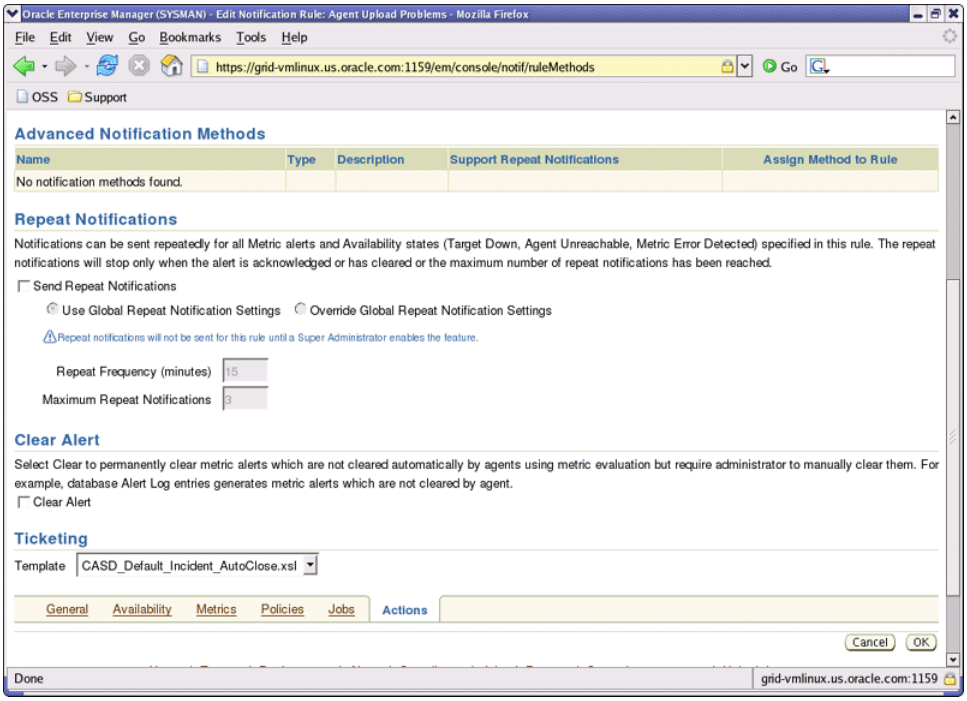
   a. From the Enterprise Manager console, click **Preferences**.
   b. In the left pane, under Notification, click **Rules**, then **Create**.
   c. In the Create Notification Rule General page, specify the rule name, a description, and the targets for which this rule should apply.
   d. In the Create Notification Rule Availability page, select the availability states for which you want to create tickets.
   e. In the Create Notification Rule Metrics page, select the metrics and their associated alert severities for which you want to create and update tickets.

      Ensure that you select all relevant alert severities if you want to update the ticket when the alert severity changes. For example, to open a ticket for a critical alert on the CPU Utilization(%) metric and the ticket is to be updated if the CPU Utilization(%) changes to warning or clear severity, in the notification rule select Critical, Warning, or Clear severities for the CPU Utilization(%) metric.
   f. In the Create Notification Rule Jobs page, select the jobs and the job statuses for which you want to create and update tickets.

g. In the Create Notification Rule: Actions page, choose the ticket template from the Ticketing Template drop-down, as shown in Figure 4–1.

See Also: "Configuring Notifications" in *Oracle Enterprise Manager Administration*

Figure 4–1 Ticketing Template Drop-down Menu



The following process occurs after you create the notification rule for your alerts:

- A notification is sent to the CA Service Desk Connector when a metric alert triggers that matches your rule. The CA Service Desk Connector creates/updates a ticket according to the ticket template as set in the notification rule.
- The ticket is created or updated on the Service Desk Ticket system.
- In Enterprise Manager, the alert annotation is updated. A comment is added to the Metric Details page of the alert to indicate that a ticket was created or updated, along with the ticket ID and ticket page URL (if the Web console settings are configured and enabled).

A ticket is updated if there is an existing active ticket for an alert. Figure 4–2 shows the ticket in the Service Desk console, and Figure 4–3 shows the alert as displayed in Enterprise Manager.

Figure 4–2 Ticket in the Service Desk Console

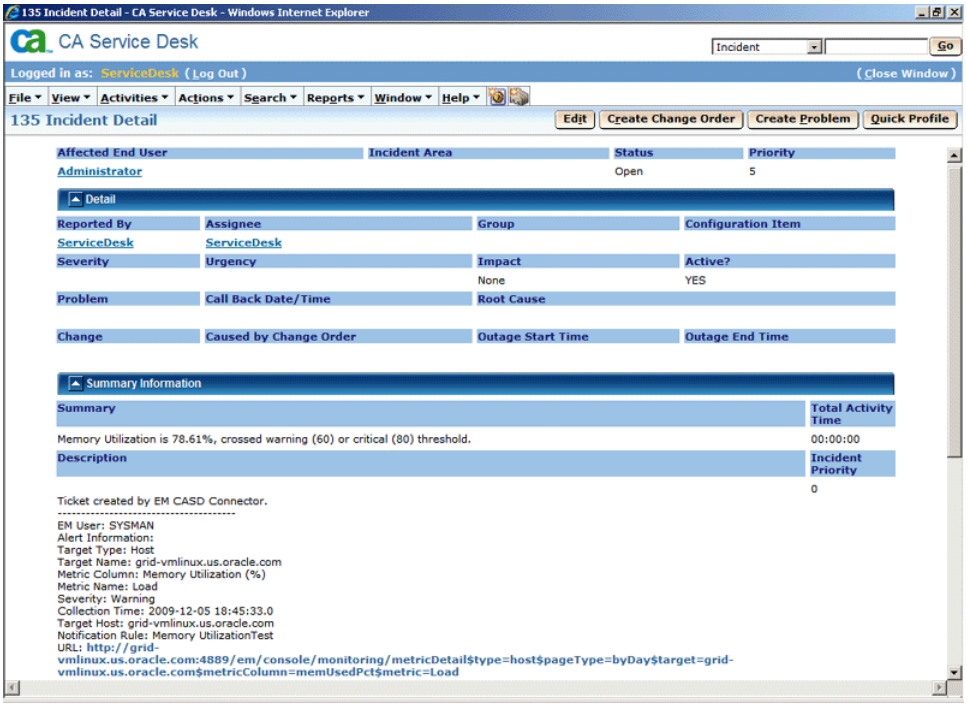
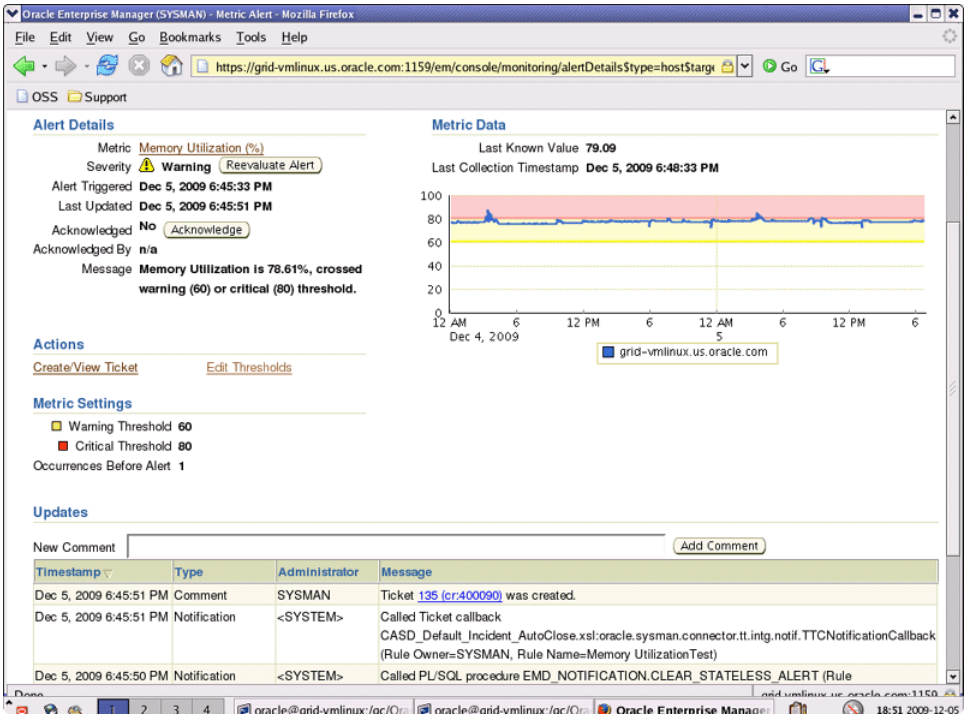


Figure 4–3 Alert As Displayed in Enterprise Manager

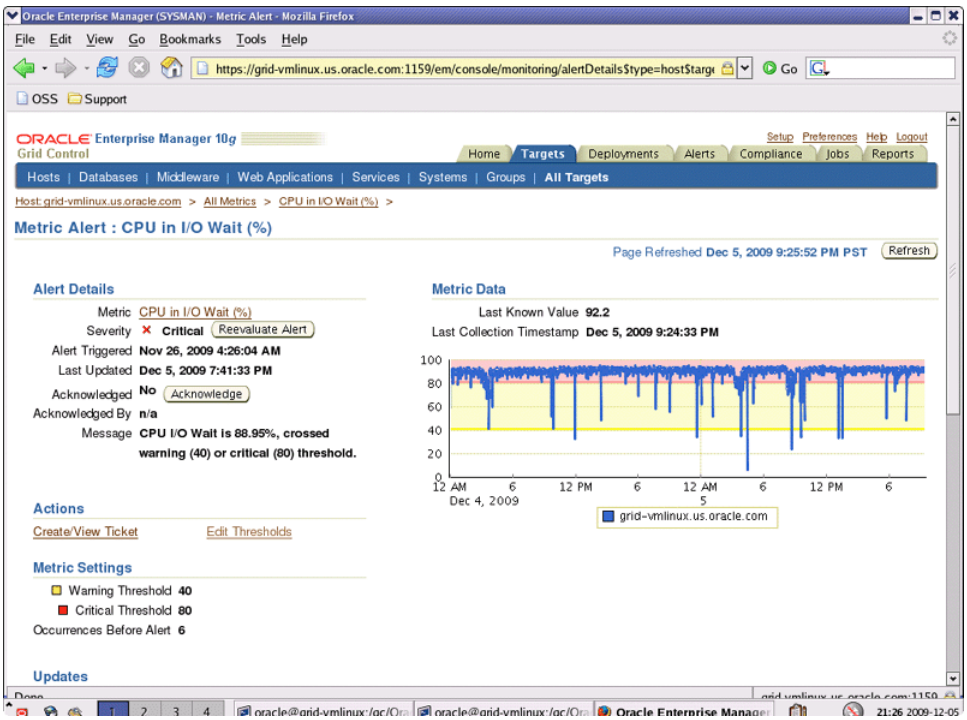


4.2 Manually Creating a Ticket

Perform the following steps to manually create a ticket:

1. After a metric alert occurs, go to its alert details page by clicking on the alert message in the Enterprise Manager console. The alert details page for the alert should appear, as shown in Figure 4–4.

Figure 4–4 Metric Alert Details Page



2. Click the **Create/View Ticket** link in the Actions section.

   The Create Ticket page appears if no active ticket exists for the alert.

3. Select a ticket template and then click **Submit**, as shown in Figure 4–5.

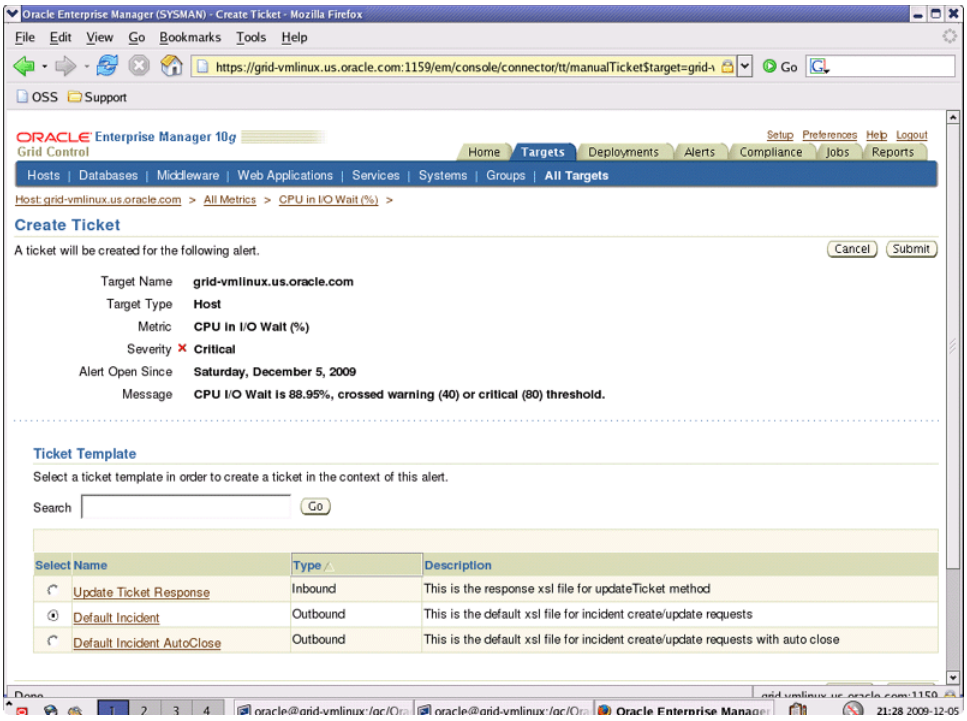
If you do not see the desired template, you can register one using the *emctl* command. See Section 3.3.1, "Registering Ticket Templates".

If creating or updating the ticket is successful, the ticket ID appears in the Last Comment column of the Alert History table for the metric alert.

If the Web console settings are configured and enabled, the ticket ID appears as a link to the ticket page in Service Desk.

Note: You cannot manually update the ticket using the CA Service Desk Connector. You need to manually update the ticket in Service Desk for any subsequent alert severity change, or you can include the metric in a notification rule.

Figure 4–5 Create Ticket Page



5

Using Default Templates

This chapter provides details on the default ticket templates shipped along with the CA Service Desk Connector. The ticket templates specify the mappings between Enterprise Manager alert attributes and Service Desk ticket attributes.

5.1 Template Process

All out-of-box templates cause the following actions to occur when you create a ticket for an alert:

- Write alert information to Description (Service Desk ticket description).
- Set the Service Desk ticket summary based on the alert message. On update, the ticket summary field is updated to include the latest alert message information.

The out-of-box templates are as follows:

- *CASD_Default_Incident.xsl*

  The *CASD_Default_Incident.xls* template creates, updates, or reopens a Service Desk ticket using the default field mapping. The template does not close the ticket when the event severity value becomes Clear.

- *CASD_Default_Incident_AutoClose.xsl*

  The *CASD_Default_Incident_AutoClose.xsl* template creates, updates, or reopens a Service Desk ticket using the default field mapping. The template sets the ticket status to *Closed* when the event severity value becomes *Clear*.

5.2 Reading and Mapping Ticket Templates

Table 5–1 illustrates the creation of a ticket using the default templates. This illustration will help you to read a ticket template. In the tables, * denotes a literal string and ** indicates whether the attribute applies.

Ticket creation mappings are the same for *CASD_Default_Incident_AutoClose.xsl* and *CASD_Default_Incident.xsl*.

Table 5–1 shows Service Desk ticket attributes and corresponding Enterprise Manager alert values for ticket creation mappings.

Table 5–1 Ticket Creation Mappings (for all templates)

Service Desk Ticket Attributes	Enterprise Manager Alert Attributes	Value
Summary	Message	N/A
Description	**For metric alerts:**	Values from alert context
	EMUser - Notification rule owner when the ticket is created through auto-ticketing, and is the Enterprise Manager log-in user when the ticket is created through manual-ticketing.	
	TargetType	
	TargetName	
	MetricColumn - Name of the metric, such as CPU Utilization (%).	
	MetricName - Category of the metric. For the CPU Utilization (%) metric, this would be 'Load.'	
	TargetProperties** - name:value pairs of defined target properties. For example:	
	Line of business:	
	Finance	
	Owner:	
	Finance-DB Team	
	KeyColumn ** - For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name.'	
	KeyValues ** - For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	URL - URL to the metric details page in the context of the alert.	

Table 5–1 (Cont.) Ticket Creation Mappings (for all templates)

Service Desk Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description (**continued**)	**For job status events:** EMUser - Notification rule owner JobName JobType JobOwner JobStatus JobTarget - Includes TargetName and TargetType, such as the host name of the targetType "Host." CollectionTime NotificationRuleName URL - URL of the Job Event page. Values from the alert context.	Values from alert context
Priority	Severity - Applies to metric alerts JobStatus - Applies to job status events	**For metric alerts:** ■ If severity is Critical, Unreachable Start or Agent Unreachable Start set Priority to Medium (3). ■ Otherwise, set Impact to Low (5). **For job status events:** ■ If the JobStatus is Initialization Error, Failed, or Failed and Retried set Priority to High(1). ■ If the JobStatus is Skipped set Priority to Medium-High(2). ■ If the JobStatus is Scheduled, Running, or Queued set Priority to Low(1). ■ If the JobStatus is Success set Priority to None. ■ Otherwise, set Priority to Medium-Low(2). ■
Reported By	N/A	Administrator
Activity Log	**For metric alerts:** Severity Message **For job status events:** JobStatus Message	**For metric alerts:** Ticket created by Oracle Enterprise Manager Connector for CA Service Desk based on an alert with <Severity> severity. Message: <Message> **For job status events:** Ticket created by Oracle Enterprise Manager Connector for CA Service Desk based on a job with a status of <JobStatus>. Message: <Message>

Table 5–1 (Cont.) Ticket Creation Mappings (for all templates)

Service Desk Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	N/A	*Open (OP)

Table 5–2 shows Service Desk ticket attributes and corresponding Enterprise Manager alert attributes and values for *CASD_Default_Incident_AutoClose.xsl* mappings.

Table 5–2 Ticket Updates (CASD_Default_Incident_AutoClose.xsl Mappings)

Service Desk Ticket Attributes	Enterprise Manager Alert Attributes	Value
Identifier	TicketID - Extracts only the internal identifier from the ticket id	N/A
Summary	Message	N/A
Priority	Severity - Applies to metric alerts JobStatus - Applies to job status events	**For metric alerts:** ■ If severity is Critical, Unreachable Start or Agent Unreachable Start set Priority to Medium (3). ■ Otherwise, set Impact to Low (5). **For job status events:** ■ If the JobStatus is Initialization Error, Failed, or Failed and Retried set Priority to High(1). ■ If the JobStatus is Skipped set Priority to Medium-High(2). ■ If the JobStatus is Scheduled, Running, or Queued set Priority to Low(1). ■ If the JobStatus is Success set Priority to None. ■ Otherwise, set Priority to Medium-Low(2).
Status	**For metric alerts:** Grace Period Severity **For job status events:** Grace Period Job Status Code	**For metric alerts:** If Grace Period is set to "Yes" set Status to Open (OP). If Severity is set to Clear, Unreachable Clear, Agent Unreachable Clear, Blackout End or Metric Error End set Status to Close (CL). Otherwise do not set Status. **For job status events:** If Grace Period is set to "Yes" set Status to Open (OP). If Job Status Code is set to Success (5) set Status to Closed (CL). Otherwise do not set Status

Table 5–2 (Cont.) Ticket Updates (CASD_Default_Incident_AutoClose.xsl Mappings)

Service Desk Ticket Attributes	Enterprise Manager Alert Attributes	Value
Activity Log	**For metric alerts:** Grace Period Severity Message **For job status events:** Grace Period JobStatus Message	**For metric alerts:** If Grace Period is set to "Yes" set Activity Log to "Ticket reopened because the associated alert re-triggered at <Severity> severity within the grace period. Message: <Message>" If Severity is set to Clear, Unreachable Clear, Agent Unreachable Clear, Blackout End or Metric Error End set Activity Log to "Ticket closed by Oracle Enterprise Manager because the associated alert has been cleared." Otherwise set Activity Log to "Ticket updated due to change in severity of the associated alert. Severity: <Severity> Message: <Message>" **For job status events:** If Grace Period is set to "Yes" set Activity Log to "Ticket reopened because the associated job re-triggered with a status of <JobStatus> within the grace period. Message: <Message>" If JobStatusCode is set to 5 (Success) set Activity Log to "Ticket closed by Oracle Enterprise Manager because the associated job has completed successfully." Otherwise set Activity Log to "Ticket updated due to change in job status of <JobStatus>. Message: <Message>"

Table 5–3 shows Service Desk ticket attributes and corresponding Enterprise Manager alert attributes and values for *CASD_Default_Incident.xsl* mappings.

Table 5–3 Ticket Updates (CASD_Default_Incident.xsl Mappings)

Service Desk Ticket Attributes	Enterprise Manager Alert Attributes	Value
Identifier	TicketID - Extracts only the internal identifier from the ticket id	N/A
Summary	Message	N/A

Table 5–3 (Cont.) Ticket Updates (CASD_Default_Incident.xsl Mappings)

Service Desk Ticket Attributes	Enterprise Manager Alert Attributes	Value
Priority	Severity - Applies to metric alerts JobStatus - Applies to job status events	**For metric alerts:** ■ If severity is Critical, Unreachable Start or Agent Unreachable Start set Priority to Medium (3). ■ Otherwise, set Impact to Low (5). **For job status events:** ■ If the JobStatus is Initialization Error, Failed, or Failed and Retried set Priority to High(1). ■ If the JobStatus is Skipped set Priority to Medium-High(2). ■ If the JobStatus is Scheduled, Running, or Queued set Priority to Low(1). ■ If the JobStatus is Success set Priority to None. ■ Otherwise, set Priority to Medium-Low(2).
Status	**For metric alerts:** Grace Period **For job status events:** Grace Period	**For metric alerts:** If Grace Period is set to "Yes" set Status to Open (OP). Otherwise do not set Status. **For job status events:** If Grace Period is set to "Yes" set Status to Open (OP). Otherwise do not set Status

Table 5–3 (Cont.) Ticket Updates (CASD_Default_Incident.xsl Mappings)

Service Desk Ticket Attributes	Enterprise Manager Alert Attributes	Value
Activity Log	**For metric alerts:**	**For metric alerts:**
	Grace Period	If Grace Period is set to "Yes" set Activity Log to "Ticket reopened because the associated alert re-triggered at <Severity> severity within the grace period. Message: <Message>"
	Severity	
	Message	
	For job status events:	Otherwise set Activity Log to "Ticket updated due to change in severity of the associated alert. Severity: <Severity> Message: <Message>"
	Grace Period	
	JobStatus	**For job status events:**
	Message	If Grace Period is set to "Yes" set Activity Log to "Ticket reopened because the associated job re-triggered with a status of <JobStatus> within the grace period. Message: <Message>"
		Otherwise set Activity Log to "Ticket updated due to change in job status of <JobStatus>. Message: <Message>"

Use the mapping tables (Table 5–1 and Table 5–2) as a reference to read the XSLT file in Example 5–1.

Example 5–1 CASD_Default_Incident_AutoClose.xsl Source Code with Annotations

```
<?xml version='1.0' encoding='UTF-8'?>
<xsl:stylesheet version="1.0"
              xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
              xmlns:ns0="http://xmlns.oracle.com/sysman/connector/tt">

  <!--
  This template creates an incident type ticket within CA Service Desk with
default settings.
  On update, the ticket summary is updated with the latest event message and
priority
  information as an activity log entry.
  -->

  <xsl:template match="ns0:EventModel">
    <xsl:choose>
      <xsl:when test="normalize-space(ns0:TicketId) = ''">
        <!-- EDIT THE TAG VALUES BELOW TO CHANGE HOW A CASD INCIDENT IS FILLED
DURING INCIDENT CREATION -->
        <iwaveaf:create
xmlns:iwaveaf="http://iwavesoftware.com/services/adapter-framework">
          <incident>
            <xsl:choose>
              <xsl:when test="ns0:EventType = 'Alert'">
                <!-- Set the CASD Incident Priority-->
                <!--     Possible values for priority: -->
                <!--       1 = High                     -->
```

```
                <!--       2 = Medium-High             -->
                <!--       3 = Medium                  -->
                <!--       4 = Medium-Low              -->
                <!--       5 = Low                     -->
                <!--       None                        -->
                <xsl:choose>
                  <!--  EM Critical -->
                  <xsl:when test="ns0:SeverityCode = '25'">
                    <priority>3</priority> <!-- CASD Medium -->
                  </xsl:when>
                  <!--  EM Warning-->
                  <xsl:when test="ns0:SeverityCode = '20'">
                    <priority>5</priority>  <!-- CASD Low -->
                  </xsl:when>
                  <!--  Unreachable Start -->
                  <xsl:when test="ns0:Severity = 'Unreachable Start'">
                    <priority>3</priority> <!-- CASD Medium -->
                  </xsl:when>
                  <!--  Agent Unreachable Start -->
                  <xsl:when test="ns0:Severity = 'Agent Unreachable Start'">
                    <priority>3</priority> <!-- CASD Medium -->
                  </xsl:when>
                  <!--  Blackout Start -->
                  <xsl:when test="ns0:Severity = 'Blackout Start'">
                    <priority>5</priority>  <!-- CASD Low -->
                  </xsl:when>
                  <!--  Metric Error Start-->
                  <xsl:when test="ns0:Severity = 'Metric Error Start'">
                    <priority>5</priority>  <!-- CASD Low -->
                  </xsl:when>
                </xsl:choose>

                <!-- Set the CASD Incident Description -->
                <description>
Ticket created by EM CASD Connector.
-------------------------------------
EM User: <xsl:value-of select="ns0:EMUser"/>
Alert Information:
  Target Type: <xsl:value-of select="ns0:TargetType"/>
  Target Name: <xsl:value-of select="ns0:TargetName"/>
  Metric Column: <xsl:value-of select="ns0:MetricColumn"/>
  Metric Name: <xsl:value-of select="ns0:MetricName"/>
                  <!-- LIST ALL THE TARGET PROPERTIES -->
                  <xsl:for-each select="ns0:TargetProperties">
                  <xsl:text>&#xa;        </xsl:text>
                  <xsl:value-of select="./ns0:name"/>: <xsl:value-of
select="./ns0:value"/>
                  </xsl:for-each>
                  <!-- EDIT THE FOLLOWING CODE TO LIST A SPECIFIC TARGET PROPERTY,
                       SUCH AS "Line of Business"

                  <xsl:choose>
                  <xsl:when test="ns0:TargetProperties/ns0:name='Line of
Business'">
                  Line of Business: <xsl:value-of
select="ns0:TargetProperties/ns0:value"/>
                  </xsl:when>
                  </xsl:choose>

                  -->
```

```
                  <xsl:choose>
                    <xsl:when test="normalize-space(ns0:KeyColumn) != ''">
  Key Column: <xsl:value-of select="ns0:KeyColumn"/>
  Key Values: <xsl:value-of select="ns0:KeyValues"/>
                    </xsl:when>
                  </xsl:choose>
  Severity: <xsl:value-of select="ns0:Severity"/>
  Collection Time: <xsl:value-of select="translate(ns0:CollectionTime, 'T', '
')"/>
  Target Host: <xsl:value-of select="ns0:TargetHost"/>
                  <xsl:choose>
                    <xsl:when test="normalize-space(ns0:NotificationRuleName) !=
''">
  Notification Rule: <xsl:value-of select="ns0:NotificationRuleName"/>
                    </xsl:when>
                  </xsl:choose>
  URL: &lt;a href="<xsl:value-of select="ns0:EventPageURL"/>" target="_
blank"&gt;<xsl:value-of select="ns0:EventPageURL"/>&lt;/a&gt;
                </description>
              </xsl:when>

              <xsl:when test="ns0:EventType = 'JobStatus'">
                <!-- Set the CASD Incident Priority-->
                <!--     Possible values for priority: -->
                <!--       1 = High                    -->
                <!--       2 = Medium-High             -->
                <!--       3 = Medium                  -->
                <!--       4 = Medium-Low              -->
                <!--       5 = Low                     -->
                <!--       None                        -->
                <xsl:choose>
                  <!--  EM Scheduled -->
                  <xsl:when test="ns0:JobStatusCode = '1'">
                    <priority>5</priority> <!-- CASD Low -->
                  </xsl:when>
                  <!--  EM Running -->
                  <xsl:when test="ns0:JobStatusCode = '2'">
                    <priority>5</priority> <!-- CASD Low -->
                  </xsl:when>
                  <!--  EM Initialization Error -->
                  <xsl:when test="ns0:JobStatusCode = '3'">
                    <priority>1</priority> <!-- CASD High -->
                  </xsl:when>
                  <!--  EM Failed -->
                  <xsl:when test="ns0:JobStatusCode = '4'">
                    <priority>1</priority> <!-- CASD High -->
                  </xsl:when>
                  <!--  EM Success -->
                  <xsl:when test="ns0:JobStatusCode = '5'">
                    <priority>None</priority> <!-- CASD None -->
                  </xsl:when>
                  <!--  EM Suspended by User -->
                  <xsl:when test="ns0:JobStatusCode = '6'">
                    <priority>4</priority> <!-- CASD Medium-Low -->
                  </xsl:when>
                  <!--  EM Suspended on Agent Unreachable -->
                  <xsl:when test="ns0:JobStatusCode = '7'">
                    <priority>4</priority> <!-- CASD Medium-Low -->
                  </xsl:when>
                  <!--  EM Stopped -->
```

```
                    <xsl:when test="ns0:JobStatusCode = '8'">
                      <priority>4</priority> <!-- CASD Medium-Low -->
                    </xsl:when>
                    <!--  EM Suspended on Lock -->
                    <xsl:when test="ns0:JobStatusCode = '9'">
                      <priority>4</priority> <!-- CASD Medium-Low -->
                    </xsl:when>
                    <!--  EM Suspended on Event -->
                    <xsl:when test="ns0:JobStatusCode = '10'">
                      <priority>4</priority> <!-- CASD Medium-Low -->
                    </xsl:when>
                    <!--  EM Suspended on Blackout -->
                    <xsl:when test="ns0:JobStatusCode = '11'">
                      <priority>4</priority> <!-- CASD Medium-Low -->
                    </xsl:when>
                    <!--  EM Stop Pending -->
                    <xsl:when test="ns0:JobStatusCode = '12'">
                      <priority>4</priority> <!-- CASD Medium-Low -->
                    </xsl:when>
                    <!--  EM Suspend Pending -->
                    <xsl:when test="ns0:JobStatusCode = '13'">
                      <priority>4</priority> <!-- CASD Medium-Low -->
                    </xsl:when>
                    <!--  EM Inactive -->
                    <xsl:when test="ns0:JobStatusCode = '14'">
                      <priority>4</priority> <!-- CASD Medium-Low -->
                    </xsl:when>
                    <!--  EM Queued -->
                    <xsl:when test="ns0:JobStatusCode = '15'">
                      <priority>5</priority> <!-- CASD Low -->
                    </xsl:when>
                    <!--  EM Failed and Retried -->
                    <xsl:when test="ns0:JobStatusCode = '16'">
                      <priority>1</priority> <!-- CASD High -->
                    </xsl:when>
                    <!--  EM Waiting -->
                    <xsl:when test="ns0:JobStatusCode = '17'">
                      <priority>4</priority> <!-- CASD Medium-Low -->
                    </xsl:when>
                    <!--  EM Skipped -->
                    <xsl:when test="ns0:JobStatusCode = '18'">
                      <priority>2</priority> <!-- CASD Medium-High -->
                    </xsl:when>
                  </xsl:choose>

                  <!-- Set the CASD Incident Description -->
                  <description>
Ticket created by EM CASD Connector.
-------------------------------------
EM User: <xsl:value-of select="ns0:EMUser"/>

Event Information:
  Job Name: <xsl:value-of select="ns0:JobName"/>
  Job Type: <xsl:value-of select="ns0:JobType"/>
  Job Owner: <xsl:value-of select="ns0:JobOwner"/>
  Job Status: <xsl:value-of select="ns0:JobStatus"/>
                  <xsl:choose>
                    <xsl:when test="ns0:JobTarget">
  Job Target: <xsl:for-each select="ns0:JobTarget">
                <xsl:value-of select="./ns0:TargetName"/>(<xsl:value-of
```

```
select="./ns0:TargetType"/>);
              </xsl:for-each>
                    </xsl:when>
                  </xsl:choose>
  Collection Time: <xsl:value-of select="translate(ns0:CollectionTime, 'T', '
')"/>
                  <xsl:choose>
                    <xsl:when test="normalize-space(ns0:NotificationRuleName) !=
''">
  Notification Rule: <xsl:value-of select="ns0:NotificationRuleName"/>
                    </xsl:when>
                  </xsl:choose>
  URL: &lt;a href="<xsl:value-of select="ns0:EventPageURL"/>" target="_
blank"&gt;<xsl:value-of select="ns0:EventPageURL"/>&lt;/a&gt;
               </description>
             </xsl:when>
           </xsl:choose>

           <!-- Set the CASD Incident Reported By -->
           <!-- This field is defaulted to Administrator but can be changed to
any to any valid -->
           <!-- CASD account. A lookup will be performed based on the first,
middle and last names. -->
           <customer>
             <firstName></firstName>
             <middleName></middleName>
             <lastName>Administrator</lastName>
           </customer>

           <!-- Set the CASD Incident Summary -->
           <summary><xsl:value-of select="ns0:Message"/></summary>

           <!-- Add a CASD Activity log entry -->
           <logs>
             <log>
               <xsl:choose>
                 <xsl:when test="ns0:EventType = 'JobStatus'">
               <description>Ticket created by Oracle Enterprise Manager Connector
for CA Service Desk based on a job with a status of <xsl:value-of
select="ns0:JobStatus"/>. Message: <xsl:value-of
select="ns0:Message"/></description>
                 </xsl:when>
                 <xsl:otherwise>
               <description>Ticket created by Oracle Enterprise Manager Connector
for CA Service Desk based on an alert with <xsl:value-of select="ns0:Severity"/>
severity. Message: <xsl:value-of select="ns0:Message"/></description>
                 </xsl:otherwise>
               </xsl:choose>
             </log>
           </logs>

       <!--  UNCOMMENT THE TAGS YOU WISH TO HAVE MODIFIED WHENEVER   -->
       <!--  THE INCIDENT IS CREATED, AND GIVE THEM DESIRED VALUES   -->

           <!-- <status></status> -->
           <!--     Possible values for status: -->
           <!--         ACK (Acknowledged) -->
           <!--         CL (Closed) -->
           <!--         OP (Open) -->
           <!--         WIP (Work In Progress) -->
```

```
                <!--         AVOID (Avoided) -->
                <!--         FIP (Fix in Progress) -->
                <!--         CLREQ (Close Requested) -->
                <!--         KE (Known Error) -->
                <!--         CNCL (Cancelled) -->
                <!--         HOLD (Hold) -->
                <!--         CLUNRSLV (Closed-Unresolved) -->
                <!--         PRBAPP (Problem-Approved) -->
                <!--         PC (Problem-Closed) -->
                <!--         PF (Problem-Fixed) -->
                <!--         PRBANCOMP (Problem-Analysis Complete) -->
                <!--         PO (Problem-Open) -->
                <!--         RSCH (Researching) -->
                <!--         RE (Resolved) -->
                <!--         PRBREJ (Problem-Rejected) -->

                <!-- <impact></impact> -->
                <!--     Possible values for impact: -->
                <!--         1-Entire Organization -->
                <!--         2-Multiple Groups -->
                <!--         3-Single Group -->
                <!--         4-Small Group -->
                <!--         5-One person -->
                <!--         None -->

                <!-- <urgency></urgency> -->
                <!--     Possible values for urgency: -->
                <!--         1-As Possible -->
                <!--         2-Soon -->
                <!--         3-Quickly -->
                <!--         4-Very Quickly -->
                <!--         5-Immediate -->

                <!-- <severity></severity> -->
                <!--     Possible values for severity: -->
                <!--         1-Escalated -->
                <!--         2-Superviser Escal. -->
                <!--         3-Mgr Escal. -->
                <!--         4-HD Mgr Escalation -->
                <!--         5-All Hands Escalation -->

              </incident>
            </iwaveaf:create>
          </xsl:when>
          <xsl:otherwise>
            <iwaveaf:update
xmlns:iwaveaf="http://iwavesoftware.com/services/adapter-framework">
              <incident>
                <identifier><xsl:value-of
select="normalize-space(substring-before(substring-after(ns0:TicketId, '('),
')'))"/></identifier>
                <summary><xsl:value-of select="ns0:Message"/></summary>
                <xsl:choose>
                  <!-- Set the CASD Incident Priority-->
                  <!--     Possible values for priority: -->
                  <!--       1 = High                    -->
                  <!--       2 = Medium-High             -->
                  <!--       3 = Medium                  -->
                  <!--       4 = Medium-Low              -->
                  <!--       5 = Low                     -->
```

```
<!--       None                          -->
<xsl:when test="ns0:EventType = 'Alert'">
  <xsl:choose>
    <!--  EM Critical -->
    <xsl:when test="ns0:SeverityCode = '25'">
      <priority>3</priority> <!-- CASD Medium -->
    </xsl:when>
    <!--  EM Warning-->
    <xsl:when test="ns0:SeverityCode = '20'">
      <priority>5</priority>  <!-- CASD Low -->
    </xsl:when>
    <!--  Unreachable Start -->
    <xsl:when test="ns0:Severity = 'Unreachable Start'">
      <priority>3</priority> <!-- CASD Medium -->
    </xsl:when>
    <!--  Agent Unreachable Start -->
    <xsl:when test="ns0:Severity = 'Agent Unreachable Start'">
      <priority>3</priority> <!-- CASD Medium -->
    </xsl:when>
    <!--  Blackout Start -->
    <xsl:when test="ns0:Severity = 'Blackout Start'">
      <priority>5</priority>  <!-- CASD Low -->
    </xsl:when>
    <!--  Metric Error Start-->
    <xsl:when test="ns0:Severity = 'Metric Error Start'">
      <priority>5</priority>  <!-- CASD Low -->
    </xsl:when>
  </xsl:choose>
</xsl:when>

<xsl:when test="ns0:EventType = 'JobStatus'">
  <xsl:choose>
    <!--  EM Scheduled -->
    <xsl:when test="ns0:JobStatusCode = '1'">
      <priority>5</priority> <!-- CASD Low -->
    </xsl:when>
    <!--  EM Running -->
    <xsl:when test="ns0:JobStatusCode = '2'">
      <priority>5</priority> <!-- CASD Low -->
    </xsl:when>
    <!--  EM Initialization Error -->
    <xsl:when test="ns0:JobStatusCode = '3'">
      <priority>1</priority> <!-- CASD High -->
    </xsl:when>
    <!--  EM Failed -->
    <xsl:when test="ns0:JobStatusCode = '4'">
      <priority>1</priority> <!-- CASD High -->
    </xsl:when>
    <!--  EM Success -->
    <xsl:when test="ns0:JobStatusCode = '5'">
      <priority>None</priority> <!-- CASD None -->
    </xsl:when>
    <!--  EM Suspended by User -->
    <xsl:when test="ns0:JobStatusCode = '6'">
      <priority>4</priority> <!-- CASD Medium-Low -->
    </xsl:when>
    <!--  EM Suspended on Agent Unreachable -->
    <xsl:when test="ns0:JobStatusCode = '7'">
      <priority>4</priority> <!-- CASD Medium-Low -->
    </xsl:when>
```

```
            <!--  EM Stopped -->
            <xsl:when test="ns0:JobStatusCode = '8'">
              <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <!--  EM Suspended on Lock -->
            <xsl:when test="ns0:JobStatusCode = '9'">
              <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <!--  EM Suspended on Event -->
            <xsl:when test="ns0:JobStatusCode = '10'">
              <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <!--  EM Suspended on Blackout -->
            <xsl:when test="ns0:JobStatusCode = '11'">
              <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <!--  EM Stop Pending -->
            <xsl:when test="ns0:JobStatusCode = '12'">
              <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <!--  EM Suspend Pending -->
            <xsl:when test="ns0:JobStatusCode = '13'">
              <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <!--  EM Inactive -->
            <xsl:when test="ns0:JobStatusCode = '14'">
              <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <!--  EM Queued -->
            <xsl:when test="ns0:JobStatusCode = '15'">
              <priority>5</priority> <!-- CASD Low -->
            </xsl:when>
            <!--  EM Failed and Retried -->
            <xsl:when test="ns0:JobStatusCode = '16'">
              <priority>1</priority> <!-- CASD High -->
            </xsl:when>
            <!--  EM Waiting -->
            <xsl:when test="ns0:JobStatusCode = '17'">
              <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <!--  EM Skipped -->
            <xsl:when test="ns0:JobStatusCode = '18'">
              <priority>2</priority> <!-- CASD Medium-High -->
            </xsl:when>
          </xsl:choose>
        </xsl:when>
      </xsl:choose>

  <!--  UNCOMMENT THE TAGS YOU WISH TO HAVE MODIFIED WHENEVER   -->
  <!--  THE INCIDENT IS UPDATED, AND GIVE THEM DESIRED VALUES   -->

      <!-- <status></status> -->
      <!--     Possible values for status: -->
      <!--         ACK (Acknowledged) -->
      <!--         CL (Closed) -->
      <!--         OP (Open) -->
      <!--         WIP (Work In Progress) -->
      <!--         AVOID (Avoided) -->
      <!--         FIP (Fix in Progress) -->
      <!--         CLREQ (Close Requested) -->
```

```
                <!--         KE (Known Error) -->
                <!--         CNCL (Cancelled) -->
                <!--         HOLD (Hold) -->
                <!--         CLUNRSLV (Closed-Unresolved) -->
                <!--         PRBAPP (Problem-Approved) -->
                <!--         PC (Problem-Closed) -->
                <!--         PF (Problem-Fixed) -->
                <!--         PRBANCOMP (Problem-Analysis Complete) -->
                <!--         PO (Problem-Open) -->
                <!--         RSCH (Researching) -->
                <!--         RE (Resolved) -->
                <!--         PRBREJ (Problem-Rejected) -->

                <!-- <impact></impact> -->
                <!--     Possible values for impact: -->
                <!--         1-Entire Organization -->
                <!--         2-Multiple Groups -->
                <!--         3-Single Group -->
                <!--         4-Small Group -->
                <!--         5-One person -->
                <!--         None -->

                <!-- <urgency></urgency> -->
                <!--     Possible values for urgency: -->
                <!--         1-As Possible -->
                <!--         2-Soon -->
                <!--         3-Quickly -->
                <!--         4-Very Quickly -->
                <!--         5-Immediate -->

                <!-- <severity></severity> -->
                <!--     Possible values for severity: -->
                <!--         1-Escalated -->
                <!--         2-Superviser Escal. -->
                <!--         3-Mgr Escal. -->
                <!--         4-HD Mgr Escalation -->
                <!--         5-All Hands Escalation -->

                <!-- <resolution>
                       <resolutionDate></resolutionDate>
                     </resolution> -->
                <!-- Resolution date must be formatted using the ISO 8601 format code.
-->
                <!--     Sample format: 2009-11-24T09:57:01Z -->
                <!--     Sample format: 2009-11-24T03:57:01-06:00 -->

                <xsl:choose>
                  <!-- Handle update caused by Alert Status change -->
                  <xsl:when test="ns0:EventType = 'Alert'">
                    <xsl:choose>
                      <xsl:when test="ns0:GracePeriodCheckMade = 'Yes'">
                        <!-- Set the CASD Incident Status back to Open -->
                        <status>OP</status>

                        <!-- Add a CASD Activity log entry -->
                        <logs>
                          <log>
                            <description>Ticket reopened because the associated alert
re-triggered at <xsl:value-of select="ns0:Severity"/> severity within the grace
period. Message: <xsl:value-of select="ns0:Message"/></description>
```

```
                    </log>
                  </logs>
                </xsl:when>

                <!-- Close the incident if the EM Severity is set to one of the
following. -->
                <!--     Clear -->
                <!--     Unreachable Clear -->
                <!--     Agent Unreachable Clear -->
                <!--     Blackout End -->
                <!--     Metric Error Clear -->
                <xsl:when test="ns0:SeverityCode = '15'
                  or ns0:Severity = 'Unreachable Clear'
                  or ns0:Severity = 'Agent Unreachable Clear'
                  or ns0:Severity = 'Blackout End'
                  or ns0:Severity = 'Metric Error End'">
                  <!-- Set the CASD Incident Status to Closed -->
                  <status>CL</status>

                  <!-- Add a CASD Activity log entry -->
                  <logs>
                    <log>
                      <description>Ticket closed by Oracle Enterprise Manager
because the associated alert has been cleared.</description>
                    </log>
                  </logs>
                </xsl:when>

                <xsl:otherwise>
                  <!-- Add activity log entry with a standard update message
since this is not a reopen.-->
                  <logs>
                    <log>
                      <description>Ticket updated due to change in severity of
the associated alert. Severity:  <xsl:value-of select="ns0:Severity"/>  Message:
<xsl:value-of select="ns0:Message"/></description>
                    </log>
                  </logs>
                </xsl:otherwise>
              </xsl:choose>
            </xsl:when>

            <!-- Handle update caused by Job Status change -->
            <xsl:when test="ns0:EventType = 'JobStatus'">
              <xsl:choose>
                <xsl:when test="ns0:GracePeriodCheckMade = 'Yes'">
                  <!-- Set the CASD Incident Status back to Open -->
                  <status>OP</status>

                  <!-- Add a CASD Activity log entry -->
                  <logs>
                    <log>
                      <description>Ticket reopened because the associated job
re-triggered with a status of <xsl:value-of select="ns0:JobStatus"/> within the
grace period. Message: <xsl:value-of select="ns0:Message"/></description>
                    </log>
                  </logs>
                </xsl:when>

                <!-- Close the incident if the job succeeded -->
```

```
                    <xsl:when test="ns0:JobStatusCode = '5'">
                      <!-- Set the CASD Incident Status to Closed -->
                      <status>CL</status>

                      <!-- Add a CASD Activity log entry -->
                      <logs>
                        <log>
                          <description>Ticket closed by Oracle Enterprise Manager
because the associated job has completed successfully.</description>
                        </log>
                      </logs>
                    </xsl:when>

                    <xsl:otherwise>
                      <!-- Add activity log entry with a standard update message
since this is not a reopen.-->
                      <logs>
                        <log>
                          <description>Ticket updated due to change in job status of
<xsl:value-of select="ns0:JobStatus"/>.  Message:  <xsl:value-of
select="ns0:Message"/></description>
                        </log>
                      </logs>
                    </xsl:otherwise>
                  </xsl:choose>
                </xsl:when>
              </xsl:choose>
            </incident>
          </iwaveaf:update>
        </xsl:otherwise>
      </xsl:choose>
    </xsl:template>
</xsl:stylesheet>
```

5.3 Customizing Ticket Templates

If the out-of-box ticket templates do not satisfy your requirements, you can modify them. To do this, Oracle recommends that you use one of the existing templates as the base template. Copy this ticket template to a new file, modify, and register the new ticket template.

In most cases, when you modify the ticket template, you might only be changing the mappings. The following examples illustrate this point:

Example 5-2: Creating a Template to set the Urgency Element

By default the Urgency field is not set whenever an incident is created in Service Desk. Both out-of-box templates have an urgency element commented out that can be used to set the urgency field. To create a template to set the Urgency to Soon, copy one of the default templates to a new file. Edit the new file and uncomment the urgency element in the template setting the contents to *2-Soon* as shown below. Register the new ticket template. The template is now ready to use in notification rules or as a template for manual ticket creation.

```
<urgency>2-Soon</urgency>
```

Example 5-3: Altering the Message Type

If you only want the alert message to appear as ticket summary instead of both message and severity, copy one of the default templates to a new file, modify the following attribute and register.

```
<summary><xsl:value-of select="ns0:Message"/></summary>
```

The templates are highly customizable. Oracle recommends that only users with advanced knowledge of XSLT make complex changes.

You can use notification rules as a filter to associate proper ticket templates with alerts. You can have as many tickets templates as you want. One notification rule can have only one ticket template.

6

Troubleshooting the Connector

This chapter provides information to assist you in troubleshooting integration issues with the CA Service Desk Connector. The connector will not work unless the appropriate components have been installed and configured. Before you start the troubleshooting steps, you must insure that you have done the following:

1. Install and test the CASD Adapter as specified in Section 2.2, "Installing the Adapter".
2. Install the CA Service Desk Connector as specified in Section 2.3, "Installing the Connector".
3. Configure the CA Service Desk Connector as specified in Section 3.1, "Configuring the Connector".
4. Set up one or more notification rules as specified step 4 of Section 4.1, "Automatically Creating a Ticket".

If all the actions above have been completed and the connector is not working, perform the following steps to diagnose the problem.

1. Verify that the CASD Adapter has been successfully started and the WSDL for the CASD Adapter can be accessed from the machine where the CASD Adapter is installed. Performing the following steps to do this:
   a. Refer to "Using the Correct URL for CASD Adapter Operations" in Appendix A to see the first five steps to use to complete this procedure.

      Note: If the adapter does not successfully complete the startup, see Section 6.1, "Troubleshooting Adapter Startup Errors" to diagnose the problem.

   b. Open a browser and paste the URL from the *framework.log* file in the address window. Append *?WSDL* to the end of the URL and attempt to load the URL.
   c. The WSDL should be loaded if the Adapter is operational.

      Note: A WSDL is an XML file that describes the web service.

2. Verify that the WSDL for the CASD Adapter can be accessed from the machine where the Enterprise Manager server is installed.
   a. Open a browser at the Enterprise Manager server and copy the URL from step 1-b above to the address window. The hostname for the URL will be *localhost*. Change localhost to the actual hostname or IP address of the machine where

the CASD Adapter is installed. If you specify a hostname, you must make sure that the hostname is recognized at the Enterprise Manager server machine. This can be done using the ping command.

For example, if the CASD Adapter is installed on the server with a hostname of *SDServer01* and the URL listed in *framework.log* is:

http://localhost:8082/services/causd/IncidentService

The URL used at the Enterprise Manager server machine would be:

http://SDServer01:8082/services/causd/IncidentService

b. Attempt to load the WSDL by appending *?WSDL* at the end of the URL. If the WSDL cannot be loaded, either the hostname is not recognized at the Enterprise Manager machine or there is a connectivity issue between the two machines. If you specified a hostname, try using the IP address instead of the hostname in the URL. If it still will not load, you have a connectivity problem. You will need to consult with your IT department to resolve this issue.

3. Verify that the CA Service Desk Connector specifies the correct URL for the createTicket, getTicket, and updateTicket operations. Determine the URL being used by the CASD Adapter as specified in "Using the Correct URL for CASD Adapter Operations" in Appendix A.

   a. Log into the Oracle Enterprise Manager console by entering a user name with a Super Administrator role, entering the appropriate password, then clicking **Login**.

   b. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.

   c. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.

   d. Click on the **Configure** icon associated with the CA Service Desk Connector. This invokes edit mode, enabling you to configure the connector.

   e. Verify that the URL identified in step 2-b is specified for all three operations (createTicket, getTicket, and updateTicket). If any of the operations are incorrect, change to the correct URL.

   Note: Do not append the WSDL to the end of the URL that is specified here.

   ---

   f. Enter a valid ticket number in the Ticket Number field and click **OK**.

   g. You will see the message *Connection test succeeded* if everything is set up correctly.

4. If there is an error in step 3-g, there is likely a configuration error in the CASD Adapter. See the section entitled Section 6.3, "Troubleshooting Adapter Operations Errors" for information on diagnosing errors.

6.1 Troubleshooting Adapter Startup Errors

To identify the cause of a startup failure, navigate to the *adapters/log* directory in the CASD Adapter install directory and open the *framework.log* file in a text editor. Search for *Exception* to find any errors in the file. If the file does not exist, it indicates that

there is a problem locating or executing the JVM. See Section 6.2, "JVM Errors" for information about resolving JVM issues.

Listed below are some possible Exceptions, an explanation of the root cause, and a description of the solution.

java.net.BindException: Address already in use: bind

This error indicates that the adapter could not start because of a port conflict. There are two possible causes for this error.

1. Another application is using a port that the Adapter is configured to use. If the adapter is configured to use SSL, the port number is 8443. If it is not configured to use SSL, the port number is 8082.

   There are two possible solutions to this. You can change the other application to use a different port or you can change the CASD Adapter to use a different port. To change the Adapter to use a different port, see "Changing the Default Adapter Port" in Appendix A.

2. There is an instance of the Adapter already running. If this is the case then there is no change required. You should only run one instance of the Adapter at a time.

org.springframework.beans.factory.BeanInitializationException: Could not load properties; nested exception is java.io.FileNotFoundException: … framework.properties (Permission denied)

This error indicates that the adapter could not start because the permissions on the *framework.properties* file in the *conf* directory were not set correctly.

To solve the problem, change the permissions to give the account or group under which the CASD Adapter runs read and execute permissions.

For any other startup errors, consult with Oracle Support.

6.2 JVM Errors

The CASD Adapter requires version 1.6 of the JVM. If there are multiple versions of the JVM installed on the machine, it is possible that an older version of the JVM is being executed whenever the adapter starts.

On UNIX systems, the *JAVA_HOME* environment variable must be set to the directory where Java 1.6 is installed in the shell where the adapter is started. To properly start the adapter on a UNIX platform, perform the following:

- Set the *JAVA_HOME* environment variable to the Java 1.6 install directory.
- Navigate to the *adapters/bin* subdirectory in the Adapter install directory.
- Execute the `./service.sh start` command.

On Windows systems, perform the following to insure that Java 1.6 is used when starting the adapter.

- Navigate to the *adapters/bin* subdirectory in the Adapter install directory.
- Run the *iWaveAdaptersw.exe* executable.
- Click on the *Java* tab.
- Make sure that the *Use Default* check box is not checked.
- In the Java Virtual Machine box, specify the path to the *jvm.dll* file in the Java 1.6 install directory.

- Click on the **OK** button.

6.3 Troubleshooting Adapter Operations Errors

In order to troubleshoot integration issues, you must modify the Oracle Enterprise Manager logging options to capture additional debug information. Perform the steps specified in the section entitled "Enabling Debug in Enterprise Manager" in Appendix A to enable debugging.

Perform the following diagnostic steps if tickets are not being generated or updated as expected in CA Service Desk.

1. Verify that the metric/job that was triggered is referenced in a notification rule that specifies one of the CA Service Desk Ticketing Templates.
2. Determine the error that Oracle Enterprise Manager has reported.
   a. To do this you need to examine the log file for errors. Perform the following steps to locate errors in the log file:

      1.) Open the *emoms.trc* file in a text editor. The file is located in this directory:

      <ORACLE_HOME>/oms10g/sysman/log

      2.) Go to the bottom of the file and search backwards for the appropriate string based on the operation that failed:

      ```
      If the getTicket operation failed, search for "ERROR
      ticketTicketConnectorConfigData".

      If the createTicket or updateTicket operation failed, search for "ERROR
      svc.TTCServiceImpl".
      ```

      The error information is contained on the same line where the search string is found or on the next line.
3. Diagnose the problem based on the error event. See Section 6.4, "Errors to Check" for information on troubleshooting common error events.

6.4 Errors to Check

This section provides cause and solution information on troubleshooting common errors reported by Enterprise Manager. Find the heading that matches your error and follow the instructions for diagnosing and correcting the problem.

javax.net.ssl.SSLException: SSL handshake failed: X509CertChainInvalidErr

Cause : The SSL handshake between the Oracle Enterprise Manager Connector Framework and the CASD Adapter failed. This failure occurs because Oracle Enterprise Manager is not configured correctly with the SSL certificate for the CASD Adapter. The SSL certificate the CASD Adapter uses must be imported into the wallet manager. The certificate is either missing from the wallet or does not match the SSL certificate provided by the CASD Adapter.

Solution : Import the SSL certificate from the CASD Adapter into the wallet manager. See Section 2.7, "Adding Signed Certificates to Wallet Manager" for details on setting up Oracle Enterprise Manager with the CASD Adapter SSL certificate.

The wallet "/gc/OracleHomes/oms10g/sysman/connector//certdb.txt" does not exist

Cause : The CASD Adapter is configured to use SSL, but the *certdb.txt* file that contains the SSL information is missing.

Solution : Import the SSL certificate from the CASD Adapter into the wallet manager. See Section 2.7, "Adding Signed Certificates to Wallet Manager" for details on setting up Oracle Enterprise Manager with the CASD Adapter SSL certificate.

Error opening socket: java.net.ConnectException: Connection refused

Cause : The CASD Adapter is down.

Solution : Perform the following steps to check the status of the adapter and start it if necessary.

If the CASD Adapter is installed on a Unix system:

1. Open a command terminal on the system where the CASD Adapter is installed.
2. Change the working directory to the *adapters/bin* directory in the CASD Adapter installation directory.
3. Enter the following command:

   ```
   ./service.sh status
   ```

4. If the command indicates that the service is not running, enter the following command:

   ```
   ./service.sh start
   ```

If the CASD Adapter is installed on a Windows system:

1. Open a command terminal on the system where the CASD Adapter is installed.
2. Change the working directory to the *adapters/log* directory in the CASD Adapter installation directory.
3. Open the *framework.log* file in a text editor.
4. Go to the bottom of the file and search backwards for the string *iWave Adapter Framework*. If the last occurrence found is *iWave Adapter Framework Started*, this indicates that the web service is started.
5. If the web service is not started, start the web service based on how the web service is installed.
   - If it is installed as a standalone application, change the working directory to the *adapters/bin* directory and run the *startAdapters.bat* command file.
   - If it is installed as a Windows service, enter the *net start iWaveAdapters* command.

Error opening socket: java.net.UnknownHostException:

Cause : The system does not recognize the host name specified in the URL.

Solution : You can use the following options to address this issue:

- Coordinate with the system administrator to change the system configuration to recognize the host name.
- Specify the IP address in the URL instead of the host name. To do this, perform the following steps:
  1. Determine the IP address of the system where the CASD Adapter is installed.

2. Log in to the Oracle Enterprise Manager console by entering a user name with a Super Administrator role, entering the appropriate password, then clicking **Login**.
3. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
4. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
5. Click on the **Configure** icon associated with the MICROSOFT CA Service Desk Connector. This invokes edit mode, enabling you to configure the connector.
6. Change the host name to the IP address in the URL specified for the createEvent and updateEvent operations.
7. Click **OK**.

Error opening socket: java.net.NoRouteToHostException: No route to host

Cause : The IP address or port number specified in the URL is invalid, or the network is down.

Solution : Verify that the hostname/IP address configured for the connector is correct:

1. Log in to the Oracle Enterprise Manager console by entering a user name with a Super Administrator role, entering the appropriate password, then click **Login**.
2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the CA Service Desk Connector. This invokes edit mode, enabling you to configure the connector.
5. Verify that the hostname/IP address and port number specified in the URL for the createEvent and updateEvent operations are correct.
6. If the hostname/IP address and port number are incorrect, provide the correct values and click **OK**.

If the URLs specify a host name, be sure that the host name resolves to the correct IP address. To determine the IP address of the host name, issue the *ping <hostname>* command, where *<hostname>* is the actual host name. This lists the IP address that was resolved for the host name. If this is incorrect, the system administrator needs to investigate why it is incorrect.

If the ping fails, the system administrator needs to investigate why there is no connectivity.

SOAPException: faultCode=SOAP-ENV:Protocol; msg=Unsupported response content type "text/html;

Cause : The web service received the request and rejected it because there was a problem. This likely indicates that an invalid path was specified in the URL.

Solution : To determine the reason for the failure, examine the HTML document listed with the Exception information in the *emoms.trc* log file. In the HTML document, it provides error information that indicates the reason why it was rejected. The error information may be difficult to spot because the HTML tag delimiters are encoded.

If the error information specifies *HTTP Error: 404*, this indicates that the path in the URL is incorrect. Perform the following steps to test the URL the connector is using.

1. Log in to the Oracle Enterprise Manager console by entering a user name with a Super Administrator role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the CA Service Desk Connector.
5. Click the **General** tab.
6. Select and copy the URL specified for the createEvent operation.
7. Open an internet browser on the system where the Oracle Enterprise Manager server is installed.
8. In the address window, enter the URL that was copied in step 6 above. Add *?wsdl* to the end of the URL. The URL should appear similar to the following example:

   http://[Hostname]:8082/services/causd/IncidentService?wsdl

   [Hostname] is the actual host name or IP address where the CASD Adapter is installed.

If the WSDL is loaded, this confirms that the URL is correct. If it fails to load, there is a problem with the URL. Perform the steps specified in the section entitled "Using the Correct URL for CASD Adapter Operations" in Appendix A to configure the connector to use the correct URL.

Error occurred while calling Web Service: - or - java.lang.Exception: Error occurred while calling Web Service:

The CASD Adapter returned a SOAP fault. To determine root cause of the SOAP fault, you must examine the contents of the soapfault element following the error message. Listed below are some of the possible errors listed in the soapfault element. Find the error listed below contained in your soapfault message for a description of possible causes/solutions.

javax.xml.ws.soap.SOAPFaultException: Could not send Message.

Cause : The CASD Adapter could not connect to the CA Service Desk Server for one of the following reasons:

- The hostname/IP address specified for the CA Service Desk Server is incorrect
- The port number specified for the CA Service Desk Server is incorrect
- The CA Service Desk Server is down

Solution : Perform the following steps to determine and correct the root cause of the problem:

1. Verify that the CA Service Desk Server is up. If it is not up, start the server.
2. Verify that hostname/IP address and the port number configured for the CA Service Desk Server are correct. Perform the following steps to determine the hostname/IP address and port number configured for the CA Service Desk Server:

- Navigate to the *adapters/conf* directory in the CASD Adapter install directory.
- Make a backup copy of the *framework.properties* file.
- Open the *framework.properties* file in a text editor.

- Search for the *causd.webservice.endpoint.r11* property. This is the URL that is used to connect to the CA Service Desk Server.
- The hostname/IP address and port number should be specified in the URL.
- Verify that the information is correct. If it is not correct, change the incorrect information and save the file.
- If the *framework.properties* file was modified, the CASD Adapter must be restarted to pick up the configuration change.

Error - invalid login name

Cause : The web service could not access the CA Service Desk Server because the user name specified for the CAUSD account is incorrect.

Solution : Perform the following steps to change the user name for accessing the CA Service Desk Server.

1. Navigate to the *adapters/conf* directory in the CASD Adapter install directory.
2. Make a backup copy of the *framework.properties* file.
3. Enter the following command to change the user name where <*username*> is the new user name to specify:

   ```
   ..\bin\propertiesEditor.bat -e causd.username=<username>
   framework.properties
   ```

   The *propertiesEditor.bat* script is specifically for the Windows platform. The equivalent script for Unix platforms is *propertiesEditor.sh*.
4. Restart the CASD Adapter.

Error - invalid login password

Cause : The web service could not access the CA Service Desk Server because the password specified for the CAUSD account is incorrect.

Solution : Perform the following steps to change the password for accessing the CA Service Desk Server.

1. Navigate to the *adapters/conf* directory in the CASD Adapter install directory.
2. Make a backup copy of the *framework.properties* file.
3. Enter the following commands to change the user name and password information where <*username*> is the new user name to specify:

   ```
   ..\bin\propertiesEditor.bat -e causd.username=<username>
   framework.properties
   ```

   The *propertiesEditor.bat* script is specifically for the Windows platform. The equivalent script for Unix platforms is *propertiesEditor.sh*.
4. Enter the following command to change the password where <*password*> is the new password to specify:

   ```
   ..\bin\propertiesEditor.bat -e causd.password=<password>
   framework.properties
   ```
5. Restart the CASD Adapter.

Error - Login service failed

Cause : The web service could not access the CA Service Desk Server because the account specified does not have sufficient permissions.

Solution : There are 2 options to correct this problem. One option is to change the account permissions in CA Service Desk to allow the account to create/update incidents. The other option is to specify a different account that has the appropriate permissions. Perform the following steps to change the account for accessing the CA Service Desk Server.

1. Navigate to the *adapters/conf* directory in the CASD Adapter install directory.
2. Make a backup copy of the *framework.properties* file.
3. Enter the following command to change the password where <*username*> is the new user name to specify:

   ```
   ..\bin\propertiesEditor.bat -e causd.username=<username>
   framework.properties
   ```

   The *propertiesEditor.bat* script is specifically for the Windows platform. The equivalent script for Unix platforms is *propertiesEditor.sh*.
4. Restart the CASD Adapter.

A

Connector Tips

This section provides various tips that might help you to use CA Service Desk Connector more effectively.

Recommended Protocol

Oracle recommends that you use HTTPS as the protocol for the communication between Enterprise Manager and the CASD Adapter. Use HTTP only if a secure connection is not required and the data can be transferred in clear text between the two systems.

Supported Alerts

This release supports the following types of alerts:

- Metric alerts
- Availability alerts

Enabling Debug in Enterprise Manager

To enable debug logging information:

1. Edit the *emomslogging.properties* file using a text editor. The file is located in the following directory where <*ORACLE_HOME*> is the Oracle installation directory:

   <*ORACLE_HOME*>*/oms10g/sysman/config*

2. Set the parameters as follows:

   ```
   log4j.appender.emlogAppender.Threshold = DEBUG
   log4j.rootCategory=DEBUG,emlogAppender,emtrcAppender
   ```

3. After setting the debug logging parameters, restart the OMS by opening a command window, changing the working directory to <*ORACLE_HOME*>*/oms10g/bin*, and issuing the following commands:

   ```
   emctl stop oms
   ```

   ```
   emctl start oms
   ```

Changing the Default Adapter Port

In most cases, you can use the default port numbers that the CASD Adapter uses. However, if there are any conflicts with existing applications, you need to change the port numbers.

8082 is the default port number for HTTP communication, and 8443 is the default port for HTTPS communication. To change the port number, perform the following steps on the system where the CASD Adapter is installed. Replace the <*dir*> in this example with the directory where the adapter is installed.

1. Open a command prompt window and change the working directory to:

   <dir>/adapters/conf

2. Make a backup copy of the *framework.properties* file.

3. Enter the following commands to configure the adapter to use a different port where <*prot*> is the protocol (HTTP or HTTPS) and <*newPort*> is the new port number:

   ```
   ..\bin\propertiesEditor.bat -p
   services.url=<prot>://localhost:<newPort>/services
   framework.properties
   ```

   ```
   ..\bin\propertiesEditor.bat -p
   notification.url=<prot>://localhost:<newPort>/services/notifi
   cation framework.properties
   ```

   ```
   ..\bin\propertiesEditor.bat -p
   acquisitionevent.url=<prot>://localhost:<newPort>/services/ac
   quisition-event framework.properties
   ```

   The *propertiesEditor.bat* script is specifically for the Windows platform. The equivalent script for Unix platforms is *propertiesEditor.sh*.

4. If the protocol being used is HTTPS, additional changes are required. Perform the following steps to complete the additional requirements.

   - Copy the *framework.xml* file from the <*dir*>*/adapters/endpoints/ca-usd* directory to the <*dir*>*/adapters/conf* directory.
   - Open the *framework.xml* file in the *adapters/conf* directory with a text editor.
   - Change port 8443 to the new port number and save the file.

5. Change the working directory to *../bin*.

6. Enter the following command to restart the CASD Adapter.

   - If the web service is installed on a Unix system:

     ```
     ./service.sh restart
     ```

   - If the web service is installed on a Windows system as a standalone application, close the window where the adapter was running, then run:

     ```
     startAdapters.bat
     ```

   - If the web service is installed on a Windows system as a Windows service, enter the following commands:

     ```
     net stop iWaveAdapters
     ```

     ```
     net start iWaveAdapters
     ```

Perform the following steps to change the URL the CA Service Desk connector is using:

1. Log in to the Oracle Enterprise Manager console by entering a user name with a Super Administrator role, entering the appropriate password, then clicking **Login**.

2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the CA Service Desk Connector. This invokes edit mode, enabling you to configure the connector.
5. Change the URLs listed in the Web Service End Points section to use the new port number.
6. Click **OK** to save your changes.

Using the Correct URL for CASD Adapter Operations

Perform the following steps to identify and configure the connector to use the correct URL for CASD Adapter operations.

1. Open a command terminal on the system where the CASD Adapter is installed.
2. Change the working directory to the *adapters/log* directory in the CASD Adapter installation directory.
3. Open the *framework.log* file in a text editor.
4. Go to the bottom of the file and search backwards for the string *iWave Adapter Framework Started*. This indicates that the adapter was successfully started.

> **Note:** If the string is not in the file, the log file might have exceeded the maximum size and rolled over. Restart the adapter and wait for it to complete the startup process. The adapter adds a line that contains *iWave Adapter Framework Started* when it has successfully started.

5. Go to the bottom of the *framework.log* file and search backwards for the string *Setting the server's publish address to be*. Continue searching backwards until the URL that contains */IncidentService* is found. This is the URL that should be specified when configuring the connector for the createTicket, getTicket, and updateTicket operations.

B

Third-Party Product License Information

This section includes third-party license information for certain third-party products that are part of CA Service Desk Connector, Release 1.0.5.1.0. Oracle acknowledges that the following third-party proprietary and open source software are used in the provided programs covered by this documentation.

JDOM 1.0

"Copyright (©) 2000-2004 Jason Hunter & Brett McLaughlin. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution. 3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact . 4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management . In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos . THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter and Brett McLaughlin . For more information on the JDOM Project, please see http://www.jdom.org/."

AspectJ 1.6.1

Information:

1. The follow files are available in source code form under the Eclipse Public License at: http://www.eclipse.org/aspectj/downloads.php. (The EPL license is reproduced below).
2. All past Contributors to the AspectJ disclaim all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose. In addition, such Contributors are not liable for any damages, including direct, indirect, special, incidental and consequential damages, such as lost profits.
3. Any provisions of the Oracle license agreement that differ from the Eclipse Public License are offered by Oracle alone and not by any other party.

Eclipse Public License - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

   "Contribution" means:

   a. in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b. in the case of each subsequent Contributor:

      i. changes to the Program, and

      ii. additions to the Program;

      where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

   a. Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform,

distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b. Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c. Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d. Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a. it complies with the terms and conditions of this Agreement; and

b. its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a. it must be made available under this Agreement; and

b. a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

   Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

   For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

   EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement , including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

   EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR

DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. The Eclipse Foundation is the initial Agreement Steward. The Eclipse Foundation may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

Spring Framework 2.5.6

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive,

no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   a. You must give any other recipients of the Work or Derivative Works a copy of this License; and

   b. You must cause any modified files to carry prominent notices stating that You changed the files; and

   c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on

an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability. END OF TERMS AND CONDITIONS APPENDIX: How to apply the Apache License to your work. To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives. Copyright [yyyy] [name of copyright owner] Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at Link2 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

CXF Web Stack 2.2.3

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Jetty Web Service Hosting 6.1.19

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Quartz Scheduler 1.6

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Apache Commons DBCP 1.2.2

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Apache Commons Configuration 1.5

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Jakarta Commons HTTP Client 3.1

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Apache Commons Collection 3.2

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Apache Derby Database 10.4.2

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Log4j 1.2.14

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Groovy 1.6.4

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

Apache Axis 1.4

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

JDOM 1.0

See the Apache License, Version 2.0 under Spring Framework 2.5.6.

LibXML2

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: * * 1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer. * * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in * the documentation and/or other materials provided with the * distribution. * * 3. All advertising materials mentioning features or use of this * software must display the following acknowledgment: * "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (Link1 /)" * * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to * endorse or promote products derived from this software without * prior written permission. For written permission, please contact * openssl-core@openssl.org. * * 5. Products derived from this software may not be called "OpenSSL" * nor may "OpenSSL" appear in their names without prior written * permission of the OpenSSL Project. * * 6. Redistributions of any form whatsoever must retain the following * acknowledgment: * "This product includes software developed by the OpenSSL Project * for use in the OpenSSL Toolkit (Link2 /)" * * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED * OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young * (eay@cryptsoft.com). This product includes software written by Tim * Hudson (tjh@cryptsoft.com). * */ Original SSLeay License ----------------------- /* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) * All rights reserved. * * This package is an SSL implementation written * by Eric Young (eay@cryptsoft.com). * The implementation was written so as to conform with Netscapes SSL. * * This library is free for commercial and non-commercial use as long as * the following conditions are aheared to. The following conditions * apply to all code found in this distribution, be it the RC4, RSA, * lhash, DES, etc., code; not just the SSL code. The SSL documentation * included with this distribution is covered by the same copyright terms * except that the holder is Tim Hudson (tjh@cryptsoft.com). * * Copyright remains Eric Young's, and as such any Copyright notices in * the code are not to be removed. * If this package is used in a product, Eric Young should be given attribution * as the author of the parts of the library used. * This can be in the form of a textual message at program startup or * in documentation (online or textual) provided with the package. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: * 1. Redistributions of source code must retain the copyright * notice, this list of conditions and the following disclaimer. * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in the * documentation and/or other materials provided with the distribution. * 3. All advertising materials mentioning features or use of this software * must display the following acknowledgement: * "This product includes cryptographic software written by * Eric Young (eay@cryptsoft.com)" * The word 'cryptographic' can be left out if the rouines from the library * being used

are not cryptographic related :-). * 4. If you include any Windows specific code (or a derivative thereof) from * the apps directory (application code) you must include an acknowledgement: * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)" * * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF * SUCH DAMAGE. * * The licence and distribution terms for any publically available version or * derivative of this code cannot be changed. i.e. this code cannot simply be * copied and put under another distribution licence * [including the GNU Public Licence.]