

# Oracle® Enterprise Manager Configuration Guide for CA Service Desk Ticketing Connector



for Enterprise Manager 13c Release 3

E95148-02

April 2019

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

E95148-02

Copyright © 2016, 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

Audience	vii
Documentation Accessibility	vii
Related Documents	vii
Conventions	viii

## 1 Introduction to the Connector

---

1.1 Auto Ticketing	1-1
1.2 Manual Ticketing	1-2
1.3 Ticket Templates	1-2
1.4 Grace Period	1-3
1.5 Retry	1-3
1.6 Versions Supported	1-3

## 2 Installing and Uninstalling the CASD Ticketing Connector

---

2.1 Prerequisites	2-1
2.2 Installing the Connector	2-2
2.2.1 Install the Connector When Enterprise Manager is in "Online" Mode	2-2
2.2.1.1 Download the CA Service Desk Connector	2-2
2.2.1.2 Install the CS Service Desk Connector	2-3
2.2.2 Installing the Connector if Enterprise Manager is in "Offline" Mode	2-4
2.3 Exporting the Adapter Installation File	2-5
2.4 Installing the Adapter	2-6
2.4.1 Security Recommendations	2-6
2.4.2 Installing and Running the CASD Adapter on Unix	2-6
2.4.2.1 Prerequisites	2-7
2.4.2.2 Installing the Adapter on Unix	2-7
2.4.2.3 Running the Adapter on Unix	2-9
2.4.2.4 Testing the Adapter on Unix	2-9
2.4.3 Installing and Running the CASD Adapter on Windows	2-9
2.4.3.1 Prerequisites	2-10

2.4.3.2	Installing the Adapter on Windows	2-10
2.4.3.3	Running the Adapter as a Windows Service (Optional)	2-12
2.4.3.4	Running the Adapter on Windows	2-13
2.4.3.5	Testing the Adapter on Windows	2-14
2.5	Uninstalling the Connector	2-14
2.6	Uninstalling the Adapter	2-15
2.6.1	Uninstalling the Adapter on Unix	2-15
2.6.2	Uninstalling the Adapter on Windows	2-15

## 3 Configuring the Connector

---

3.1	Creating a Connector Instance	3-1
3.2	Configuring the Connector	3-2
3.3	Enabling or Disabling the Connector	3-2
3.4	Providing General Settings	3-3
3.4.1	Connection Settings	3-3
3.4.2	Web Console Settings	3-3
3.4.3	Grace Period	3-4
3.4.4	Retry Option	3-4
3.5	Working with Ticket Templates	3-4
3.6	Changing Web Service Credentials	3-4

## 4 Creating Service Desk Tickets

---

4.1	Automatically Creating a Ticket	4-1
4.2	Manually Creating a Ticket	4-4
4.3	Post-creation Advisory Information	4-4
4.4	Navigating Between CASD and Enterprise Manager	4-4
4.4.1	Navigating from CASD to Enterprise Manager	4-5
4.4.2	Navigating from Enterprise Manager to CASD	4-5

## 5 Using Default Templates

---

5.1	Understanding the Template Process	5-1
5.2	Reading and Mapping Ticket Templates	5-1
5.3	Customizing Ticket Templates	5-11
5.4	Modifying Ticket Templates	5-12
5.5	Exporting the Ticket Template Files	5-12
5.6	Adding Ticket Templates	5-13

## 6 Troubleshooting the Connector

---

6.1	Diagnosing the Problem	6-1
6.2	Troubleshooting Adapter Startup Errors	6-3
6.3	JVM Errors	6-3
6.4	Troubleshooting Adapter Operations Errors	6-4
6.5	Errors to Check	6-5

## 7 Enabling SSL for HTTPS

---

7.1	Installing a Self-Signed Certificate	7-1
7.2	Installing a Certificate from a Certificate Authority	7-1
7.3	Importing the Adapter Certificate into Enterprise Manager	7-2

## 8 Customizing Support Ticketing Inbound Operations

---

8.1	Adding a Custom Field to CASD	8-1
8.2	Setting Up EM CLI	8-3
8.3	Installing the Notification Script	8-4
8.4	Setting up Status Notification	8-5
8.5	Exporting the Notification Script Files	8-8
8.6	Uninstalling the Customization to CASD	8-9
8.7	Uninstalling EM CLI	8-10

## A Connector Tips

---

A.1	Recommended Protocol	A-1
A.2	Supported Alerts	A-1
A.3	Changing the Default Adapter Port	A-1
A.4	Using the Correct URL for CASD Adapter Operations	A-2

## B Third-Party Product License Information

---

B.1	JDOM 1.0	B-1
B.2	AspectJ 1.6.1	B-1
B.3	Spring Framework 2.5.6	B-5
B.4	CXF Web Stack 2.2.3	B-8
B.5	Jetty Web Service Hosting 6.1.19	B-8
B.6	Quartz Scheduler 1.6	B-8
B.7	Apache Commons DBCP 1.2.2	B-8
B.8	Apache Commons Configuration 1.5	B-8
B.9	Jakarta Commons HTTP Client 3.1	B-9

B.10	Apache Commons Collection 3.2	B-9
B.11	Apache Derby Database 10.4.2	B-9
B.12	Log4j 1.2.14	B-9
B.13	Groovy 1.6.4	B-9
B.14	Apache Axis 1.4	B-9
B.15	JDOM 1.0	B-9
B.16	LibXML2	B-9
B.17	OpenSSL	B-10

# Preface

This *Connector Configuration* guide provides the information that you require to 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 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/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Related Documents

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

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*
- *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*
- *Oracle Enterprise Manager Cloud Control Administrator's Guide*
- *Oracle Enterprise Manager Cloud Control Upgrade Guide*
- *Oracle Enterprise Manager Framework, Host, and Services Metric Reference Manual*
- *Oracle Enterprise Manager Command Line Interface*
- *Oracle Enterprise Manager Cloud Control Extensibility Programmer's Guide*
- *Oracle Database 2 Day DBA*

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

<http://docs.oracle.com/en/enterprise-manager/>

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
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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, 12, 14, or 17 with Enterprise Manager through either an HTTP or HTTPS connection. Using this connector, you can create, update, close, or reopen a ticket for any incident in Enterprise Manager. Note that the term *ticket* refers to a CA Service Desk incident.

The ticket generated by the connector contains the relevant information about the Enterprise Manager incident, including a link to the Enterprise Manager console to enable helpdesk analysts leverage Enterprise Manager's diagnostic and resolution features to resolve the incident. In Enterprise Manger, the ticket ID, ticket status, and link to the CASD console is the shown in the context of the incident. This provides Enterprise Manager administrators with ticket status information and an easy way to quickly access the ticket.

### Note:

the CASD Connector attempts to populate a custom field when you create a ticket, and cannot function without the customizations to CASD. You should only use the CASD Connector if you intend to make the necessary customizations.

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

- [Auto Ticketing](#)
- [Manual Ticketing](#)
- [Ticket Templates](#)
- [Grace Period](#)
- [Retry](#)
- [Versions Supported](#)

### 1.1 Auto Ticketing

Auto ticketing refers to creating or updating tickets automatically for any matching rule(s) in Enterprise Manager. You can define a set of event or incident rules for which tickets must be opened/updated for changes in underlying event or incident attributes. For example, changing event severity from Warning to Critical can update the associated ticket.



**See Also:**

"Incident Management" chapter in the Oracle Enterprise Manager Administrator's Guide.

After the ticket is opened, any subsequent update of the incident attributes or underlying event attributes, such as a change in underlying events severity, updates the ticket. After the incident is cleared in Enterprise Manager, the ticket is updated and you can optionally go to CA Service Desk to close the ticket.



**See Also:**

[Automatically Creating a Ticket](#)

## 1.2 Manual Ticketing

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



**See Also:**

[Manually Creating a Ticket](#)

## 1.3 Ticket Templates

Ticket templates are XML transformation style sheets that transform Enterprise Manager incidents to a ticket format before the requests are sent to CASD. A ticket template specifies how an Enterprise Manager incident and its associated event attributes can be mapped to the ticket attributes of CASD.

In Auto Ticketing, while setting up a rule, you select a configured connector and select the ticket template from the template list. The selected ticket template is used when a ticketing request is sent to CASD. For manual ticketing, you have to select a connector instance and ticket template before submitting a request for ticket creation.

The CASD Connector includes some out-of-box default ticket templates. You can customize default templates according to your functional needs. Oracle recommends that you back up these factory-built templates before customizing them.



**See Also:**

[Using Default Templates](#)

## 1.4 Grace Period

The grace period enables you to prevent creating a large number of tickets for frequently created incidents due to reoccurrence of the same event

For example, an event is raised and causes an incident to be created in Enterprise Manager. The rule defined to create the ticket enforces the ticket to be created on the CASD system. If the grace period is one hour and the event is cleared at 10:00 a.m., this clears the incident and ticket. If the same event reoccurs before 11:00 a.m. and enforces creation of another incident, the grace period functionality stops creation of a new ticket for this, and reopens the same ticket instead.

### Note:

In CASD, after a ticket is set to a Closed status, it cannot be reopened. Consequently, an incident that re-triggers within the grace period cannot reopen the ticket but only annotate it.

If you want to reopen a ticket for incident occurrences that fall within the grace period, set the ticket status to Resolved instead of Closed when the incident clears. This enables the CASD Connector to reopen the ticket if the same incident reoccurs within the grace period.

## 1.5 Retry

The "Retry" section, available on the connector configuration page, enables you to specify whether a failed ticketing request needs to be retried within a configurable expiration time.

Enabling the Retry option gives you the option of specifying whether you want to resend a ticketing request if the request fails the first time, and specifying the time period after which you want to abandon the retry. Enterprise Manager retries every 2 minutes until the request is successful or the retry interval expires.

## 1.6 Versions Supported

The base Enterprise Manager version number for the *CA Service Desk Connector Release 12.1.0.2.0* is *Enterprise Manager 12c Release 1*.

CA Service Desk Connector Release 12.1.0.3.0 supports version 11, 12, 14, and 17 of the CA Service Desk application.

# 2

## Installing and Uninstalling the CASD Ticketing Connector

The CA Service Desk (CASD) ticketing connector is comprised of the CASD adapter and CASD connector components. The CASD adapter provides a web service interface for manipulating tickets in CA Service Desk.

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

- [Prerequisites](#)
- [Installing the Connector](#)
- [Exporting the Adapter Installation File](#)
- [Installing the Adapter](#)
- [Uninstalling the Connector](#)
- [Uninstalling the Adapter](#)

### 2.1 Prerequisites

Ensure that the following prerequisites have been met before continuing:

- Before using CA Service Desk Connector, ensure that CA Service Desk 11, 12, 14, or 17 is installed and configured.
- As a prerequisite to installing the CASD Adapter, Oracle Java Development Kit (JDK) must be installed on the system where the CASD Adapter is being installed, and the system must be one of the following platforms:
  - Microsoft Windows
  - Oracle Solaris
  - Linux
- You must set up an account in the CASD system to access the CASD API. The CASD adapter must use the account exclusively, and the account must have permission to create, update, and retrieve ticket (incident) information.
- The connectivity between the adapter and CASD is HTTP. The connectivity between the Enterprise Manager and the adapter can be HTTP or HTTPS.
- Verify that the connector is available in Enterprise Manager or available for download from the Self Update feature.

The latest version of the CASD connectors come pre-installed and do not need to be downloaded through Self Update. If the connector you wish to install is not pre-installed, the My Oracle Support (MOS) Preferred Credentials must be set to enable the download of connectors through Self Update. To determine whether the connector needs to be downloaded from self update, perform the following steps:

1. From the Setup menu, select Extensibility, then select Self Update.
  2. On the Self Update page, select Management Connector to display a list of available connectors.
  3. If the CASD connector that you need is not listed here you will need to set up My Oracle Support (MOS) Preferred Credentials as described below.
- My Oracle Support Preferred Credentials must be set. To set the credentials, perform the following steps:

 **Note:**

These My Oracle Support credentials are required when there is an internet connection between your Enterprise Manager installation and the Oracle Management Service (OMS). If there is no connection, see [Installing the Connector if Enterprise Manager is in "Offline" Mode](#) for details.

1. From the Enterprise Manager console Setup menu, select **My Oracle Support**, then **Set Credentials**.
2. Enter the user name and password information, then click **Apply**.

## 2.2 Installing the Connector

This section provides the procedure required to download and install (apply) the connector. The CASD connector is not included out-of-the-box, so you need to download it from the Oracle Enterprise Manager store. All connectors in the Enterprise Manager store are available on the Self Update page for downloading.

- [Install the Connector When Enterprise Manager is in "Online" Mode](#)
- [Installing the Connector if Enterprise Manager is in "Offline" Mode](#)

### 2.2.1 Install the Connector When Enterprise Manager is in "Online" Mode

In most cases, there is an internet connection between your Enterprise Manager installation and the Oracle Management Service (OMS). There are two main steps for installing the connector when Enterprise Manager is in "online" mode:

1. [Download the CA Service Desk Connector](#)
2. [Install the CS Service Desk Connector](#)

#### 2.2.1.1 Download the CA Service Desk Connector

To download the connector:

1. From the Enterprise Manager console Setup menu, select **Extensibility**, then **Self Update**.
2. From the Self Update page, look for the CASD connector in the table list. If it does not appear, go to the next step.

3. Click **Check Updates** to schedule a job to collect the metadata for the connector.

 **See Also:**

Refer to the "Setting up Self Update" section of the "Updating Cloud Control" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for more details:

[http://docs.oracle.com/cd/E24628\\_01/doc.121/e24473/self\\_update.htm#BEJJEHDJ](http://docs.oracle.com/cd/E24628_01/doc.121/e24473/self_update.htm#BEJJEHDJ)

 **Note:**

You can also set up Self Update in offline mode. See the "Applying an Update in Offline Mode" section from the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details:

[http://docs.oracle.com/cd/E24628\\_01/doc.121/e24473/self\\_update.htm#BEJICEBD](http://docs.oracle.com/cd/E24628_01/doc.121/e24473/self_update.htm#BEJICEBD)

## 2.2.1.2 Install the CS Service Desk Connector

To install the connector:

1. From the Enterprise Manager console Setup menu, select **Setup**, then select **Extensibility**.
2. Click on the **Management Connector** link in the Type column.  
The CASD connectors appear in the list with a status of Available.
3. Click on the appropriate CASD connector to select it, and then click **Download**.  
The Schedule Download window appears, where you can determine when the download should be performed.
4. Click **Select** to download immediately.  
If you want to schedule the download for a later time, specify the date and time when the download should occur, and click **Select**. You will need to return and finish the remainder of this procedure after the scheduled download date and time.
5. If necessary, refresh the screen until the status of the connector changes to Downloaded.
6. Click on the CASD connector to select it, and then click **Apply**.  
After you respond to the prompt to confirm the operation, a page appears that indicates the request has been submitted.
7. Refresh the screen until the status of the connector changes from Apply Scheduled to Applied.

## 2.2.2 Installing the Connector if Enterprise Manager is in "Offline" Mode

Under certain circumstances, such as in high security environments, an active Internet connection between Enterprise Manager and the Enterprise Manager Update Store may not be available. In such situations, Enterprise Manager can be set to install the connector in an "offline" mode.

The installation process still requires that a computer exist at your site that has Internet access, as a connection to the Enterprise Manager Update Store is still required to obtain the necessary files. The files that you download to this computer can then be transferred to a computer behind your firewall.

To install the connector if Enterprise Manager is in "offline" mode:

1. From the system that you will ultimately deploy the connector, set Enterprise Manager Cloud Control to Offline Mode:
  - a. From the Setup menu, select **Provisioning and Patching**, then select **Offline Patching**.
  - b. In the Online and Offline Settings page, select **Offline**.
2. From the Setup menu, select **Extensibility**, then select **Self Update**.
3. On the Self Update page, click **Check Updates**. A message appears with the following URL to an Oracle site from where the updates catalog file can be downloaded:

```
https://updates.oracle.com/Orion/Download/download_patch/  
p9348486_112000_Generic.zip
```

4. From an Internet-enabled computer, download the catalog file using the aforementioned URL.
5. Copy the downloaded catalog file to the OMS host or the Management Agent host where you plan to import the connector.
6. Import the catalog file to Enterprise Manager:
  - If the catalog file is on the OMS host:

```
emcli import_update_catalog -file="file" -omslocal
```

Where:

- `-file`: is the direct path to the connector archive (\*.zip).
- `-omslocal`: indicates that the path mentioned in the `-file` option is directly accessible to the Enterprise Manager server

- If the catalog file is on a different host:

```
emcli import_update_catalog -file="file" -host="hostname" [-  
credential_set_name="setname"] | -credential_name="name" -  
credential_owner="owner"
```

**Example 2-1** shows a sample for importing the catalog archive.

7. On the Self Update page, in the table, click **Management Connectors**.
8. On the Connector Updates page, select the imported update that is available for download. Click **Download**.

A message appears with a URL to an Oracle site from where the update can be downloaded.

9. From a computer that is connected to the internet, download the update using the aforementioned URL.
10. Copy the downloaded file to the OMS host or the Management Agent host where you plan to deploy the connector.
11. To import the downloaded connector archive into Enterprise Manager, run the following command:

```
emcli import_update -file="<path to *.zip file>" -omslocal
```

Where:

- `-file`: is the direct path to the connector archive (\*.zip).
- `-omslocal`: indicates that the path mentioned in the `-file` option is directly accessible to the Enterprise Manager server

### Example 2-1 Sample for Importing Catalog Archive

```
emcli import_update_catalog -file="/u01/common/p9348486_112000_Generic.zip" -omslocal
```

Imports the master catalog file `p9348486_112000_Generic.zip`. The file must exist on the OMS host. In a multiple OMS setup, the request can be processed by any OMS, so the file should be accessible from the OMS processing the request. This means that the file must be kept on a shared location that is accessible from all the OMS instances.

```
emcli import_update_catalog -file="/u01/common/p9348486_112000_Generic.zip" -host="host1.example.com" -credential_set_name="HostCredsNormal"
```

Imports the master catalog file `p9348486_112000_Generic.zip` that is present on the host `host1.example.com`. The host must be a managed host target in Enterprise Manager, and the Management Agent on this host must be up and running. The preferred unprivileged credentials for host `host1.example.com` are used to retrieve the remote file.

## 2.3 Exporting the Adapter Installation File

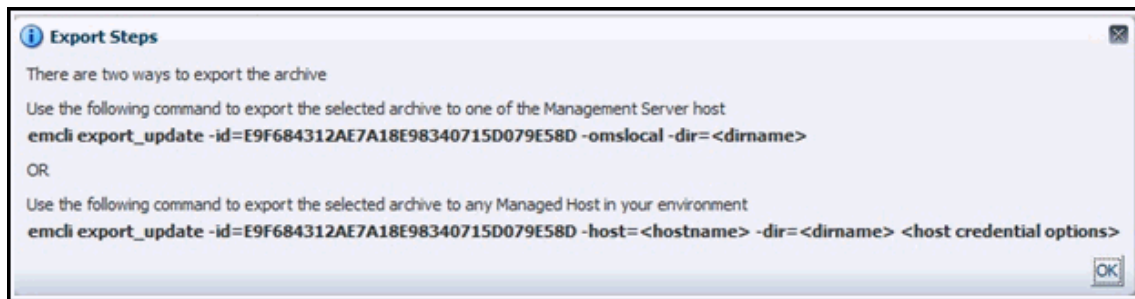
The adapter installation file is included in the connector that was installed in the previous section.

To extract the installation file:

1. Determine the command required to export the adapter installation file. To do this, perform the following steps:
  - a. From the **Setup** menu, select **Extensibility**, then **Self Update**.
  - b. Click on the **Management Connector** link in the Type column.
  - c. Click on the CASD connector to select it, then select **Export** from the **Actions** list.

A pop-up window, like the example shown in [Figure 2-1](#), appears with the command required to export the file.



**Figure 2-1 Export Command Example**

2. Open a command window on the Management Server host system and navigate to a temporary directory where you can copy and unzip the file.
3. Log into EM CLI using the following command. You will be asked to provide the password information for the sysman account.

```
emcli login -username=sysman
```

EM CLI must be executed from the OMS host. See the *Oracle Enterprise Manager Command Line Interface* for information about setting up EM CLI.

4. Run the EM CLI `export_update` command from your system, changing `<dirname>` to the full path of the temporary directory.

This action creates a zip file. The file name is comprised of the id value you specify in the `export_update` command with a `.zip` extension. In the example command in [Figure 2-1](#), the zip file name would be `E9F684312AE7A18E98340715D079E58D.zip`.

5. Extract the adapter installation `.jar` file from the `.zip` file using the following command:

```
unzip *.zip archives/casd_adapter.jar
```

## 2.4 Installing the Adapter

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

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

### 2.4.1 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.

### 2.4.2 Installing and Running the CASD Adapter on Unix

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

## 2.4.2.1 Prerequisites

The following prerequisites must be met before proceeding to the next section:

1. CA Service Desk Ticketing Connector Release 13.2.1.0.0 and 13.2.2.0.0 requires JDK 8 Update 5 and later or JDK 11 (any version) installed on the Unix platform.
2. CA Service Desk Ticketing Connector Release 12.1.0.x.0 supports only JDK 6 and requires JDK 6 Update 11 and later.
3. `JAVA_HOME` environment variable must be set to the JDK installation directory.

 **Note:**

CA Service Desk Ticketing Connector does not support JDK 7, JDK 9, and JDK 10.

## 2.4.2.2 Installing the Adapter on Unix

To install the adapter on a Unix platform:

1. Log in as a user that is a member of the adapter group. See [Security Recommendations](#) 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. Obtain a copy of the `casd_adapter.jar` file from the Management Server host system as specified in [Exporting the Adapter Installation File](#), and copy it 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 host name or IP address of the system where the CASD server is deployed. The host name defaults to *localhost* if no value is provided.
13. When the script prompts for the port number of the CASD server, enter the port number the CASD web server uses (Tomcat or IIS). The port number defaults 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 referenced in [Prerequisites](#).
15. When the script prompts for the password to use when accessing CASD, enter the password of the CASD account referenced in [Prerequisites](#).
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 adapters/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 perform the following steps:
  - a. Install an SSL certificate in the adapter keystore. You must either install a self-signed certificate, or install a certificate obtained from a Certificate Authority (CA).

- To install a self-signed certificate, perform the steps specified in [Installing a Self-Signed Certificate](#).
  - To install a certificate from a CA, perform the steps specified in [Installing a Certificate from a Certificate Authority](#).
- b. Import the SSL certificate from the adapter keystore into the Enterprise Manager keystore. Perform the steps specified in [Importing the Adapter Certificate into Enterprise Manager](#).

The adapter framework is now installed and ready to start.

### 2.4.2.3 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
```

The following commands are available for running the adapter:

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

### 2.4.2.4 Testing the Adapter on Unix

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 prompts for the password information. At the prompt, enter the password that was configured for accessing the Adapter web service in step 11 of [Installing the Adapter on Unix](#).

For information on setting the user name and password, see [Changing Web Service Credentials](#).

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

#### Note:

Starting with CA Service Desk Connector Release 13.2.1.0.0, the `testAdapter` script is no longer available.

## 2.4.3 Installing and Running the CASD Adapter on Windows

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

### 2.4.3.1 Prerequisites

The following prerequisites must be met before proceeding to the next section:

1. CA Service Desk Ticketing Connector Release 13.2.1.0.0 and 13.2.2.0.0 requires JDK 8 Update 5 and later or JDK 11 (any version) installed on the Windows platform.
2. CA Service Desk Ticketing Connector Release 12.1.0.x.0 supports only JDK 6 and requires JDK 6 Update 11 and later.
3. `JAVA_HOME` environment variable must be set to the JDK installation directory.

 **Note:**

CA Service Desk Ticketing Connector does not support JDK 7, JDK 9, and JDK 10.

### 2.4.3.2 Installing the Adapter on Windows

To install the adapter on a Windows platform:

1. Log in as a user that is a member of the adapter group. See [Security Recommendations](#) 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. Obtain a copy of the `casd_adapter.jar` file from the Management Server host system as specified in [Exporting the Adapter Installation File](#), and copy it 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 is 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 is 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 host name or IP address of the system where the CASD server is deployed. The host name defaults to *localhost* if no value is provided.
13. When the script prompts for the port number of the CASD server, enter the port number the CASD web server uses (Tomcat or IIS). The port number defaults 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 referenced in [Prerequisites](#).
15. When the script prompts for the password to use when accessing CASD, enter the password of the CASD account referenced in [Prerequisites](#).
16. Enter the following command to change the working directory to the *conf* directory.

```
cd adapters\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 perform the following steps:
  - a. Install an SSL certificate in the adapter keystore. You must either install a self-signed certificate, or install a certificate obtained from a Certificate Authority (CA).
    - To install a self-signed certificate, perform the steps specified in [Installing a Self-Signed Certificate](#).

- To install a certificate from a CA, perform the steps specified in [Installing a Certificate from a Certificate Authority](#).
- b. Import the SSL certificate from the adapter keystore into the Enterprise Manager keystore. Perform the steps specified in [Importing the Adapter Certificate into Enterprise Manager](#).

The adapter framework is now installed and ready to start.

### 2.4.3.3 Running the Adapter as a Windows Service (Optional)

Optionally, 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.

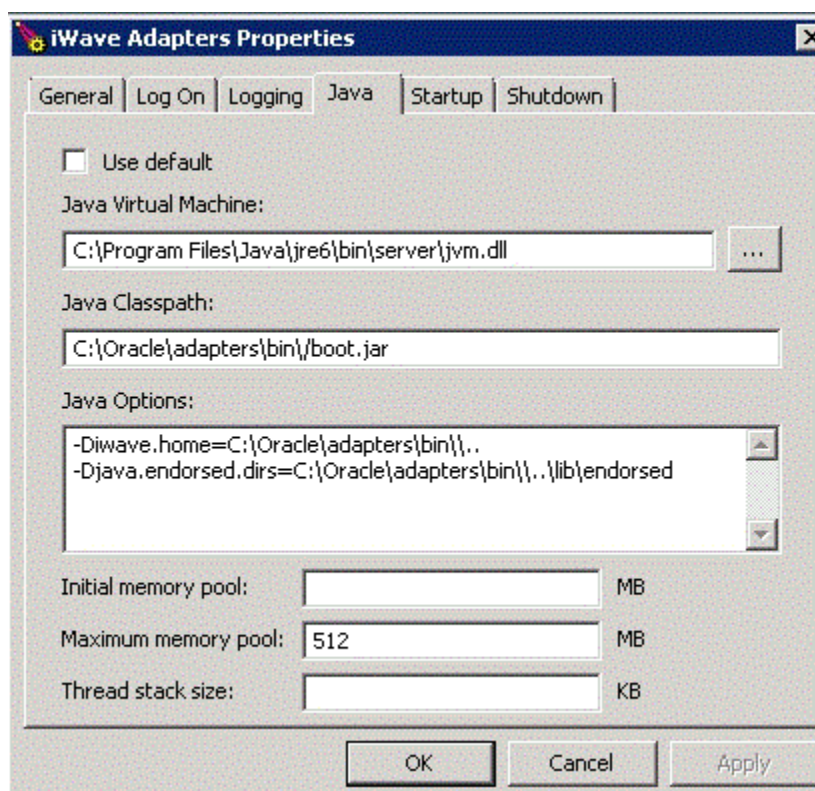
 **Note:**

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. If the adapter will be run using a 64-bit JRE, copy the `iWaveAdapters.exe` and `iWaveAdaptersw.exe` files from the `x64` directory to the current directory (`.`) overwriting the existing files.
5. Enter the following command to install the adapter as a Windows service:  

```
service.bat install
```
6. If the adapter will be run using a 64-bit JRE, perform the following substeps to configure the service to use the 64-bit JRE:
  - a. In the `adapters\bin` directory, double click the `iWaveAdaptersw.exe` file. This will cause the iWave Adapters Properties window to be displayed.
  - b. Click the **Java** tab. The Java tab will be displayed that shows the JVM settings as shown in [Figure 2-2](#).

Figure 2-2 Java Tab on the iWave Adapters Properties Window



- c. Uncheck the **Use default** check box if it is checked.
- d. Click



to open the Select Java Virtual Machine DLL window.

- e. Navigate to the `jvm.dll` file in the 64-bit JRE installation directory and click **Open**.
- f. Click **OK**.

## 2.4.3.4 Running the Adapter on Windows

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

### 2.4.3.4.1 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.

#### 2.4.3.4.2 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
```

#### 2.4.3.5 Testing the Adapter on Windows

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 prompts for the password information. At the prompt, enter the password that was configured for accessing the Adapter web service in step 11 of [Installing the Adapter on Windows](#).
4. If the test completes successfully, the last line the utility displays is *Test completed successfully*.



#### Note:

Starting with CA Service Desk Connector Release 13.2.1.0.0, the `testAdapter` script is no longer available.

## 2.5 Uninstalling the Connector

To uninstall the connector, you must first delete all defined instances of the connector, and then you must delete the connector from the Self Update page.

To uninstall the connector:

1. From the **Setup** menu, select **Extensibility**, then **Management Connectors**.
2. Select an instance of the connector you want to delete, then click **Delete**.
3. On the Confirmation page, click **Yes**.
4. Repeat steps 2 and 3 until all instances of the connector have been deleted.
5. From the **Setup** menu, select **Extensibility**, then **Self Update**.
6. Click on the **Management Connector** link in the Type column.  
A list of updates appears for Management Connectors.
7. Click on the connector you want to delete, select **Actions**, then select **Delete**.

The Delete Update window appears.

8. Click **Delete** to delete the connector.

The confirmation window appears.

9. Click **OK**.

## 2.6 Uninstalling the Adapter

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

### 2.6.1 Uninstalling the Adapter on Unix

To uninstall the adapter on a Unix platform:

1. Stop the adapter as specified in [Running the Adapter on Unix](#).
2. Delete the adapters folder from the adapter installation directory.

### 2.6.2 Uninstalling the Adapter on Windows

To uninstall the adapter on a Windows platform:

1. Stop the adapter as specified in [Running the Adapter on Windows](#).
2. If the adapter is installed as a Windows 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.

# 3

## Configuring the Connector

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

- [Creating a Connector Instance](#)
- [Configuring the Connector](#)
- [Enabling or Disabling the Connector](#)
- [Providing General Settings](#)
- [Working with Ticket Templates](#)
- [Changing Web Service Credentials](#)

### 3.1 Creating a Connector Instance

To create a connector instance:

1. From the **Setup** menu of the Enterprise Manager console, select **Extensibility**, then **Management Connectors**.
2. Select a connector from the Create Connector drop-down list, and then click **Go**.

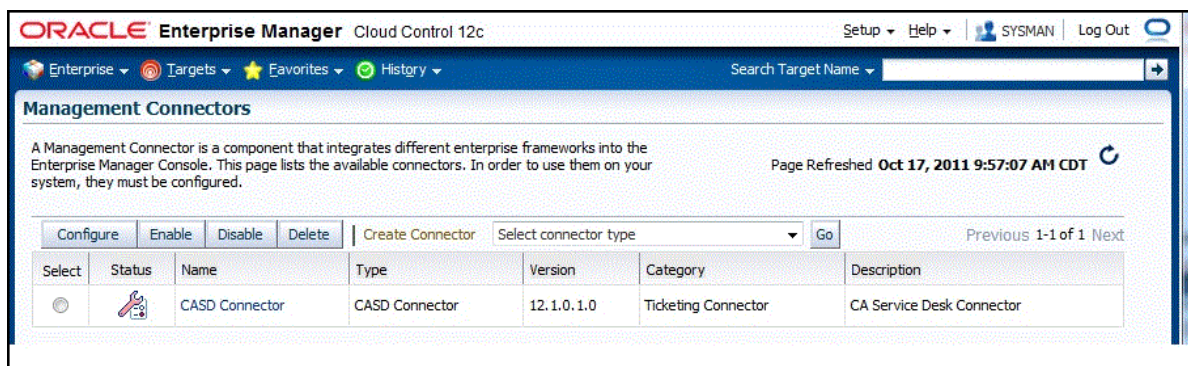


#### Note:

See [Introduction to the Connector](#) for information about which CASD connector to select.

3. Enter the connector name and description on the next page, then click **OK**.  
The connector instance appears as unconfigured in the Management Connectors page, as shown in [Figure 3-1](#).

**Figure 3-1 Unconfigured CASD Connector**



## 3.2 Configuring the Connector

To perform a basic configuration:

1. Click on the name of the CA Service Desk Connector.

The General tab of the Configure Management Connector page appears, as shown in [Figure 3-2](#).

**Figure 3-2 Configure Management Connector Page**

**Management Connectors**

Management Connectors > Configure Management Connector: CASD Connector

**Configure Management Connector: CASD Connector** Cancel OK

**General** Template

**Connection Settings**

Enter a set of administrator credentials and the webservice end points for relevant operations of the ticketing system. These are required for communications.

* Web Service End Points	Operation	Web Service End Point (URL)
	createTicket	http://[hostname]:8082/services/causd/IncidentService
	getTicket	http://[hostname]:8082/services/causd/IncidentService
	updateTicket	http://[hostname]:8082/services/causd/IncidentService

**TIP** Replace <midtier-server> and <servername> in the above URLs with the midtier server and server of your Ticketing System. If you have customized the webservice, you may need to change the webservice operations at the end of the URL.

\* CASD Adapter Username

\* CASD Adapter Password

\* Ticket ID

Enter a valid ticket number from the ticketing system to test connection to this system.

**Web Console Settings**

If you're using a web console, you can enable the connector to provide URL links to the ticket on the metric details page and vice versa.

Enable web console features

CASD Server Port

CASD Server Host

**Grace Period**

The grace period is a time value that is compared against the data of the time an alert cleared to the time it transitioned out of clear. If the time data is greater than the grace period, then a new ticket is created for the alert; otherwise, the ticket is reopened.

Enable grace period

Grace Period (Hours)

**Retry**

Specify whether or not you want to retry this connector operations if they fail, as well as the expiration time after which retry is aborted.

Enable Retry

Expiration (Hours)

2. Provide the required settings. See [Providing General Settings](#) for details.
3. Click **OK**.

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

4. Optionally, you can click the configure icon again to check for the available ticket templates.
5. Click the **Ticket Templates** tab.

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

If you choose HTTPS as the protocol to establish a connection between CASD and Enterprise Manager, see [Importing the Adapter Certificate into Enterprise Manager](#).

## 3.3 Enabling or Disabling the Connector

You can enable or disable a connector from the Management Connectors page by selecting the connector and clicking either Enable or Disable. After a connector is

disabled, a red cross icon appears under the status column. By default, the connector instance is enabled as soon as it is configured.

 **Note:**

Only enabled connectors are available for ticketing operations.

## 3.4 Providing General Settings

The following sections explain how to provide various configuration details.

### 3.4.1 Connection Settings

The CA Service Desk Connector communicates with the Service Desk through a web service provided by the CASD Adapter. All fields are mandatory.

- 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 ([Installing the Adapter on Unix](#) for Unix and [Installing the Adapter on Windows](#) for Windows).
- CASD Adapter Password - Password that was configured for accessing the Adapter web service in step 11 of the appropriate adapter installation section ([Installing the Adapter on Unix](#) for Unix and [Installing the Adapter on Windows](#) for Windows).
- Ticket Number - Enter a required valid ticket number to test the connection when you save the configuration.
  - 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 enter incorrect Web service endpoints or 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 not previously saved the connector configuration and enter incorrect Web service endpoints or an invalid ticket number, the following message appears on the Management Connectors page after you click OK:  
*Connection test failed. The configuration was not saved.*

### 3.4.2 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 incident.

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

- Enable Web Console - Check this box to launch the CASD ticket page within the 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.

### 3.4.3 Grace Period

You can enable and disable the grace period and configure its value. By default, the grace period is disabled. See [Grace Period](#) for details. This setting applies to all incidents the CA Service Desk Connector processes.

### 3.4.4 Retry Option

You can enable and disable the Retry option and configure its interval, which is an integer value in hours. By default, the Retry is disabled. See [Retry](#) for details. This setting applies to all incidents the CA Service Desk Connector processes.

## 3.5 Working with Ticket Templates

When a connector instance is created in Enterprise Manager, all associated templates are available for ticket create/update operations. For Auto Ticketing, a notification method is created based on the ticket template selected while creating an incident rule. For manual ticketing, a ticket template is selected while creating a ticket from the Enterprise Manager console.

There are two default templates for the CASD Connector:

- CASD\_Default\_Incident\_AutoClose.xsl
- CASD\_Default\_Incident.xsl



**Tip:**

See [Understanding the Template Process](#) for detailed information about these templates.

## 3.6 Changing Web Service Credentials

Sometimes problems occur when accessing the web service, because the credentials provided are incorrect. Whenever this happens, you receive an HTTP 403 error from the web service. You first want to check the specified credentials and verify that you entered the correct information. If the credentials you have specified appear to be correct, but you still receive the 403 error, the best option is to reset the web service credentials.

Perform the following steps to reset the web service credentials:

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

```
<CASD_ADAP_INSTALL>/adapters/conf
```

... where <CASD\_ADAP\_INSTALL> is the installation directory for the CASD connector.

2. Enter the following command to change the user name and password for accessing the CASD web service:

```
../bin/propertiesEditor.sh -h  
framework.username=<username> -e  
framework.password=<password> framework.properties
```

... where <username> is the user name to specify for the web service and <password> is the password.

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

3. Stop and then start the web service as instructed in [Installing and Running the CASD Adapter on Unix](#) and [Installing and Running the CASD Adapter on Windows](#).

# 4

## Creating Service Desk Tickets

You can create tickets automatically or manually. The following sections explain how to create both types, understand post-creation advisory information, and then switch from one console to the other:

- [Automatically Creating a Ticket](#)
- [Manually Creating a Ticket](#)
- [Post-creation Advisory Information](#)
- [Navigating Between CASD and Enterprise Manager](#)

### Note:

If the default templates do not provide the desired mappings, you can create custom templates to map data as desired. See [Customizing Ticket Templates](#) for additional information.

### 4.1 Automatically Creating a Ticket

To automatically create a ticket in CASD, you need to create an incident rule that references a template from the CASD connector.

To create an incident rule to automatically create a ticket in CASD:

1. From the Enterprise Manager console, click **Setup**, then **Incidents and Incident Rules**.
2. Click **Create Rule Set**.  
The Create Rule Set page appears.
3. Provide a Name and Description.
4. Click the **Rules** tab.
  - For events —  
This is the typical option to choose to create a ticket for an event, such as a target down availability event.
    - Click **Create** and select **Incoming events or updates to events** as a type of rule to create from the pop-up window, then click **Continue**.  
The Create New Rule wizard appears.
    - Follow the steps to create a rule. (Refer to the "Configuring Incident Rule" section in the *Oracle Enterprise Manger Advanced Configuration Guide*.)
  - For incidents —



You can use this option to create tickets based on incident attributes, such as priority 1 incidents or incidents based on fatal or critical severity.

- Click **Create** and select **Newly created incidents or updates to incidents** as a type of rule to create from the pop-up window, then click **Continue**.

The Create New Rule wizard appears.

- Follow the steps to create a rule. (Refer to the "Configuring Incident Rule" section in the *Oracle Enterprise Manger Advanced Configuration Guide*.)

5. While configuring the above rule in the Add Actions page:

- For events —

Enable the **Create Incident** check box. This makes the Create Ticket option visible. Now enable the **Create Ticket** check box, which displays lists to select the Connector Type, Connector Name, and Template Name as shown in [Figure 4-1](#).

**Figure 4-1 Event Add Actions**

- For incidents —

Enable the **Create Ticket** check box, which displays lists to select the Connector Type, Connector Name, and Template Name as shown in [Figure 4-2](#).

**Figure 4-2 Incident Add Actions**

6. After completing all of the wizard steps, click **Save**.

The following process occurs after you create the incident rule for your incidents:

- A request is sent to the CASD Connector when an incident is created due to an event that matches your rule.
- The ticket is created or updated in the CASD system.
- In Enterprise Manager, the incident annotation is updated. A comment is added to the event Detail page of the incident to indicate that a ticket was created or updated, along with the ticket ID, status, and ticket URL.

A ticket is updated if there is an existing active ticket for an incident. [Figure 4-3](#) shows the ticket in the CASD console.

 **Tip:**

For information about configuring CASD to return the ticket status to Enterprise Manager, see [Customizing Support Ticketing Inbound Operations](#).

Figure 4-3 CASD Console Incident

The screenshot displays the CA Service Desk interface for incident 456. The incident is in an 'Open' status with a priority of 3. The description states: 'Memory utilization is 74.437%, crossed warning (50) or critical (70) threshold. Incident created by Oracle Enterprise Manager CA Service Desk Connector. EM User: SYSMAN'. The incident information includes source and target details for 'orcsrv1.iwavesoftware.com'. The interface also shows a table for incident tracking with columns for Open Date/Time, Last Modified, Resolve Date/Time, and Close Date/Time. At the bottom, there are tabs for 1. Activities, 2. Event Log, 3. Attachments, 4. Service Type, 5. Parent / Child, 6. Knowledge, 7. Solutions, and 8. Properties.

## 4.2 Manually Creating a Ticket

To manually create a ticket:

1. After a metric incident occurs, go to its incident details page by clicking on the incident message in the Incident Manager console in Enterprise Manager. The incident details page for the incident should appear.
2. In the Tracking section, select **More**, then **Create Ticket**.

The Create Ticket pop-up appears. The Create Ticket option is only available if there is at least one ticketing connector configured, and no prior ticket exists for the same incident.

## 4.3 Post-creation Advisory Information

- If you have successfully created the ticket, the ticket ID appears in the Last Comment column in the Event Details for the incident and in the Ticket ID column. If the Web console settings are configured and enabled, the ticket ID appears as a link to the ticket page in Service Desk.
- For tickets that were created manually, 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 incident severity change.

## 4.4 Navigating Between CASD and Enterprise Manager

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

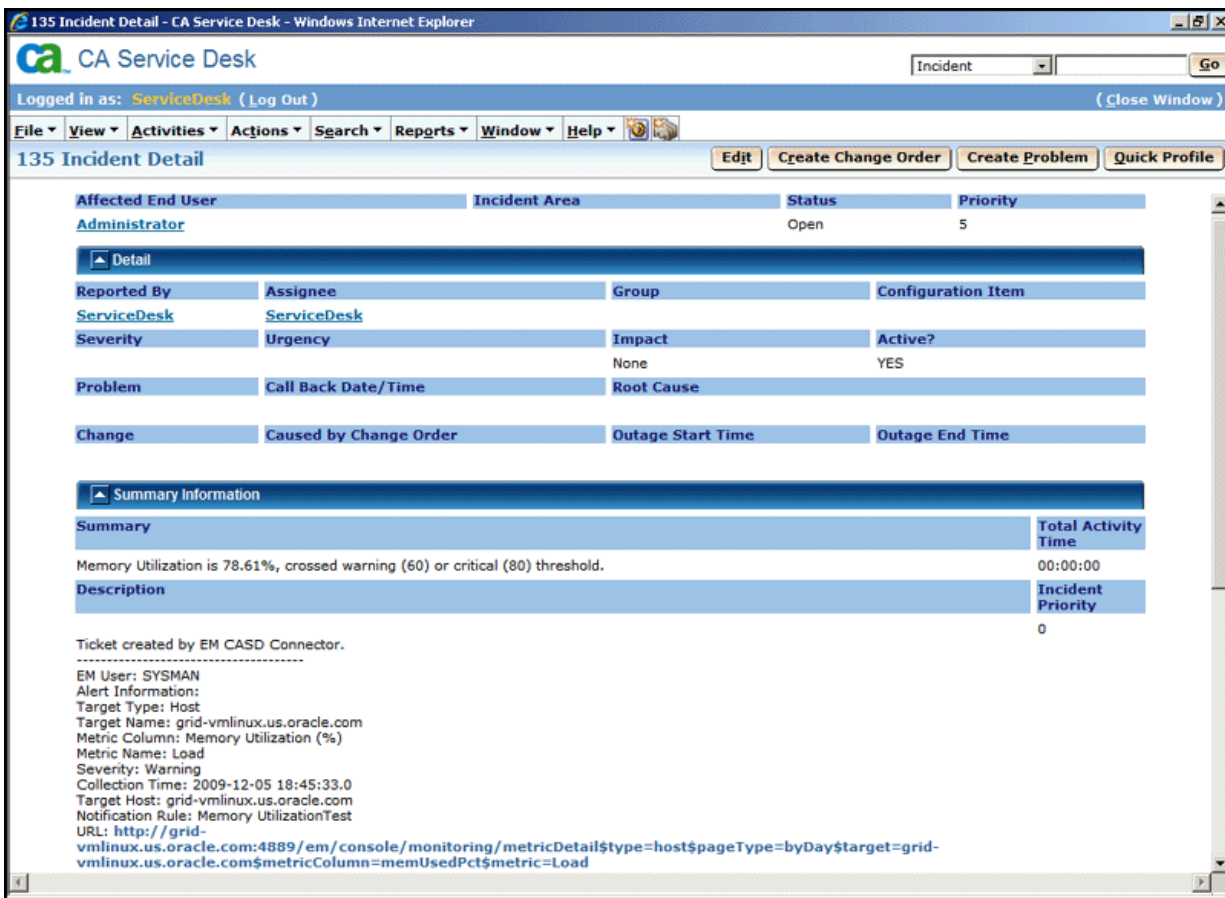
## 4.4.1 Navigating from CASD to Enterprise Manager

From the ticket Detail page of the CASD console, click the link to the URL label in the Description field, as shown in [Figure 4-4](#). 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 Enterprise Manager ticket related to this CASD ticket.

 **Note:**

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

**Figure 4-4 Incident Detail in CASD Console**



## 4.4.2 Navigating from Enterprise Manager to CASD

To navigate from Enterprise Manager to CASD:

1. From the **Enterprise** menu, select **Monitoring**, then **Incident Manager**.  
The open tickets appear on the Incident Manager page.
2. Click on the desired incident.  
Detailed information for the incident appears in the lower half of the page.
3. Click on the ticket identifier listed to the right of the Ticket ID label in the Tracking section.  
You will be forwarded to the CASD Web console login page.
4. Provide valid CASD account details.  
The CASD incident details associated with this incident are displayed through the CASD web console.

# 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 incident attributes and Service Desk ticket attributes.

- [Understanding the Template Process](#)
- [Reading and Mapping Ticket Templates](#)
- [Customizing Ticket Templates](#)
- [Modifying Ticket Templates](#)
- [Exporting the Ticket Template Files](#)
- [Adding Ticket Templates](#)

### 5.1 Understanding the Template Process

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

- Write incident information to Description (Service Desk ticket description).
- Set the Service Desk ticket summary based on the incident message.
- Add a Log Comment to the Incident Activity Log List that shows the incident details. This provides a record of the changes that have occurred to the incident.
- Sets the Service Desk priority based on the severity of the incident in Enterprise Manager.

The out-of-box templates are as follows:

- *CASD\_Default\_Incident.xml*

The *CASD\_Default\_Incident.xml* 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.xml*

The *CASD\_Default\_Incident\_AutoClose.xml* 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.xml* and *CASD\_Default\_Incident.xml*.

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

**Table 5-1 Ticket Creation Mappings (for all templates)**

Service Desk Ticket Attributes	Enterprise Manager incident Attributes	Value
Summary	Message	N/A
Description	<p><b>For incidents:</b></p> <p>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.</p> <p>Other Incident information includes:</p> <p>Source Name</p> <p>Source Owner - Example: Sysman</p> <p>Source Type</p> <p>Source SubType</p> <p>Target Name</p> <p>Target Type</p> <p>Target URL</p> <p>TargetProperties** - name:value pairs of defined target properties. For example:</p> <p>Line of business:</p> <p>Finance</p> <p>Owner:</p> <p>Finance-DB Team</p> <p>Severity</p> <p>Priority</p> <p>Creation Date - Incident Creation Date</p> <p>Last Updated Date</p> <p>Owner - Incident Owner</p> <p>Notification Rule Name</p> <p>URL - URL to the metric details page in the context of the incident.</p> <p>Incident Status</p> <p>Incident Acknowledge Flag</p> <p>Incident Auto Close</p> <p>Incident Escalation Level</p>	Values from incident context
Priority	<b>Based on Severity Code</b>	<p><b>For metric incidents:</b></p> <ul style="list-style-type: none"> <li>• If severity is Fatal, set Priority to Medium-High (2).</li> <li>• If severity is Critical, set Priority to Medium (3).</li> <li>• If severity is Warning, set Priority to Medium-Low (4).</li> <li>• Otherwise, set Priority to Low (5).</li> </ul>

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

Service Desk Ticket Attributes	Enterprise Manager incident Attributes	Value
Reported By	N/A	Administrator
Activity Log	<b>Same content as the Description attribute.</b>	<b>See the Description attribute above.</b>
z_em_connector_id (Custom field)	Connector GUID	Only set for the CASD Connector. This field is not set for the CASD No Publish Connector.

Table 5-2 shows Service Desk ticket attributes and corresponding Enterprise Manager alert incident attributes for ticket update mappings. The CASD\_Default\_Incident.xml and CASD\_Default\_Incident\_AutoClose.xml mappings templates are almost identical. The only difference is in the status field. The AutoClose template sets it to CL, and the other template does not set the field. This difference is noted in the table.

**Table 5-2 Ticket Updates (For All Templates)**

Service Desk Ticket Attributes	Enterprise Manager incident Attributes	Value
Identifier	TicketID - Extracts only the internal identifier from the ticket id	N/A
Summary	Message	N/A
Description	Same content as the Description attribute for create transactions.	See <a href="#">Table 5-1</a> .
Priority	Based on Severity code. JobStatus - Applies to job status events	<b>For metric incidents:</b> <ul style="list-style-type: none"> <li>• If severity is Fatal, set Priority to Medium-High (2).</li> <li>• If severity is Critical, set Priority to Medium (3).</li> <li>• If severity is Warning, set Priority to Medium-Low (4).</li> <li>• Otherwise, set Impact to Low (5).</li> </ul>
Status	<b>For metric incidents:</b> Grace Period Severity	<b>For metric incidents:</b> If Grace Period is set to "Yes" set Status to Open (OP). If an Autoclose template and Severity is set to Clear, set Status to Close (CL). Otherwise do not set Status.
Activity Log	<b>Same content as the Description attribute.</b>	<b>See <a href="#">Table 5-1</a>.</b>
z_em_connector_id (Custom field)	Connector GUID	Only set for the CASD Connector. This field is not set for the CASD No Publish Connector.

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">

  <!--
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:EMIncident">
    <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>

            <!-- Set the CASD Incident Priority-->
            <!-- Possible values for priority: -->
            <!-- 1 = High -->
            <!-- 2 = Medium-High -->
            <!-- 3 = Medium -->
            <!-- 4 = Medium-Low -->
            <!-- 5 = Low -->
            <!-- None -->
            <xsl:choose>
              <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'FATAL'">
                <priority>2</priority> <!-- CASD Medium-High -->
              </xsl:when>
              <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'CRITICAL'">
                <priority>3</priority> <!-- CASD Medium -->
              </xsl:when>
              <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'WARNING'">
                <priority>4</priority> <!-- CASD Medium-Low -->
              </xsl:when>
              <xsl:otherwise>
                <priority>5</priority> <!-- CASD Low -->
              </xsl:otherwise>
            </xsl:choose>

            <!-- Set the CASD Incident Description -->
            <description>
              <xsl:call-template name="getDescription">
                <xsl:with-param name="message">Incident created by Oracle
Enterprise
                Manager CA Service Desk Connector</xsl:with-param>
                <xsl:with-param name="addHref">true</xsl:with-param>
              </xsl:call-template>
            </description>

            <!-- 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 Priority-->
<!-- Possible values for priority: -->
<!-- 1 = High -->
<!-- 2 = Medium-High -->
<!-- 3 = Medium -->
<!-- 4 = Medium-Low -->
<!-- 5 = Low -->
<!-- None -->
<xsl:choose>
  <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'FATAL'">
    <priority>2</priority> <!-- CASD Medium-High -->
  </xsl:when>
  <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'CRITICAL'">
    <priority>3</priority> <!-- CASD Medium -->
  </xsl:when>
  <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'WARNING'">
    <priority>4</priority> <!-- CASD Medium-Low -->
  </xsl:when>
  <xsl:otherwise>
    <priority>5</priority> <!-- CASD Low -->
  </xsl:otherwise>
</xsl:choose>

<!-- Set the CASD Incident Description -->
<description>
  <xsl:call-template name="getDescription">
    <xsl:with-param name="message">Incident created by Oracle
Enterprise
    Manager CA Service Desk Connector</xsl:with-param>
    <xsl:with-param name="addHref">true</xsl:with-param>
  </xsl:call-template>
</description>

<!-- 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:SystemAttributes/ns0:Summary"/></summary>

<!-- Add a CASD Activity log entry -->
<logs>
  <log>
    <description>
      <xsl:call-template name="getDescription">
        <xsl:with-param name="message">Incident created by Oracle

```

```
Enterprise Manager CA Service Desk Connector</xsl:with-param>
  <xsl:with-param name="addHref">false</xsl:with-param>
</xsl:call-template>
</description>
</log>
</logs>

<!-- Set the z_em_connector_id custom field in CASD to the EM event identifier. The
custom field is required for the publishTicket operation and must be added by an
CASD administrator -->
<!-- If the publishTicket operation is not going to be used, this code can be
commented out. -->
  <extended-fields>
    <string-field name="z_em_connector_id"><xsl:value-of
      select="ns0:ConnectorGUID"/></string-field>
  </extended-fields>

<!-- 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-Supervisor 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/adaptor-framework">
    <incident>
        <identifier><xsl:value-of select=
            "normalize-space(substring-before(substring-after(ns0:TicketID,
                '(', ')')))" /></identifier>

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

        <!-- Set the CASD Incident Description -->
        <description>
            <xsl:call-template name="getDescription">
                <xsl:with-param name="message">Incident updated by Oracle
                    Enterprise Manager CA Service Desk Connector</xsl:with-param>
                <xsl:with-param name="addHref">true</xsl:with-param>
            </xsl:call-template>
        </description>

        <!-- Set the CASD Incident Priority-->
        <!-- Possible values for priority: -->
        <!-- 1 = High -->
        <!-- 2 = Medium-High -->
        <!-- 3 = Medium -->
        <!-- 4 = Medium-Low -->
        <!-- 5 = Low -->
        <!-- None -->
        <xsl:choose>
            <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'FATAL'">
                <priority>2</priority> <!-- CASD Medium-High -->
            </xsl:when>
            <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'CRITICAL'">
                <priority>3</priority> <!-- CASD Medium -->
            </xsl:when>
            <xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'WARNING'">
                <priority>4</priority> <!-- CASD Medium-Low -->
            </xsl:when>
            <xsl:otherwise>
                <priority>5</priority> <!-- CASD Low -->
            </xsl:otherwise>
        </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-Supervisor 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>
  <xsl:when test="ns0:ReopenTicket = 'Yes'">
    <!-- Set the CASD Incident Status back to Open -->
    <status>OP</status>

    <!-- Add a CASD Activity log entry -->
    <logs>
      <log>
        <description>
          <xsl:call-template name="getDescription">
```

```

        <xsl:with-param name="message">Incident reopened by Oracle
        Enterprise Manager CA Service Desk Connector</xsl:with-param>
        <xsl:with-param name="addHref">>false</xsl:with-param>
        </xsl:call-template>
    </description>
</log>
</logs>
</xsl:when>

<!-- Close the incident if the EM Severity is set to Clear. -->
<xsl:when test="ns0:SystemAttributes/ns0:SeverityCode = 'CLEAR'">
    <!-- Set the CASD Incident Status to Closed -->
    <status>CL</status>

    <!-- Add a CASD Activity log entry -->
    <logs>
        <log>
            <description>
                <xsl:call-template name="getDescription">
                    <xsl:with-param name="message">Incident closed by Oracle
                    Enterprise Manager CA Service Desk Connector</xsl:with-param>
                    <xsl:with-param name="addHref">>false</xsl:with-param>
                </xsl:call-template>
            </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>
                <xsl:call-template name="getDescription">
                    <xsl:with-param name="message">Incident updated by Oracle
                    Enterprise Manager CA Service Desk Connector</xsl:with-param>
                    <xsl:with-param name="addHref">>false</xsl:with-param>
                </xsl:call-template>
            </description>
        </log>
    </logs>
</xsl:otherwise>
</xsl:choose>
</incident>
</iwaveaf:update>
</xsl:otherwise>
</xsl:choose>
</xsl:template>

<xsl:template name="getDescription">
    <xsl:param name="message"/>
    <xsl:param name="addHref"/>

    <xsl:variable name="msg">
        <xsl:choose>
            <xsl:when test="normalize-space(ns0:SystemAttributes/ns0:UpdatedAttributes) !
            = ''">
                <xsl:value-of select="$message"/> for change in attributes : <xsl:value-of
                select="ns0:SystemAttributes/ns0:UpdatedAttributes"/>
            </xsl:when>

```

```

        <xsl:otherwise>
<xsl:value-of select="$message"/>
        </xsl:otherwise>
    </xsl:choose>
</xsl:variable>

<xsl:value-of select="$msg"/>.
-----
----
EM User: <xsl:value-of select="ns0:NotificationRuleOwner"/>

Incident Information:
<xsl:for-each select="ns0:SystemAttributes/ns0:SourceInfo"><xsl:text>&#xa;</
xsl:text>    Source Name: <xsl:value-of select="./ns0:SourceObjInfo/ns0:ObjName" />
    <xsl:choose>
        <xsl:when test="normalize-space(./ns0:SourceObjInfo/ns0:ObjOwner) != ''">
    Source Owner: <xsl:value-of select="./ns0:SourceObjInfo/ns0:ObjOwner" />
        </xsl:when>
    </xsl:choose>
    Source Type: <xsl:value-of select="./ns0:SourceObjInfo/ns0:SourceObjType"/>
    Source SubType: <xsl:value-of select="./ns0:SourceObjInfo/ns0:SourceObjSubType"/>
    Target Name: <xsl:value-of select="./ns0:TargetInfo/ns0:TargetName"/>
    Target Type: <xsl:value-of select="./ns0:TargetInfo/ns0:TargetType"/>
    Target Type Label: <xsl:value-of select="./ns0:TargetInfo/ns0:TargetTypeLabel"/>
<xsl:choose>
    <xsl:when test="$addHref = 'true' and ./ns0:TargetInfo/ns0:TargetURL != ''">
    Target URL: <a href="<xsl:value-of select="./ns0:TargetInfo/ns0:TargetURL"/>"
target="_blank"><xsl:value-of select="./ns0:TargetInfo/ns0:TargetURL"/>&lt;/
a><xsl:text/>
    </xsl:when>
    <xsl:otherwise>
    Target URL: <xsl:value-of select="./ns0:TargetInfo/ns0:TargetURL"/>
    </xsl:otherwise>
</xsl:choose>
<xsl:if test="position() &lt; last()">
    <xsl:text>&#xa;</xsl:text>
</xsl:if>
</xsl:for-each>
<xsl:for-each select="ns0:SystemAttributes/ns0:SourceInfo/ns0:TargetInfo/
ns0:TargetProperty">
    <xsl:if test="position() = 1">
        <xsl:text>&#xa;&#xa;    Target Properties:&#xa;</xsl:text>
    </xsl:if>
    <xsl:text>        </xsl:text><xsl:value-of select="./ns0:Name"/>: <xsl:value-of
select="./ns0:Value"/>
        <xsl:if test="position() &lt; last()">
            <xsl:text>&#xa;</xsl:text>
        </xsl:if>
    </xsl:for-each>
<!-- EDIT THE FOLLOWING CODE TO LIST A SPECIFIC TARGET PROPERTY, SUCH AS "Line of
Business"
    <xsl:choose>
        <xsl:when test="ns0:SystemAttributes/ns0:SourceInfo/ns0:TargetInfo/
ns0:TargetProperty/ns0:Name='Line of Business'">
            Line of Business: <xsl:value-of select="ns0:ns0:SystemAttributes/
ns0:SourceInfo/ns0:TargetInfo/ns0:TargetProperty/ns0:value"/>
        </xsl:when>
    </xsl:choose>
-->
    Severity: <xsl:value-of select="ns0:SystemAttributes/ns0:Severity"/>
    Priority: <xsl:value-of select="ns0:SystemAttributes/ns0:Priority" />

```

```

CreationDate: <xsl:value-of select="ns0:SystemAttributes/ns0:CreationDate"/>
LastUpdatedDate: <xsl:value-of select="ns0:SystemAttributes/
ns0:LastUpdatedDate"/>
Owner: <xsl:value-of select="ns0:SystemAttributes/ns0:Owner" />
<xsl:choose>
  <xsl:when test="normalize-space(ns0:NotificationRuleName) != ''">
Notification Rule: <xsl:value-of select="ns0:NotificationRuleName"/>
  </xsl:when>
</xsl:choose>
<xsl:choose>
  <xsl:when test="$addHref = 'true' and ns0:SystemAttributes/ns0:IncidentURL !=
''">
URL: &lt;a href="<xsl:value-of select="ns0:SystemAttributes/ns0:IncidentURL"/>"
target="_blank"&gt;<xsl:value-of select="ns0:SystemAttributes/ns0:IncidentURL"/>&lt;
a&gt;<xsl:text/>
  </xsl:when>
  <xsl:otherwise>
URL: <xsl:value-of select="ns0:SystemAttributes/ns0:IncidentURL"/>
  </xsl:otherwise>
</xsl:choose>

EM Incident Status: <xsl:value-of select="ns0:SystemAttributes/
ns0:ResolutionState"/>
EM Acknowledge: <xsl:value-of select="ns0:SystemAttributes/ns0:Acknowledge"/>
EM Auto Close: <xsl:value-of select="ns0:SystemAttributes/ns0:AutoClose"/>
EM Escalation Level: <xsl:value-of select="ns0:SystemAttributes/
ns0:EscalationLevel"/>

<xsl:for-each select="ns0:SystemAttributes/ns0:AdditionalDetails">
  <xsl:text>&#xa;  </xsl:text><xsl:value-of select="./ns0:VariableName"/>:
<xsl:value-of select="./ns0:VariableValue"/>
  </xsl:for-each>
</xsl:template>

</xsl:stylesheet>

```

## 5.3 Customizing Ticket Templates

If the out-of-box ticket templates do not satisfy your requirements, you can create custom templates tailored to your environment. To do this, Oracle recommends that you use one of the existing templates as the base template.

To create a custom template:

1. Export the default template XSLT files from Enterprise Manager to use as a baseline. Follow the instructions in [Exporting the Ticket Template Files](#) to obtain copies of the default template files.
2. Determine which file you want to use as a baseline and copy the file to a new file with a different name.
3. Make the desired mapping changes to the new template file. See [Modifying Ticket Templates](#) for information on mapping changes.
4. Register the new template with Enterprise Manager as specified in [Adding Ticket Templates](#).



## 5.4 Modifying Ticket Templates

The templates are highly customizable. However, 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 incidents. You can have as many tickets templates as desired. One notification rule can have only one ticket template.

Generally, when you modify the ticket template, you might only be changing the existing mappings. The following examples illustrate this concept.

### 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 you can use 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>
```

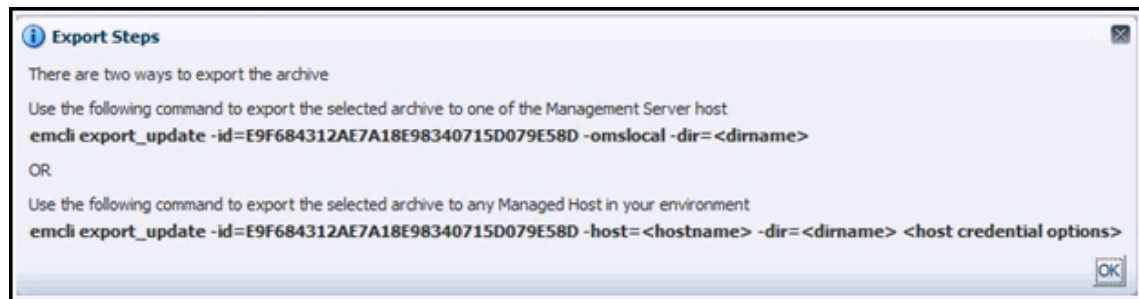
## 5.5 Exporting the Ticket Template Files

The connector installation jar file is included in the Self Update archive that was installed in [Installing the Connector](#).

To extract the installation file:

1. Determine the command required to export the adapter installation file. To do this, perform the following steps:
  - a. From the Setup menu in the Enterprise Manager console, select **Extensibility**, then **Self Update**.
  - b. Click on the **Management Connector** link.
  - c. Click on the **CASD connector** and then select **Export** from the Actions list.

A pop-up window appears with the command required to export the file. [Figure 5-1](#) shows an example of the window.

**Figure 5-1 Export Command Example**

- Open a command window on the Management Server host system and navigate to a temporary directory where you can copy the file.
- Log into EM CLI using the following command. You are asked to provide the password information for the sysman account.

```
emcli login -username=sysman
```

EM CLI must be executed from the OMS host. See the *Oracle Enterprise Manager Command Line Interface* for information about setting up EM CLI.

- Run the EM CLI `export_update` command from your system, changing `<dirname>` to the full path of the temporary directory.

This creates a zip file. The file name is comprised of the id value specified in the `export_update` command with a `.zip` extension. In the example command in [Figure 5-1](#), the zip file name would be:

```
E9F684312AE7A18E98340715D079E58D.zip
```

- Extract the adapter installation jar file from the zip file using the following command:

```
unzip *.zip archives/*connector.jar
```

- Extract the templates from the connector jar file using the following command:

```
$JAVA_HOME/bin/jar xf archives/*.jar templates
```

#### Note:

If the system where the connector file is located 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 template files after they have been extracted.

## 5.6 Adding Ticket Templates

If you want to create a custom template, you need to add ticket templates before they are recognized in Enterprise Manager. For each new custom template, run the following `emctl register_template connector` command as a user with execute privilege on `emctl` and the ability to read the ticket template:

```
$ORACLE_HOME/bin/emctl register_template connector  
-t <template.xml> -repos_pwd <reposPassword>
```

```
-cname <connectorName> -iname <internalName>  
-tname <templateName> -ttype 2 [-d <description>]
```

#### Where —

<template.xml> is the full path name of the template file.

<reposPassword> is the Enterprise Manager root (SYSMAN) password.

<connectorName> is the name of the connector instance installed in step 3 of [Creating a Connector Instance](#).

<internalName> is the internal name to use for the template.

<templateName> is the name to display for the template.

<description> is the description of the template.

For example, the following command adds a new outbound template (newTemplate.xml) for the connector instance:

```
emctl register_template connector  
-t /home/oracle/custom_templates/template.xml  
-repos_pwd sysmanpass  
-cname "CASD Connector Instance"  
-iname "newTemplate"  
-tname "New Template"  
-ttype 2  
-d "Demo template"
```

# 6

## Troubleshooting the Connector

This chapter provides information to assist you in troubleshooting integration issues with the CA Service Desk Connector. The connector cannot function unless the appropriate components have been installed and configured.

This chapter discusses the following topics:

- [Diagnosing the Problem](#)
- [Troubleshooting Adapter Startup Errors](#)
- [JVM Errors](#)
- [Troubleshooting Adapter Operations Errors](#)
- [Errors to Check](#)

Before you start the troubleshooting process, ensure that you have done the following:

1. Installed the CA Service Desk Connector as specified in [Installing the Connector](#).
2. Installed and tested the CASD Adapter as specified in [Installing the Adapter](#).
3. Configured the CA Service Desk Connector as specified in [Configuring the Connector](#).
4. Set up one or more notification rules as specified step 4 of [Automatically Creating a Ticket](#).

If all the actions above have been completed and the connector is not working, perform the steps in [Diagnosing the Problem](#).

### 6.1 Diagnosing the Problem

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 system where the CASD Adapter is installed. Perform the following steps to do this:
  - a. Perform the steps in the section entitled "[Using the Correct URL for CASD Adapter Operations](#)" in [Connector Tips](#) to determine the URL used by the CASD adapter.

#### Note:

If the adapter does not successfully complete the startup, see [Troubleshooting Adapter Startup Errors](#) to diagnose the problem.

- b. Open a browser and paste the URL from the previous step 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 system 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 host name for the URL will be *localhost*. Change localhost to the actual host name or IP address of the system where the CASD Adapter is installed. If you specify a host name, make sure that the host name is recognized at the Enterprise Manager server system. This can be done using the ping command.

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

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

The URL used at the Enterprise Manager server system 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 host name is not recognized at the Enterprise Manager system or there is a connectivity issue between the two systems. If you specified a host name, try using the IP address instead of the host name in the URL. If it still does 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.
  - a. Log into the Oracle Enterprise Manager console with an account that has Super Administrator permissions.
  - b. From the **Setup** menu of the Enterprise Manager console, select **Extensibility**, then **Management Connectors**.

The Management Connectors page appears, which shows the installed connectors.
  - c. Click on the **Configure** icon associated with the CA Service Desk Connector. This invokes edit mode, enabling you to configure the connector.
  - d. 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.

- e. Enter a valid ticket number in the Ticket Number field and click **OK**.
      - f. If everything is set up correctly, you will see the message *Connection test succeeded. The configuration was saved.*

4. If there is an error in step 3f, there is likely a configuration error in the CASD Adapter. See the section entitled [Troubleshooting Adapter Operations Errors](#) for information on diagnosing errors.

## 6.2 Troubleshooting Adapter Startup Errors

To identify the cause of a startup failure, navigate to the *adapters/log* directory in the CASD Adapter installation 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 [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 [Connector Tips](#).

2. There is an instance of the Adapter already running. If this is the case, no change is 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.

## 6.3 JVM Errors

The CASD Adapter requires version 1.6 of the JVM. If multiple versions of the JVM are installed on the system, 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 installation directory.
- Navigate to the *adapters/bin* sub-directory in the Adapter installation 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` sub-directory in the Adapter installation 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 system box, specify the path to the `jvm.dll` file in the Java 1.6 installation directory.
- Click **OK**.

## 6.4 Troubleshooting Adapter Operations Errors

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

1. Verify that the incident that was triggered is referenced in a notification rule that specifies one of the CA Service Desk Ticketing Templates.
2. Determine the error that Enterprise Manager has reported.

To do this, you need to examine the log file for errors. Perform the following steps to locate errors in the log file:

- a. Open the `emoms_pbs.trc` file in a text editor. The file is located in the log directory at the following location:

```
<EM_INSTANCE_BASE>/em/<OMS_NAME>/sysman/log/
```

... where `<EM_INSTANCE_BASE>` is the OMS instance base directory. By default, the OMS instance base directory is `gc_inst`, which is present under the parent directory of the Oracle middleware home.

For example, if the Oracle Middleware Home is:

```
/u01/app/Oracle/Middleware
```

... the instance base directory is:

```
/u01/app/Oracle/Middleware/gc_inst
```

... and the log and trace files are available in the following directory path:

```
/u01/app/Oracle/Middleware/gc_inst/em/EMGC_OMS1/sysman/log/
```

- b. Go to the bottom of the file and search backwards for "Caused by." Lines that start with "Caused by" contain error information. The error information appears after the text in the line that reads:

```
"oracle.sysman.emSDK.webservices.outbound.WSInvokeException: caught  
WebServiceException :"
```

3. Diagnose the problem based on the error information. See [Errors to Check](#) for information on troubleshooting common error events.

## 6.5 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.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target**

**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 Enterprise Manager keystore. The certificate is either missing from the keystore or does not match the SSL certificate provided by the CASD Adapter.

**Solution :** Verify that the CASD adapter has a valid SSL certificate, and that the certificate has been imported into the Enterprise Manager keystore.

The following instructions explain how to set up a certificate in the adapter and import the certificate into the Enterprise Manager keystore:

1. Install an SSL certificate in the adapter keystore. You must either install a self-signed certificate or install a certificate obtained from a Certificate Authority (CA).
  - To install a self-signed certificate, perform the steps specified in [Installing a Self-Signed Certificate](#).
  - To install a certificate from a CA, perform the steps specified in [Installing a Certificate from a Certificate Authority](#).
2. Restart the CASD adapter.
3. Import the SSL certificate from the adapter keystore into the Enterprise Manager keystore as documented in [Importing the Adapter Certificate into Enterprise Manager](#).

**javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Bad response: 404 Not Found from url**

**Cause :** The port number or the path in the URL is incorrect.

**Solution :** Perform the following steps to correct the URL:

1. Perform the steps in the section entitled "[Using the Correct URL for CASD Adapter Operations](#)" in [Connector Tips](#) to determine the URL used by the CASD adapter.
2. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator privileges.
3. From the **Setup** menu of the Enterprise Manager console, select **Extensibility**, then **Management Connectors**.  
The Management Connectors page appears.
4. Click on the name of the CA Service Desk Connector.  
This invokes edit mode, enabling you to configure the connector.



5. Change the URL for the createTicket, getTicket, and updateTicket operations to the URL identified in step 1.
6. Click **OK**.

**javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: Connection refused**

**Cause** : The host name/IP Address specified in the URL is valid, but not the system where CASD adapter is installed, or the CASD Adapter is down.

**Solution** : Verify that the host name/IP address configured for the connector is correct:

1. Determine the host name/IP address of the system where the CASD Adapter is installed.
2. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator privileges.
3. From the **Setup** menu of the Enterprise Manager console, select **Extensibility**, then **Management Connectors**.  
The Management Connectors page appears.
4. Click on the name of the CA Service Desk Connector.  
This invokes edit mode, enabling you to configure the connector.
5. Verify that the host name/IP address specified in the URL for the createTicket, getTicket, and updateTicket operations are correct.
6. If the host name/IP address is incorrect, correct the URL and click **OK**.

If the host name/IP Address is correct, 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.

**javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: Connection timed out**

**Cause** : A firewall is blocking access to the system where the CASD adapter is installed.

**Solution** : Contact your IT department to give Enterprise Manager access to the port the CASD adapter uses. Perform the steps in the section entitled "[Using the Correct URL for CASD Adapter Operations](#)" in [Connector Tips](#) to determine the URL used by the CASD adapter. The port number specified in the URL is the port number the IT department should open in the firewall.

**javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: hostname**

**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 with an account that has Super Administrator privileges.
  3. From the **Setup** menu of the Enterprise Manager console, select **Extensibility**, then **Management Connectors**.  
The Management Connectors page appears.
  4. Click on the name of the CA Service Desk Connector.  
This invokes edit mode, enabling you to configure the connector.
  5. Change the host name to the IP address in the URL specified for the createTicket, getTicket, and updateTicket operations.
  6. Click **OK**.

**javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: No route to host**

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

**Solution** : Verify that the host name/IP address configured for the connector is correct:

1. Determine the IP address of the system where the CASD Adapter is installed.
2. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator privileges.

3. From the **Setup** menu of the Enterprise Manager console, select **Extensibility**, then **Management Connectors**.

The Management Connectors page appears.

4. Click on the name of the CA Service Desk Connector.

This invokes edit mode, enabling you to configure the connector.

5. Verify that the host name/IP address specified in the URL for the createTicket, getTicket, and updateTicket operations are correct.
6. If the host name/IP address is 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.

#### **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 host name/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 the host name/IP address and the port number configured for the CA Service Desk Server are correct. Perform the following steps to determine the host name/IP address and port number configured for the CA Service Desk Server:
  - Navigate to the `adapters/conf` directory in the CASD Adapter installation 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 host name/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 installation 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 caud.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 installation directory.
2. Make a backup copy of the *framework.properties* file.
3. Enter the following command to change the password, where *<password>* is the new password to specify:

```
..\bin\propertiesEditor.bat -e caud.password=<password>  
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.

#### **AHD03301: This operation requires Function Access for Requests equal to View or Modify**

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

**Solution** : There are two 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 installation directory.
2. Make a backup copy of the *framework.properties* file.
3. Enter the following command to change the user name and password, where *<username>* is the new user name to specify, and *<password>* is the password for the new user:

```
..\bin\propertiesEditor.bat -e caud.username=<username> -e  
caud.password=<password> 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.

# 7

## Enabling SSL for HTTPS

This chapter provides the following procedures for configuring the CASD connector to use the HTTPS protocol:

- [Installing a Self-Signed Certificate](#)
- [Installing a Certificate from a Certificate Authority](#)
- [Importing the Adapter Certificate into Enterprise Manager](#)

### 7.1 Installing a Self-Signed Certificate

To generate and install a self-signed SSL certificate for the CASD adapter:

1. Open a command prompt window and change the working directory to the adapters/conf directory in the CASD adapter installation directory.
2. Execute the following command to delete the default SSL entry for the CASD adapter.
  - **Unix:**

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

```
"%JAVA_HOME%\bin\keytool" -delete -alias iwave -keypass iwavepw -storepass iwavepw -keystore keystore.jks
```
3. Enter the following command to generate a new certificate and place it in the adapter keystore. You will need to replace <hostname> with the host name or IP address of the system where the CASD adapter is installed.
  - **Unix:**

```
$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
```
  - **Windows:**

```
"%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
```

### 7.2 Installing a Certificate from a Certificate Authority

To request and install a signed SSL certificate for the CASD adapter:

1. Request a certificate for the CASD adapter from a Certificate Authority, such as VeriSign.

 **Note:**

In the certificate request, make sure to specify the host name or IP address of the system where the CASD adapter is installed. The host name in the certificate must match the host name or IP address the adapter uses. If they do not match, the adapter cannot function.

2. After you obtain the certificate from the Certificate Authority, perform the following steps to install the certificate:
  - a. Open a command prompt window and change the working directory to the adapters/conf directory in the CASD adapter installation directory.
  - b. Enter the following command to install the certificate, where <certificateFile> is the full path name of the file provided by the Certificate Authority:

- **Unix:**

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

- **Windows:**

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

## 7.3 Importing the Adapter Certificate into Enterprise Manager

To import the adapter SSL certificate into the Enterprise Manager keystore:

1. Open a command prompt window and change the working directory to the adapters/conf directory in the CASD adapter installation directory.
2. Enter the following command to extract the SSL certificate from the CASD adapter keystore and place it in the CASDws.cer certificate file:

- **Unix:**

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

- **Windows:**

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

3. Transfer the certificate file CASDws.cer to the system where Enterprise Manager is installed.
4. Append the contents of the CASDws.cer file to:

```
$INSTANCE_HOME/sysman/config/b64LocalCertificate.txt
```

- Only append the following lines to the b64LocalCertificate.txt file (that is, do not include blank lines or comments or any other special characters):

```
-----BEGIN CERTIFICATE-----  
<<<Certificate in Base64 format>>>  
-----END CERTIFICATE-----
```

5. Restart the OMS by entering the following commands:

```
emctl stop oms  
emctl start oms
```

 **Note:**

Do not run the `emctl secure oms/agent` command after adding the external certificate to the `b64LocalCertificate.txt` file. If you run the `emctl secure` command later, repeat steps 4 and 5 to make sure the external certificate exists in the `b64certificate.txt` file.



# 8

## Customizing Support Ticketing Inbound Operations

Ticketing Inbound is a new feature added in Enterprise Manager 12c. This feature synchronizes the ticket status between Service Desk and Enterprise Manager.

When a ticket or incident created by Enterprise Manager is updated manually at the Service Desk console, the new ticket status is updated in Enterprise Manager. The update at the Service Desk console triggers a notification method that calls the EM CLI utility to send the new status to Enterprise Manager.

This chapter provides the following procedures to set up the ticketing inbound feature:

- [Adding a Custom Field to CASD](#)
- [Setting Up EM CLI](#)
- [Installing the Notification Script](#)
- [Setting up Status Notification](#)
- [Exporting the Notification Script Files](#)
- [Uninstalling the Customization to CASD](#)
- [Uninstalling EM CLI](#)

### 8.1 Adding a Custom Field to CASD

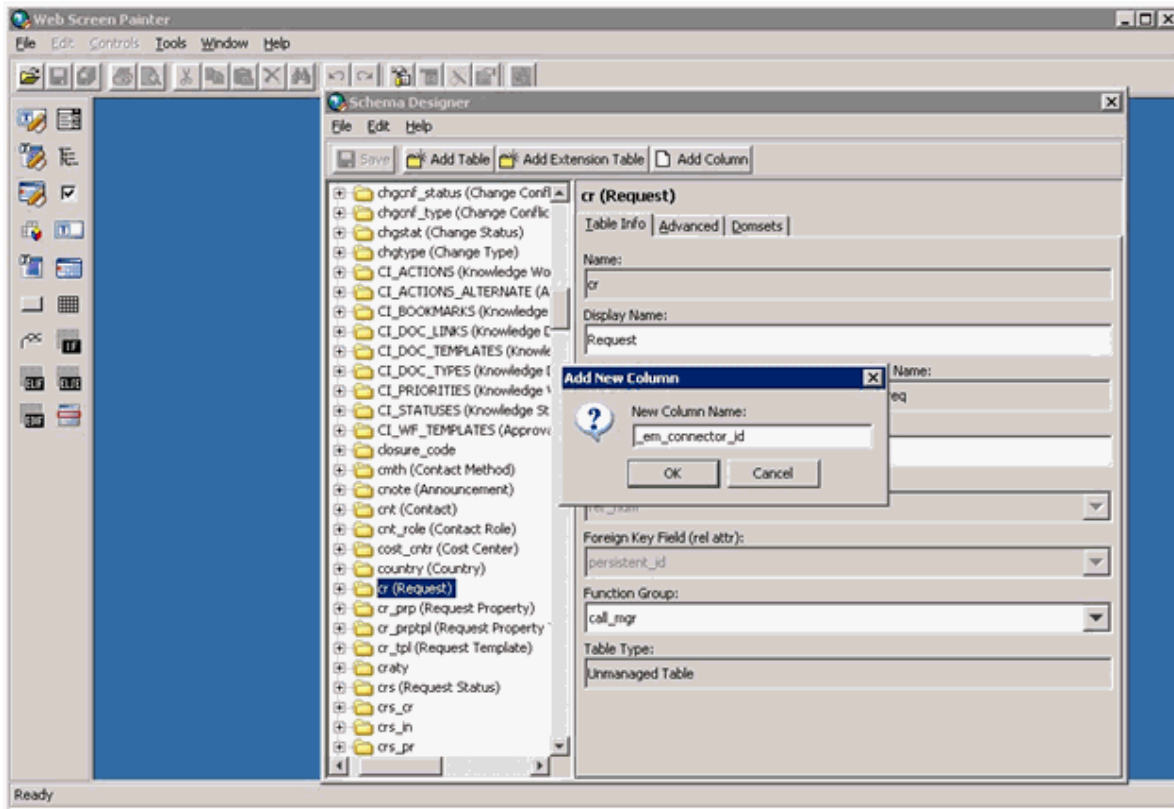
This section provides instructions to add a custom field to the CASD database schema to contain the Enterprise Manager connector identifier information. The identifier must be stored with the incident, because it is a required value that must be supplied when status updates are sent to Enterprise Manager.

To add the custom field:

1. Start the Web Screen Painter and log in using an account that has permission to update database schemas.
2. Select **Tools** from the menu, then **Schema Designer**.  
The Schema Designer window appears.
3. Scroll down through the list of tables, right-click on cr (Request), and select **Add Column**.

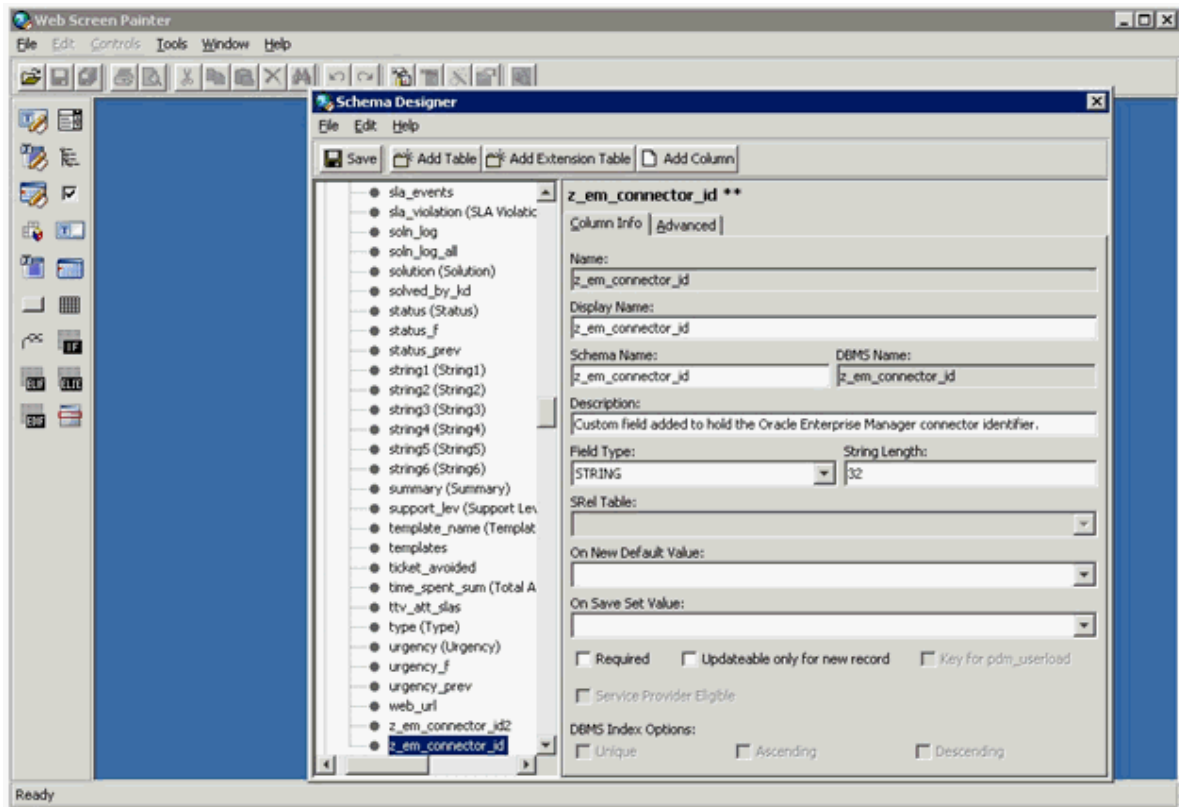
The Add New Column pop-up appears, as shown in [Figure 8-1](#).

Figure 8-1 Add New Column Window



4. Enter a column name of `_em_connector_id` and click **OK**.  
A form appears that contains the new column information.
5. Set the Field Type to `STRING` and the String Length to `32`. You can also optionally add a description.
6. Click **Save** after you have entered the information.  
[Figure 8-2](#) shows an example of a completed form.

Figure 8-2 Example of New Column Input



7. From the File menu, click **Save and Publish**.
8. Click **Yes** on the confirmation window when it appears.
9. Click **OK** on the informational window when it appears.
10. Stop the CA Server.
11. Run the pdm\_publish utility to publish the changes to the CA Server.
12. Start the CA Server.

## 8.2 Setting Up EM CLI

Install the Enterprise Manager EM CLI Client on the system where the CA Server is installed. The EM CLI Client will need to be able to communicate with your OMS.

To install the Enterprise Manager EM CLI Client:

1. Log into the Enterprise Manager console.
2. From the Setup menu, select **Command Line Interface**.
3. Click the **Download the EM CLI kit to your workstation** link, and download the .jar file to the CASD server.
4. At the CASD server, set your JAVA\_HOME environment variable and ensure that it is part of your PATH. You must be running Java 1.6.0\_25 or greater. For example:

```
setenv JAVA_HOME /usr/local/packages/j2sdk1.6.0_2
setenv PATH $JAVA_HOME/bin:$PATH
```

5. Install the EM CLI Client on the CASD server. You can install the client portion of EM CLI in any directory using the following command, where `<emcli_dir>` is the installation directory:

```
java -jar emclikit.jar client -install_dir=<emcli_dir>
```

6. Open a window using the account that runs the CA Server. On a Windows system, this should be the System account.

To open a window running the System account, run the following command with `<time>` being 1 minute in the future. At the time specified, a window opens at the system console running under the context of the System account.

```
at <time> /interactive cmd.exe
```

7. Run the following command to configure the EM CLI Client to connect to OMS, where `<hostname>` is the host name or IP address where the OMS server is located, and `<sysman_pwd>` is the password for the sysman account in OMS:

```
<emcli_dir>\emcli setup -url=https://<hostname>:7801/em -username=sysman -
password=<sysman_pwd>
```

8. Run the following command to synchronize the EM CLI Client with OMS:

```
<emcli_dir>\emcli sync
```

## 8.3 Installing the Notification Script

CASD calls the notification script whenever a status change occurs to call the EM CLI Client to send the status update to OMS. The script that is used depends on the platform of the CASD Server. On Windows platforms, the notification script is named `lferun.cmd`, and on Unix platforms the script is named `lferun.sh`. On Windows platforms, the `lferun.exe` and `send2em.cmd` files are also required.

All of the files are packaged in the `casd_notification.zip` file. Obtain a copy of this file from the Management Server host system as specified in [Exporting the Notification Script Files](#). To install the files, copy and unzip the `casd_notification.zip` file into any directory on the CASD Server system.

The following sections explain how to set up the scripts based on platform.

### Windows Platforms

1. Open the `lferun.cmd` file with a text editor. Set the `NOTIF_DIR` variable to the full path of the notification script, and then save the file.
2. Open the `send2em.cmd` file with a text editor. Set the `EMCLI_DIR` variable to the full path of the installation directory for the EM CLI Client, and then save the file.

### Unix Platforms

1. Open the `lferun.sh` file with a text editor. Set the `EMCLI_DIR` variable to the full path of the installation directory for the EM CLI Client, and then save the file.
2. Execute the following command to change the permissions on the script file:

```
chmod 755 ./lferun.sh
```

## 8.4 Setting up Status Notification

To configure CASD to call the notification script:

1. Log into the CASD console with an account that has Administrative permissions.
2. Click on the **Administration** tab and expand **Notifications**.
3. Click on **Notification Methods**, then click on **Create New**.

The Create New Notification Method window appears.

4. Enter information in the fields as shown in [Figure 8-3](#). The path in the Notification Method field should be the path where the notification script is installed.

 **Note:**

On Windows platforms, you must use double backslashes to separate directory names in the path.

Figure 8-3 Create New Notification Method Window

CA Service Desk Incident Go

Logged in as: ServiceDesk (Log Out) (Close Window)

File View Window Help

Create New Notification Method Save Cancel Reset

Symbol \* OracleEM

Record Status \* Active

Write to file

Description Spelling

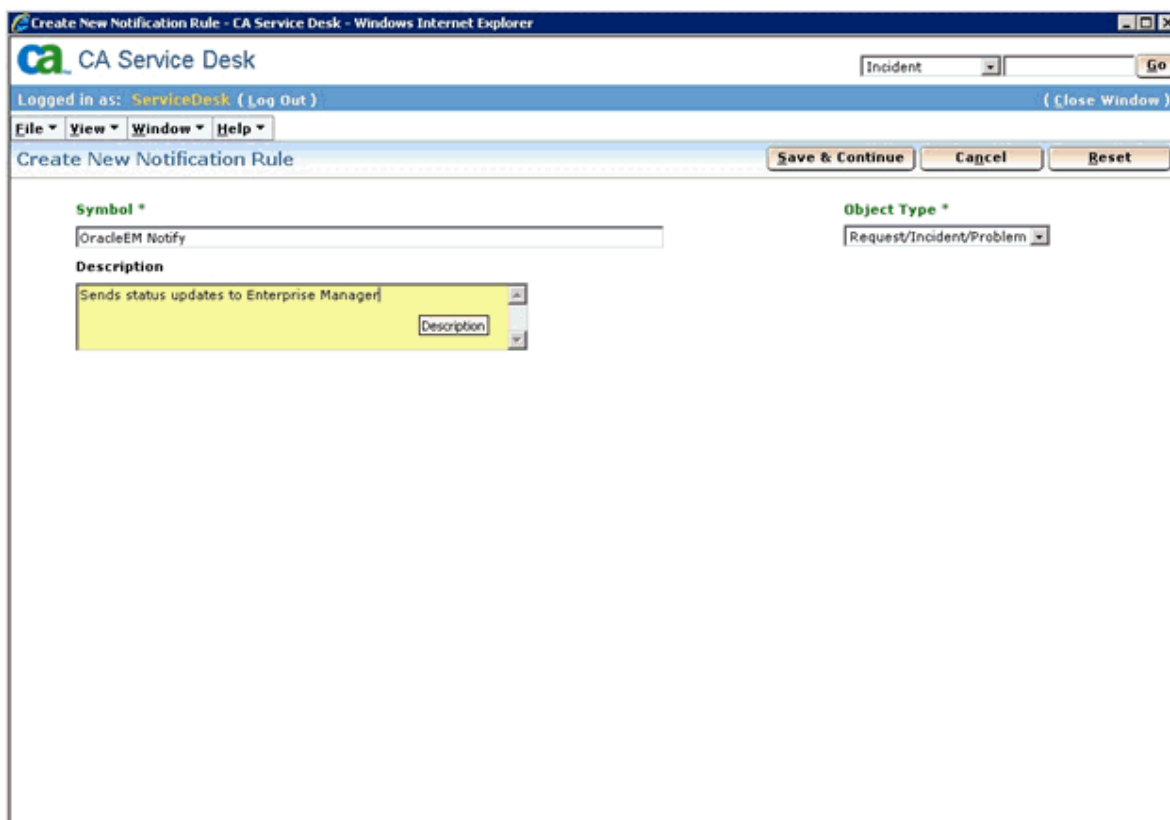
Send status updates to Oracle EM

Notification Method

C:\\EnterpriseManager\\NotificationScripts\\lferun.cmd

5. Click **Save**.
6. Click on **Notification Rules**, then click on **Create New**.  
The Create New Notification Rule window appears.
7. Enter information in the fields as shown in [Figure 8-4](#), then click **Save & Continue**.

Figure 8-4 Create New Notification Rule Window



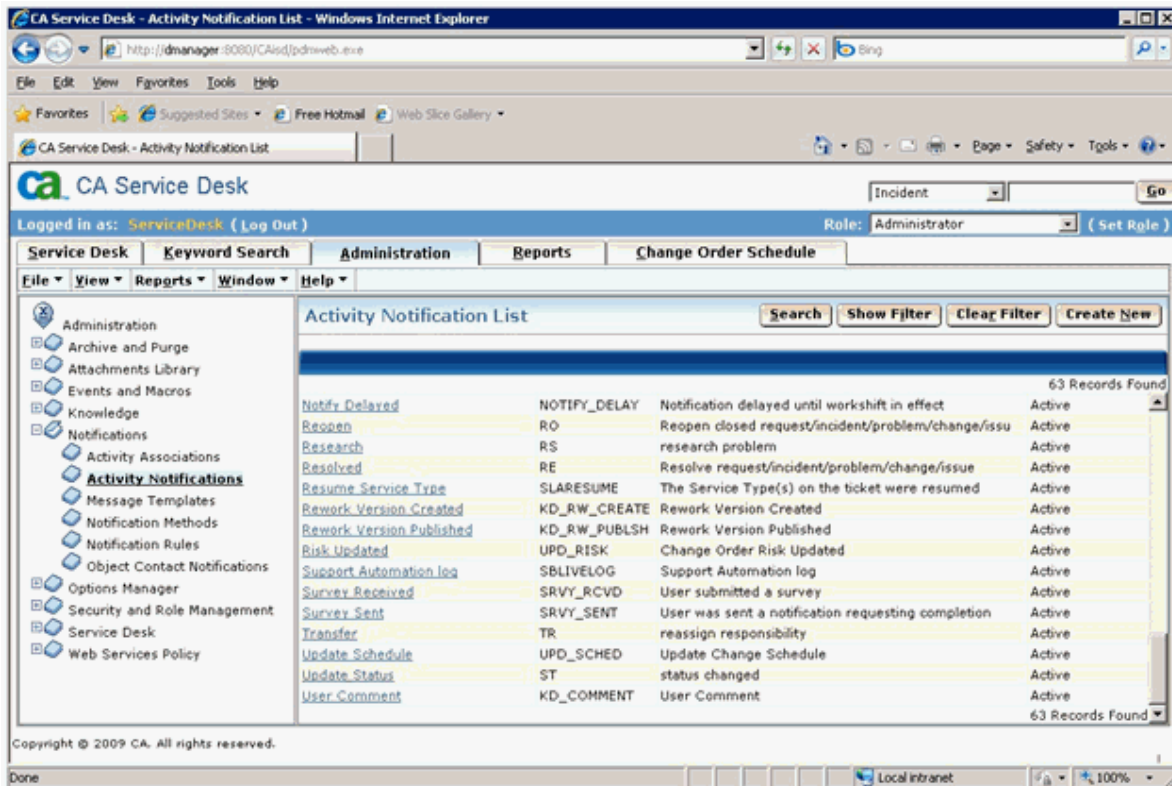
8. Select a Message Template of **Default Update Status message template for request/incident/problem** or any other appropriate template.

 **Note:**

It is imperative that the template selected has the Auto Notification set to Yes. If the template you want to use does not have it set to Yes, edit the template and check the Auto Notification check box.

9. Click on the **Contacts** tab, then click on **Update Contacts**.  
The Contact Search window appears.
10. Enter information for the account the CASD adapter uses exclusively, and click **Search** to retrieve the contact information.
11. Click on the account name in the left column, click on the >> button to move it to the right column, then click **OK**.
12. Click **Save** to save the new notification rule.
13. Click on **Activity Notifications** and find **Update Status** in the Activity Notification List. See [Figure 8-5](#) for an example of the Activity Notification List.

Figure 8-5 Activity Notification List



14. Click on **Update Status**, then click **Edit**.  
The Update Status Activity Notification Detail window appears.
15. Click on **Update Notification Rules**.  
The Notification Rules Search window appears.
16. Enter **OracleEM Notify** in the Symbol field and click **Search**.
17. Click on **OracleEM Notify** in the left column, click the >> button to move it to the right column, then click **OK**.  
The Update Status Activity Notification Detail window should appear.

## 8.5 Exporting the Notification Script Files

The notification script files are included in the Self Update archive that was installed in [Installing the Connector](#).

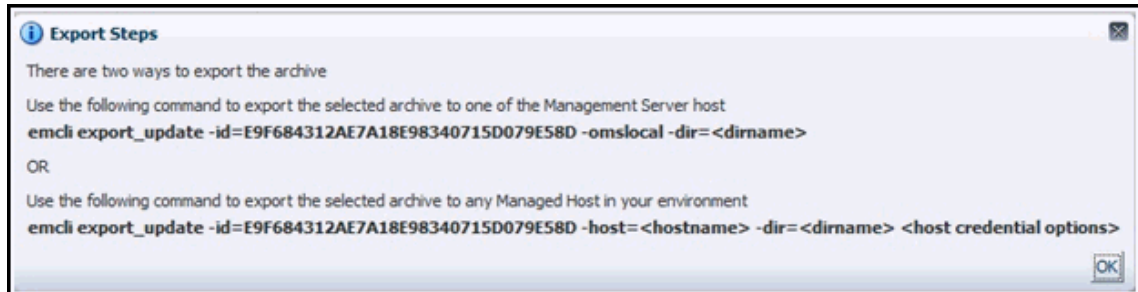
To extract the script files:

1. Determine the command required to export the archive files. To do this, perform the following steps:
  - a. From the **Setup** menu, select **Extensibility**, then **Self Update**.
  - b. Click on the **Management Connector** link in the Type column.  
The CASD connectors appear in the list with a status of Available.
  - c. Click on the CASD connector, then select **Export** from the Actions list.



A pop-up window, like the example shown in [Figure 8-6](#), appears with the command required to export the file.

**Figure 8-6 Export Command Example**



2. Open a command window on the Management Server host system and navigate to a temporary directory where you can copy and unzip the file.
3. Log into EM CLI using the following command. You will be asked to provide the password information for the sysman account.

```
emcli login -username=sysman
```

4. Run the EM CLI export\_update command from your system, changing <dirname> to the full path of the temporary directory.

This action creates a zip file. The file name is comprised of the id value you specify in the export\_update command with a .zip extension. In the example command in [Figure 8-6](#), the zip file name would be:

```
E9F684312AE7A18E98340715D079E58D.zip
```

5. Extract the adapter installation jar file from the zip file using the following command:

```
unzip *.zip archives/casd_notification.zip
```

## 8.6 Uninstalling the Customization to CASD

To uninstall changes made to CASD to allow for inbound ticketing operations, you must remove the notification method setup to call the notification script. Perform the following steps:

1. Log in to the CASD console with an account with Administrative permissions.
2. Click the **Administration** tab and expand **Notifications**.
3. Click **Message Templates** and select the **Default Update Status** message template for request/incident/problem or the template used for initial setup.
4. Click the **Contacts** tab, then click **Update Contacts**.
5. Click on the account name in the right column, and move it to the left column, then click **OK**.
6. Click **Save**.
7. Click **Activity Notifications** and find **Update Status** in the Activity Notification List.

8. Click **Update Status**, then click **Edit**.
9. Click **Update Notification Rules**.
10. Enter **OracleEM Notify** in the Symbol field and click **Search**.
11. Click **OracleEM Notify** in the right column and move it to the left column, then click **OK**.

## 8.7 Uninstalling EM CLI

To uninstall the Enterprise Manager command line interface (emcli) perform the following steps:

1. Navigate to the `emcli` installation directory.
2. Delete the `emcli` directory from the system.

# A

## Connector Tips

This appendix provides the following tips that might help you to use CA Service Desk Connector more effectively:

- [Recommended Protocol](#)
- [Supported Alerts](#)
- [Changing the Default Adapter Port](#)
- [Using the Correct URL for CASD Adapter Operations](#)

### A.1 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.

### A.2 Supported Alerts

This release supports the following types of alerts:

- Metric alerts
- Availability alerts

### A.3 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/notification framework.properties

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

The *propertiesEditor.bat* script is intended 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 with an account that has Super Administrator privileges.
2. From the Setup menu of the Enterprise Manager console, select **Extensibility**, then **Management Connectors**.  
The Management Connectors page appears.
3. Click on the name of the CA Service Desk connector.  
This invokes edit mode, enabling you to configure the connector.
4. Change the URLs listed in the Web Service End Points section to use the new port number.
5. Click **OK**.

## A.4 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.

### B.1 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/>."

### B.2 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.

## B.3 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.

## B.4 CXF Web Stack 2.2.3

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.5 Jetty Web Service Hosting 6.1.19

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.6 Quartz Scheduler 1.6

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.7 Apache Commons DBCP 1.2.2

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.8 Apache Commons Configuration 1.5

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.9 Jakarta Commons HTTP Client 3.1

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.10 Apache Commons Collection 3.2

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.11 Apache Derby Database 10.4.2

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.12 Log4j 1.2.14

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.13 Groovy 1.6.4

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.14 Apache Axis 1.4

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.15 JDOM 1.0

See the Apache License, Version 2.0 under [Spring Framework 2.5.6](#).

## B.16 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.

## B.17 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 routines 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.]



# Index

## I

---

install  
    offline mode, [2-4](#)

## O

---

offline mode, [2-4](#)

## W

---

web service  
    run as a Windows service, [2-12](#)