Oracle® Enterprise Manager

Connectors Installation and Configuration Guide

10*g* Release 4 (10.2.0.4)

E10323-06

August 2008

ORACLE®

Oracle Enterprise Manager Connectors Installation and Configuration Guide, 10*g* Release 4 (10.2.0.4)

E10323-06

Primary Author: Michael Zampiceni

Contents

3 Installing and Configuring the BMC Remedy Service Desk 7 Connector

4 Installing and Configuring the Siebel Connector

Index

Preface

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

Audience

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

You should already be familiar with Oracle Enterprise Manager.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Related Documents

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

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

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

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

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

Printed documentation is available for sale in the Oracle Store at

`http://oraclestore.oracle.com/`

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

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

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

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

Conventions

The following text conventions are used in this document:

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

1

Installing and Configuring the Microsoft Operations Manager Connector

The Microsoft Operations Manager Connector enables Oracle Enterprise Manager to send alerts to and retrieve alerts from Microsoft Operations Manager (MOM). The retrieved alerts are stored in the Enterprise Manager repository and displayed through the Enterprise Manager console.

This chapter provides the following information on setting up and configuring the MOM Connector:

1.1 Introduction to the MOM Connector

Connectors to MOM are bi-directional, meaning that you can send Enterprise Manager alerts to MOM as well as receive MOM alerts in Enterprise Manager. Beginning with Enterprise Manager 10g Release 4, you can send alerts to external systems in real time through Web services. For information about how to do this, see "Sending Enterprise Manager Alerts to MOM" on page 1-7.

Using a polling mechanism, the MOM Connector retrieves data through Web Services on HTTP and HTTPS protocols. The polling interval is user-definable, but cannot be shorter than 5 minutes. If an interval shorter than 5 minutes is defined, it defaults to 5 minutes.

The default `target_type` defined in Enterprise Manager is `mom_managed_host`. The retrieved alerts are stored in the default target instance `generic_mom_managed_host`. You can create more target instances based on your requirements. See "Configuring the MOM Connector" on page 1-3.

1.2 Prerequisites

Before using MOM Connector, ensure that the following pre-requisites are met:

- Microsoft Operations Manager 2005 is installed.
- MOM Connector framework Web services are enabled during the installation of MOM 2005.
- Internet Information Services (IIS) 6.0 or higher is deployed on the Windows server that hosts MOM.
- IP-based authentication is enabled on the Windows system that hosts MOM. See "Enabling IP-based Authentication" for the procedure.

> **See Also:** MOM 2005 Product Documentation at the following URL:
> http://www.microsoft.com/mom/techinfo/productdoc/default.mspx

1.3 Installing and Uninstalling the MOM Connector

The MOM Connector is installed as part of the Enterprise Manager base installation. After you install Enterprise Manager, you should see the MOM Connector listed on the Management Connectors page.

> **See Also:** *Enterprise Manager Grid Control Installation and Basic Configuration Guide* available at:
> http://www.oracle.com/technology/documentation/oem.html

After you install Enterprise Manager, when you access the Enterprise Manager console as a Super Administrator, you can see the MOM Connector in the Management Connector Setup page as shown in Figure 1–1. See "Configuring the MOM Connector" for instructions.

To uninstall the MOM Connector, select it in the Management Connectors page, then click **Delete**.

1.4 Re-registering Removed Connectors

The MOM Connector is automatically registered when Enterprise Manager is installed. However, you may remove this connector at some point and then want to subsequently re-register it.

To re-register a connector that has been removed:

1. From the Oracle Management Server (OMS) host command window, run the following `emctl` command from the `$ORACLE_HOME/bin` directory:

   ```
   emctl extract_jar connector <jarfile> <connectorTypeName> <OracleHome>
   ```

   The command replaces spaces with underscores in `<connectorTypeName>` and extracts the jar file to:

   ```
   $ORACLE_HOME/sysman/connector/<connectorTypeName_without_space/
   ```

   For example:

   ```
   emctl extract_jar connector momconnector.jar "Microsoft Operations Manager
   Connector" $ORACLE_HOME
   ```

This extracts the `.jar` file to this folder:

```
$ORACLE_HOME/sysman/connector/Microsoft_Operations_Manager_Connector/
```

2. Run the following `emctl` command from the `$ORACLE_HOME`/bin directory:

```
emctl register_connector connector <connectorType.xml> <server> <port>
<database sid> <username> <oracleHome>
```

For example:

```
emctl register_connector connector $ORACLE_HOME/sysman/connector/Microsoft_
Operations_Manager_Connector/MOMConnector.xml host.us.oracle.com 15041 EMREP
SYSMAN $ORACLE_HOME
```

> **Note:** For multiple Oracle Management Servers, you only need to register the connector once from any of the Oracle Management Servers.

1.5 Configuring the MOM Connector

1. From the Enterprise Manager console, click **Setup.**
2. Click the **Management Connectors** link in the left pane.

   The Management Connectors page appears. For the MOM Connector row, the Configured column should be blank (Figure 1–1).

   > **Note:** A check mark in the Configured column indicates that the Connector is already configured.

3. Click the **Configure** icon for the MOM Connector.

   The General tab of the Configure Management Connector page appears.
4. Provide the required settings. See "General Settings" on page 1-5 for details (Figure 1–2).
5. Click **OK.**
6. **Optional:** Go to the Targets tab and specify the details for creating additional target instances. See "Creating Additional Target Instances" on page 1-5 for details.
7. Click **OK.**

   The Management Connectors page reappears. The MOM Connector row should have a check mark in the Configured column.

   If you choose HTTPS as the protocol to establish a connection between MOM and Enterprise Manager, see "Enabling SSL for HTTPS" on page 1-10.

Figure 1–1 Management Connectors Page

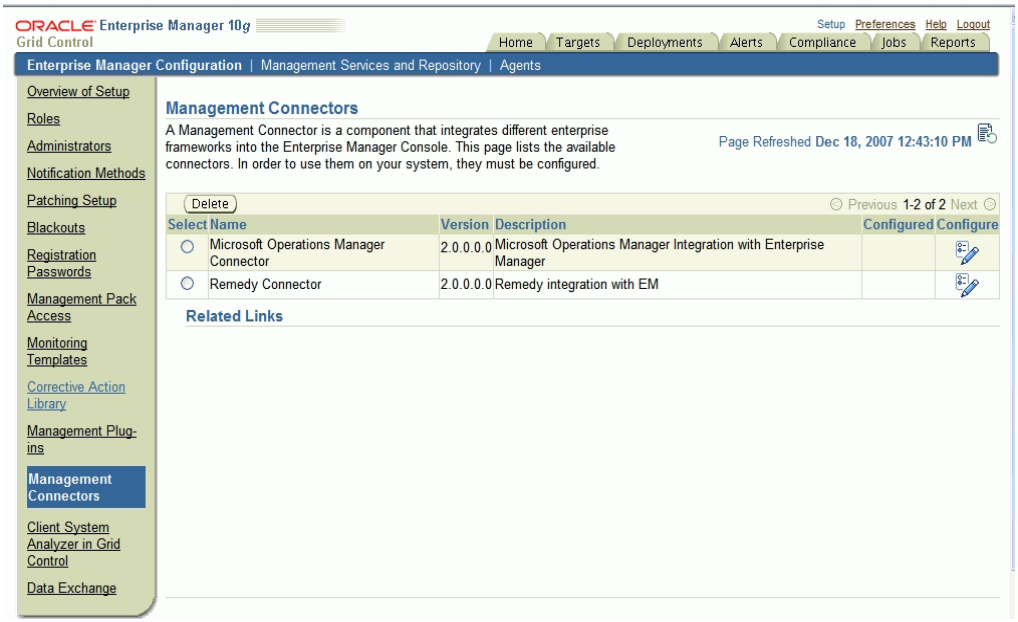
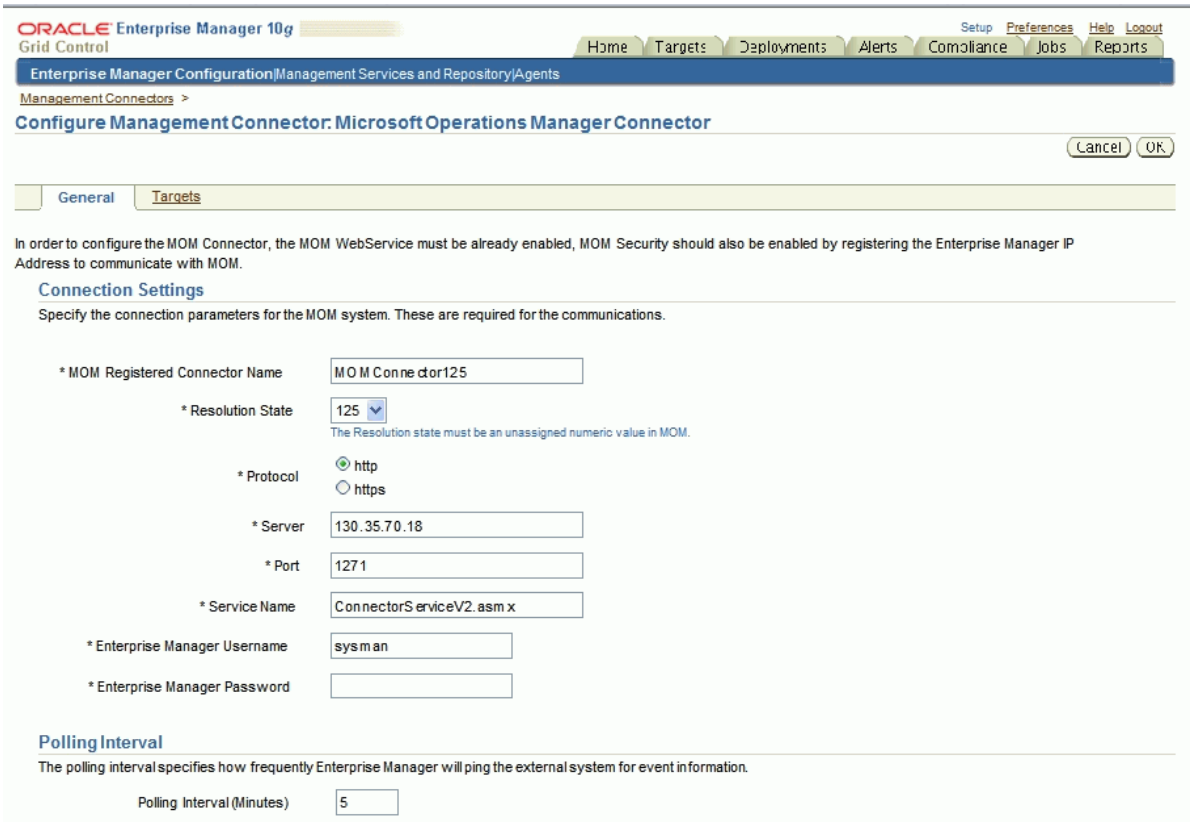


Figure 1–2 Configure Management Connector Page



1.5.1 General Settings

This section provides the communication details required for configuring the connector.

- **MOM Registered Connector Name —** Specify the connector name that you want to register with MOM. This is the name that the MOM administrator identifies for marking alerts to Enterprise Manager. This should be a unique name you set up within Enterprise Manager that identifies this connector.

  MOM Registered Connector Name is the connector name that appears in MOM as the name for the resolution state you specified when configuring the MOM Connector. For example, if you specify Microsoft Operations Manager Connector in this field and 218 as the Resolution State, you can see a resolution state called Microsoft Operations Manager Connector in MOM (when right-clicking on an alert and selecting the Set Resolution State menu). You can see that this resolution state corresponds to 218 in MOM from the administrator's console.

- **Resolution State —** Specify a value between 1 and 255. Make sure that you do not specify a value already in use, including the standard values such as 85 or 255. The default value for the MOM Connector is 218.

  To verify whether a value is currently being used, go the the MOM server's Administrator Console. On the left panel, find Microsoft Operations Manager, then select Administration, Global Settings, and then select Alert Resolution State on the right panel. Right-click this and select Properties. This displays a table with the first two columns named Resolution State, which is a string, and ID, which is a number from 0 to 255.

- **Protocol —** Select either HTTP or HTTPS based on the protocol the MOM Web services are running on.

- **Server —** Enter the IP address or the DNS name of the MOM server.

- **Port —** Enter the port number the MOM Web server uses. The default is 1271.

  For an HTTPS connection, you must change the port to the HTTPS port enabled in MOM.

- **Service Name —** Enter the MOM Web service name. The default is `ConnectorServiceV2.asmx`. In most cases, you need not change this.

- **Polling Interval —** Enter the time interval between event collections. The polling interval should not be shorter than 5 minutes. If you define an interval shorter than 5 minutes, it defaults to 5 minutes.

- **Enterprise Manager Username —** Enter the user name to be used to insert alerts; for example, `SYSMAN`. The user must have full privileges on the target of type MOM Managed Host.

  Administrator privileges are recommended; for instance, you should be a super user such as `SYSMAN`.

- **Enterprise Manager Password —** Enter a password for the user name you specified.

1.5.2 Creating Additional Target Instances

When you deploy or install a MOM Connector, a default target instance `generic_mom_managed_host` is created. In addition, you can create specific target instances.

An alert is assigned to the respective targets based on the computer name in MOM. If the name specified under `Computer` column in the MOM Operator console matches

the target name you specify in the `Target Name` column in the section "Targets Managed by External System (Optional)", the alert is assigned to this target. If the target does not exist, the alert is assigned to the default target instance.

In the Configure Management Connector page, click the **Targets** tab to create specific target instances. Figure 1–3 shows the Configure Management Connector Target page.

Default Connector Target

The default target instance holds external alerts that are not associated with any particular Enterprise Manager target. Oracle recommends that you do not remove this default connector target when you create additional targets.

If the default target is removed accidentally, you can recreate it by clicking the **Enable** button in the Targets tab of the Configure Management Connector page.

If the default target is removed for alerts that cannot be mapped to any target, error messages are logged in the file `emoms.log`.

Targets Managed by External System (Optional)

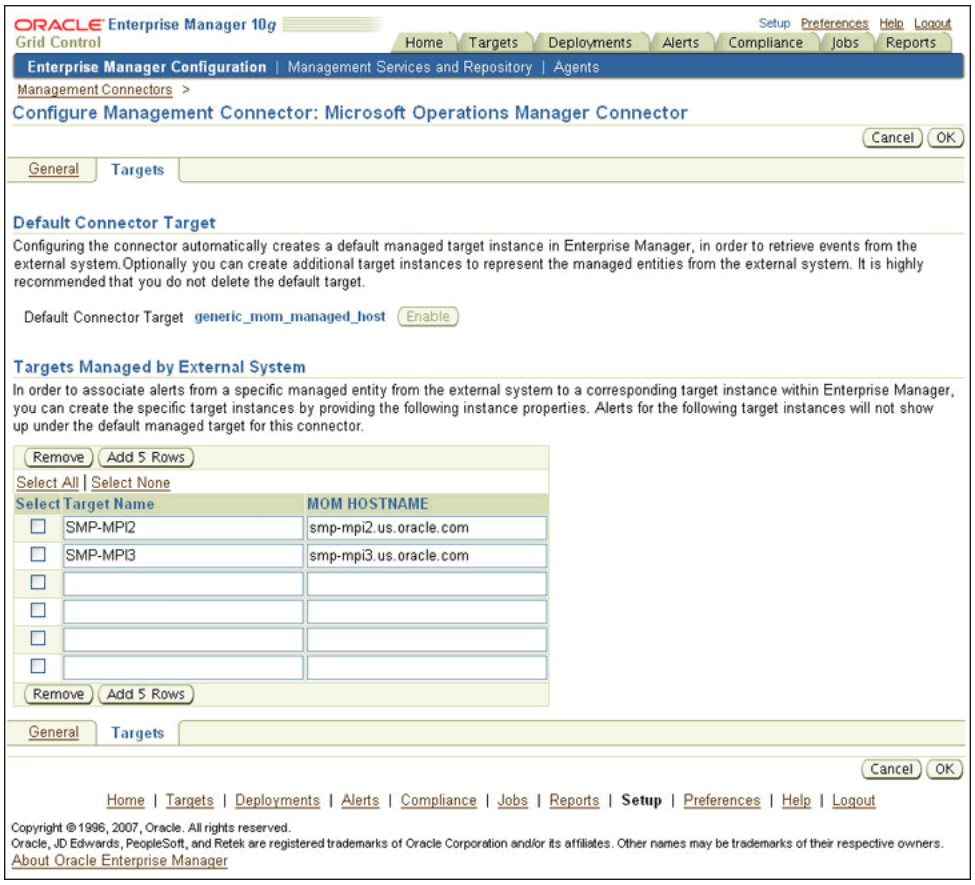
In this section, you can optionally create target instances and associate external alerts with these target instances.

To add a new target:

1. Specify the target name in the **Target Name** column.
2. In the **MOM HOSTNAME** column, specify the fully qualified hostname (hostname along with the domain name; for example, `smp-mpi2.us.oracle.com`) of the target.
3. Click **OK.**

Note: If you want to create more target instances, click **Add Rows** to add additional rows and then specify the target information. To remove a target, check the **Select** check box corresponding to the target, click **Remove,** then click **OK.**

Figure 1–3 Configure Management Connector Target Page



1.5.3 Response Status of Targets

The response status of `generic_mom_managed_host` asserts whether or not the MOM server is running. Immediately after registration, the status shows `Pending`.

After you configure the MOM Connector and the first event collection job runs (within a polling interval), the status shows either `Up` or `Down`. The response status of individual targets represent whether the host (represented by that target) is up or down.

When the target is created, Enterprise Manager pings the host. If the server is reachable, the status is marked `Up`. Subsequently, if Enterprise Manager receives any alerts (indicating that the host is down), it marks the target as `Down`.

If the target is down, the alert retrieval is interrupted until the target is up again.

Note: In Enterprise Manager, the response status of targets managed by MOM might not be definitive and can be used only for reference purposes. For accurate information of its managed entities, use MOM.

1.6 Sending Enterprise Manager Alerts to MOM

You can send Enterprise Manager alerts to MOM in real-time. You can also choose which type of alerts to send, such as critical alerts on a production database. Additionally, Enterprise Manager 10g Release 4 supports metric alerts.

1.6.1 Prerequisites

To send alerts, MOM needs to support the following:

- `"createEvent"` and `"updateEvent"` literal-document style Web services, as described in the section "Providing Deployment Descriptor Mappings" in the Oracle Enterprise Manager Connectors Integration Guide.
- IP-based or SOAP header-based authentication. For more information, see the "Building a Help Desk Connector" chapter in the Oracle Enterprise Manager Connectors Integration Guide.

1.6.2 Configuring Rules to Send Alerts

You need to configure rules for sending out alerts through the MOM connector as follows:

1. From the Grid Control console, click **Preferences** in the upper right corner. The General Preferences page appears.
2. In the menu at the left, click **My Rules**. The My Notification Rules page appears.
3. Select a rule, then click **Edit**. The Edit Notification Rule page appears.
4. Select the **Methods** sub-tab. The E-mail Notification page appears.
5. Select the **Microsoft Operations Manager Connector** advanced notification method, then click **OK**.
6. Repeat this process for each rule you want to set.

1.6.3 Migrating from 10.2.0.3 to 10.2.0.4

If you have already configured the MOM Connector in version 10.2.0.3 and want to upgrade to version 10.2.0.4, do the following to enable bi-directional capability:

1. From the Grid Control console, click **Setup** in the upper right corner. The Overview of Setup page appears.
2. In the menu at the left, click **Management Connectors**. The Management Connectors page appears.
3. Select **Microsoft Operations Manager Connector**, then click the **Configure** icon. The Configure Management Connector page for MOM appears.
4. Click **OK**. No other action is needed to enable bi-directional capability.

1.7 Receiving MOM Alerts in Enterprise Manager

The MOM Connector also enables you to forward MOM events to Enterprise Manager, thereby enabling better correlation of IT problems across the technology stack. You can specify when and how alerts should be triggered by configuring event rules in the Microsoft Operations Manager console. When an alert is raised, it is assigned a default resolution state that you specify. The MOM Connector creates a new resolution state specifically for the purpose of sending it across to Enterprise Manager.

1.7.1 Prerequisites

MOM needs to support the following literal-document style Web services:

- `"getNewAlerts"`

- "getUpdatedAlerts"
- "acknowledgeAlerts"
- "updateAlerts"

1.7.2 Forwarding Alerts to Enterprise Manager

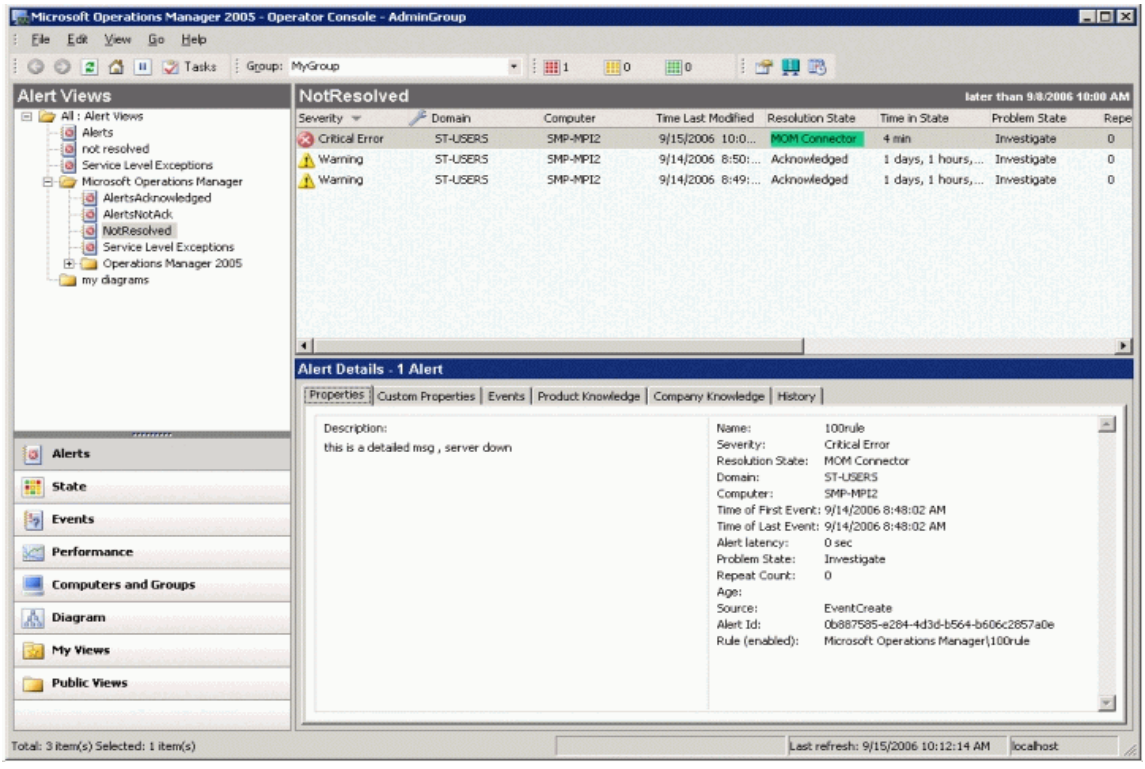
You can forward MOM alerts to Enterprise Manager automatically or manually as follows:

- Automatically forward alerts by specifying the connector resolution state in the event rules and alert rules.
- Manually forward any existing MOM event to Enterprise Manager by changing the resolution state of the alert.

Refer to the Microsoft Operations Manager guide for more details.

Figure 1–4 shows alerts in the Operator Console of Microsoft Operations Manager. The first alert has a Resolution State set to MOM Connector, which indicates that the alert is waiting to be forwarded to Enterprise Manager. When the polling job picks up the alert and forwards it to Enterprise Manager, the alert's resolution state returns to its original state.

Figure 1–4 Alert Forwarded to Enterprise Manager



1.7.3 How Enterprise Manager Responds

After the alerts have been forwarded to Enterprise Manager, they are associated with the appropriate targets, depending on the mapping option(s) you select. The MOM Connector keeps track of all the events forwarded from MOM, and automatically updates information in Enterprise Manager after changes in MOM occur. This ensures

that the two systems are always synchronized, providing you with timely information about your Microsoft environment.

1.8 Enabling SSL for HTTPS

Follow the instructions provided in this section if you choose HTTPS as the protocol to establish a connection between MOM and Enterprise Manager.

1.8.1 Generating a Certificate Request File

Generate a certificate request file from the MOM server by doing the following:

1. On the Windows task bar, go to **Start**, then click **Run.**
2. Type `inetmgr` in the **Open** field.

   The Internet Information Services (IIS) Manager screen appears.
3. In the left pane, navigate to **Web Sites** and select the **Microsoft Operations Manager 2005** connector framework.
4. Right-click and select **Properties.**

   The Microsoft Operations Manager 2005 Connector Framework Properties dialog box appears.
5. In the **Directory Security** tab, go to the **Secure Communications** section and click **Server Certificate.**
6. Using the wizard, create a new certificate.

   Note: When you specify details for certificate generation, do not use abbreviated forms for city and state names, as the wizard does not recognize abbreviations. For example, CA is not accepted for California.

   When the wizard completes, a `certreq.txt` text file is generated.
7. Send this request file to the Certificate authority, such as VeriSign.

1.8.2 Using the Certificate from the Certificate Authority

After processing your request, the certificate authority sends you the certificate. After you receive the certificate, do the following:

1. Paste the content into a text file.

   The content looks like the following:

```
-----BEGIN CERTIFICATE-----
MIICdzCCAV8CAQAwDQYJKoZIhvcNAQEEBQAwITELMAkGA1UEBhMCVVMxEjAQBgNVBAMMCXJvb3Rf
dGVzdDAeFw0wNjExMTAxMDI5MzJaFw0xNjExMDcxMDI5MzJaMGYxCzAJBgNVBAYTAlVTMQ4wDAYD
VQQIEwVUZXhhczEPMA0GA1UEBxMGRGFsbGFzMQ8wDQYDVQQKEwZvcmFjbGUxCzAJBgNVBAsTAkVN
MRgwFgYDVQQDEw9zbXAtbXBpMi1vcmFwa2kwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOch
GIHp6MFW78OQw/mSdU0xfVq5u9pgqndnTqoh4aGFg1bTZD6/Azf3Nn8ibtKVJmGp3PLa3xP/gk7S
tjZ/9sM4bvnw0Y4U9xsj0BiDG4JBo35uXAUxDHLReh8F4x45Wtv/SxvE0tjNnESlBMYynLip7P9l
fSzcGKjSViyFW9M9AgMBAAEwDQYJKoZIhvcNAQEEBQADggEBAIktFTvDs7ULf0PclYXsJPeK4vFq
7HZ86omktA9lYS+oA6SaudwDGY5yxcl9O2s78o+EK9e8Wz4wM4dmUg4aSuHVHWs75W86uh7gpEFo
wssH9mtcxkqIbdPVwQoeAUTVOifNaujfXtgClvlvOjkfzvvD7SieRjD9mP2rJ2pRWUbv7xR7oJmt
RXp6t22a+MKMQQR8ofAZV/WxFJcgmBR/JxLA28X+jnzmIH/yqHK/b6Agwwy7PgbJrwPI7WQ/busm
6ASeV8ZgSfAkJ83nWz4NICnH5Y8Dyu8vDtERsOQ8z/WttrBDEmcGikkO9P+o2Y9w1pEJQhh4bKtD
```

```
PyO9YLmlrLM=
-----END CERTIFICATE-----
```

2. Save the file as `cert.cer`.
3. On the Windows task bar, go to **Start**, then click **Run.**
4. Type `inetmgr` in the **Open** field.

   The Internet Information Services (IIS) Manager screen appears.
5. In the left panel, navigate to **Web Sites** and select the **Microsoft Operations Manager 2005** connector framework.
6. Right-click and select **Properties.**

   The Microsoft Operations Manager 2005 Connector Framework Properties dialog box appears.
7. In the Directory Security tab, go to the **Secure Communications** section, and click **Server Certificate.**
8. Add the certificate file to the server.

1.8.3 Adding Signed Certificates to Wallet Manager

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

1. Create a wallet using the `orapki utility` by entering the following command:

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

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

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

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

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

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

   Ensure that a file named `ewallet.p12` is available.
4. In the Oracle Wallet Manager, open the client certificate `ewallet.p12`.
5. Go to Select Trusted Certificates and select **Operations** on the main menu.
6. Select **Export All Trusted Certificates**.
7. Save the file as `certdb.txt`.
8. Place the `certdb.txt` in the connector home root directory (`$OMS_HOME/sysman/connector`).

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

Now Java SSL can use this file for communication between Enterprise Manager and the MOM server in HTTP mode.

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

1.9 MOM Connector Tips

The following sections provide various tips that might help you resolve issues you encounter while configuring or using the MOM Connector.

Enabling IP-based Authentication

The following procedure is only applicable if you have not already enabled IP-based authentication.

1. Open Inetmgr (Internet Information Services) in the system where the MOM server is running by doing the following:
   a. In Windows, select **Start**, then **Run**. The Run pop-up window appears.
   b. Type inetmgr, then click **OK**. The Internet Information Services (IIS) Manager window appears.
2. Expand the computer name (local computer), then expand the **WebSites** folder.
3. Select the **MOM 2005 Connector Framework**, then right-click and select **Properties**. The Framework Properties window appears.
4. Select **Directory Security**.
5. Set up the IP address as follows:
   a. In the "IP address and domain name restrictions" section, click **Edit**. The IP Address and Domain Name Restrictions window appears.
   b. Click **Add**. The Deny Access window appears.
   c. Enter the IP address where Enterprise Manager is located, then click **OK** to return to the Framework Properties window.
6. Set up authentication and access control as follows:
   a. In the "Authentication and access control" section, click **Edit**. The Authentication Methods window appears.
   b. Click the **Enable Anonymous Access** check box to enable it.
   c. Provide a user name and password that grant Administrator rights, then click **OK** to return to the Framework Properties window.
7. Click **OK** to save your settings and exit the Framework Properties window.
8. Restart the MOM server.

Recommended Protocol

Oracle recommends that you use HTTPS as the protocol for the communication between Enterprise Manager and MOM.

Use HTTP only if a secure connection is not required and the data can be transferred in clear text between the two systems.

For an HTTPS connection, you need to change the port to the HTTPS port enabled in MOM. Because Enterprise Manager polls data from MOM to Enterprise Manager, this means configuring MOM in HTTPS mode.

Connector Configuration Fails

If the connector configuration fails, ensure the following in the MOM Administrator Console:

- Resolution state is not already in use.
- Connector name is unique.

MOM Connector Fails to Retrieve Alerts

Ensure the following conditions if Enterprise Manager fails to retrieve alerts although the MOM server is marked for forwarding alerts:

- Valid resolution state is correctly marked.
- Connector is not accidentally disabled on the MOM server.
- Enterprise Manager user name and password that you specified in the MOM Configuration page are valid.

Alert Logging to Additional Target Instance Fails

Even if you define additional target instances, alerts are logged to the default target instance if the target name has characters with a case mismatch.

The target name is case-sensitive and therefore should match the case of the target name in Enterprise Manager.

Targets Added in the Same Transaction

You cannot delete and add the same target in the same transaction.

Polling Interval

The value of the polling interval is in minutes. The minimum value is 5 minutes. If you specify a shorter polling interval, it defaults to 5 minutes.

Alerts per Polling

The connector can process alerts up to twenty times the value of the polling interval at an instance. For example, if the Schedule Interval is 5, the maximum number of alerts retrieved is 100 (20*5). This is also the default value. This number need not be the same as the maximum number of alerts the connector is capable of requesting from MOM.

The maximum number of alerts the connector is capable of requesting from MOM depends on the number you specify in the files `generic_request_newalerts.xml` and `generic_request_updatedalerts.xml`. For example, if you have specified 100 (`<maxCount>100</maxCount>`), the connector can request up to 100 alerts at an instance. To optimize the network usage, Oracle recommends that you set the same maximum value for both the processing and the requesting capabilities.

Metric/Target Does Not Exist

- **Target**

  If the target does not exist, the alert is assigned to `generic_mom_managed_host`.

- **Metric**

  If the metric does not exist, Enterprise Manager creates one.

- **Generic MOM Target**

If the alert does not match any target and the generic MOM target (`generic_mom_managed_host`) does not exist, the alerts are discarded and a message is logged to the log file.

2

Installing and Configuring the Remedy Help Desk 6 Connector

The Remedy Connector integrates Remedy Help Desk 6.x with Enterprise Manager. Using this connector, you can create a Remedy trouble ticket, update an existing ticket, or close a ticket based on alerts in Enterprise Manager.

This chapter provides the following information for setting up and configuring the Remedy Connector:

2.1 Introduction to the Remedy Connector

The Remedy Connector integrates Enterprise Manager with Remedy Help Desk through either an HTTP or HTTPS connection. You can create, update, or close tickets based on only the following types of alerts in Enterprise Manager:

- Metric alerts
- Availability alerts (includes alerts for `Up, Down, Blackout Started, Blackout Ended, Agent Unreachable,Agent Unreachable Resolved, Metric Error Detected,` and `Mertic Error Resolved).`

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

2.1.1 Auto Ticketing

Whenever an alert is triggered in Enterprise Manager, the Remedy Connector can automatically open or update a ticket. You can specify the set of alerts for which tickets must be opened and the alert severity for which this should happen.

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

> **See Also:** "Configuring Notifications" in *Oracle Enterprise Manager Advanced Configuration Guide*

After the ticket is opened, any subsequent update of the alert, such as a change in alert severity, causes an annotation to the ticket. After you clear the alert (severity is set to `Clear`), you can optionally close the alert.

> **See Also:** "Automatically Creating a Trouble Ticket" on page 2-9

2.1.2 Manual Ticketing

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

> **See Also:** "Manually Creating a Trouble Ticket" on page 2-12

2.1.3 Ticket Templates

Ticket templates are transformation style sheets in XSLT format that transform Enterprise Manager alerts to ticket format before the requests are sent to Remedy Help Desk.

These template specify how Enterprise Manager alert attributes can populate the fields of a Remedy ticket. A ticket template helps in the mapping of Enterprise Manager Alert fields into Remedy ticket fields.

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

The Enterprise Manager installation includes some out-of-box ticket templates to facilitate easy usage of this feature.

> **See Also:** "Out-of-Box Templates" on page 2-15

2.1.4 Grace Period

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

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

For example, an alert triggers and a ticket is opened for it. If the grace period is one hour and the alert is cleared at 10:00 a.m., and if the same alert retriggers before 11:00

a.m. (one-hour grace period), the ticket that had been originally created for the alert is updated/reopened rather than creating a new ticket.

2.2 Prerequisites

Before using Remedy Connector, ensure that you meet the following prerequisites:

- Remedy HelpDesk 6.x is installed and configured.
- Remedy HelpDesk Web services are up and running. See "Web Service Details" on page 2-68.

2.3 Installing and Uninstalling the Remedy Connector

Remedy Connector is installed as part of the Enterprise Manager base installation. That is, Connector installation is part of the Oracle Management Server (OMS) installation.

After you install Enterprise Manager, when you access the Enterprise Manager console as a Super Administrator, you can see the Remedy Connector in the Management Connector Setup page as shown in Figure 2–1. See "Configuring the Remedy Connector" for instructions.

The default installation is based on default Remedy Web services that do not support any annotation history through `Worklog` (the history option in the Remedy ticket). For details of Worklog and registering the Worklog template, see "Using Worklog" on page 2-68.

To uninstall the Remedy Connector, select it in the Management Connectors page, then click **Delete**.

2.4 Configuring the Remedy Connector

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

   The Overview of Setup page appears.

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

   The Management Connectors page appears. For the Remedy Connector row, the Configured column should be blank (Figure 2–1).

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

3. Click the **Configure** icon for the Remedy Connector.

   The General tab of the Configure Management Connector page appears (Figure 2–2).

4. Provide the required settings. See "General Settings" for details.

5. Click **OK.**

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

6. **Optional:** To check for the available ticket templates, click the configure icon again.

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

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

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

Run the following command as a user with `execute` privilege on `emctl` and the ability to read the ticket template:

```
emctl register_ticket_template connector <ticketTemplate.xsl>
<server> <port> <database sid/service name for RAC DB>
<username> <password> <connectorTypeName> <connectorName>
<templateName> <description>
```

> **Note:** For multiple OMS installations, you need to run this command only once from any of the OMSs.

Example 2–1

```
emctl register_ticket_template connector Remedy_DefaultCategory_LowPriority.xsl
$emHost $dbPort $dbSID sysman $sysmanPwd "Remedy Connector" "Remedy Connector"
"Low Priority Template" "This template creates a ticket with low priority and
default categorization"
```

emctl Parameters

Table 2–1 emctl Parameters

Parameter	Description
`ticketTemplate.xsl`	Fully qualified name of the ticket template file. The file resides in the Connector home directory: `$OMS_HOME/sysman/connector/Remedy_Connector` Oracle recommends that you use intuitive names since there might be notification methods created with the same names and you have to choose one of them when you use the Auto Ticketing feature. Use `xsl` as the file extension, since the format is XSLT. For example, `Remedy_DefaultCategory_LowPriority.xsl`. If the file is in a different directory, provide the complete path for the file.
`server`	Host name of the Enterprise Manager repository.
`port`	Listener port of the repository.
`database sid/ Service Name for RAC DB`	Repository database instance ID or service name if you are using RAC database as the repository.
`username`	Specify `SYSMAN`.
`password`	Password for `SYSMAN`.
`connectorTypeName`	Specify `"Remedy Connector"`. The double quotes ("") are mandatory.
`connectorName`	Specify `"Remedy Connector"`. The double quotes ("") are mandatory.
`templateName`	An intuitive name for the ticket template that will be displayed in Enterprise Manager.

Table 2–1 (Cont.) emctl Parameters

Parameter	Description
`description`	A short description for the ticket template. This description is also displayed in Enterprise Manager.

If you choose HTTPS as the protocol to establish a connection between MOM and Enterprise Manager, see "Enabling SSL for HTTPS" on page 2-66.

Figure 2–1 Management Connectors Page

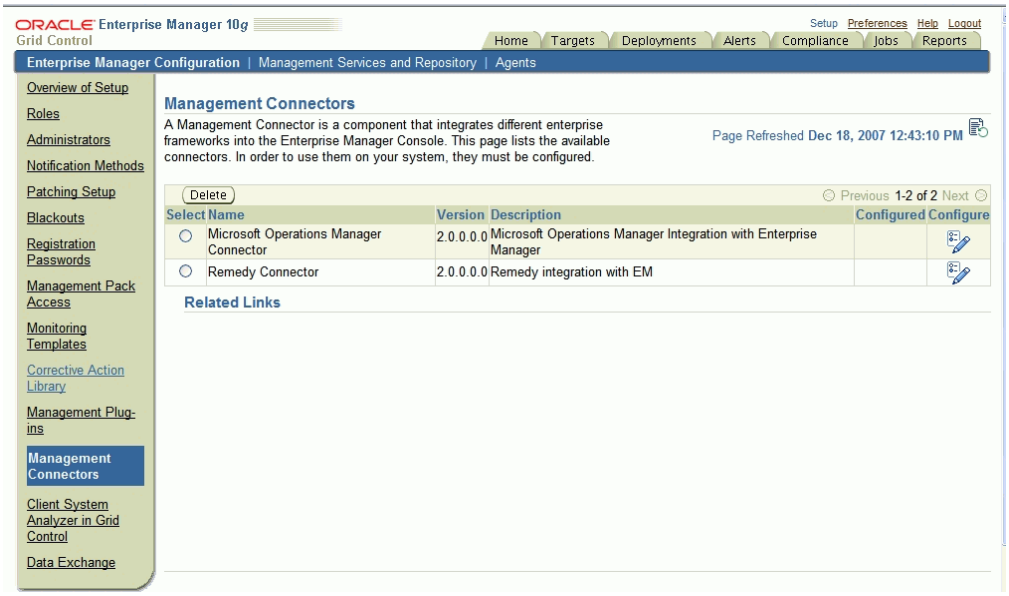
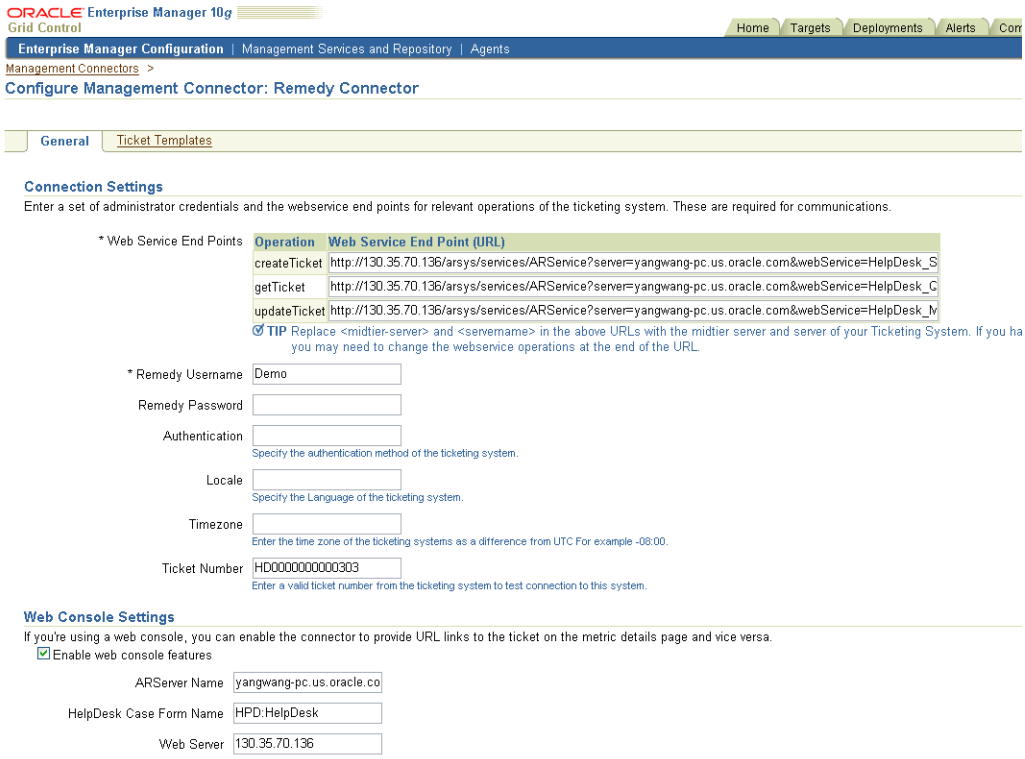


Figure 2–2 Configure Management Connector Page



2.4.1 General Settings

The following sections explain how to provide various configuration details.

2.4.1.1 Connection Settings

The Remedy Trouble Ticket connector communicates with the Help Desk through their Web services. Mandatory fields are indicated by an asterisk (*).

- **Web Service End Points** — End points to `createTicket`, `updateTicket`, and `getTicket` Web services exposed by Remedy Help Desk. See "Web Service Details" for additional details.

  If your Remedy installation does not have an operation to query a ticket by case ID, you need to import the `HelpDesk_Query_Service_By_Case_ID.def` file into your Remedy instance. This file is located here:

  `$ORACLE_HOME/sysman/connector/Remedy Connector`

- **Remedy Username** — User with the privilege to create, update, and query tickets in Remedy.
- **Remedy Password** — Password associated with the supplied Remedy user.
- **Authentication** — String that a Remedy administrator sets for additional security. Applies only if the Remedy Administrator has configured it on the Remedy AR

server. It communicates with the server if there is a secondary authentication server that can be used to verify the Remedy credentials.

- **Locale** — Language of the Remedy system (optional).
- **Time Zone** — Time zone of the Remedy AR System Server (optional).
- **Ticket Number** — Enter a valid ticket number if you want to test the connection when you save the configuration. There are four possibilities for this field:
  - If you do not enter a ticket number, no message appears on the Management Connectors page after you click OK and the configuration is saved.
  - If you specify the correct Web service end points and enter a valid ticket number, the following message appears on the Management Connectors page after you click OK:

    "Connection test succeeded. The configuration was saved."
  - If you have not previously saved the connector configuration and enter an invalid ticket number, the following message appears on the Management Connectors page after you click OK:

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

    "Connection test failed. The configuration was not saved."

    See Also: Section "Remedy User preferences settings" in the Remedy Remedy AR System Server product manual *Remedy Action Request System 6.3 - Developing AR System Applications: Advanced*

2.4.1.2 Web Console Settings

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

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

- **Enable web console** — Check this box to enable launching of the Remedy ticket page within context from Enterprise Manager.
- **ARServer Name** — Remedy AR Server name.
- **HelpDesk Case Form Name** — Remedy form name that the Remedy Web Services (you configured the connector to use) is based on. The Remedy default Help Desk Web services, for example, use the form HPD:HelpDesk.
- **Web Server** — The name or IP address of the server that hosts Remedy Mid-Tier.

2.4.1.3 Grace Period

You can enable and disable the grace period and configure its value. By default, the grace period is disabled. See "Grace Period" on page 2-2 for details. This setting applies to all alerts the Remedy Connector processes.

2.4.2 Working with Ticket Templates

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

2.4.2.1 Registering Ticket Templates

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

All registered ticket templates are displayed in the Configure Management Connector Ticket Templates page. By default, all out-of-box ticket templates are registered. To register additional ticket templates that you create, see step 7 in Section 2.4, "Configuring the Remedy Connector" on page 2-4.

> **See Also:** "emctl Parameters" on page 2-4

2.4.2.2 Viewing Template Code

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

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

2.4.2.3 Removing a Template

To remove a template, do the following:

> **Important:** If the template you delete has a notification rule associated with it, the notification fails.

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

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

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

2.4.2.4 Replacing Templates

To replace an existing ticket template, do the following:

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

2.4.2.5 Adding New Templates

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

> **See Also:** "Defining New Templates" on page 2-62

2.4.3 Re-registering Removed Connectors

The Remedy Connector is automatically registered when Enterprise Manager is installed. However, you may remove this connector at some point and then want to subsequently re-register it.

To re-register a connector that has been removed:

1. From the Oracle Management Server (OMS) host command window, run the following `emctl` command from the `$ORACLE_HOME/bin` directory:

   ```
   emctl extract_jar connector <jarfile> <connectorType.xml> <OracleHome>
   ```

   This extracts the `.jar` file to this folder:

   ```
   $ORACLE_HOME/sysman/connector/Remedy_Connector/
   ```

   For example:

   ```
   emctl extract_jar connector momconnector.jar "Remedy Connector" $ORACLE_HOME
   ```

2. Run the following `emctl` command from the directory `$ORACLE_HOME`:

   ```
   emctl register_connector connector <connectorType.xml> <server> <port>
   <database sid> <username> <oracleHome>
   ```

   For example:

   ```
   emctl register_connector connector $ORACLE_HOME/sysman/connector/Remedy_
   Connector/RemedyConnector.xml/host port database_SID username/$ORACLE_HOME
   ```

3. Perform step 7 in Section 2.4, "Configuring the Remedy Connector" on page 2-4.

> **Note:** For multiple Oracle Management Servers, you only need to register the connector once from any of the Oracle Management Servers.

2.5 Creating Remedy Trouble Tickets

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

2.5.1 Automatically Creating a Trouble Ticket

Perform the following steps to automatically create a trouble ticket:

1. Review the Out-of-Box Templates.
2. Select an appropriate ticket template with the desired mapping of Enterprise Manager alert fields to the Remedy ticket fields.
3. If you do not have a ticket template that satisfies your requirement, create one and register it.
4. Create a notification rule using the following steps:

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

   a. From the Enterprise Manager console, click **Preferences.**

b. In the left pane, under Notification, click **Rules,** then **Create**.

c. In the Create Notification Rule General page, specify the rule name, a description, and the targets for which this rule should apply.

d. In the Create Notification Rule Availability page, select the availability states for which you want to create tickets.

e. In the Create Notification Rule Metrics page, select the metrics and their associated alert severities for which you want to create and update tickets.

Ensure that you select all relevant alert severities if you want to update the ticket when the alert severity changes. For example, to open a ticket for a critical alert on the CPU Utilization(%) metric and the ticket is to be updated if the CPU Utilization(%) changes to warning or clear severity, in the notification rule select `Critical`, `Warning`, or `Clear` severities for the CPU Utilization(%) metric.

f. In the Create Notification Rule Methods page, choose the ticket template from the Advanced Notification Methods table (Figure 2–3).

In the table, registered ticket templates appear as Java Callback type notification methods under the same name as the ticket template's file name. This ticket template is used to open tickets for all availability and metric alerts specified in this notification rule.

This makes the ticket templates available for use to open tickets.

See Also: "Configuring Notifications" in *Oracle Enterprise Manager Advanced Configuration Guide*

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

- A notification is sent to the Remedy Connector when a metric alert triggers that matches your rule. The Remedy connector creates/updates a ticket according to the ticket template as set in the notification rule.
- The ticket is created or updated on the Remedy Trouble Ticket system.
- In Enterprise Manager, the alert annotation is updated. A comment is added to the Metric Details page of the alert to indicate that a ticket was created or updated, along with the ticket ID and ticket page URL.

A ticket is updated if there is an existing active ticket for an alert. In Figure 2–4, the first screen shows the ticket in Remedy console, and the second screen shows the alert as displayed in Enterprise Manager.

Figure 2–3 Notification Methods

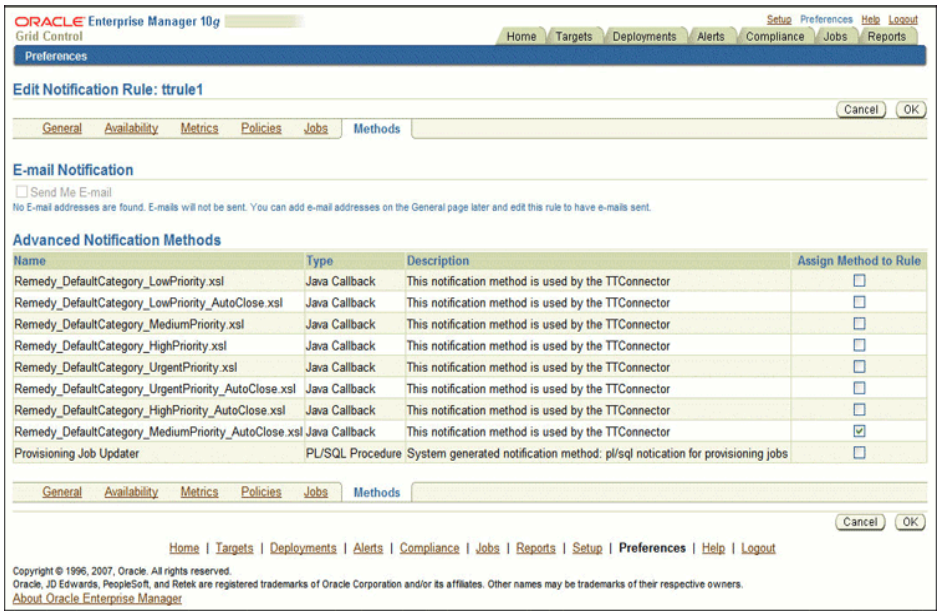
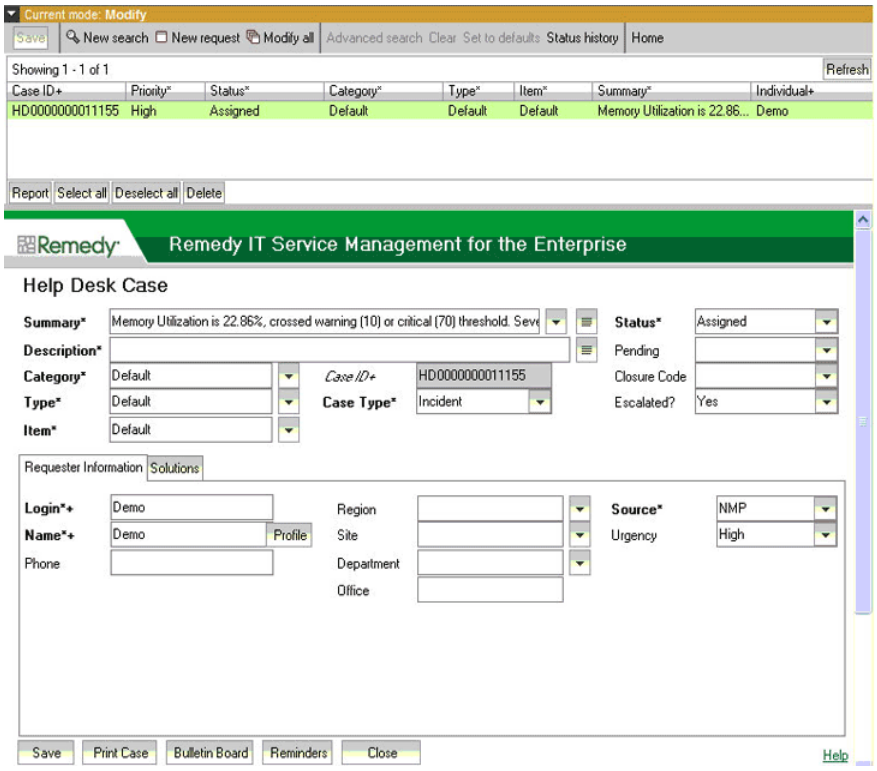
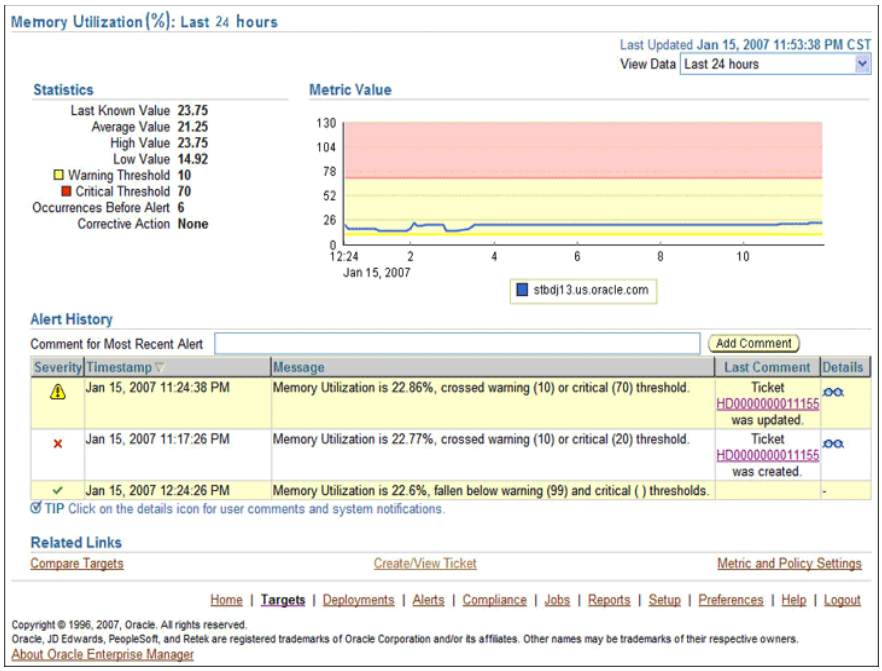


Figure 2–4 Remedy Ticket and the Alert as Displayed in Enterprise Manager





2.5.2 Manually Creating a Trouble Ticket

Perform the following steps to manually create a trouble ticket:

1. After a metric alert occurs, go to the associated metric details page for the alert. To access this page, click the alert message in the Enterprise Manager console (Figure 2–5).
2. Click the **Create/View Ticket** link in the Related Links section.

   The Create Ticket page appears if no active ticket exists for the alert.
3. Select a ticket template and then click **Submit** (Figure 2–6).

   If you do not see the desired template, you can register one using the `emctl` command. See "Registering Ticket Templates" on page 2-8.

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

   If the Web console settings are configured and enabled, the ticket ID appears as a link to the ticket page in the Remedy Help Desk. If there is no annotation, the ticket creation fails and error information is logged in the file `emoms.log`.

Note: You cannot manually update the ticket using Remedy Connector. You have to manually update the ticket in the Remedy AR server for any subsequent alert change.

Figure 2–5 Metric Details Page

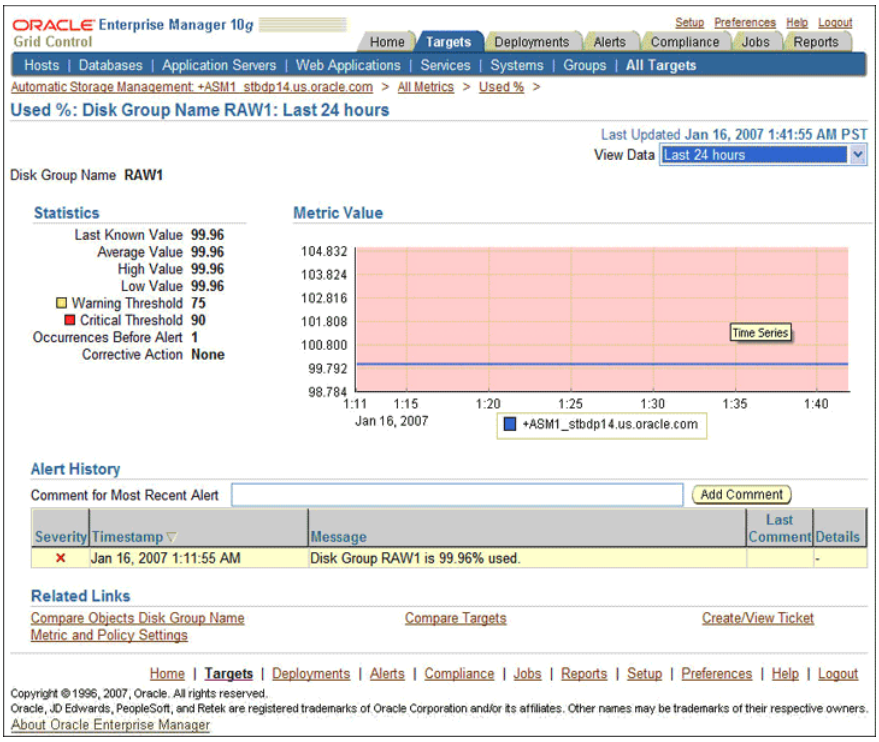
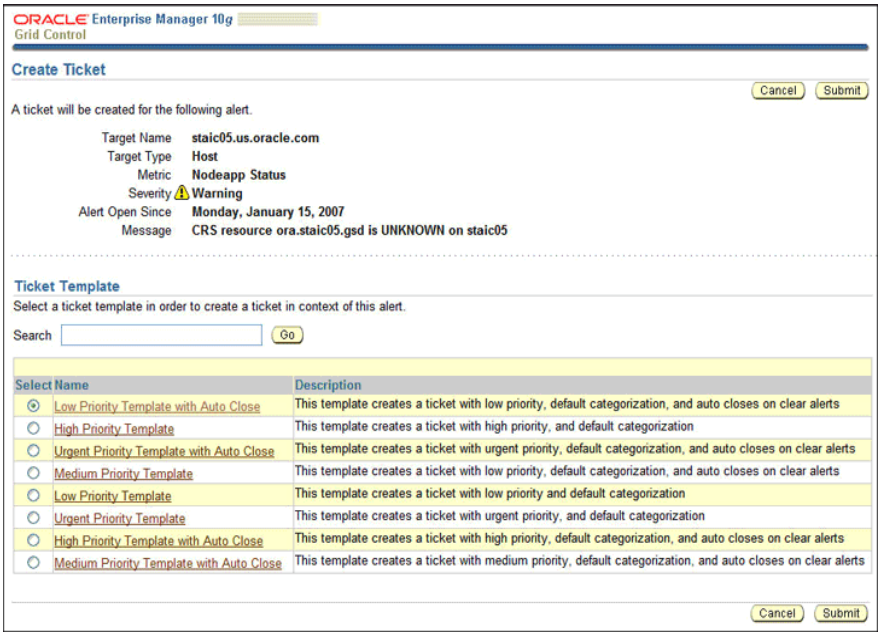


Figure 2–6 Create Ticket Page



2.6 Navigating Between Remedy and Enterprise Manager

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

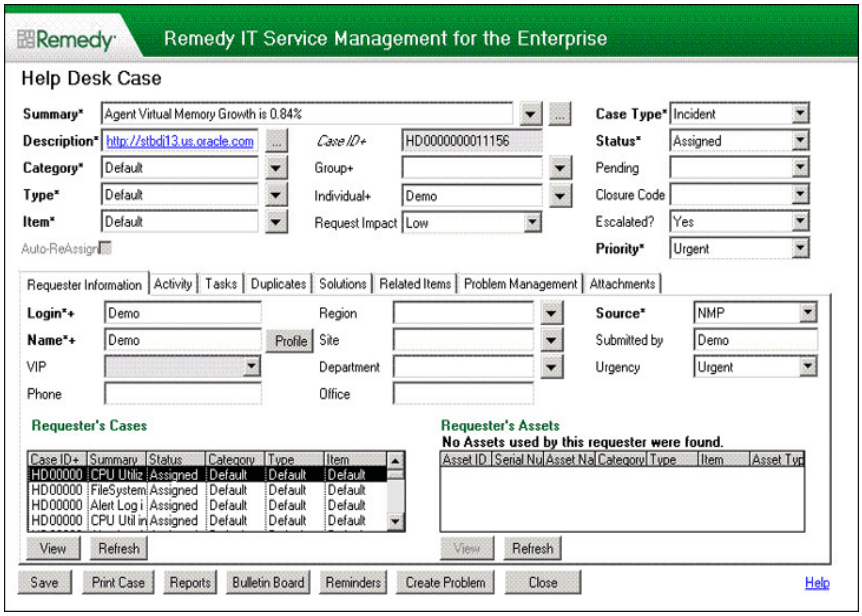
2.6.1 Navigating from Remedy to Enterprise Manager

From a ticket page, click the link in the **Description** field to the Alert Details page in the ticket message body (Figure 2–7). This takes you to the Enterprise Manager console login page. After you provide the Enterprise Manager user name and password, you are forwarded to the alert related to this ticket.

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

On the Remedy console, if the URL appears as text, you need to cut and paste the URL into the browser.

Figure 2–7 Alert Details in Remedy Console



2.6.2 Navigating from the Enterprise Manager to Remedy

1. In the Enterprise Manager console, click the alert message to go to the metric details page for the alert.
2. In the Alert History table, locate the ticket ID link in the Last Comment column.
3. (If not found) Click the icon in the Details column to get more information about the alert.
4. On the page that appears, locate the ticket ID in the Alert Details table.
5. Click the ticket ID link. You are forwarded to the Remedy Web console login page.
6. Provide valid Remedy account details.

The ticket page associated with this alert is displayed.

Note: If you do not use the Remedy Web console, uncheck the Enable web console option in the Web Console Settings section so that ticket ID is shown in plain text. Otherwise, it is displayed as a link that does not work.

2.7 Out-of-Box Templates

This section provides details on the out-of-box ticket templates shipped along with the Remedy Connector. The ticket templates specify the mappings between Enterprise Manager alert attributes and Remedy ticket attributes.

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

- Write alert information to `Description` (Remedy ticket description).
- Set the Remedy ticket summary based on the alert message. On update, the ticket summary field is updated to include the latest alert message information.
- Set the `Category`, `Item`, and `Type` fields in Remedy to the default.
- Set the `Priority` (ticket's priority) to the value indicated by the file name of the ticket template. For instance, `Remedy_DefaultCategory_HighPriority.xsl` sets the ticket priority to `High`.

Following are the out-of-box templates:

- `Remedy_DefaultCategory_LowPriority.xsl`
- `Remedy_DefaultCategory_MediumPriority.xsl`
- `Remedy_DefaultCategory_HighPriority.xsl`
- `Remedy_DefaultCategory_UrgentPriority.xsl`

Following are the out-of-box templates with the `AutoClose` suffixed to the file names. They set the ticket status to `Close` when the event severity value becomes `Clear`.

- `Remedy_DefaultCategory_LowPriority_AutoClose.xsl`
- `Remedy_DefaultCategory_MediumPriority_AutoClose.xsl`
- `Remedy_DefaultCategory_HighPriority_AutoClose.xsl`
- `Remedy_DefaultCategory_UrgentPriority_AutoClose.xsl`

Following are the out-of-box templates with `Wlog` suffixed to the file names. They are customized for the Web services with worklog enabled.

- `Remedy_DefaultCategory_LowPriority_w_Wlog.xsl`
- `Remedy_DefaultCategory_MediumPriority_w_Wlog.xsl`
- `Remedy_DefaultCategory_HighPriority_w_Wlog.xsl`
- `Remedy_DefaultCategory_UrgentPriority_w_Wlog.xsl`
- `Remedy_DefaultCategory_LowPriority_AutoClose_w_Wlog.xsl`
- `Remedy_DefaultCategory_MediumPriority_AutoClose_w_Wlog.xsl`
- `Remedy_DefaultCategory_HighPriority_AutoClose_w_Wlog.xsl`
- `Remedy_DefaultCategory_UrgentPriority_AutoClose_w_Wlog.xsl`

On update, the `Description` (Remedy ticket description) is updated with the latest event information, and the work log is updated with the latest severity and timestamp information.

2.7.1 Reading Ticket Templates

Table 2–2 and Table 2–3 illustrate the creation of a ticket using `Remedy_DefaultCategory_HighPriority_AutoClose.xsl`. This illustration will help you to read a ticket template. In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–2 Ticket Creation (Remedy_DefaultCategory_HighPriority_AutoClose.xsl Mappings)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser — Notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing.	Values from the alert context.
	TargetType	
	MetricColumn — Name of the metric, for example, CPU Utilization(%).	
	MetricName — Category of the metric. For the CPU Utilization(%) metric, this would be 'Load.	
	KeyColumn** — For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name.	
	KeyValues** — For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL — URL to the metric details page in the context of the alert.	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank

Table 2–2 (Cont.) Ticket Creation (Remedy_DefaultCategory_HighPriority_AutoClose.xsl Mappings)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Orig Submitter	HDUser	The user name that is provided in the "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		High*
Region		Blank
Request Urgency		High*
Requester Login Name	HDUser	The user name that is provided in the "Remedy Username" field during the configuration.
Requester Name	HDUser	
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–3 Ticket Updates (Remedy_DefaultCategory_HighPriority_AutoClose.xsl Mappings)

Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	▪ If severity is `Clear`, set the ticket to the status `Closed`. ▪ If the grace period test has already been done and the alert is still within the grace period, reopen the ticket by setting the ticket to the status `Assigned`.
Summary	Message, Severity	
Case ID	TicketId — The connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated.	

Remedy_DefaultCategory_HighPriority_AutoClose.xsl Source Code with Annotations

Use the mapping table (Table 2–2) as a reference to read the following XSLT file.

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

  <!--
  This template creates an incident type ticket with default categorization
  (Category: Default, Type:Default, Item:Default), and high priority. On update,
  the description and message fields are updated, and the ticket is closed if the
  associated alert has cleared.
  -->

  <xsl:template match="ns0:EventModel">
    <xsl:choose>
       <!-- Create the ticket if there is no ticket ID. -->
      <xsl:when test="normalize-space(ns0:TicketId) = ''">
        <urn:Create_Helpdesk_Case xmlns:urn="urn:HelpDesk_Submit_Service">

           <!-- EDIT THE TAG VALUES BELOW TO CHANGE HOW A TICKET IS FILLED
                DURING TICKET CREATION. REFER TO THE REMEDY HELPDESK MANUAL
                FOR DESCRIPTION OF THESE HELPDESK SUPPORT DATAFIELDS -->

        <urn:Case_Type>Incident</urn:Case_Type>
          <urn:Category>Default</urn:Category>
          <urn:Department></urn:Department>
          <urn:Description>
              Ticket created by EM Remedy Connector.
              -------------------------------------
              EM User: <xsl:value-of select="ns0:EMUser"/>

              Event Information:
              Target Type: <xsl:value-of select="ns0:TargetType"/>
              Metric Column: <xsl:value-of select="ns0:MetricColumn"/>
              Metric Name: <xsl:value-of select="ns0:MetricName"/>
              <xsl:choose>
              <xsl:when test="normalize-space(ns0:KeyColumn) != ''">
              Key Column: <xsl:value-of select="ns0:KeyColumn"/>
              Key Values: <xsl:value-of select="ns0:KeyValues"/>
              </xsl:when>
              </xsl:choose>
              Severity: <xsl:value-of select="ns0:Severity"/>
              Collection Time: <xsl:value-of select="ns0:CollectionTime"/>
              Target Host: <xsl:value-of select="ns0:TargetHost"/>
              <xsl:choose>
              <xsl:when test="normalize-space(ns0:NotificationRuleName) != ''">
              Notification Rule: <xsl:value-of select="ns0:NotificationRuleName"/>
              </xsl:when>
              </xsl:choose>
              URL: <xsl:value-of select="ns0:EventPageURL"/>
          </urn:Description>
          <urn:Escalated></urn:Escalated>
          <urn:Hotlist></urn:Hotlist>
          <urn:Item>Default</urn:Item>
          <urn:Office></urn:Office>
```

```
            <urn:Orig_Submitter>
              <xsl:value-of select="ns0:HDUser"/>
            </urn:Orig_Submitter>
            <urn:Pending></urn:Pending>
            <urn:Phone_Number></urn:Phone_Number>
            <urn:Priority>High</urn:Priority>
            <urn:Region></urn:Region>
            <urn:Request_Urgency>High</urn:Request_Urgency>
            <urn:Requester_Login_Name>
              <xsl:value-of select="ns0:HDUser"/>
            <urn:Requester_Login_Name>
              <xsl:value-of select="ns0:HDUser"/>
            </urn:Requester_Login_Name>
            <urn:Requester_Name>
              <xsl:value-of select="ns0:HDUser"/>
            </urn:Requester_Name>
            <urn:Site></urn:Site>
            <urn:Source>NMP</urn:Source>
            <urn:Status>New</urn:Status>
            <urn:Summary>
              <xsl:value-of select="ns0:Message"/>
            </urn:Summary>
            <urn:Type>Default</urn:Type>
            <urn:WorkLog></urn:WorkLog>
            <urn:Create_Time></urn:Create_Time>
          </urn:Create_Helpdesk_Case>
        </xsl:when>
        <!-- Update the ticket otherwise.. -->
        <xsl:otherwise>
          <urn:SetBy_Case_ID xmlns:urn="urn:HelpDesk_Modify_Service">
           <!--
                           UNCOMMENT THE TAGS YOU WISH TO HAVE MODIFIED WHENEVER THE
TICKET IS UPDATED, AND GIVE THEM DESIRED VALUES
            -->
            <!-- <urn:Accounting_Code></urn:Accounting_Code>           -->
            <!--  <urn:Assignee_Login_Name></urn:Assignee_Login_Name>  -->
            <!--  <urn:Case_Type></urn:Case_Type>                      -->
            <!--  <urn:Category></urn:Category>                        -->
            <!--  <urn:Department></urn:Department>                    -->
             <!--  <urn:Description></urn:Description>                            -->
             <!-- <urn:Escalated></urn:Escalated>                      -->
             <!-- <urn:Hotlist></urn:Hotlist>                          -->
             <!-- <urn:Item></urn:Item>                                -->
             <!-- <urn:Office></urn:Office>                            -->
             <!-- <urn:Pending></urn:Pending>                          -->
             <!-- <urn:Phone_Number></urn:Phone_Number>                -->
             <!-- <urn:Priority></urn:Priority>                        -->
             <!-- <urn:Region></urn:Region>                            -->
             <!-- <urn:Request_Urgency></urn:Request_Urgency>          -->
             <!-- <urn:Requester_Login></urn:Requester_Login>          -->
             <!-- <urn:Requester_Name></urn:Requester_Name>            -->
             <!-- <urn:Site></urn:Site>                                -->
             <!-- <urn:Solution_Description></urn:Solution_Description>-->
             <!-- <urn:Solution_Summary></urn:Solution_Summary>        -->
             <!-- <urn:Source></urn:Source>                            -->
             <xsl:choose>
               <xsl:when test="ns0:Severity = 'Clear'">
                 <urn:Status>Closed</urn:Status>
               </xsl:when>
               <xsl:when test="ns0:GracePeriodCheckMade = 'Yes'">
```

```
              <urn:Status>Assigned</urn:Status>
            </xsl:when>
          </xsl:choose>
          <!-- <urn:Submitted_By></urn:Submitted_By>                -->
          <urn:Summary>
            <xsl:value-of select="ns0:Message"/> Severity:<xsl:value-of
select="ns0:Severity"/>
          </urn:Summary>
          <!-- <urn:Type></urn:Type>                                 -->
          <urn:Case_ID>
            <xsl:value-of select="ns0:TicketId"/>
          </urn:Case_ID>

        </urn:SetBy_Case_ID>
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:transform>
```

2.7.2 Mapping the Fields

The tables in this section map the fields in all out-of-box ticket templates shipped with the Remedy Connector.

Remedy_DefaultCategory_LowPriority.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–4 Ticket Creation (Remedy_DefaultCategory_LowPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*

Table 2–4 (Cont.) Ticket Creation (Remedy_DefaultCategory_LowPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser — Notification rule owner when the ticket is created through auto-ticketing, and is the Enterprise Manager log-in user when the ticket is created through manual-ticketing. TargetType MetricColumn — Name of the metric, for example, CPU Utilization(%). MetricName — Category of the metric. For the CPU Utilization(%) metric, this would be Load. KeyColumn** — For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is Tablespace Name. KeyValues** — For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity. Severity CollectionTime TargetHost NotificationRuleName EventPageURL — URL to the metric details page in the context of the alert.	Values from the alert context.
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The user name provided in the "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		Low
Region		Blank
Request Urgency		Low

Table 2–4 (Cont.) Ticket Creation (Remedy_DefaultCategory_LowPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Requester Login Name	HDUser	The user name provided in the "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The user name provided in the "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context.
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–5 Ticket Updates (Remedy_DefaultCategory_LowPriority.xsl)

Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	If the grace period test has already been done, and the alert is still within the grace period, reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Summary	Message, Severity	The alert message in context with the severity appended.
Case ID	TicketId — The connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated.	

Remedy_DefaultCategory_MediumPriority.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–6 Ticket Creation (Remedy_DefaultCategory_MediumPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser — Notification rule owner when the ticket is created through auto-ticketing, and is the Enterprise Manager log-in user when the ticket is created through manual-ticketing. TargetType MetricColumn — Name of the metric, for example, CPU Utilization(%). MetricName — Category of the metric. For CPU Utilization(%) metric, this would be 'Load. KeyColumn** — For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name. KeyValues** — For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity. Severity CollectionTime TargetHost NotificationRuleName EventPageURL — URL to the metric details page in context of the alert.	Values from the alert context.
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The user name provided in the "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		Medium
Region		Blank

Table 2–6 (Cont.) Ticket Creation (Remedy_DefaultCategory_MediumPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Request Urgency		Medium
Requester Login Name	HDUser	The user name provided in the "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The user name provided in the "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context.
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–7 Ticket Updates (Remedy_DefaultCategory_MediumPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	If the grace period test has already been done and the alert is still within the grace period, reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Summary	Message, Severity	The alert message in context with the severity appended.
Case ID	TicketId — The connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated.	

Remedy_DefaultCaterogry_HighPriority.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–8 Ticket Creation (Remedy_DefaultCaterogry_HighPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*

Table 2–8 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_HighPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for theTablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		High
Region		Blank
Request Urgency		High

Table 2–8 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_HighPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Requester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–9 Ticket Updates (Remedy_DefaultCaterogry_HighPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Summary	Message, Severity	The alert message in context with the severity appended.
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCaterogry_UrgentPriority.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–10 Ticket Creation (Remedy_DefaultCaterogry_UrgentPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*

Table 2–10 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_UrgentPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for theTablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		Urgent
Region		Blank
Request Urgency		Urgent

Table 2–10 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_UrgentPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Requester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–11 Ticket Update (Remedy_DefaultCaterogry_UrgentPriority.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Summary	Message, Severity	The alert message in context with the severity appended.
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Following are the templates with the `AutoClose` suffixed to the file names. They set the ticket status to `Close` when the event severity value becomes `Clear`:

Remedy_DefaultCaterogry_LowPriority_AutoClose.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–12 Ticket Creation (Remedy_DefaultCaterogry_LowPriority_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		Low
Region		Blank
Request Urgency		Low

*Table 2–12 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_LowPriority_*

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Requester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–13 Ticket Update (Remedy_DefaultCaterogry_LowPriority_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	▪ If severity is `Clear`, then set the ticket to the status `Closed`. ▪ If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Summary	Message, Severity	The alert message in context with the severity appended.
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCaterogry_MediumPriority_AutoClose.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–14 Ticket Creation (Remedy_DefaultCaterogry_MediumPriority_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType, EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values from the alert context.
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.

*Table 2–14 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_MediumPriority_*

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Pending		Blank
Phone Number		Blank
Priority		Medium
Region		Blank
Request Urgency		Medium
Requester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–15 Ticket Updates (Remedy_DefaultCaterogry_MediumPriority_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	▪ If severity is `Clear`, then set the ticket to the status `Closed`. ▪ If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Summary	Message, Severity	The alert message in context with the severity appended.

*Table 2–15 (Cont.) Ticket Updates (Remedy_DefaultCaterogry_MediumPriority_*

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCaterogry_HighPriority_AutoClose.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–16 Ticket Creation (Remedy_DefaultCaterogry_HighPriority_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values from the alert context.
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank

*Table 2–16 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_HighPriority_*

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		High
Region		Blank
Request Urgency		High
Requester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–17 Ticket Updates (Remedy_DefaultCaterogry_HighPriority_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	▪ If severity is `Clear`, then set the ticket to the status `Closed`. ▪ If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.

*Table 2–17 (Cont.) Ticket Updates (Remedy_DefaultCaterogry_HighPriority_*

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Summary	Message, Severity	The alert message in context with the severity appended.
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCategory_UrgentPriority_AutoClose.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–18 Ticket Creation (Remedy_DefaultCategory_UrgentPriority_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank

*Table 2–18 (Cont.) Ticket Creation (Remedy_DefaultCategory_UrgentPriority_*

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		Urgent
Region		Blank
Request Urgency		Urgent
Requester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log		Blank
Create Time		Blank

Table 2–19 Ticket Updates (Remedy_DefaultCategory_UrgentPriority_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Status	Severity	▪ If severity is `Clear`, then set the ticket to the status `Closed`. ▪ If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Summary	Message, Severity	The alert message in context with the severity appended.
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Following are the templates with `Wlog` suffixed to the file names. They are customized for the worklog `Web_service`.

On update, the `Description` (Remedy ticket description) is updated with the latest event information, and the work log is updated with the latest severity and timestamp information.

Remedy_DefaultCategory_LowPriority_w_Wlog.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–20 Ticket Creation (Remedy_DefaultCaterogry_LowPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*

Table 2–20 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_LowPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values from the alert context.
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		Urgent
Region		Blank
Request Urgency		Urgent
UrgentRequester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.

Table 2–20 (Cont.) Ticket Creation (Remedy_DefaultCaterogry_LowPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log	Severity, CollectionTime	The alert severity and collection time in context.
Create Time		Blank

Table 2–21 Ticket Updates (Remedy_DefaultCaterogry_LowPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values of the alert in context
Status	Severity	If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Worklog	Severity, CollectionTime	The values in context
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated).	

Remedy_DefaultCategory_MediumPriority_w_Wlog.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–22 Ticket Creation (Remedy_DefaultCategory_MediumPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values from the alert context.
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		Medium
Region		Blank

*Table 2–22 (Cont.) Ticket Creation (Remedy_DefaultCategory_MediumPriority_w_*

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Request Urgency		Medium
UrgentRequester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log	Severity, CollectionTime	The alert severity and collection time in context.
Create Time		Blank

Table 2–23 Ticket Updates (Remedy_DefaultCategory_MediumPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values of the alert in context
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Status	Severity	If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Worklog	Severity, CollectionTime	The values in context
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCategory_HighPriority_w_Wlog.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–24 Ticket Creation (Remedy_DefaultCategory_HighPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		High
Region		Blank
Request Urgency		High

Table 2–24 (Cont.) Ticket Creation (Remedy_DefaultCategory_HighPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
UrgentRequester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log	Severity, CollectionTime	The alert severity and collection time in context.
Create Time		Blank

Table 2–25 Ticket Updates (Remedy_DefaultCategory_HighPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values of the alert in context
Status	Severity	If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Worklog	Severity, CollectionTime	The values in context
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCategory_UrgentPriority_w_Wlog.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–26 Ticket Creation (Remedy_DefaultCategory_UrgentPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		Urgent
Region		Blank
Request Urgency		Urgent

*Table 2–26 (Cont.) Ticket Creation (Remedy_DefaultCategory_UrgentPriority_w_*

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
UrgentRequester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
	Default*	
Type		
Work Log	Severity, CollectionTime	The alert severity and collection time in context.
Create Time		Blank

Table 2–27 Ticket Updates (Remedy_DefaultCategory_UrgentPriority_w_Wlog.xsl)

Remedy Ticket Attributes	Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values of the alert in context
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Status	Severity	If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Worklog	Severity, CollectionTime	The values in context
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCategory_LowPriority_AutoClose_w_Wlog.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–28 Ticket Creation (Remedy_DefaultCategory_LowPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank

Table 2–28 (Cont.) Ticket Creation (Remedy_DefaultCategory_LowPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Priority		Low
Region		Blank
Request Urgency		Low
UrgentRequester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log	Severity, CollectionTime	The alert severity and collection time in context.
Create Time		Blank

Table 2–29 Ticket Updates (Remedy_DefaultCategory_LowPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values of the alert in context
Status	Severity	▪ If severity is `Clear`, then set the ticket to the status `Closed`. ▪ If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Worklog	Severity, CollectionTime	The values in context
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCategory_MediumPriority_AutoClose_w_Wlog.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–30 Ticket Creation (Remedy_DefaultCategory_MediumPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank

Table 2–30 (Cont.) Ticket Creation (Remedy_DefaultCategory_MediumPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Priority		Medium
Region		Blank
Request Urgency		Medium
UrgentRequester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log	Severity, CollectionTime	The alert severity and collection time in context.
Create Time		Blank

Table 2–31 Ticket Updates (Remedy_DefaultCategory_MediumPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values of the alert in context
Status	Severity	▪ If severity is `Clear`, then set the ticket to the status `Closed`. ▪ If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Worklog	Severity, CollectionTime	The values in context

Table 2–31 (Cont.) Ticket Updates (Remedy_DefaultCategory_MediumPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCategory_HighPriority_AutoClose_w_Wlog.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–32 Ticket Creation (Remedy_DefaultCategory_HighPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank

Table 2–32 (Cont.) Ticket Creation (Remedy_DefaultCategory_HighPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank
Priority		High
Region		Blank
Request Urgency		High
UrgentRequester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log	Severity, CollectionTime	The alert severity and collection time in context.
Create Time		Blank

Table 2–33 Ticket Updates (Remedy_DefaultCategory_HighPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load) KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values of the alert in context
Status	Severity	■ If severity is `Clear`, then set the ticket to the status `Closed`. ■ If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Worklog	Severity, CollectionTime	The values in context
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

Remedy_DefaultCategory_UrgentPriority_AutoClose_w_Wlog.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 2–34 Ticket Creation (Remedy_DefaultCategory_UrgentPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Case Type		"Incident"*
Category		"Default"*
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing)	Values from the alert context.
	TargetType	
	MetricColumn (name of the metric, for example, CPU Utilization(%))	
	MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load)	
	KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name)	
	KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if USERS tablespace triggered at warning or critical severity.)	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL (URL to the metric details page in context of the alert)	
Escalated		Blank
Hotlist		Blank
Item		"Default"*
Office		Blank
Orig Submitter	HDUser	The username that is provided in "Remedy Username" field during the configuration.
Pending		Blank
Phone Number		Blank

Table 2–34 (Cont.) Ticket Creation (Remedy_DefaultCategory_UrgentPriority_AutoClose_w_Wlog.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Priority		Urgent
Region		Blank
Request Urgency		Urgent
UrgentRequester Login Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Requester Name	HDUser	The username that is provided in "Remedy Username" field of the Connection Settings configuration.
Site		Blank
Source		NMP* (Network Management Program)
Status		New*
Summary	Message	The alert message in context
Type		Default*
Work Log	Severity, CollectionTime	The alert severity and collection time in context.
Create Time		Blank

Table 2–35 Ticket Updates (Remedy_DefaultCategory_UrgentPriority_AutoClose)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Description	EMUser (notification rule owner when the ticket is created through auto-ticketing, and is the EM log-in user when the ticket is created through manual-ticketing) TargetType MetricColumn (name of the metric, for example, CPU Utilization(%)) MetricName (Category of the metric. For CPU Utilization(%) metric, this would be 'Load') KeyColumn** (For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name) KeyValues** (For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyValues is 'USERS' if USERS tablespace triggered at warning or critical severity.) Severity CollectionTime TargetHost NotificationRuleName EventPageURL (URL to the metric details page in context of the alert)	Values of the alert in context
Status	Severity	▪ If severity is `Clear`, then set the ticket to the status `Closed`. ▪ If the grace period test has already been done, and the alert is still within the grace period, then reopen the ticket by setting the ticket to the status `Assigned`; otherwise, leave the status as it is.
Worklog	Severity, CollectionTime	The values in context
Case ID	TicketId (the connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated)	

2.7.3 Customizing Ticket Templates

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

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

Example 2–2 Marking a Category to MyCategory

To create a template to mark the category to `MyCategory`, modify the following attribute in the template:

```
<urn:Category>MyCategory</urn:Category>
```

Example 2–3 Altering the Message Type

If you only want the alert message to appear as ticket summary instead of both message and severity, modify the following attribute:

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

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

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

2.7.4 Defining New Templates

The out-of-box templates are based on the HPD:HelpDesk form. If the new ticket templates you define are based on the HPD:HelpDesk form, Customizing Ticket Templates applies.

However, if you use a custom Remedy Form, such as HPD:CustomHelpDesk, you need to define a new ticket template.

Enterprise Manager Attributes

Table 2–36 provides the Enterprise Manager fields that you can map when using the default Remedy Help Desk Web services:

Table 2–36 Enterprise Manager Attributes

Data Fields	Description
EMUser	▪ For auto-ticketing, this is the notification rule owner. ▪ For manual ticketing, this is the console user that triggered the ticket creation.
HDUser	Help desk user registered with the Connector; this is same as the user name specified for the WS authentication.
TicketID	Identifies the ticket associated with the current alert (available after ticket creation).
ConnectorID	Identifies the connector that processed the event and issued the ticket creation or ticket update. This is the ID for Remedy Connector.
TargetType	Type of target that the alert is associated with, such as `host`.

Table 2–36 (Cont.) Enterprise Manager Attributes

Data Fields	Description
TargetName	Name of the target that the alert is associated with. For example, `Database1` or `stadc40.us.oracle.com`.
MetricColumn	Name of the metric that triggered the alert. For example, CPU Utilization(%).
MetricName	Category of the metric. For example, `Load` for the memory utilization alert.
KeyColumn	For metrics that monitor a set of objects, the KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespaceobjects, the KeyColumn is 'Tablespace Name'.
KeyValues	Key values associated with a key value base alert. For metrics that monitor a set of objects, the KeyValues indicates the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.
Message	Description of the alert. For example, CPU Utilization is 100%, crossed warning (80) or critical (95) threshold.
Severity	Severity of the alert: `critical, warning, clear,` or `down.`
CollectionTime	Timestamp of an alert occurrence.
EventPageURL	URL to the alert details page of the alert.
NotificationRuleName	Name of the notification rule that generated the notification during auto-ticketing.
TargetTimezone	Timezone of the target associated with the alert.
GracePeriodCheckMade	Value `Yes` indicates that the alert is cleared since the last update or creation, but is within the configured grace period.
TargetHost	Name of the server hosting the target that generated the alert.

The following XML schema describes the model that contains the attributes above:

Example 2–4 XML Schema for Attributes

```
<?xml version="1.0" encoding="US-ASCII" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns="http://xmlns.oracle.com/sysman/connector/tt"
            targetNamespace="http://xmlns.oracle.com/sysman/connector/tt"
            elementFormDefault="qualified">

  <xsd:element name= "EventModel" type="EMEventModel"/>

  <xsd:complexType name="EMEventModel">
<xsd:sequence>
      <xsd:element name="TicketId" type="xsd:string" minOccurs="0" maxOccurs="1"
/>
      <xsd:element name="ConnectorId" type="xsd:string" minOccurs="1"
maxOccurs="1" />
      <xsd:element name="EventId" type="EventIdType" minOccurs="1" maxOccurs="1"
/>
<xsd:element name="TargetType" type="xsd:string" minOccurs="1" maxOccurs="1" />
<xsd:element name="TargetName" type="xsd:string" minOccurs="1" maxOccurs="1" />
```

```
<xsd:element name="MetricColumn" type="xsd:string" minOccurs="1" maxOccurs="1" />
<xsd:element name="MetricName" type="xsd:string" minOccurs="1" maxOccurs="1" />
<xsd:element name="KeyColumn" type="xsd:string" minOccurs="0" maxOccurs="1" />
<xsd:element name="KeyValues" type="xsd:string" minOccurs="0"
maxOccurs="unbounded" />
<xsd:element name="Message" type="xsd:string" minOccurs="1" maxOccurs="1" />
<xsd:element name="Severity" type="SeverityType" minOccurs="1" maxOccurs="1" />
<xsd:element name="SeverityCode" type="SeverityCodeType" minOccurs="1"
maxOccurs="1" />
<xsd:element name="CollectionTime" type="xsd:dateTime" minOccurs="1" maxOccurs="1"
/>
<xsd:element name="EventPageURL" type="xsd:string" minOccurs="0" maxOccurs="1" />
      <xsd:element name="EMUser" type="xsd:string" minOccurs="1" maxOccurs="1" />
      <xsd:element name="HDUser" type="xsd:string" minOccurs="1" maxOccurs="1" />
      <xsd:element name="NotificationRuleName" type="xsd:string" minOccurs="0"
maxOccurs="1" />
      <xsd:element name="TargetHost" type="xsd:string" minOccurs="1" maxOccurs="1"
/>
      <xsd:element name="GracePeriodCheckMade" type="xsd:string" minOccurs="0"
maxOccurs="1" />
      <xsd:element name="TargetTimezone" type="xsd:string" minOccurs="1"
maxOccurs="1" />
    </xsd:sequence>
</xsd:complexType>

  <xsd:complexType name="EventIdType">
    <xsd:sequence>
      <xsd:element name="TargetId" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xsd:element name="MetricId" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xsd:element name="KeyId" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    </xsd:sequence>
  </xsd:complexType>

<xsd:simpleType name="SeverityType">
<xsd:restriction base="xsd:string">
<xsd:enumeration value="Clear" />
<xsd:enumeration value="Info" />
<xsd:enumeration value="Warning" />
<xsd:enumeration value="Critical" />
<xsd:enumeration value="Agent Unreachable Clear" />
      <xsd:enumeration value="Blackout End" />
      <xsd:enumeration value="Blackout Start" />
      <xsd:enumeration value="Metric Error End" />
      <xsd:enumeration value="Metric Error Start" />
      <xsd:enumeration value="Unknown" />
</xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="SeverityCodeType">
<xsd:restriction base="xsd:string">
<xsd:enumeration value="15" />
<xsd:enumeration value="18" />
<xsd:enumeration value="20" />
<xsd:enumeration value="25" />
<xsd:enumeration value="115" />
      <xsd:enumeration value="125" />
      <xsd:enumeration value="215" />
      <xsd:enumeration value="225" />
      <xsd:enumeration value="315" />
      <xsd:enumeration value="325" />
```

```
</xsd:restriction>
</xsd:simpleType>

</xsd:schema>
```

Remedy Attributes

The following list shows the Remedy attributes available for mapping when using the default Remedy Help Desk Web services.

Case Type
Category
Description
Escalated
Escalated
Hotlist
Item
Office
Orig Submitter
Pending
Phone Number
Priority
Region
Request Urgency
Requester Login Name
Requester Name
Site
Source
Status
Summary
Type
Work Log
Create Time

See Also: *Remedy Help Desk for the Enterprise 6.0 User's Guide*

Format for Creating Ticket Templates

To create ticket templates for custom Remedy forms, adhere to the following format:

Example 2–5 Template Format for Custom Remedy Forms

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

<!--
This template creates an incident type ticket with default categorization
(Category: Default, Type:Default, Item:Default), and low priority. On update,
the description and message fields are updated, and the ticket is closed if the
associated alert has cleared.
-->

<xsl:template match="ns0:EventModel">
```

```
<xsl:choose>
<xsl:when test="normalize-space(ns0:TicketId) = ''">

*[Insert your mappings from EMModel into your custom Create Ticket Webservice SOAP
Document] *

</xsl:when>
<xsl:otherwise>

* [Insert your mappings from EMModel schema into your Custom Update Ticket
Webservice SOAP Document]*

</xsl:otherwise>
</xsl:choose>
</xsl:template>
</xsl:transform>
```

2.8 Enabling SSL for HTTPS

Follow the instructions provided in this section if you choose HTTPS as the protocol to establish a connection between the Remedy AR server and Enterprise Manager.

2.8.1 Generating a Certificate Request File

Generate a certificate request file for the Remedy AR server and send it to the Certificate authority, such as VeriSign.

> **Note:** The certificate request file is dependent on the Web server that Remedy uses.

2.8.2 Importing the Certificate from the Certificate Authority

After you get the certificate, import it to the Web server that Remedy uses. The import mechanism varies depending on the Web server that the Remedy Help Desk uses.

2.8.3 Adding Signed Certificates to Wallet Manager

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

Do the following on Enterprise Manager:

1. As Super Administrator, create a wallet using the following `orapki utility` command at the OMS host:

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

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

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

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

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

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

   Ensure that `ewallet.p12` is available.

4. In Oracle Wallet Manager, open the client certificate `ewallet.p12`.
5. Go to Select Trusted Certificates and select **Operations** on the main menu.
6. Select **Export All Trusted Certificates**.
7. Save the file as `certdb.txt`.
8. Place the file `certdb.txt` in the connector home root directory (`$OMS_HOME/sysman/connector`).

   If the file `certdb.txt` already exists in the root directory, open the file and add the contents of your `certdb.txt` to the existing content. If your Remedy installation does not have an operation to query a ticket by case ID, you need to import `HelpDesk_Query_Service_By_Case_ID.def` into your Remedy instance. You can get this file from `$ORACLE_HOME/sysman/connector/Remedy_Connector`.

Now Java SSL can use this file for communication between Enterprise Manager and the Remedy AR server in HTTPS mode.

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

2.9 Remedy Connector Tips

This section provides various tips that might help you to use Remedy Connector effectively.

2.9.1 Recommended Protocol

Oracle recommends that you use HTTPS as the protocol for the communication between Enterprise Manager and Remedy AR server.

Use HTTP only if a secure connection is not required and the data can be transferred in clear text between the two systems.

2.9.2 Supported Alerts

This release supports the following types of alerts:

- Metric alerts
- Availability alerts

2.9.3 Notification Failure

Notification is blocked for processing if the notification device is down due to any issues. For instance, the Remedy AR server is down, the Remedy configuration on Enterprise Manager is wrong, or the ticket is removed in Remedy.

Notification failure on one target impacts all other targets of the same target type for which the rule applies. That is, subsequent notifications are blocked until the issue is fixed or the maximum retrials fail.

Note: The maximum retrial period is one day.

2.9.4 Using Worklog

Worklog is a history option in the Remedy ticket that lets you maintain an alert history in the ticket. The Remedy default Web services do not allow modification of this option.

To use worklog, perform the following steps before using the Remedy Connector:

1. In the Remedy AR server, import the Web service definition `HelpDesk_Modify_Service_w_Worklog.def` from the Remedy Connector home directory (`$OMS_HOME/sysman/connector_Remedy_Connector`).

   See Also: Section "Importing Object Definitions" in the Remedy Remedy AR System Server product manual *Remedy Action Request System 6.3 - Developing AR System Applications: Advanced*

2. Configure the Connector to use the `HelpDesk_Modify_Service_w_Worklog` Web service by setting the `Update Ticket` endpoint accordingly.
3. Import all packaged work log templates (select the files with names ending in `Wlog.xsl`) using the `emctl` command provided in "Registering Ticket Templates" on page 2-8.

2.9.5 Web Service Details

This section provides information about the Web services that you require depending on the ticket template you choose.

2.9.5.1 For Default Templates (without Worklog Support)

If you choose default ticket templates, ensure that the following HPD:HelpDesk related Web services are up and running on the Remedy AR server:

- HelpDesk_Modify_Service
- HelpDesk_Query_Service
- HelpDesk_Submit_Service

2.9.5.2 For Worklog Templates

If you choose Worklog templates (*_Wlog), then you have to import `HelpDesk_Modify_Service_w_Worklog.def`, which is part of the `remedyconnector.jar`, to register the HelpDesk_Modify_Service_w_Worklog in Remedy.

3

Installing and Configuring the BMC Remedy Service Desk 7 Connector

The Oracle Management Connector for BMC Remedy Service Desk integrates BMC Remedy Service Desk v7 with Enterprise Manager. Using this connector, you can create, update, close, or reopen a ticket based on alerts in Enterprise Manager.

This chapter provides the following information for setting up and configuring the Remedy Service Desk Connector:

3.1 Introduction to the Remedy Service Desk Connector

The Remedy Service Desk Connector integrates Enterprise Manager with Remedy Service Desk through either an HTTP or HTTPS connection. You can create, update, close, or reopen tickets based on only the following types of alerts in Enterprise Manager:

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

Note that the term *ticket* refers to a Remedy incident.

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

3.1.1 Auto Ticketing

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

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

> **See Also:** "Configuring Notifications" in *Oracle Enterprise Manager Advanced Configuration Guide*

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

> **See Also:** Section 3.5.1, "Automatically Creating a Ticket"

3.1.2 Manual Ticketing

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

> **See Also:** Section 3.5.2, "Manually Creating a Ticket"

3.1.3 Ticket Templates

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

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

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

> **See Also:** Section 3.7, "Using Default Templates"

3.1.4 Grace Period

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

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

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

Note: In Remedy, after a ticket is set to a Closed status, it cannot be reopened. Consequently, an alert that re-triggers within the grace period cannot reopen the ticket but only annotate it. If you want to reopen a ticket for alert occurrences that fall within the grace period, set the ticket status to Resolved instead of Closed when the alert clears. This enables the Remedy Service Desk Connector to reopen the ticket if the same alert reoccurs within the grace period.

3.2 Prerequisites

Before using Remedy Service Desk Connector, ensure that you meet the following prerequisites:

- Remedy Service Desk IT Service Management 7.0.03 with the latest Incident Management patch, "IT Service Management Patch 008" is installed and configured.
- Remedy Service Desk web services are up and running. See Section 3.9.3, "Web Service Details for Default Templates".

3.3 Installing and Uninstalling the Remedy Service Desk Connector

The Remedy Service Desk connector is packaged as a single jar file, remedy_service_desk_connector.jar, that you can deploy by using Enterprise Manager emctl command.

There can only be one ticketing connector in Oracle Enterprise Manager. Before proceeding to the next section, do the following:

1. Click the **Setup** link in the upper right corner of the Oracle Enterprise Manager console.
2. Click the **Management Connectors** link in the left column of the Overview of Setup page.
3. Remove any ticketing connector you may have.

3.3.1 Installing the Connector

Perform the following steps to install the connector:

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

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

   This extracts the `.jar` file to this folder:

   ```
   $ORACLE_HOME/sysman/connector/Remedy_Service_Desk_Connector/
   ```

   For example:

   ```
   emctl extract_jar connector remedy_service_desk_connector.jar "Remedy Service Desk Connector"
   ```

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

```
$ORACLE_HOME/bin/emctl register_connector connector <connectorType.xml>
<server> <port> <database sid> <username> <oracleHome>
```

For example:

```
emctl register_connector connector $ORACLE_HOME/sysman/connector/Remedy_
Service_Desk_Connector/RemedyDeploy.xml $emHost $dbPort $dbSID sysman $ORACLE_
HOME
```

The Remedy Service Desk Connector should now appear in the Management Connector page.

Registering the Ticket Template

There are three default templates:

- Remedy_DefaultCategory_AutoResolve.xsl
- Remedy_DefaultCategory_AutoClose.xsl
- Remedy_DefaultCategory.xsl

Run the following command as a user with `execute` privilege on `emctl` and the ability to read the ticket template:

$ORACLE_HOME/bin/`emctl register_ticket_template connector <ticketTemplate.xsl> <server> <port> <database sid/service name for RAC DB> <username> <password> <connectorTypeName> <connectorName> <templateName> <description>`

Note: You need to run this command for every Remedy template that is shipped as part of the connector. For multiple OMS installations, you need to run this command only once from any of the OMSes.

Example 3–1 Ticket Template Registration

```
emctl register_ticket_template connector Remedy_DefaultCategory_AutoResolve.xsl
$emHost $dbPort $dbSID sysman $sysmanPwd "Remedy Service Desk Connector" "Remedy
Service Desk Connector" "Auto Resolve Template" "This template creates a ticket
with priority based on event severity and auto resolve"
```

Table 3–1 provides descriptions for the parameters shown in the emctl command above.

Table 3–1 emctl Parameters

Parameter	Description
`ticketTemplate.xsl`	Fully qualified name of the ticket template file. The file resides in the Connector home directory: `$OMS_HOME/sysman/connector/Remedy_service_Desk_Connector` Oracle recommends that you use intuitive names since there might be notification methods created with the same names, and you have to choose one of them when you use the Auto Ticketing feature. Use `xsl` as the file extension, since the format is XSLT. For example, `Remedy_DefaultCategory.xsl`. If the file is in a different directory, provide the complete path for the file.
`server`	Host name of the Enterprise Manager repository.
`port`	Listener port of the repository.
`database sid/ Service Name for RAC DB`	Repository database instance ID or service name if you are using RAC database as the repository.
`username`	Specify `SYSMAN`.
`password`	Password for `SYSMAN`.
`connectorTypeName`	Specify `"Remedy Service Desk Connector"`. The double quotes ("") are mandatory.
`connectorName`	Specify `"Remedy Service Desk Connector"`. The double quotes ("") are mandatory.
`templateName`	Intuitive name for the ticket template that will be displayed in Enterprise Manager.
`description`	Short description for the ticket template. This description is also displayed in Enterprise Manager.

3.3.2 Uninstalling the Connector

To uninstall the connector, do the following:

1. Click the **Setup** link in the upper right corner of the Oracle Enterprise Manager console.
2. Click the **Management Connectors** link in the left column of the Overview of Setup page.
3. Select the connector, then click **Delete**.

3.4 Configuring the Remedy Service Desk Connector

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

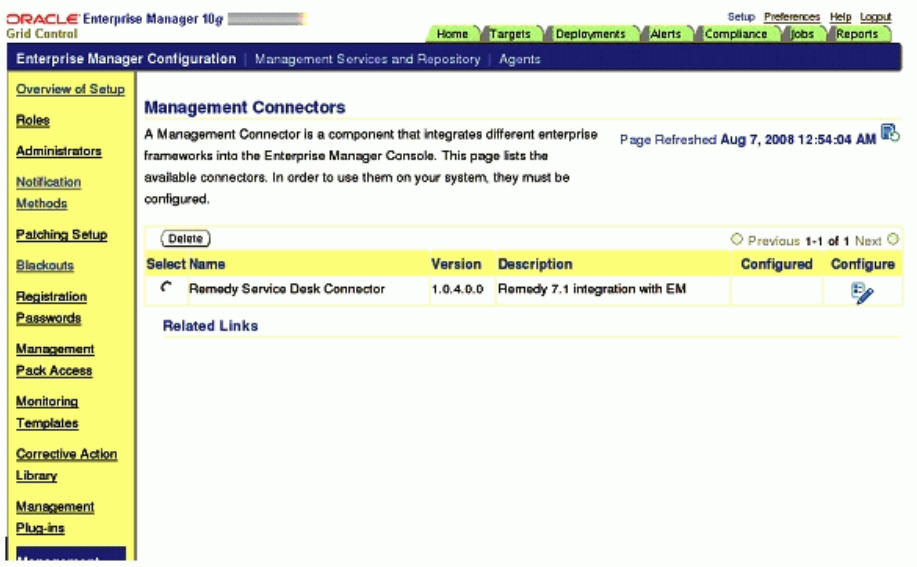
   The Overview of Setup page appears.

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

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

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

Figure 3–1 Management Connectors Page



3. Click the **Configure** icon for the Remedy Service Desk Connector.

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

4. Provide the required settings. See "General Settings" for details.

5. Click **OK.**

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

6. **Optional:** To check for the available ticket templates, click the configure icon again.

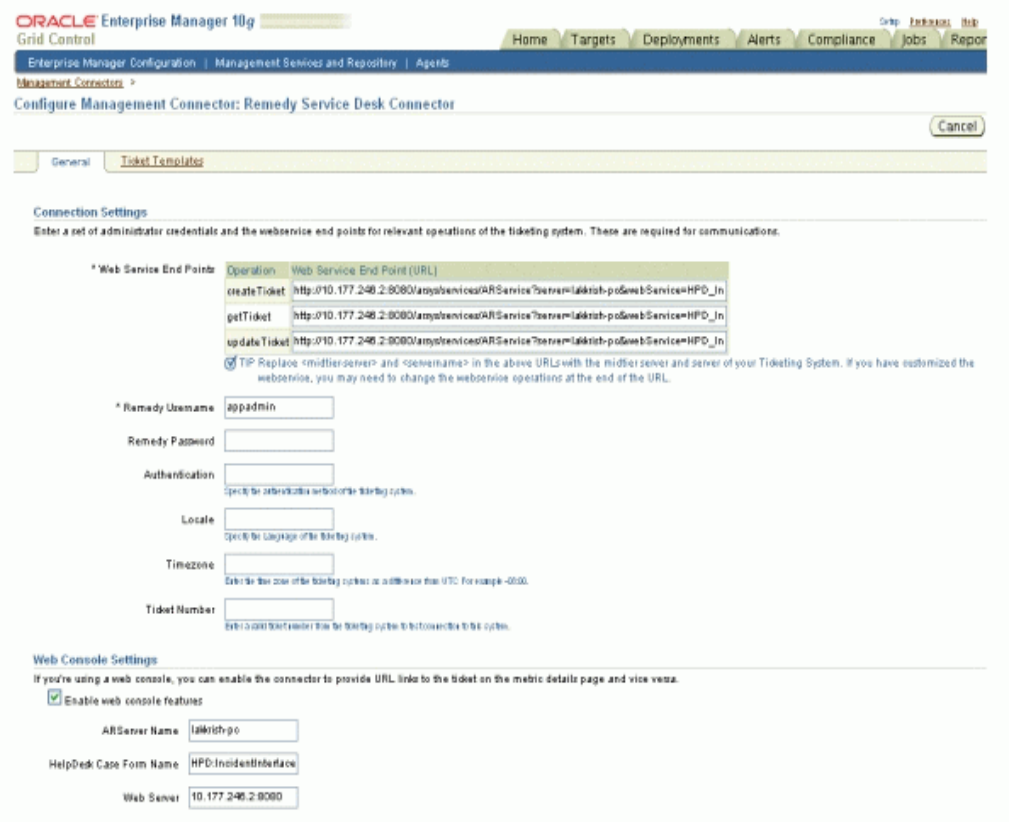
7. Click the **Ticket Templates** tab.

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

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

If you choose HTTPS as the protocol to establish a connection between Remedy and Enterprise Manager, see "Enabling SSL for HTTPS" on page 3-38.

Figure 3–2 Configure Management Connector Page



3.4.1 General Settings

The following sections explain how to provide various configuration details.

3.4.1.1 Connection Settings

The Remedy Service Desk Connector communicates with the Service Desk through their Web services. Mandatory fields are indicated by an asterisk (*).

- **Web Service End Points** — End points to `createTicket`, `updateTicket`, and `getTicket` web services exposed by Remedy Service Desk. See Section 3.9.3, "Web Service Details for Default Templates" for additional information.

  You need to import HelpDesk_Query_Service_getIncident.def into your Remedy instance for a getTicket operation. By default on the Enterprise Manager Management Connector page, the web service endpoint for getTicket appears as HPD_IncidentInterface_get_WS.

  If you want to use the Remedy_DefaultCategory_AutoResolve.xsl template, you need to import HPD_IncidentInterface_CustomWS.def. Back up HPD_IncidentInterface_WS web service before importing.

  The *def files are located here:

  $ORACLE_HOME/sysman/connector/Remedy_Service_Desk_Connector

- **Remedy Username** — User with the privilege to create, update, and query tickets in Remedy.
- **Remedy Password** — Password associated with the supplied Remedy user.
- **Authentication** — String that a Remedy administrator sets for additional security. Applies only if the Remedy Administrator has configured it on the Remedy AR server (optional).
- **Locale** — Language of the Remedy system (optional).
- **Time Zone** — Time zone of the Remedy AR System Server (optional).
- **Ticket Number** — Enter a valid ticket number if you want to test the connection when you save the configuration.
  - If you do not enter a ticket number, no message appears on the Management Connectors page after you click OK and the configuration is saved.
  - If you specify the correct Web service end points and enter a valid ticket number, the following message appears on the Management Connectors page after you click OK:

    "Connection test succeeded. The configuration was saved."
  - If you have not previously saved the connector configuration and enter an invalid ticket number, the following message appears on the Management Connectors page after you click OK:

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

    "Connection test failed. The configuration was not saved."

3.4.1.2 Web Console Settings

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

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

- **Enable web console** — Check this box to enable launching of the Remedy ticket page within context from Enterprise Manager.
- **ARServer Name** — Remedy AR Server name.
- **HelpDesk Case Form Name** — Remedy form name that the Remedy Web Services (you configured the connector to use) is based on. The Remedy default Service Desk Web services, for example, use the form HPD:IncidentInterface.
- **Web Server** — The name or IP address of the server that hosts Remedy Mid-Tier.

3.4.1.3 Grace Period

You can enable and disable the grace period and configure its value. By default, the grace period is disabled. See Section 3.1.4, "Grace Period" for details. This setting applies to all alerts the Remedy Service Desk Connector processes.

3.4.2 Working with Ticket Templates

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

3.4.2.1 Registering Ticket Templates

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

All registered ticket templates are displayed in the Configure Management Connector Ticket Templates page. To register additional ticket templates that you create, see Section 3.3.1, "Installing the Connector".

See Also: Table 3–1, " emctl Parameters" on page 3-5

3.4.2.2 Viewing Template Code

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

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

3.4.2.3 Removing a Template

To remove a template, do the following:

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

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

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

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

3.4.2.4 Replacing Templates

To replace an existing ticket template, do the following:

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

3.4.2.5 Adding New Templates

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

See Also: Section 3.7.4, "Defining New Templates"

3.5 Creating Remedy Tickets

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

3.5.1 Automatically Creating a Ticket

Perform the following steps to automatically create a ticket:

1. Review Section 3.7, "Using Default Templates".
2. Select an appropriate ticket template with the desired mapping of Enterprise Manager alert fields to the Remedy ticket fields.
3. If you do not have a ticket template that satisfies your requirement, create one and register it.
4. Create a notification rule using the following steps:

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

---

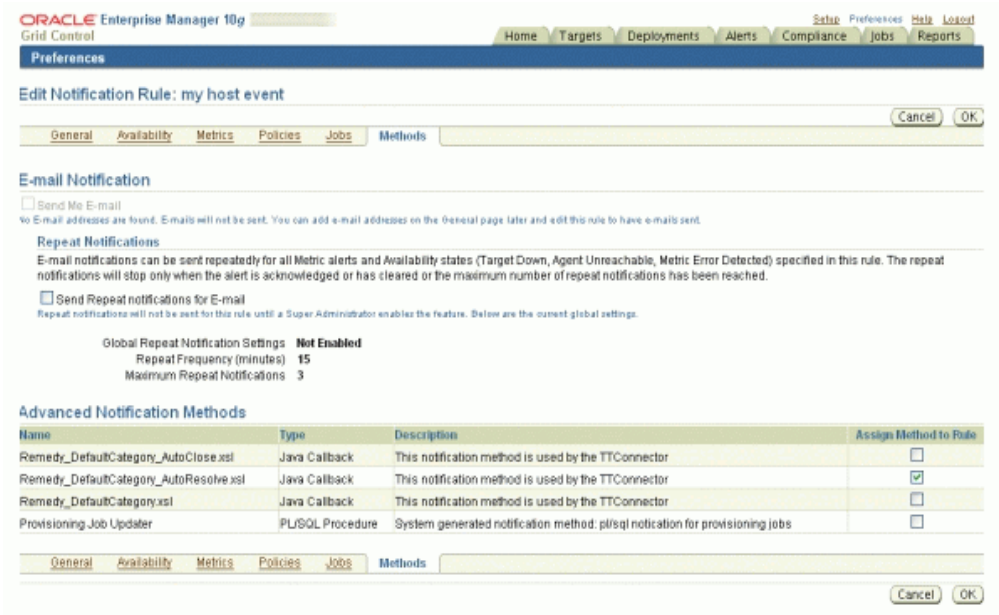
   a. From the Enterprise Manager console, click **Preferences.**
   b. In the left pane, under Notification, click **Rules,** then **Create**.
   c. In the Create Notification Rule General page, specify the rule name, a description, and the targets for which this rule should apply.
   d. In the Create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

      Ensure that you select all relevant alert severities if you want to update the ticket when the alert severity changes. For example, to open a ticket for a critical alert on the CPU Utilization(%) metric and the ticket is to be updated if the CPU Utilization(%) changes to warning or clear severity, in the notification rule select `Critical`, `Warning`, or `Clear` severities for the CPU Utilization(%) metric.
   f. In the Create Notification Rule Methods page, choose the ticket template from the Advanced Notification Methods table, as shown in Figure 3–3.

      In the table, registered ticket templates appear as Java Callback type notification methods under the same name as the ticket template's file name.

      See Also: "Configuring Notifications" in *Oracle Enterprise Manager Advanced Configuration Guide*

Figure 3–3 Notification Methods



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

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

A ticket is updated if there is an existing active ticket for an alert. Figure 3–4 shows the ticket in the Remedy console, and Figure 3–5 shows the alert as displayed in Enterprise Manager.

Figure 3–4 Ticket in the Remedy Console

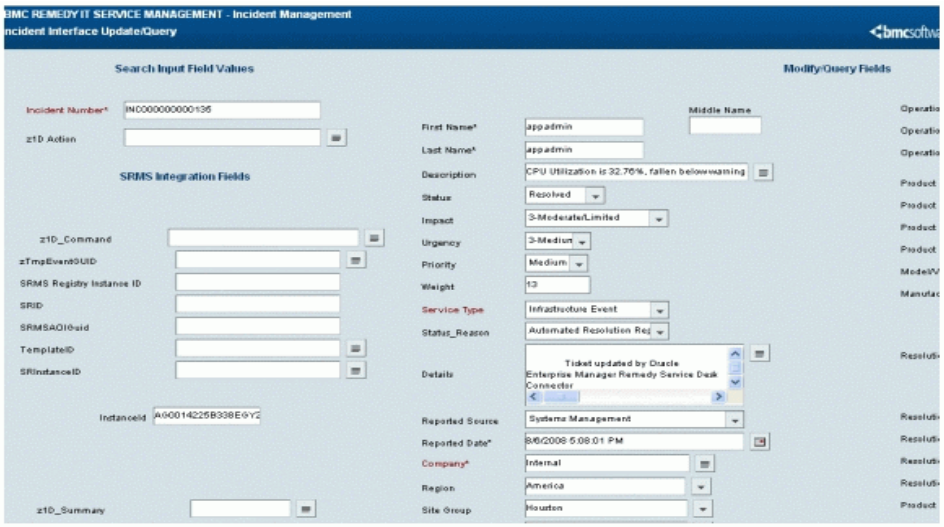
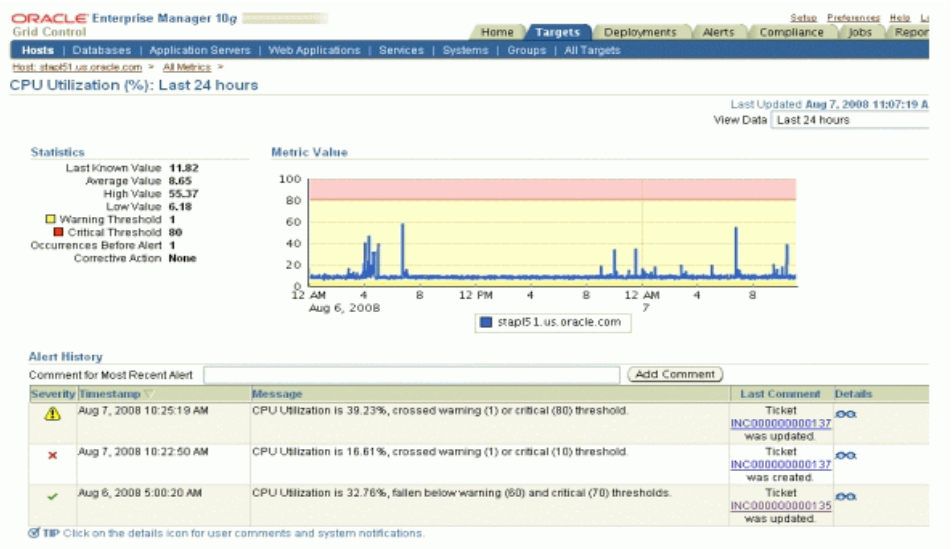


Figure 3–5 Alert as Displayed in Enterprise Manager

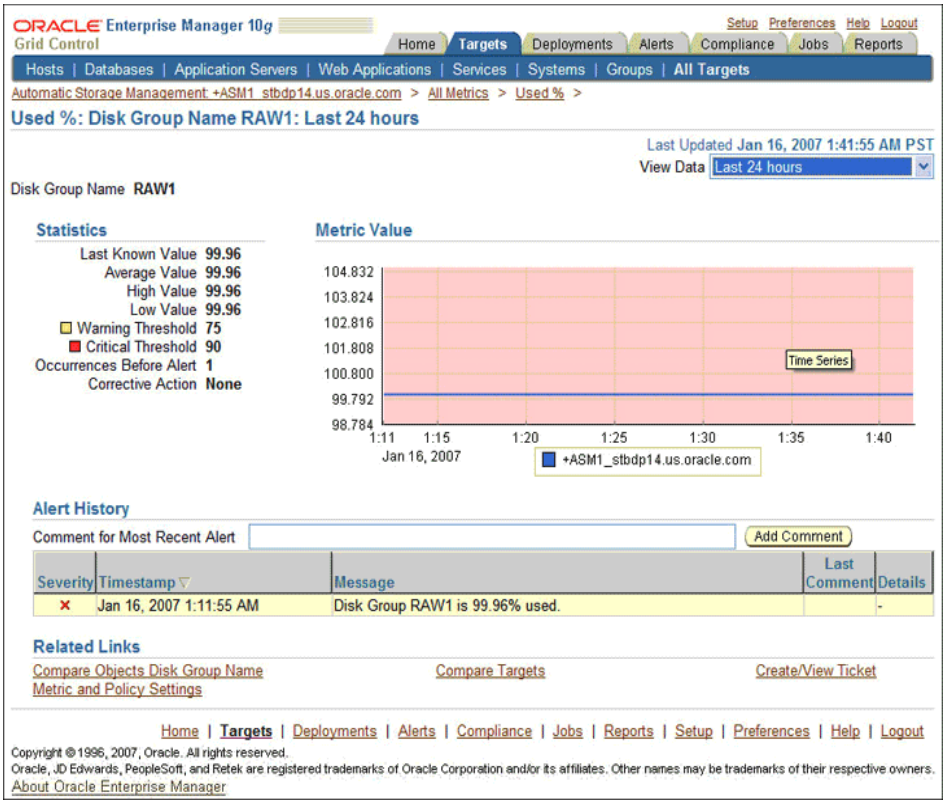


3.5.2 Manually Creating a Ticket

Perform the following steps to manually create a ticket:

1. After a metric alert occurs, go to the associated metric details page for the alert. To access this page, click the alert message in the Enterprise Manager console, as shown in Figure 3–6.

Figure 3–6 Metric Details Page



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

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

3. Select a ticket template and then click **Submit, as shown in** Figure 3–7.

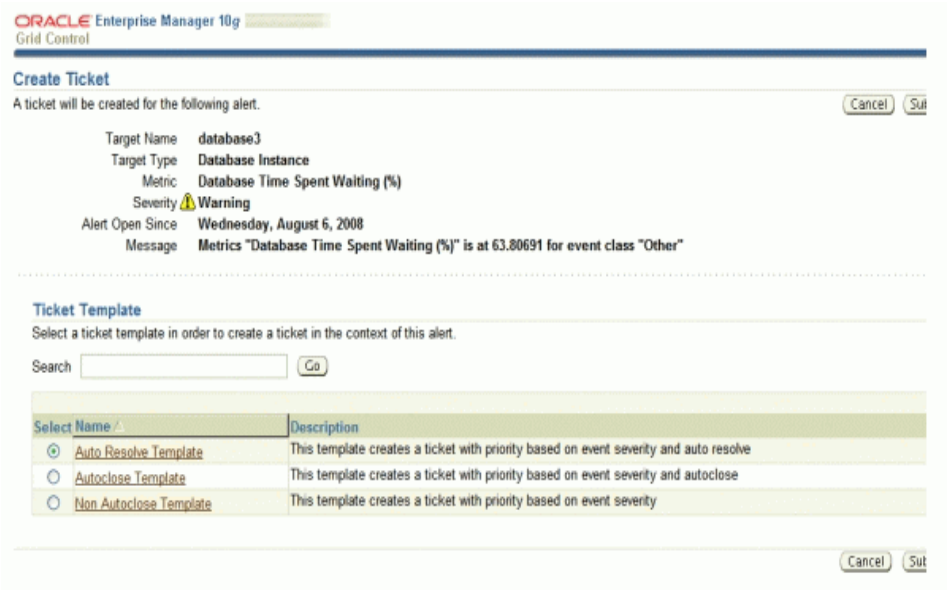
   If you do not see the desired template, you can register one using the `emctl` command. See Section 3.4.2.1, "Registering Ticket Templates".

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

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

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

Figure 3–7 Create Ticket Page



3.6 Navigating Between Remedy and Enterprise Manager

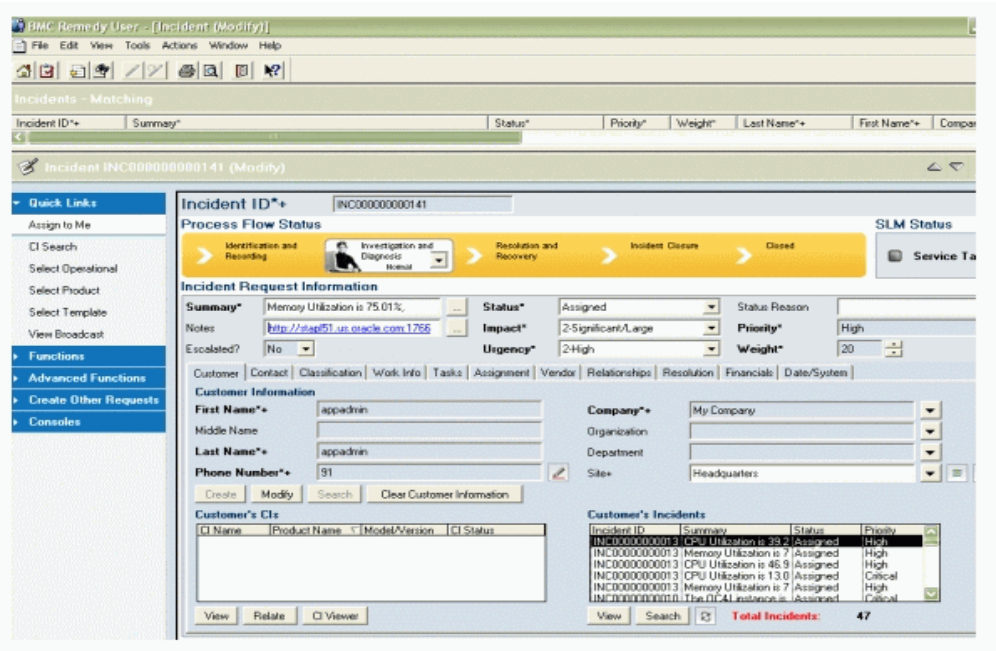
The following sections explain how to switch from one console to the other.

3.6.1 Navigating from Remedy to Enterprise Manager

From a ticket page, click the link in the **Notes** field to the Alert Details page in the ticket message body, as shown in Figure 3–8. This action takes you to the Enterprise Manager console login page. After you provide the Enterprise Manager user name and password, you are forwarded to the alert related to this ticket.

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

Figure 3–8 Alert Details in the Remedy Console



3.6.2 Navigating from Enterprise Manager to Remedy

1. In the Enterprise Manager console, click the alert message to go to the metric details page for the alert.
2. In the Alert History table, locate the ticket ID link in the Last Comment column.
3. (If not found) Click the icon in the Details column to get more information about the alert.
4. On the page that appears, locate the ticket ID in the Alert Details table.
5. Click the ticket ID link. You are forwarded to the Remedy Web console login page.
6. Provide valid Remedy account details.

   The ticket page associated with this alert is displayed.

Note: If you do not use the Remedy Web console, uncheck the Enable web console option in the Web Console Settings section so that ticket ID is shown in plain text. Otherwise, it is displayed as a link that does not work.

3.7 Using Default Templates

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

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

- Write alert information to `Description` (Remedy ticket description).

- Set the Remedy ticket summary based on the alert message. On update, the ticket summary field is updated to include the latest alert message information.

The out-of-box templates are as follows:

- `Remedy_DefaultCategory_AutoResolve.xsl`
- `Remedy_DefaultCategory_AutoClose.xsl`
- `Remedy_DefaultCategory.xsl`

`Remedy_DefaultCategory_AutoResolve.xsl`

The Remedy_DefaultCategory_AutoResolve.xsl template sets the ticket status to Resolved when the event severity value becomes clear. When the same event with a Critical or Warning severity occurs within the grace period time, the following occurs:

- The ticket is reopened.
- The status field is set as Assigned.
- The ticket Summary, Notes, Work Info Summary, and Work Info Notes fields are updated with the latest event information. If you leave an incident as resolved, the Incident Management application closes the incident after 15 days. See the *BMC Remedy Service Desk: Incident Management 7.0 User's Guide* for more information.

`Remedy_DefaultCategory_AutoClose.xsl`

The Remedy_DefaultCategory_AutoClose.xsl template ets the ticket status to Closed when the event severity value becomes Clear. After the Ticket Status is closed, it cannot be reassigned to other values. When the same event with critical or warning severity occurs within the grace period time, the following occurs:

- The ticket is not reopened.
- The status field remains Closed, but the ticket Summary, Notes, Work Info Summary, and Work Info Notes fields are updated with the latest event information.

> **Note:** Oracle recommends that you do not select Remedy_DefaultCategory_AutoClose.xsl if you want tickets to be reopened when a critical or warning event has occurred within the grace period.

`Remedy_DefaultCategory.xsl`

The Remedy_DefaultCategory.xsl template does not close the ticket when the event severity value becomes clear. When the same event with a Critical or Warning severity occurs within the grace period time, the ticket Summary, Notes, Work Info Summary, and Work Info Notes fields are updated with the latest event information.

3.7.1 Reading Ticket Templates

Table 3–2 and Table 3–3 illustrate the creation of a ticket using `Remedy_DefaultCategory_AutoResolve.xsl`. This illustration will help you to read a ticket template. In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Ticket creation mappings are the same for Remedy_DefaultCategory_AutoResolve.xsl, Remedy_DefaultCategory_AutoClose.xsl, and Remedy_DefaultCategory.xsl.

Table 3–2 shows Remedy ticket attributes and corresponding Enterprise Manager alert values for ticket creation mappings.

Table 3–2 Ticket Creation Mappings (for all templates)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Assigned_Group		Blank
Assigned_Group_Shift_ Name		Blank
Assigned_Support_ Company		Blank
Assigned_Support_ Organization		Blank
Assignee		Blank
Categorization_Tier_1		Blank
Categorization_Tier_2		Blank
Categorization_Tier_3		Blank
CI_Name		Blank
Closure_Manufacturer		Blank
Closure_Product_Category_ Tier1		Blank
Closure_Product_Category_ Tier2		Blank
Closure_Product_Category_ Tier3		Blank
Closure_Product_Model_ Version		Blank
Closure_Product_Name		Blank
Department		Blank
First_Name	HDUser	User name provided in the "Remedy Username" field during the configuration.
Impact	Severity	■ If severity is Critical, set Impact to 1-Extensive/ Widespread. ■ If severity is Warning, set Impact to 2-Significant/Large. ■ Otherwise, set Impact to 3-Moderate/Limited.
Last_Name	HDUser	
Lookup_Keyword		Blank
Manufacturer		Blank

Table 3–2 (Cont.) Ticket Creation Mappings (for all templates)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Product_Categorization_ Tier_1		Blank
Product_Categorization_ Tier_2		Blank
Product_Categorization_ Tier_3		Blank
Product_Model_Version		Blank
Product_Name		Blank
Reported_Source		"Systems Management" *
Resolution		Blank
Resolution_Category_Tier_1		Blank
Resolution_Category_Tier_2		Blank
Resolution_Category_Tier_3		Blank
Service_Type		"Infrastructure Event" *
Status		New *
Action		CREATE *
Create_Request		Blank
Summary	Message	

Table 3–2 (Cont.) Ticket Creation Mappings (for all templates)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Notes	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.	Values from the alert context.
	TargetName	
	TargetType	
	MetricColumn — Name of the metric, such as CPU Utilization (%).	
	MetricName — Category of the metric. For the CPU Utilization (%) metric, this would be 'Load.'	
	KeyColumn ** — For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name.'	
	KeyValues ** — For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.	
	Severity	
	CollectionTime	
	TargetHost	
	NotificationRuleName	
	EventPageURL — URL to the metric details page in the context of the alert.	
Urgency	Severity	■ If severity is Critical, set Urgency to 1-Critical. ■ If severity is Warning, set Urgency to "2-High" ■ Otherwise, set Urgency to 3-Medium.
Work_Info_Summary	Message	
Work_Info_Notes	Message, Severity	
Work_Info_Type		"Incident Task/Action" *

Table 3–2 (Cont.) Ticket Creation Mappings (for all templates)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Work_Info_Date		Blank
Work_Info_Source		"System Assignment" *
Work_Info_Locked		Blank
Work_Info_View_Access		"Public" *
Middle_Initial		Blank

Table 3–3 shows Remedy ticket attributes and corresponding Enterprise Manager alert attributes and values for Remedy_DefaultCategory_AutoResolve.xsl mappings.

Table 3–3 Ticket Updates (Remedy_DefaultCategory_AutoResolve.xsl Mappings)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Categorization_Tier_1		Blank
Categorization_Tier_2		Blank
Categorization_Tier_3		Blank
Closure_Manufacturer		Blank
Closure_Product_Category_Tier1		Blank
Closure_Product_Category_Tier2		Blank
Closure_Product_Category_Tier3		Blank
Closure_Product_Model_Version		Blank
Closure_Product_Name		Blank
Company		"Internal" *
Summary	Message, Severity	

Table 3–3 (Cont.) Ticket Updates (Remedy_DefaultCategory_AutoResolve.xsl Mappings)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Notes	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. TargetName TargetType MetricColumn — Name of the metric, such as CPU Utilization (%). MetricName — Category of the metric. For the CPU Utilization (%) metric, this would be 'Load.' KeyColumn ** — For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name.' KeyValues ** — For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity. Severity CollectionTime TargetHost NotificationRuleName EventPageURL — URL to the metric details page in the context of the alert.	.
Impact	Severity	■ If severity is Critical, set Impact to 1-Extensive/ Widespread. ■ If severity is Warning, set Impact to 2-Significant/Large. ■ Otherwise, set Impact to 3-Moderate/Limited.

Table 3–3 (Cont.) Ticket Updates (Remedy_DefaultCategory_AutoResolve.xsl Mappings)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Incident_Number	TicketId — The connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web Service to identify the ticket that must be updated.	
Manufacturer		Blank
Product_Categorization_ Tier_1		Blank
Product_Categorization_ Tier_2		Blank
Product_Categorization_ Tier_3		Blank
Product_Model_Version		Blank
Product_Name		Blank
Reported_Source		"Systems Management" *
Resolution	Severity	If severity is Clear
Resolution_Category		Blank
Resolution_Category_Tier_2		Blank
Resolution_Category_Tier_3		Blank
Resolution_Method		Blank
Service_Type		"Infrastructure Event" *
Status	Severity	■ If severity is Clear, set the ticket to the status Resolved. ■ If the grace period test has already been done and the alert is still within the grace period, reopen the ticket by setting the ticket to the status Assigned.
Status_Reason	Severity	If severity is Clear, set the Status_Reason to "Automated Resolution Reported."
Urgency	Severity	■ If severity is Critical, set Urgency to 1-Critical. ■ If severity is Warning, set Urgency to "2-High" ■ Otherwise, set Urgency to 3-Medium.
Action		CREATE *
Work_Info_Summary	Message	
Work_Info_Notes	Severity	
Work_Info_Type		"Incident Task/Action" *

Table 3–3 (Cont.) Ticket Updates (Remedy_DefaultCategory_AutoResolve.xsl Mappings)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Work_Info_Date		Blank
Work_Info_Source		"System Assignment" *
Work_Info_Locked		"No" *
Work_Info_View_Access		"Public" *

Use the mapping table (Table 3–2) as a reference to read the XSLT file in Example 3–2.

Example 3–2 Remedy_DefaultCategory_ AutoResolve.xsl Source Code with Annotations

```
?xml version='1.0' encoding='UTF-8'?>
<xsl:transform version="1.0"
              xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
               xmlns:ns0="http://xmlns.oracle.com/sysman/connector/tt"
               targetNamespace="http://xmlns.oracle.com/sysman/connector/tt"
               elementFormDefault="qualified">
 <!--   This template creates an incident type ticket within Remedy Service Desk
with default settings. On update, the worklog is updated with the latest event
message and severity information. The ticket is set to status Resolved if the
associated alert has cleared. Ticket can be reopend if a severity occured with in
the grace period. If the ticket is not reopened for 15 days, ticket will be closed
by incident management.
 -->
  <xsl:template match="ns0:EventModel">
    <xsl:choose>
      <xsl:when test="normalize-space(ns0:TicketId) = ''">
        <urn:HelpDesk_Submit_Service xmlns:urn="urn:HPD_IncidentInterface_
          Create_WS">
           <!-- EDIT THE TAG VALUES BELOW TO CHANGE HOW A TICKET IS FILLED
                DURING TICKET CREATION. REFER TO THE REMEDY SERVICE DESK MANUAL
                FOR DESCRIPTION OF THESE HELPDESK SUPPORT DATAFIELDS-->
    <urn:Assigned_Group/>
    <urn:Assigned_Group_Shift_Name/>
    <urn:Assigned_Support_Company/>
    <urn:Assigned_Support_Organization></urn:Assigned_Support_Organization>
    <urn:Assignee/>
    <urn:Categorization_Tier_1/>
    <urn:Categorization_Tier_2/>
    <urn:Categorization_Tier_3/>
    <urn:CI_Name/>
    <urn:Closure_Manufacturer/>
    <urn:Closure_Product_Category_Tier1/>
    <urn:Closure_Product_Category_Tier2/>
    <urn:Closure_Product_Category_Tier3/>
    <urn:Closure_Product_Model_Version/>
    <urn:Closure_Product_Name/>
    <urn:Department/>
        <urn:First_Name><xsl:value-of select="ns0:HDUser"/></urn:First_Name>
        <xsl:choose>
              <!--  EM Critical -->
              <xsl:when test="ns0:SeverityCode = '25'">
                <urn:Impact>1-Extensive/Widespread</urn:Impact>
              </xsl:when>
              <!--  EM Warning-->
              <xsl:when test="ns0:SeverityCode = '20'">
```

```
                <urn:Impact>2-Significant/Large</urn:Impact>
              </xsl:when>
                 <!--  Unreachable Start -->
<xsl:when test="ns0:Severity = 'Unreachable Start'">
                <urn:Impact>1-Extensive/Widespread</urn:Impact>
              </xsl:when>
                <!--  Agent Unreachable Start -->
              <xsl:when test="ns0:Severity = 'Agent Unreachable Start'">
                <urn:Impact>1-Extensive/Widespread</urn:Impact>
                </xsl:when>
                <!--  Blackout Start -->
              <xsl:when test="ns0:Severity = 'Blackout Start'">
                <urn:Impact>2-Significant/Large</urn:Impact>
                </xsl:when>
                <!--  Metric Error Start-->
              <xsl:when test="ns0:Severity = 'Metric Error Start'">
                <urn:Impact>2-Significant/Large</urn:Impact>
              </xsl:when>
              <xsl:otherwise>
                <urn:Impact>3-Moderate/Limited</urn:Impact>
              </xsl:otherwise>
        </xsl:choose>
        <urn:Last_Name><xsl:value-of select="ns0:HDUser"/></urn:Last_Name>
<urn:Lookup_Keyword/>
     <urn:Manufacturer/>
     <urn:Product_Categorization_Tier_1/>
     <urn:Product_Categorization_Tier_2/>
     <urn:Product_Categorization_Tier_3/>
     <urn:Product_Model_Version/>
     <urn:Product_Name/>
        <urn:Reported_Source>Systems Management</urn:Reported_Source>
      <urn:Resolution/>
     <urn:Resolution_Category_Tier_1/>
     <urn:Resolution_Category_Tier_2/>
     <urn:Resolution_Category_Tier_3/>
        <urn:Service_Type>Infrastructure Event</urn:Service_Type>
        <urn:Status>New</urn:Status>
        <urn:Action>CREATE</urn:Action>
        <urn:Create_Request/>
         <urn:Summary>
                <xsl:value-of select="ns0:Message"/>
          </urn:Summary>
         <urn:Notes>
Ticket created by Oracle Enterprise Manager Remedy Service Desk Connector.

--------------------------------------------------------------------------
              EM User: <xsl:value-of select="ns0:EMUser"/>
              Event Information:
              Target Name: <xsl:value-of select="ns0:TargetName"/>
Target Type: <xsl:value-of select="ns0:TargetType"/>
              Metric Column: <xsl:value-of select="ns0:MetricColumn"/>
              Metric Name: <xsl:value-of select="ns0:MetricName"/>
              <xsl:choose>
              <xsl:when test="normalize-space(ns0:KeyColumn) != ''">
              Key Column: <xsl:value-of select="ns0:KeyColumn"/>
              Key Values: <xsl:value-of select="ns0:KeyValues"/>
              </xsl:when>
              </xsl:choose>
              Severity: <xsl:value-of select="ns0:Severity"/>
              Collection Time: <xsl:value-of select="ns0:CollectionTime"/>
```

```
                Target Host: <xsl:value-of select="ns0:TargetHost"/>
                <xsl:choose>
                <xsl:when test="normalize-space(ns0:NotificationRuleName) != ''">
                Notification Rule: <xsl:value-of select="ns0:NotificationRuleName"/>
                </xsl:when>
                </xsl:choose>
                URL: <xsl:value-of select="ns0:EventPageURL"/>
            </urn:Notes>
            <xsl:choose>
                <!--  EM Critical -->
                <xsl:when test="ns0:SeverityCode = '25'">
                  <urn:Urgency>1-Critical</urn:Urgency>
                </xsl:when>
                <!--  EM Warning-->
                <xsl:when test="ns0:SeverityCode = '20'">
                  <urn:Urgency>2-High</urn:Urgency>
                </xsl:when>
                   <!--  Unreachable Start -->
                <xsl:when test="ns0:Severity = 'Unreachable Start'">
                  <urn:Urgency>1-Critical</urn:Urgency>
                </xsl:when>
                  <!--  Agent Unreachable Start -->
                <xsl:when test="ns0:Severity = 'Agent Unreachable Start'">
                  <urn:Urgency>1-Critical</urn:Urgency>
                  </xsl:when>
                  <!--  Blackout Start -->
                <xsl:when test="ns0:Severity = 'Blackout Start'">
                  <urn:Urgency>2-High</urn:Urgency>
                  </xsl:when>
                  <!--  Metric Error Start-->
                <xsl:when test="ns0:Severity = 'Metric Error Start'">
                  <urn:Urgency>2-High</urn:Urgency>
                </xsl:when>
                <xsl:otherwise>
                <urn:Urgency>3-Medium</urn:Urgency>
</xsl:otherwise>
        </xsl:choose>
          <urn:Work_Info_Summary>
                <xsl:value-of select="ns0:Message"/>
          </urn:Work_Info_Summary>
          <urn:Work_Info_Notes>
                Incident created by Oracle Enterprise Manager Remedy Service Desk
Connector based on an alert with <xsl:value-of select="ns0:Severity"/> severity.
Message: <xsl:value-of select="ns0:Message"/>
           </urn:Work_Info_Notes>
          <urn:Work_Info_Type>Incident Task / Action</urn:Work_Info_Type>
          <urn:Work_Info_Date/>
          <urn:Work_Info_Source>System Assignment</urn:Work_Info_Source>
          <urn:Work_Info_Locked/>
          <urn:Work_Info_View_Access>Public</urn:Work_Info_View_Access>
          <urn:Middle_Initial/>
        </urn:HelpDesk_Submit_Service>
      </xsl:when>
      <xsl:otherwise>
<urn:HelpDesk_Modify_Status_Service xmlns:urn="urn:HPD_IncidentInterface_WS">
        <urn:Categorization_Tier_1></urn:Categorization_Tier_1>
        <urn:Categorization_Tier_2></urn:Categorization_Tier_2>
        <urn:Categorization_Tier_3></urn:Categorization_Tier_3>
        <urn:Closure_Manufacturer></urn:Closure_Manufacturer>
        <urn:Closure_Product_Category_Tier1></urn:Closure_Product_Category_Tier1>
```

```
        <urn:Closure_Product_Category_Tier2></urn:Closure_Product_Category_Tier2>
        <urn:Closure_Product_Category_Tier3></urn:Closure_Product_Category_Tier3>
        <urn:Closure_Product_Model_Version></urn:Closure_Product_Model_Version>
        <urn:Closure_Product_Name></urn:Closure_Product_Name>
        <urn:Company>Internal</urn:Company>
        <urn:Summary>
            <xsl:value-of select="ns0:Message"/>
          </urn:Summary>
        <urn:Notes>
Ticket updated by Oracle Enterprise Manager Remedy Service Desk Connector

----------------------------------------------------------------------
              EM User: <xsl:value-of select="ns0:EMUser"/>
              Event Information:
              Target Name: <xsl:value-of select="ns0:TargetName"/>
              Target Type: <xsl:value-of select="ns0:TargetType"/>
              Metric Column: <xsl:value-of select="ns0:MetricColumn"/>
              Metric Name: <xsl:value-of select="ns0:MetricName"/>
              <xsl:choose>
              <xsl:when test="normalize-space(ns0:KeyColumn) != ''">
              Key Column: <xsl:value-of select="ns0:KeyColumn"/>
              Key Values: <xsl:value-of select="ns0:KeyValues"/>
</xsl:when>
              </xsl:choose>
              Severity: <xsl:value-of select="ns0:Severity"/>
              Collection Time: <xsl:value-of select="ns0:CollectionTime"/>
              Target Host: <xsl:value-of select="ns0:TargetHost"/>
              <xsl:choose>
              <xsl:when test="normalize-space(ns0:NotificationRuleName) != ''">
              Notification Rule: <xsl:value-of select="ns0:NotificationRuleName"/>
              </xsl:when>
              </xsl:choose>
              URL: <xsl:value-of select="ns0:EventPageURL"/>
          </urn:Notes>
        <xsl:choose>
              <!--  EM Critical -->
              <xsl:when test="ns0:SeverityCode = '25'">
                <urn:Impact>1-Extensive/Widespread</urn:Impact>
              </xsl:when>
              <!--  EM Warning-->
              <xsl:when test="ns0:SeverityCode = '20'">
                <urn:Impact>2-Significant/Large</urn:Impact>
              </xsl:when>
                 <!--  Unreachable Start -->
              <xsl:when test="ns0:Severity = 'Unreachable Start'">
                <urn:Impact>1-Extensive/Widespread</urn:Impact>
              </xsl:when>
                <!--  Agent Unreachable Start -->
              <xsl:when test="ns0:Severity = 'Agent Unreachable Start'">
                <urn:Impact>1-Extensive/Widespread</urn:Impact>
                </xsl:when>
                <!--  Blackout Start -->
              <xsl:when test="ns0:Severity = 'Blackout Start'">
                <urn:Impact>2-Significant/Large</urn:Impact>
                </xsl:when>
                <!--  Metric Error Start-->
              <xsl:when test="ns0:Severity = 'Metric Error Start'">
                <urn:Impact>2-Significant/Large</urn:Impact>
              </xsl:when>
              <xsl:otherwise>
```

```
                <urn:Impact>3-Moderate/Limited</urn:Impact>
              </xsl:otherwise>
</xsl:choose>
        <urn:Incident_Number>
            <xsl:value-of select="ns0:TicketId"/>
          </urn:Incident_Number>
        <urn:Manufacturer></urn:Manufacturer>
        <urn:Product_Categorization_Tier_1></urn:Product_Categorization_Tier_1>
<urn:Product_Categorization_Tier_2></urn:Product_Categorization_Tier_2>
        <urn:Product_Categorization_Tier_3></urn:Product_Categorization_Tier_3>
        <urn:Product_Model_Version></urn:Product_Model_Version>
        <urn:Product_Name></urn:Product_Name>
        <urn:Reported_Source>Systems Management</urn:Reported_Source>
        <xsl:choose>
           <xsl:when test="ns0:Severity = 'Clear'">
                <urn:Resolution>Incident resolved by Oracle Enterprise Manager
                   because the associated alert has been cleared</urn:Resolution>
           </xsl:when>
            <xsl:when test="ns0:Severity = 'Agent Unreachable Clear'">
                <urn:Resolution>Incident resolved by Oracle Enterprise Manager
                   because the associated alert has been cleared</urn:Resolution>
</xsl:when>
            <xsl:when test="ns0:Severity = 'Blackout End'">
                <urn:Resolution>Incident resolved by Oracle Enterprise Manager
                   because the associated alert has been cleared</urn:Resolution>
            </xsl:when>
            <xsl:when test="ns0:Severity = 'Metric Error End'">
                <urn:Resolution>Incident resolved by Oracle Enterprise Manager
                    because the associated alert has been cleared</urn:Resolution>
            </xsl:when>
            <xsl:when test="ns0:Severity = 'Unreachable Clear'">
                <urn:Resolution>Incident resolved by Oracle Enterprise Manager
                    because the associated alert has been cleared</urn:Resolution>
            </xsl:when>
                <xsl:otherwise>
                        <urn:Resolution></urn:Resolution>
                </xsl:otherwise>
        </xsl:choose>
        <urn:Resolution_Category/>
        <urn:Resolution_Category_Tier_2/>
        <urn:Resolution_Category_Tier_3/>
        <urn:Resolution_Method/>
        <urn:Service_Type>Infrastructure Event</urn:Service_Type>
    <!--<urn:Status>Assigned</urn:Status>-->
        <xsl:choose>
           <xsl:when test="ns0:Severity = 'Clear'">
                <urn:Status>Resolved</urn:Status>
           </xsl:when>
            <xsl:when test="ns0:Severity = 'Agent Unreachable Clear'">
                <urn:Status>Resolved</urn:Status>
            </xsl:when>
            <xsl:when test="ns0:Severity = 'Blackout End'">
                <urn:Status>Resolved</urn:Status>
</xsl:when>
            <xsl:when test="ns0:Severity = 'Metric Error End'">
                <urn:Status>Resolved</urn:Status>
            </xsl:when>
            <xsl:when test="ns0:Severity = 'Unreachable Clear'">
                <urn:Status>Resolved</urn:Status>
            </xsl:when>
```

```
              <xsl:when test="ns0:GracePeriodCheckMade = 'Yes'">
                <urn:Status>Assigned</urn:Status>
              </xsl:when>
              <xsl:otherwise>
                  <urn:Status>Assigned</urn:Status>
              </xsl:otherwise>
          </xsl:choose>
          <xsl:choose>
             <xsl:when test="ns0:Severity = 'Clear'">
                  <urn:Status_Reason>Automated Resolution Reported</urn:
                         Status_Reason>
             </xsl:when>
              <xsl:when test="ns0:Severity = 'Agent Unreachable Clear'">
                  <urn:Status_Reason>Automated Resolution Reported</urn:
                         Status_Reason>
</xsl:when>
              <xsl:when test="ns0:Severity = 'Blackout End'">
                  <urn:Status_Reason>Automated Resolution Reported</urn:
                         Status_Reason>
              </xsl:when>
              <xsl:when test="ns0:Severity = 'Metric Error End'">
                  <urn:Status_Reason>Automated Resolution Reported</urn:
                         Status_Reason>
              </xsl:when>
              <xsl:when test="ns0:Severity = 'Unreachable Clear'">
                  <urn:Status_Reason>Automated Resolution Reported</urn:
                         Status_Reason>
              </xsl:when>
              <xsl:otherwise>
                  <urn:Status_Reason></urn:Status_Reason>
              </xsl:otherwise>
           </xsl:choose>
          <xsl:choose>
<!--  EM Critical -->
                <xsl:when test="ns0:SeverityCode = '25'">
                  <urn:Urgency>1-Critical</urn:Urgency>
                </xsl:when>
                <!--  EM Warning-->
                <xsl:when test="ns0:SeverityCode = '20'">
                  <urn:Urgency>2-High</urn:Urgency>
                </xsl:when>
                   <!--  Unreachable Start -->
                <xsl:when test="ns0:Severity = 'Unreachable Start'">
<urn:Urgency>1-Critical</urn:Urgency>
                </xsl:when>
                  <!--  Agent Unreachable Start -->
                <xsl:when test="ns0:Severity = 'Agent Unreachable Start'">
                  <urn:Urgency>1-Critical</urn:Urgency>
                  </xsl:when>
<!--  Blackout Start -->
                <xsl:when test="ns0:Severity = 'Blackout Start'">
                  <urn:Urgency>2-High</urn:Urgency>
                  </xsl:when>
                  <!--  Metric Error Start-->
                <xsl:when test="ns0:Severity = 'Metric Error Start'">
                  <urn:Urgency>2-High</urn:Urgency>
                </xsl:when>
                <xsl:otherwise>
                <urn:Urgency>3-Medium</urn:Urgency>
                </xsl:otherwise>
```

```
        </xsl:choose>
        <urn:Action>MODIFY</urn:Action>
        <urn:Work_Info_Type>Incident Task / Action</urn:Work_Info_Type>
        <urn:Work_Info_Date/>
         <urn:Work_Info_Source>System Assignment</urn:Work_Info_Source>
        <xsl:choose>
           <xsl:when test="ns0:Severity = 'Clear'">
                <urn:Work_Info_Notes>
                        Incident resolved by Oracle Enterprise Manager because the
                          associated alert has been cleared.</urn:Work_Info_Notes>
</xsl:when>
            <xsl:when test="ns0:Severity = 'Agent Unreachable Clear'">
                <urn:Work_Info_Notes>
                        Incident resolved by Oracle Enterprise Manager because the
                         associated alert has been cleared.</urn:Work_Info_Notes>
            </xsl:when>
            <xsl:when test="ns0:Severity = 'Blackout End'">
                <urn:Work_Info_Notes>
                        Incident resolved by Oracle Enterprise Manager because the
                         associated alert has been cleared.</urn:Work_Info_Notes>
            </xsl:when>
            <xsl:when test="ns0:Severity = 'Metric Error End'">
                <urn:Work_Info_Notes>
                        Incident resolved by Oracle Enterprise Manager because the
                         associated alert has been cleared.</urn:Work_Info_Notes>
            </xsl:when>
            <xsl:when test="ns0:Severity = 'Unreachable Clear'">
                <urn:Work_Info_Notes>
Incident resolved by Oracle Enterprise Manager because the associated alert has
been cleared.</urn:Work_Info_Notes>
</xsl:when>
            <xsl:when test="ns0:GracePeriodCheckMade = 'Yes'">
                <urn:Work_Info_Notes>
                Ticket reopened because the associated alert re-triggered at
<xsl:value-of select="ns0:Severity"/> severity within the grace period. Message:
<xsl:value-of select="ns0:Message"/>  </urn:Work_Info_Notes>
            </xsl:when>
        <xsl:otherwise>
                <urn:Work_Info_Notes>
                Ticket updated due to change in severity of the associated alert.
Severity:  <xsl:value-of select="ns0:Severity"/>  Message:  <xsl:value-of
select="ns0:Message"/>.
                </urn:Work_Info_Notes>
        </xsl:otherwise>
          </xsl:choose>
         <urn:Work_Info_Locked>No</urn:Work_Info_Locked>
         <urn:Work_Info_View_Access>Public</urn:Work_Info_View_Access>
        <urn:Work_Info_Summary>
                <xsl:value-of select="ns0:Message"/>
          </urn:Work_Info_Summary>
        </urn:HelpDesk_Modify_Status_Service>
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:transform>
```

3.7.2 Mapping the Fields

The tables in this section map the fields in all out-of-box ticket templates shipped with the Remedy Service Desk Connector.

Remedy_DefaultCategory_AutoClose.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 3–4 Ticket Updates (Remedy_DefaultCategory_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Categorization_Tier_1		Blank
Categorization_Tier_2		Blank
Categorization_Tier_3		Blank
Closure_Manufacturer		Blank
Closure_Product_Category_Tier1		Blank
Closure_Product_Category_Tier2		Blank
Closure_Product_Category_Tier3		Blank
Closure_Product_Model_Version		Blank
Closure_Product_Name		Blank
Company		"Internal" *
Summary	Message	

Table 3–4 (Cont.) Ticket Updates (Remedy_DefaultCategory_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Notes	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. TargetName TargetType MetricColumn — Name of the metric, such as CPU Utilization (%). MetricName — Category of the metric. For the CPU Utilization (%) metric, this would be 'Load.' KeyColumn ** — For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name.' KeyValues ** — For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity. Severity CollectionTime TargetHost NotificationRuleName EventPageURL — URL to the metric details page in the context of the alert.	
Impact	Severity	■ If severity is Critical, set Impact to 1-Extensive/ Widespread. ■ If severity is Warning, set Impact to 2-Significant/Large. ■ Otherwise, set Impact to 3-Moderate/Limited.
Manufacturer		Blank

Table 3–4 (Cont.) Ticket Updates (Remedy_DefaultCategory_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Product_Categorization_ Tier_1		Blank
Product_Categorization_ Tier_2		Blank
Product_Categorization_ Tier_3		Blank
Product_Model_Version		Blank
Product_Name		Blank
Reported_Source		"Systems Management" *
Resolution		Blank
Resolution_Category		Blank
Resolution_Category_Tier_2		Blank
Resolution_Category_Tier_3		Blank
Resolution_Method		Blank
Service_Type		"Infrastructure Event" *
Status		New *
Urgency	Severity	■ If severity is Critical, set Urgency to 1-Critical. ■ If severity is Warning,, set Urgency to "2-High" ■ Otherwise, set Urgency to 3-Medium.
Action		"MODIFY" *
Work_Info_Summary	Message	
Work_Info_Notes	Message, Severity	
Work_Info_Type		"Incident Task/Action" *
Work_Info_Date		Blank
Work_Info_Source		"System Assignment" *
Work_Info_Locked		Blank
Work_Info_View_Access		"Public" *
Incident_Number	TicketId — The connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated.	

Remedy_DefaultCategory.xsl

In the tables, * denotes a literal string and ** indicates `if the attribute applies.`

Table 3–5 Ticket Updates (Remedy_DefaultCategory_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Categorization_Tier_1		Blank
Categorization_Tier_2		Blank
Categorization_Tier_3		Blank
Closure_Manufacturer		Blank
Closure_Product_Category_Tier1		Blank
Closure_Product_Category_Tier2		Blank
Closure_Product_Category_Tier3		Blank
Closure_Product_Model_Version		Blank
Closure_Product_Name		Blank
Company		"Internal" *
Summary	Message	

Table 3–5 (Cont.) Ticket Updates (Remedy_DefaultCategory_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Notes	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. TargetName TargetType MetricColumn — Name of the metric, such as CPU Utilization (%). MetricName — Category of the metric. For the CPU Utilization (%) metric, this would be 'Load.' KeyColumn ** — For metrics that monitor a set of objects, KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, the KeyColumn is 'Tablespace Name.' KeyValues ** — For metrics that monitor a set of objects, the KeyValues indicate the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity. Severity CollectionTime TargetHost NotificationRuleName EventPageURL — URL to the metric details page in the context of the alert.	
Impact	Severity	■ If severity is Critical, set Impact to 1-Extensive/ Widespread. ■ If severity is Warning, set Impact to 2-Significant/Large. ■ Otherwise, set Impact to 3-Moderate/Limited.
Manufacturer		Blank

Table 3–5 (Cont.) Ticket Updates (Remedy_DefaultCategory_AutoClose.xsl)

Remedy Ticket Attributes	Enterprise Manager Alert Attributes	Value
Product_Categorization_ Tier_1		Blank
Product_Categorization_ Tier_2		Blank
Product_Categorization_ Tier_3		Blank
Product_Model_Version		Blank
Product_Name		Blank
Reported_Source		"Systems Management" *
Resolution		Blank
Resolution_Category		Blank
Resolution_Category_Tier_2		Blank
Resolution_Category_Tier_3		Blank
Resolution_Method		Blank
Service_Type		"Infrastructure Event" *
Status		If the grace period test has already been done and the alert is still within the grace period, reopen the ticket by setting the ticket to the Assigned status. Otherwise, set the status Assigned.
Urgency	Severity	■ If severity is Critical, set Urgency to 1-Critical. ■ If severity is Warning,, set Urgency to "2-High" ■ Otherwise, set Urgency to 3-Medium.
Action		"MODIFY" *
Work_Info_Summary	Message	
Work_Info_Notes	Message, Severity	
Work_Info_Type		"Incident Task/Action" *
Work_Info_Date		Blank
Work_Info_Source		"System Assignment" *
Work_Info_Locked		"No" *
Work_Info_View_Access		"Public" *
Incident_Number	TicketId — The connector adds this into the alert context before handling the ticketing action. Required by the Remedy Web service to identify the ticket that must be updated.	

3.7.3 Customizing Ticket Templates

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

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

Example 3–3 Creating a Template to Mark the <Company/> Element to MyCompany

To create a template to mark the category to `MyCompany`, modify the following attribute in the template:

```
<urn:Company>MyCompany</urn:Company>
```

Example 3–4 Altering the Message Type

If you only want the alert message to appear as ticket summary instead of both message and severity, modify the following attribute:

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

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

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

3.7.4 Defining New Templates

The out-of-box templates are based on the default HPD:IncidentInterface_Create,HPD:IncidentInterface forms. If the new ticket templates you define are based on these forms, Customizing Ticket Templates applies.

However, if you use a different form, you need to define a new ticket template.

Enterprise Manager Attributes

Table 3–6 provides the Enterprise Manager fields that you can map when using the default Remedy Service Desk Web services:

Table 3–6 Enterprise Manager Attributes

Data Fields	Description
EMUser	▪ For auto-ticketing, this is the notification rule owner. ▪ For manual ticketing, this is the console user that triggered the ticket creation.
HDUser	Service Desk user registered with the Connector; this is the same as the user name specified for the WS authentication.
TicketID	Identifies the ticket associated with the current alert (available after ticket creation).
ConnectorID	Identifies the connector that processed the event and issued the ticket creation or ticket update. This is the ID for the Remedy Service Desk Connector.
TargetType	Type of target that the alert is associated with, such as `host`.

Table 3–6 (Cont.) Enterprise Manager Attributes

Data Fields	Description
TargetName	Name of the target that the alert is associated with. For example, `Database1` or `stadc40.us.oracle.com`.
MetricColumn	Name of the metric that triggered the alert. For example, CPU Utilization(%).
MetricName	Category of the metric. For example, `Load` for the memory utilization alert.
KeyColumn	For metrics that monitor a set of objects, the KeyColumn indicates the type of object monitored. For example, for the Tablespace Space Used (%) metric that monitors tablespaceobjects, the KeyColumn is 'Tablespace Name'.
KeyValues	Key values associated with a key value base alert. For metrics that monitor a set of objects, the KeyValues indicates the specific object that triggered the severity. For example, for the Tablespace Space Used (%) metric that monitors tablespace objects, KeyValues is 'USERS' if the USERS tablespace triggered at warning or critical severity.
Message	Description of the alert. For example, CPU Utilization is 100%, crossed warning (80) or critical (95) threshold.
Severity	Severity of the alert: `critical, warning, clear,` or `down.`
CollectionTime	Timestamp of an alert occurrence.
EventPageURL	URL to the alert details page of the alert.
NotificationRuleName	Name of the notification rule that generated the notification during auto-ticketing.
TargetTimezone	Timezone of the target associated with the alert.
GracePeriodCheckMade	Value `Yes` indicates that the alert is cleared since the last update or creation, but is within the configured grace period.
TargetHost	Name of the server hosting the target that generated the alert.

Format for Creating Ticket Templates

To create ticket templates for custom Remedy forms, adhere to the following format:

Example 3–5 Template Format for Custom Remedy Forms

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

<!--
This template creates an incident type ticket with default categorization
(Category: Default, Type:Default, Item:Default), and low priority. On update,
the description and message fields are updated, and the ticket is closed if the
associated alert has cleared.
-->

<xsl:template match="ns0:EventModel">
<xsl:choose>
<xsl:when test="normalize-space(ns0:TicketId) = ''">
```

```
*[Insert your mappings from EMModel into your custom Create Ticket Webservice SOAP
Document] *

</xsl:when>
<xsl:otherwise>

* [Insert your mappings from EMModel schema into your Custom Update Ticket
Webservice SOAP Document]*

</xsl:otherwise>
</xsl:choose>
</xsl:template>
</xsl:transform>
```

3.8 Enabling SSL for HTTPS

Follow the instructions provided in this section if you choose HTTPS as the protocol to establish a connection between the Remedy AR server and Enterprise Manager.

3.8.1 Generating a Certificate Request File

Generate a certificate request file for the Remedy AR server and send it to the Certificate authority, such as VeriSign.

> **Note:** The certificate request file is dependent on the Web server that Remedy uses.

3.8.2 Importing the Certificate from the Certificate Authority

After you get the certificate, import it to the Web server that Remedy uses. The import mechanism varies depending on the Web server that the Remedy Service Desk uses.

3.8.3 Adding Signed Certificates to Wallet Manager

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

Do the following on Enterprise Manager:

1. As Super Administrator, create a wallet using the following `orapki utility` command at the OMS host:

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

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

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

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

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

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

Ensure that `ewallet.p12` is available.

4. In Oracle Wallet Manager, open the client certificate `ewallet.p12`.
5. Go to Select Trusted Certificates and select **Operations** on the main menu.
6. Select **Export All Trusted Certificates**.
7. Save the file as `certdb.txt`.
8. Place the file `certdb.txt` in the connector home root directory (`$OMS_HOME/sysman/connector`).

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

   You need to import HelpDesk_Query_Service_getIncident.def into your Remedy instance for a getTicket operation. By default on the Enterprise Manager Management Connector page, the web service endpoint for getTicket appears as HPD_IncidentInterface_get_WS. If you are not importing HelpDesk_Query_Service_getIncident.def, you need to modify the web service name in the web service endpoint with your custom web service name.

   If you want to use the Remedy_DefaultCategory_AutoResolve.xsl template, you need to import HPD_IncidentInterface_CustomWS.def. Back up the HPD_IncidentInterface_WS web service before importing. You can get this file from the $ORACLE_HOME/sysman/connector/Remedy_Service_Desk_Connector directory.

Now Java SSL can use this file for communication between Enterprise Manager and the Remedy AR server in HTTPS mode.

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

3.9 Remedy Service Desk Connector Tips

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

3.9.1 Recommended Protocol

Oracle recommends that you use HTTPS as the protocol for the communication between Enterprise Manager and Remedy AR server.

Use HTTP only if a secure connection is not required and the data can be transferred in clear text between the two systems.

3.9.2 Supported Alerts

This release supports the following types of alerts:

- Metric alerts
- Availability alerts

3.9.3 Web Service Details for Default Templates

If you choose default ticket templates, ensure that the following HPD:HelpDesk related Web services are up and running on the Remedy AR server:

- HPD_IncidentInterface_Create_WS
- HPD_IncidentInterface_WS

4

Installing and Configuring the Siebel Connector

The Siebel Connector integrates Siebel HelpDesk 8.x with Enterprise Manager. Using this connector, you can create a Siebel HelpDesk request, update an existing service request, or close a service request based on metric alerts in Enterprise Manager.

This chapter provides the following information for setting up and configuring the Siebel Connector:

4.1 Introduction to the Siebel Connector

The Siebel Connector integrates Enterprise Manager with Siebel HelpDesk through either an HTTP or HTTPS connection. You can create, update, or close tickets based on only the following types of alerts in Enterprise Manager:

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

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

4.1.1 Auto Ticketing

Whenever an alert is triggered in Enterprise Manager, the Siebel Connector can automatically open or update a service request. You can specify the set of alerts for which tickets must be opened and the alert severity for which this should happen.

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

> **See Also:** "Configuring Notifications" in *Oracle Enterprise Manager Advanced Configuration Guide*

After the ticket is opened, any subsequent update of the alert, such as a change in alert severity, causes an annotation to the ticket. After the alert is cleared (severity is set to `Clear`), the ticket can be optionally closed.

> **See Also:** "Creating Service Requests Automatically" on page 4-8

4.1.2 Manual Ticketing

From the Enterprise Manager Grid Control, you can choose to manually open a Siebel HelpDesk service request based on an open alert in Enterprise Manager. The Siebel Connector populates the ticket with details based on the alert and the ticket template.

4.1.3 Ticket Templates

Ticket templates are transformation style sheets in XSLT format that transform Enterprise Manager alerts to ticket format before the requests are sent to Siebel HelpDesk.

These templates specify how Enterprise Manager alert attributes can populate the fields of a Siebel service request.

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

4.1.4 Grace Period

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

For recurring alerts, the Grace Period is a time period during which reoccurrences of the same alert cause an existing ticket for the alert to be updated (or re-opened) instead of causing a new ticket to be opened.

For example, an alert triggers and a ticket is opened for it. If the Grace Period is one hour and the alert is cleared at 10:00 am, then if the same alert retriggers before 11:00 am (one hour grace period), the ticket that had been originally created for the alert is updated/reopened rather than creating a new ticket.

4.2 Prerequisites

Before using Siebel Connector, ensure that you meet the following prerequisites:

- Siebel HelpDesk 8.x is installed and configured.
- Siebel HelpDesk Web services are up and running.

4.3 Installing and Uninstalling the Siebel Connector

To install the Siebel Connector:

1. Copy the file `EMHelpdesk.jar` to the Oracle Management Service (OMS). In case of multiple OMSs, you have to copy the jar file for all OMSs.
2. Run the following command on all OMS's:

   ```
   emctl extract_jar connector EMHelpdesk.jar Siebel_Connector $ORACLE_HOME
   ```

   Files are extracted from the jar file to the following directory:

   ```
   $ORACLE_HOME/sysman/connector/Siebel_Connector
   ```

3. Ensure that the following files are extracted:
   - **SiebelDeploy.xml** — Connector Descriptior
   - **SiebelHelpdeskTemplate.xsl** — Ticket Template
   - **CreateResponse.xsl** — Ticket Response Template
   - **EMModel.xml** — Alert Schema

After you install Enterprise Manager, when you access the Enterprise Manager console as a Super Administrator, you can see the Siebel Connector in the Management Connectors. See "Configuring the Siebel Connector" for instructions.

To uninstall the Siebel Connector, select it in the Management Connectors page, then click **Delete**.

4.4 Registering the Connector Descriptor

After you install the Siebel connector, register the connector descriptor file `SiebelDeploy.xml` to describe the connector metadata and the configuration properties of the connector, such as Web service end points, authentication schema, and ticket URL pattern.

From the Oracle Management Server (OMS) host command window, run the following `emctl` command from the `$ORACLE_HOME/bin` directory:

```
emctl register_connector connector $ORACLE_HOME/sysman/connector/Siebel_
Connector/SiebelDeploy.xml host port database_SID username password $ORACLE_HOME
```

Table 4–1 emctl Parameters

Parameter	Description
`host`	Host name of the Enterprise Manager repository.
`port`	Listener port of the repository.
`database sid/ Service Name for RAC DB`	Repository database instance ID or service name if you are using RAC database as the repository.
`username`	Specify `SYSMAN`.
`password`	Password for `SYSMAN`.

4.5 Registering Ticket Templates

Ticket templates need to be registered before they are recognized in Enterprise Manager.

From the Oracle Management Server (OMS) host command window, run the following `emctl` command from the `$ORACLE_HOME/bin` directory:

```
emctl register_ticket_template connector $ORACLE_HOME/sysman/connector/Siebel_
Connector/siebelTemplates/SiebelHelpdeskTemplate.xsl host port database_SID
username password connector_type_name connector_name template_name template_
description
```

Table 4–2 emctl Parameters

Parameter	Description
`host`	Host name of the Enterprise Manager repository.
`port`	Listener port of the repository.
`database sid/ Service Name for RAC DB`	Repository database instance ID or service name if you are using RAC database as the repository.
`username`	Specify `SYSMAN`.
`password`	Password for `SYSMAN`.
`connectorTypeName`	Connector type name you define in `connectorType.xml`. For example, `"My Ticketing Connector"`. The double quotes ("") are mandatory.
`connectorName`	Connector name. This should be the same as the connector type name. For example, `"My Ticketing Connector"`.
`templateName`	An intuitive name for the ticket template to be displayed in Enterprise Manager.
`description`	A short description for the ticket template. This description is also displayed in Enterprise Manager.

4.6 Configuring the Siebel Connector

To configure the connector:

1. As Super Administrator, from Enterprise Manager Grid Control, click **Setup.**

   The Overview of Setup page appears.

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

   The Management Connectors page appears. The row for the ticketing connector should appear in this page.

3. Click the **Configure** icon for the connector that you just registered.

   The General tab of the Configure Management Connector page appears (Figure 4–1).

4. Configure the following:
   - Connection settings
     - Web Service End Points
     - Authentication details
   - Web Console settings

- Grace Period

See "General Settings" on page 5 for details.

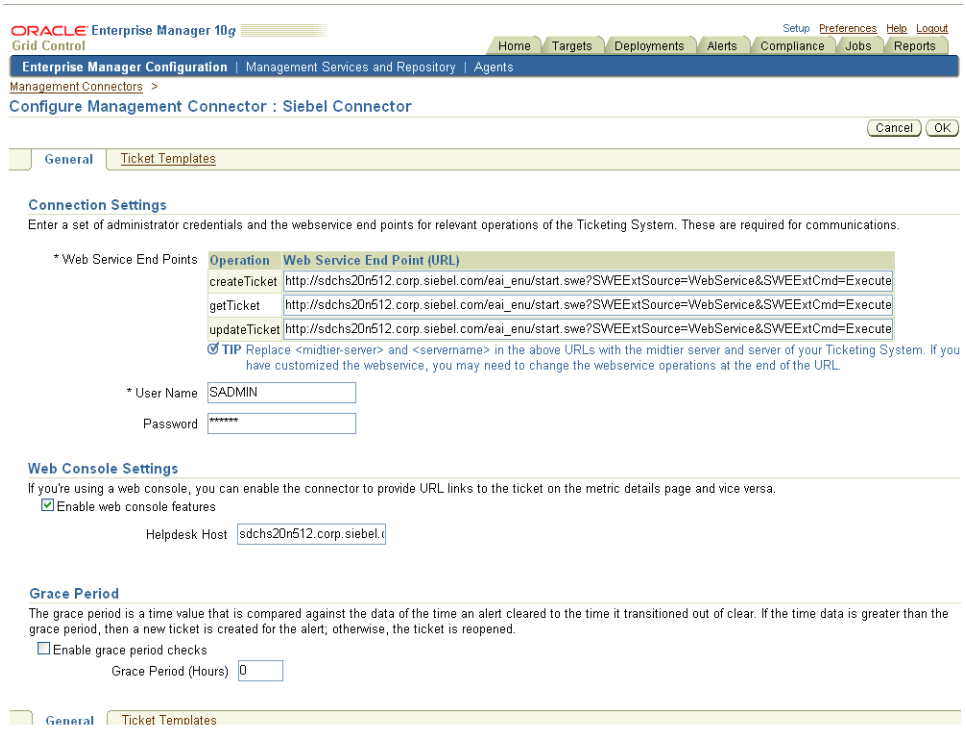
5. Click **OK.**

   The Management Connectors page reappears. The ticketing connector row should have a check mark in the Configured column.

6. In the Configure Management Connector page, go to the Ticket Templates tab (Figure 4–2) and ensure that ticket templates are successfully loaded.

If you choose HTTPS as the protocol to establish a connection between MOM and Enterprise Manager, see "Enabling SSL for HTTPS" on page 4-16.

Figure 4–1 Configure Management Connector General Page



4.6.1 General Settings

The following sections explain how to provide various configuration details.

4.6.1.1 Connection Settings

The HelpDesk Connector communicates with the Help Desk through their Web services. Mandatory fields are indicated by an asterisk (*).

- ***Web Service End Points** — Endpoints to `CreateTroubleTicket`, `UpdateTroubleTicket`, and `GetTroubleTicket` Web services exposed by Siebel Help Desk.
- ***Username**— User with the privilege to create, update, and query tickets in Siebel. All service requests created through the connector are generated using this user account.
- ***Password**— Password associated with the supplied Siebel user.

4.6.1.2 Web Console Settings

Web Console settings are required if you want the Connector to provide links from Enterprise Manager to the Siebel Help Desk application user interface. These links are the User Interface navigational links from Enterprise Manager to the Siebel Help Desk application user interface.

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

- **Enable Web console**— Check to launch the Siebel Service Request page within the context from Enterprise Manager.
- **HelpDesk Host**— Siebel HelpDesk hostname. Provide the machine name and port details of the Web server that hosts the Siebel Application User Interface (and not the details of Web services or the database server).

4.6.1.3 Grace Period

You can enable and disable the grace period and configure its value. By default, the grace period is disabled. See "Grace Period" on page 4-2 for details.

This setting applies to all alerts processed by Siebel Connector.

4.6.2 Working with Ticket Templates

The following sections provide information about viewing, removing, replacing, and adding ticket templates. Use the Configure Management Connector Ticket Templates page (Figure 4–2) to perform any of the activities mentioned in the following sections.

4.6.2.1 Viewing Template Code

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

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

4.6.2.2 Removing Templates

Important: If the template you delete has a notification rule associated with it, the notification fails.

---

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

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

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

4.6.2.3 Replacing Templates

To replace an existing ticket template, do the following in sequence:

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

4.6.2.4 Adding New Templates

To add templates, you should define new templates and register them using `emctl`.

See Also: "Customizing Ticket Templates" on page 18

Figure 4–2 Configure Management Connector Ticket Templates Page

4.6.3 Re-registering Removed Connectors

The Siebel Connector is automatically registered when Enterprise Manager is installed. However, you may remove this connector at some point and then want to subsequently re-register it.

To re-register a connector that has been removed:

1. Run the following command on all Oracle Management Servers:

   ```
   emctl extract_jar connector EMHelpdesk.jar Siebel_Connector $ORACLE_HOME
   ```

   Files are extracted from the jar file to the following directory:

   ```
   $ORACLE_HOME/sysman/connector/Siebel_Connector
   ```

2. From the Oracle Management Server (OMS) host command window, run the following `emctl` command from the `$ORACLE_HOME/bin` directory:

   ```
   emctl register_connector connector $ORACLE_HOME/sysman/connector/Siebel_
   Connector/SiebelDeploy.xml host port database_SID username password
   $ORACLE_HOME
   ```

3. Run the following `emctl` command from the same directory:

   ```
   emctl register_ticket_template connector $ORACLE_HOME/sysman/connector/Siebel_
   Connector/siebelTemplates/SiebelHelpdeskTemplate.xsl host port database_SID
   username password connector_type_name connector_name template_name template_
   description
   ```

Note: For multiple Oracle Management Servers, you only need to register the connector once from any of the Oracle Management Servers.

4.7 Creating Siebel Service Requests

You can create service requests automatically, or you can create them manually. The following sections explain how to create both types.

4.7.1 Creating Service Requests Automatically

Perform the following steps to create a ticket automatically:

1. From Enterprise Manager Grid Control, click **Preferences.**
2. In the left pane, under Notification, click **Rules,** then **Create**.
3. In the Create Notification Rule General page, specify the rule name, description, and the targets for which this rule should apply.
4. In the Create Notification Rule Availability page, select the availability states for which you want to create tickets.
5. In the Create Notification Rule Metrics page, select the metrics and their associated alert severities for which you want to create and update tickets.

   Ensure that you select all relevant alert severities if you want to update the ticket when the alert severity changes. For example, to open a ticket for a critical alert on the CPU Utilization(%) metric, and the ticket to be updated if the CPU Utilization(%) changes to warning or clear severity, then in the notification rule select `Critical`, `Warning`, or `Clear` severities for the CPU Utilization(%) metric.
6. In the Create Notification Rule Methods page, choose the ticket template from the Advanced Notification Methods table (Figure 4–3).

   In the table, registered ticket templates appear as Java Callback type notification methods under the same name as the ticket template's file name. This ticket template opens tickets for all availability and metric alerts specified in this notification rule.

   This makes the ticket templates available for use to open tickets.

   See Also: "Configuring Notifications" in *Oracle Enterprise Manager Advanced Configuration Guide*

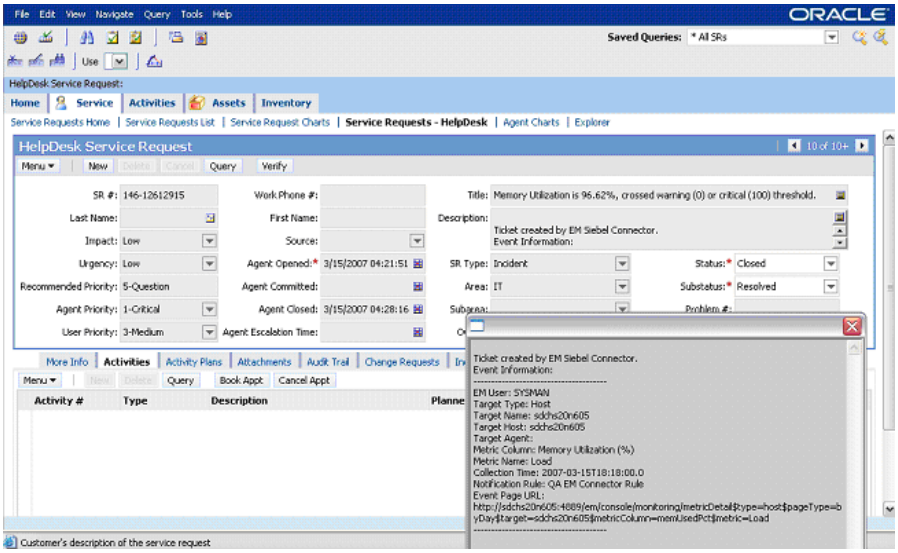
The following process occurs after you create the notification rule for your alerts:

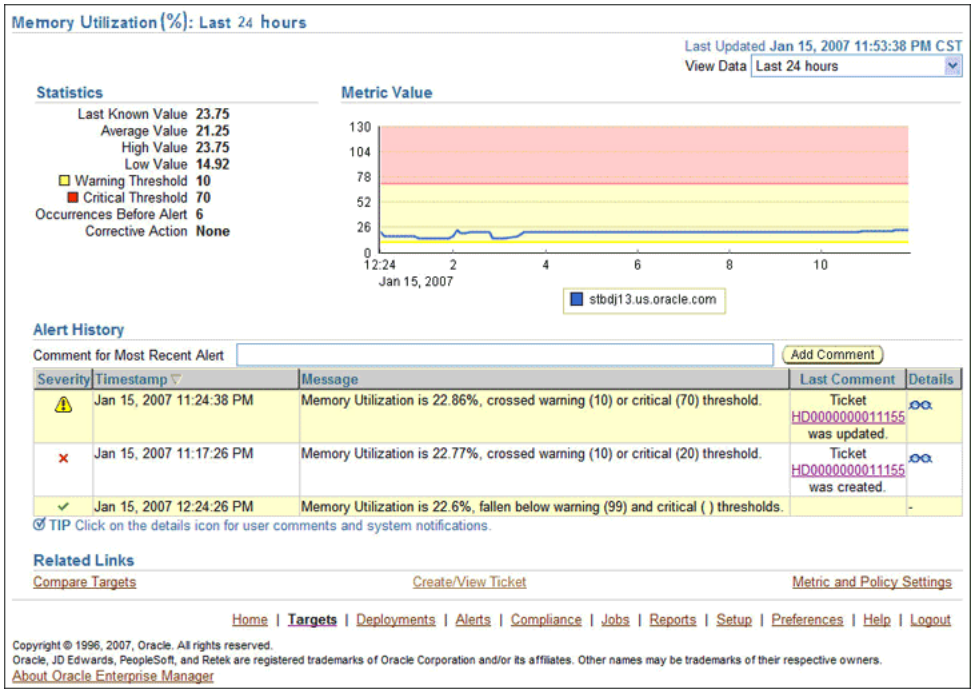
- A notification is sent to the Siebel Connector when a metric alert that matches your rule triggers.
- The Siebel connector creates/updates a ticket according to the ticket template as set in the notification rule.
- In Enterprise Manager, the alert annotation is updated. A comment is added to the Metric Details page of the alert to indicate that a ticket was created or updated, along with the ticket ID and ticket page URL.

A ticket is updated if there is an existing active ticket for an alert. In Figure 4–4, the first screen shows the ticket in the Siebel HelpDesk page, and the second screen shows the alert as it is displayed in Enterprise Manager.

Figure 4–3 Notification Methods

Figure 4–4 Siebel Service Request and the Alert as Displayed in Enterprise Manager





4.7.2 Creating Service Requests Manually

Perform the following steps to create a ticket manually:

1. After a metric alert occurs, go to the associated metric details page for the alert. To access this page, click the alert message in Enterprise Manager Grid Control (Figure 4–5).
2. Click the **Create/View Ticket** link in the Related Links section.

   The Create Ticket page appears if no active ticket exists for the alert.
3. Select a ticket template and then click **Submit** (Figure 4–6).

   If you do not see the desired template, you can register one using the `emctl` command. See "Registering Ticket Templates" on page 4-4.

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

   If the Web console settings are configured and enabled, the ticket ID appears as a link to the ticket page in the Siebel Help Desk. If there is no annotation, the ticket creation fails and error information is logged in the file `emoms.log`.

Note: You cannot manually update the ticket using the Siebel Connector. You have to manually update the ticket in the Siebel Help Desk for any subsequent alert change.

Figure 4–5 Metric Details Page

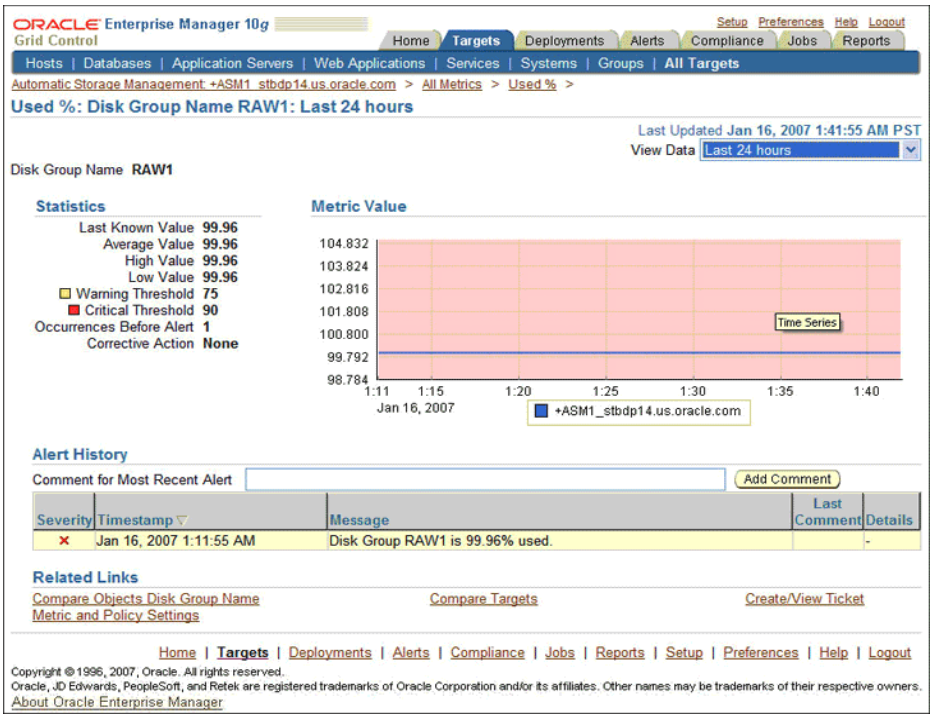


Figure 4–6 Create Ticket Page

4.8 Navigating Between Siebel HelpDesk and Enterprise Manager

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

4.8.1 Navigating from Enterprise Manager to Siebel

1. In Enterprise Manager Grid Control, click the alert message to go to the metric details page for the alert.
2. In the Alert History table, locate the ticket ID link in the Last Comment column.
3. (If not found) Click the icon in the Details column to get more information about the alert.
4. On the page that appears, locate the ticket ID in the Alert Details table.
5. Click the ticket ID link. You are forwarded to the Siebel HelpDesk login page.
6. Provide valid Siebel account details.

   The service request associated with this alert is displayed.

Note: If you do not use Siebel Web console, uncheck the Enable web console option in the Web Console Settings section so that the ticket ID is shown in plain text. Otherwise, it displays as a link that does not work.

4.8.2 Navigating from Siebel HelpDesk to Enterprise Manager

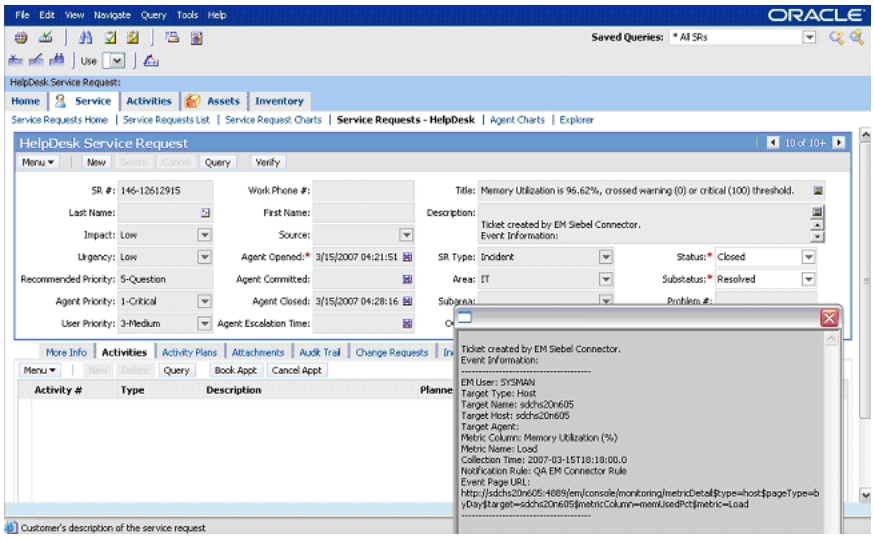
1. From the HelpDesk Service Request page (Figure 4–7), go to Description and copy the Event Page URL.
2. Search the URL using a Web browser.

   The Enterprise Manager Grid Control login page is displayed.
3. Specify the Enterprise Manager username and password.

   You are forwarded to the alert related to this service request.

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

Figure 4–7 Alert Details in Siebel HelpDesk Service Request Page



4.9 Reading Ticket Templates

When the Enterprise Manager connector creates an incident service request record, a data transformation occurs that maps the attributes of the Alert in Enterprise Manager with the attributes of a Service Request on the HelpDesk system. The trouble ticket template and response files specify this mapping. The logical mapping is summarized in Table 4–3. This table will help you to read the Siebel Ticket Template (`SiebelHelpdeskTemplate.xsl`).

Table 4–3 Service Request Payload and Enterprise Manager Event Mapping

Service Request Attributes	Enterprise Manager Event Attributes	Data Type	Default Value for Create	Default Value for Update
Id		DTYPE_ID		N/A
SR Number		DTYPE_TEXT		N/A
Status (SR_STAT_ID)		DTYPE_TEXT	Open/Closed	▪ Open if EM's Severity = Clear. ▪ Closed if EM's Severity = Clear
SR Type (SR_CAT_TYPE_CD)		DTYPE_TEXT	Internal	N/A
Service Request Type		DTYPE_TEXT	Internal	N/A

Table 4–3 (Cont.) Service Request Payload and Enterprise Manager Event Mapping

Service Request Attributes	Enterprise Manager Event Attributes	Data Type	Default Value for Create	Default Value for Update
Severity (SR_SEV_CD)	Severity **Helpdesk:** ■ 1—Critical ■ 2—High ■ 3—Medium **Enterprise Manager:** ■ Critical ■ Warning ■ Down	DTYPE_TEXT		
Abstract	Message. For example, CPU utilization increases from 50% to 95%.	DTYPE_TEXT		N/A
Area (SR_AREA)		DTYPE_TEXT	IT	N/A
Description	■ **TargetType:** Type of target that this event is associated with. For example, host or database. ■ **TargetName:** Name of the target that this event is associated with. For example, DB1 or stadc40.us.oracle.com. ■ **TargetHost:** Name of the host of the target that the event/alert was generated by. ■ **TargetAgent:** Name of the server hosting the agent that monitors the generated event. ■ **MetricColumn:** Name of the metric column as it appears on Enterprise Manager Grid Control. ■ **MetricName:** Name of the metric. For example, CPU utilization or memory usage. ■ **KeyValues:** Values associated with a key value base event. ■ **CollectionTime:** Time at which the event occurred. ■ **NotificationRuleName:** Name of the notification rule that generated the notification during auto-ticketing. ■ **Event Page URL:** URL for event details page.	DTYPE_TEXT		N/A

Siebel Ticket Template (SiebelHelpdeskTemplate.xsl)

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

```
      xmlns:ser="http://siebel.com/Service/ServiceReqEMHelpDesk"
      xmlns:data="http://www.siebel.com/xml/ServiceReqIO/Data"
      elementFormDefault="qualified">

  <!--
  This template creates an incident type ticket with default categorization
  (Category: Default, Type:Default, Item:Default), and high priority. On update,
  the description and message fields are updated.
  -->
   <xsl:template match="ns0:EventModel">
    <xsl:choose>
      <xsl:when test="normalize-space(ns0:TicketId) = ''">
        <!-- EDIT THE TAG VALUES BELOW TO CHANGE HOW A TICKET IS FILLED
             DURING TICKET CREATION. REFER TO THE MANUAL
             FOR DESCRIPTION OF THESE HELPDESK SUPPORT DATAFIELDS-->
       <ser:ServiceReqEMHelpDeskInsertAndQuery_Input
xmlns:data="http://www.siebel.com/xml/ServiceReqIO/Data">
          <data:ListOfServicereqio>
            <!--Zero or more repetitions:-->
            <data:ServiceRequest operation="?">
              <data:Abstract><xsl:value-of select="ns0:Message"/></data:Abstract>
              <data:Status>Open</data:Status>
              <data:ServiceRequestType>Internal</data:ServiceRequestType>
              <xsl:choose>
                <xsl:when test="normalize-space(ns0:Severity) = 'Critical'">
                  <data:Severity>1-Critical</data:Severity>
                </xsl:when>
                <xsl:when test="normalize-space(ns0:Severity) = 'Down'">
                  <data:Severity>2-High</data:Severity>
                </xsl:when>
                <xsl:when test="normalize-space(ns0:Severity) = 'Warning'">
                  <data:Severity>3-Medium</data:Severity>
                </xsl:when>
                <xsl:otherwise>
                  <data:Severity>5-Question</data:Severity>
                </xsl:otherwise>
              </xsl:choose>
              <data:Area>IT</data:Area>
              <data:Description>
Ticket created by EM Siebel Connector.
Event Information:
---------------------------------------
Target Type: <xsl:value-of select="ns0:TargetType"/>
Target Name: <xsl:value-of select="ns0:TargetName"/>
Target Host: <xsl:value-of select="ns0:TargetHost"/>
Target Agent: <xsl:value-of select="ns0:TargetAgent"/>
Metric Column: <xsl:value-of select="ns0:MetricColumn"/>
Metric Name: <xsl:value-of select="ns0:MetricName"/>
                <xsl:choose>
                  <xsl:when test="normalize-space(ns0:KeyColumn) != ''">
Key Column: <xsl:value-of select="ns0:KeyColumn"/>
Key Values: <xsl:value-of select="ns0:KeyValues"/>
                  </xsl:when>
                </xsl:choose>
Collection Time: <xsl:value-of select="ns0:CollectionTime"/>
                <xsl:choose>
                  <xsl:when test="normalize-space(ns0:NotificationRuleName) !=
''">
Notification Rule: <xsl:value-of select="ns0:NotificationRuleName"/>
                  </xsl:when>
```

```
                </xsl:choose>
Event Page URL: <xsl:value-of select="ns0:EventPageURL"/>
-------------------------------------
              </data:Description>
            </data:ServiceRequest>
          </data:ListOfServicereqio>
          <ser:LOVLanguageMode>LIC</ser:LOVLanguageMode>
          <!--Optional:-->
          <ser:ViewMode>All</ser:ViewMode>
        </ser:ServiceReqEMHelpDeskInsertAndQuery_Input>
      </xsl:when>
      <xsl:otherwise>
        <!-- EDIT THE TAG VALUES BELOW TO CHANGE HOW A TICKET IS FILLED
             DURING TICKET UPDATE. REFER TO THE MANUAL
             FOR DESCRIPTION OF THESE HELPDESK SUPPORT DATAFIELDS-->
        <ser:ServiceReqEMHelpDeskQueryAndUpdate_Input
xmlns:data="http://www.siebel.com/xml/ServiceReqIO/Data">
          <data:ListOfServicereqio>
            <!--Zero or more repetitions:-->
            <data:ServiceRequest operation="?">
            <data:SRNumber><xsl:value-of select="ns0:TicketId"/></data:SRNumber>
              <xsl:choose>
                <xsl:when test="normalize-space(ns0:Severity) = 'Critical'">
                  <data:Severity>1-Critical</data:Severity>
                  <data:Status>Open</data:Status>
                </xsl:when>
                <xsl:when test="normalize-space(ns0:Severity) = 'Down'">
                  <data:Severity>2-High</data:Severity>
                  <data:Status>Open</data:Status>
                </xsl:when>
                <xsl:when test="normalize-space(ns0:Severity) = 'Warning'">
                  <data:Severity>3-Medium</data:Severity>
                  <data:Status>Open</data:Status>
                </xsl:when>
                <xsl:when test="normalize-space(ns0:Severity) = 'Clear'">
                  <data:Status>Closed</data:Status>
                </xsl:when>
                <xsl:otherwise>
                  <data:Severity>5-Question</data:Severity>
                  <data:Status>Open</data:Status>
                </xsl:otherwise>
              </xsl:choose>
            </data:ServiceRequest>
          </data:ListOfServicereqio>
          <ser:LOVLanguageMode>LIC</ser:LOVLanguageMode>
          <!--Optional:-->
          <ser:ViewMode>All</ser:ViewMode>
        </ser:ServiceReqEMHelpDeskQueryAndUpdate_Input>
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:transform>
```

4.10 Enabling SSL for HTTPS

Follow the instructions provided in this section if you choose HTTPS as the protocol to establish a connection between Siebel Help Desk and Enterprise Manager.

4.10.1 Generating a Certificate Request File

Generate a certificate request file for the Siebel Help Desk and send it to the Certificate authority; for example, VeriSign.

> **Note:** The certificate request file is dependent on the Web server Siebel uses.

4.10.2 Importing the Certificate from the Certificate Authority

After you get the certificate, import it to the Web server Siebel uses. The import mechanism varies depending on the Web server used by Siebel Help Desk.

4.10.3 Adding Signed Certificates to Wallet Manager

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

Do the following in Enterprise Manager:

1. As Super Administrator, create a wallet by entering the following `orapki utility` command at the OMS host:

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

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

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

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

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

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

   Ensure that `ewallet.p12` is available.

4. In Oracle Wallet Manager, open the client certificate `ewallet.p12`.
5. Go to Select Trusted Certificates and select **Operations** on the main menu.
6. Select **Export All Trusted Certificates**.
7. Save the file as `certdb.txt`.
8. Place the file `certdb.txt` in the connector home root directory (`$OMS_HOME/sysman/connector`).

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

Now the Java SSl can use this file for communication between Enterprise Manager and the Siebel server in HTTPS mode.

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

4.11 Siebel Connector Tips

This section provides various tips that might help you to use the Siebel Connector effectively.

4.11.1 Recommended Protocol

Oracle recommends that you use HTTPS as the protocol for the communication between Enterprise Manager and Siebel HelpDesk.

Use HTTP only if a secure connection is not required and the data can be transferred in clear text between the two systems.

4.11.2 Supported Alerts

This release supports the following types of alerts:

- Metric alerts
- Availability alerts

4.11.3 Notification Failure

Notification is blocked for processing if the notification device is down due to any issues. For instance, the Siebel HelpDesk server is down, the Siebel HelpDesk configuration on Enterprise Manager is wrong, or the service request is removed in Siebel HelpDesk.

Notification failure on one target impacts all other targets of the same target type for which the rule applies. That is, subsequent notifications are blocked until the issue is fixed or the maximum retrials fail.

Note: The maximum retrial period is one day.

4.11.4 Customizing Ticket Templates

If the Siebel ticket templates do not satisfy your requirements, you can modify them. To do this, Oracle recommends that you use `SiebelHelpdeskTicketTemplate.xsl` as the base template. Copy this ticket template to a new file, modify, and register the new ticket template.

For example, to change the mapping or add more severity attributes based on Enterprise Manager Alert's severity, modify the following attributes:

```
<xsl:choose>
  <xsl:when test="normalize-space(ns0:Severity) = 'Critical'">
    <data:Severity>1-Critical</data:Severity>
  </xsl:when>
  <xsl:when test="normalize-space(ns0:Severity) = 'Down'">
    <data:Severity>2-High</data:Severity>
  </xsl:when>
  <xsl:when test="normalize-space(ns0:Severity) = 'Warning'">
    <data:Severity>3-Medium</data:Severity>
  </xsl:when>
  <xsl:otherwise>
    <data:Severity>5-Question</data:Severity>
  </xsl:otherwise>
</xsl:choose>
```

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

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

4.11.5 Customizing the Connector Descriptor

You can customize the connector descriptor. You can modify the URL that navigates from Enterprise Manager to the Siebel application User Interface. This might be required, for instance, when you do a non-English deployment. The default URL to the Siebel application User Interface is for an English language deployment and therefore, for other languages, you have to modify the default URL.

To customize the connector descriptor, do the following:

1. Modify the connector descriptor XML file `SiebelDeploy.xml`.
   a. Modify the bookmark URL.

      For instance, in the following sample URL, modify *`eai_enu`* for a non-English deployment.

      ```
      http://hostname/eai_
      enu/start.swe?SWEExtSource=WebService&SWEExtCmd=Execute
      ```

   b. Based on the format of the URL, parameterize the information that you want to configure using the Connector Configuration page. For details, refer to the section "Defining XML and XSL Files" in the *Oracle Enterprise Manager Integration Guide*.
2. Register the new connector descriptor.

Index

L

M

N

O

P

R

S

T

U

V

W

X