

## **Oracle® Enterprise Manager**

Installation and Configuration Guide for Microsoft Operations  
Manager Connector

10g Release 4 (10.2.0.4)

**E14984-01**

May 2009

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

# Contents

<b>Preface</b> .....	v
Audience .....	v
Documentation Accessibility .....	v
Related Documents .....	vi
Conventions .....	vi
 <b>1 Introduction to the Connector</b>	
 <b>2 Installing and Configuring the Connector</b>	
Prerequisites .....	2-1
Installing and Uninstalling the MOM Connector .....	2-1
Re-registering Removed Connectors .....	2-2
Configuring the MOM Connector .....	2-2
General Settings .....	2-4
Creating Additional Target Instances .....	2-5
Response Status of Targets .....	2-6
 <b>3 Sending and Receiving Alerts</b>	
Sending Enterprise Manager Alerts to MOM .....	3-1
Prerequisites .....	3-1
Configuring Rules to Send Alerts .....	3-1
Migrating from 10.2.0.3 to 10.2.0.4 .....	3-2
Receiving MOM Alerts in Enterprise Manager .....	3-2
Prerequisites .....	3-2
Forwarding Alerts to Enterprise Manager .....	3-2
How Enterprise Manager Responds .....	3-3

## **4 Enabling SSL for HTTPS**

Generating a Certificate Request File .....	4-1
Using the Certificate from the Certificate Authority .....	4-1
Adding Signed Certificates to Wallet Manager.....	4-2

## **A Connector Tips**

## **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

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

## Related Documents

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

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

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

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

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

Printed documentation is available for sale in the Oracle Store at

<http://oraclestore.oracle.com/>

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

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

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

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

## Conventions

The following text conventions are used in this document:

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





---

## Introduction to the Connector

The Microsoft Operations Manager (MOM) 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.

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 3-1.

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 2-2.



---

# Installing and Configuring the 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 for installing and configuring the connector:

- [Prerequisites](#)
- [Installing and Uninstalling the MOM Connector](#)
- [Re-registering Removed Connectors](#)
- [Configuring the MOM Connector](#)

## 2.1 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"](#) on page A-1 for the procedure.

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

## 2.2 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 2–1](#). See "[Configuring the MOM Connector](#)" for instructions.

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

## 2.3 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.

---

---

## 2.4 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 2–1](#)).

---

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

---

**Figure 2–1 Management Connectors Page**

Oracle Enterprise Manager 10g  
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports

Enterprise Manager Configuration | Management Services and Repository | Agents

Overview of Setup  
Roles  
Administrators  
Notification Methods  
Patching Setup  
Blackouts  
Registration  
Passwords  
Management Pack Access  
Monitoring Templates  
Corrective Action Library  
Management Plug-ins  
**Management Connectors**  
Client System Analyzer in Grid Control  
Data Exchange

### Management Connectors

A Management Connector is a component that integrates different enterprise frameworks into the Enterprise Manager Console. This page lists the available connectors. In order to use them on your system, they must be configured.

Page Refreshed Dec 18, 2007 12:43:10 PM

Select Name	Version	Description	Configured	Configure
<input type="radio"/> Microsoft Operations Manager Connector	2.0.0.0	Microsoft Operations Manager Integration with Enterprise Manager	<input checked="" type="checkbox"/>	
<input type="radio"/> Remedy Connector	2.0.0.0	Remedy integration with EM	<input type="checkbox"/>	

Related Links

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](#)" for details ([Figure 2–2](#)).
5. Click **OK**.
6. **Optional:** Go to the Targets tab and specify the details for creating additional target instances. See "[Creating Additional Target Instances](#)" 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 [Chapter 4, "Enabling SSL for HTTPS"](#).

**Figure 2–2 Configure Management Connector Page**

ORACLE Enterprise Manager 10g  
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports

Enterprise Manager Configuration/Management Services and Repository/Agents  
Management Connectors >

**Configure Management Connector: Microsoft Operations Manager Connector** [Cancel] [OK]

**General** **Targets**

In order to configure the MOM Connector, the MOM WebService must be already enabled, MOM Security should also be enabled by registering the Enterprise Manager IP Address to communicate with MOM.

**Connection Settings**

Specify the connection parameters for the MOM system. These are required for the communications.

\* MOM Registered Connector Name: MOM Connector125

\* Resolution State: 125  
The Resolution state must be an unassigned numeric value in MOM.

\* Protocol: ☒ http ☐ https

\* Server: 130.35.70.18

\* Port: 1271

\* Service Name: ConnectorServiceV2.asmx

\* Enterprise Manager Username: sysman

\* Enterprise Manager Password:

**Polling Interval**

The polling interval specifies how frequently Enterprise Manager will ping the external system for event information.

Polling Interval (Minutes): 5

## 2.4.1 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 to 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.

## 2.4.2 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 \(Optional\)](#)" below, 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 2–3](#) 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 host name (host name 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 2–3 Configure Management Connector Target Page**

ORACLE Enterprise Manager 10g  
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports

Enterprise Manager Configuration | Management Services and Repository | Agents

Management Connectors >

Configure Management Connector: Microsoft Operations Manager Connector

Cancel OK

General Targets

**Default Connector Target**

Configuring the connector automatically creates a default managed target instance in Enterprise Manager, in order to retrieve events from the external system. Optionally you can create additional target instances to represent the managed entities from the external system. It is highly recommended that you do not delete the default target.

Default Connector Target `generic_mom_managed_host` Enable

**Targets Managed by External System**

In order to associate alerts from a specific managed entity from the external system to a corresponding target instance within Enterprise Manager, you can create the specific target instances by providing the following instance properties. Alerts for the following target instances will not show up under the default managed target for this connector.

Remove Add 5 Rows

Select All | Select None

Select Target Name	MOM HOSTNAME
<input type="checkbox"/> SMP-MPI2	smp-mpi2.us.oracle.com
<input type="checkbox"/> SMP-MPI3	smp-mpi3.us.oracle.com
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

Remove Add 5 Rows

General Targets

Cancel OK

Home | Targets | Deployments | Alerts | Compliance | Jobs | Reports | Setup | Preferences | Help | Logout

Copyright © 1996, 2007, Oracle. All rights reserved.  
Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.  
[About Oracle Enterprise Manager](#)

## 2.4.3 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.

---



---

## Sending and Receiving Alerts

You can either send Enterprise Manager alerts to MOM in real-time, or you can forward MOM events to Enterprise Manager as explained in the following sections:

- [Sending Enterprise Manager Alerts to MOM](#)
- [Receiving MOM Alerts in Enterprise Manager](#)

### 3.1 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.

#### 3.1.1 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.

#### 3.1.2 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.

### 3.1.3 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.

## 3.2 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.

### 3.2.1 Prerequisites

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

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

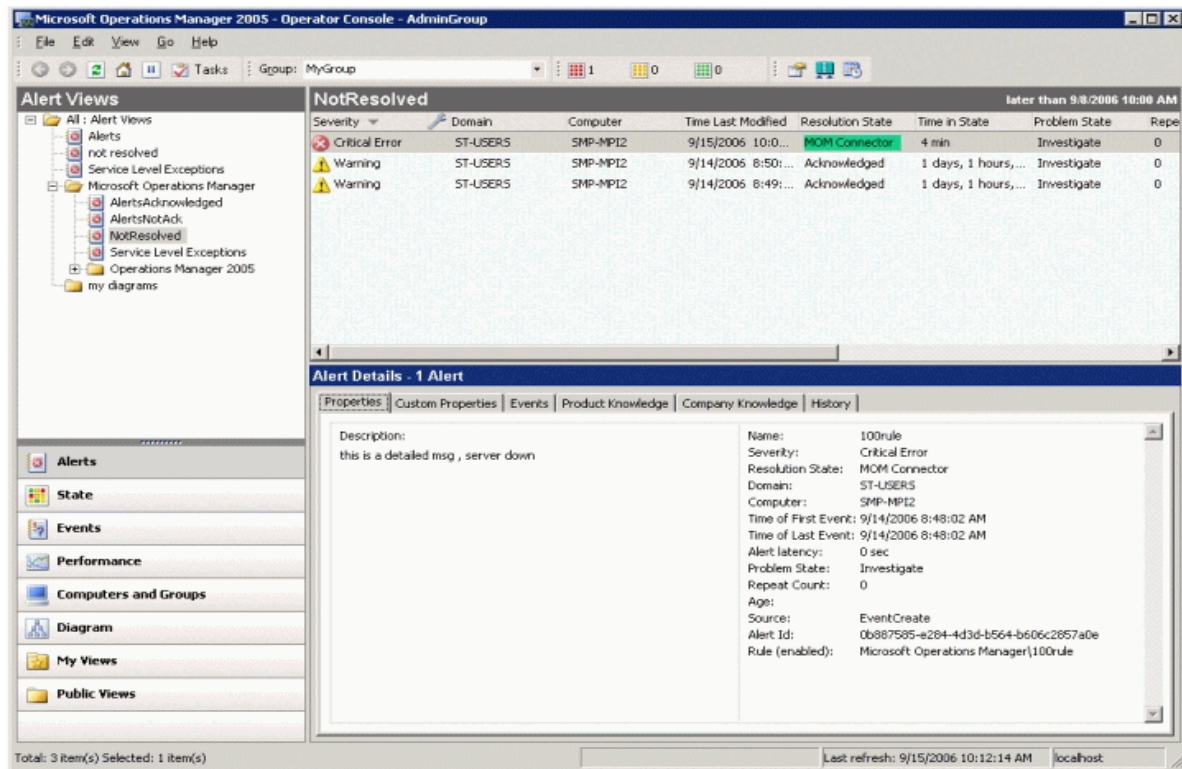
### 3.2.2 Forwarding Alerts to Enterprise Manager

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 3–1](#) 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 3–1 Alert Forwarded to Enterprise Manager**

### 3.2.3 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.



---

## Enabling SSL for HTTPS

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

### 4.1 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.

### 4.2 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 example:

```

-----BEGIN CERTIFICATE-----
MIICdzCCA8CAQAwDQYJKoZIhvcNAQEEBQAwITELMAkGA1UEBhMCVVMxEjAQBgNVBAMMCXJvb3Rf
dGVzdDAeFw0wNjExMTAxMDI5MzJaFw0xNjExMDcxMDI5MzJaMGYxCzAJBgNVBAYTAlVTMQ4wDAYD
VQIIEWUZXhhczEPMA0GA1UEBxMGRGFsbGFzMQ8wDQYDVQQKEWZvcmljYUx0CzAJBgNVBAsTAkVN
MRgwFgYDVQQDEw9zbXAtdXBpMi1vcmlvcmFwa2kgZ8wDQYJKoZIhvcNAQEEBQADgY0AMIGJAoGBAOch
GIHp6MFW78OQw/mSdU0xfVq5u9pgqndnTqoh4aGFg1bTZD6/Azf3Nn8ibtKVJmGp3PLa3xP/gk7S
tjZ/9sM4bvnw0Y4U9xsj0BiDG4JBo35uXAUxDHLReh8F4x45Wtv/SxvE0tjNnESlBMynLip7P9l
fSzcGKjSViyFW9M9AgMBAAEwDQYJKoZIhvcNAQEEBQADggEBAIktFTvDs7ULf0PclYXsJPek4vFq
7HZ86omktA9lYS+oA6SaudwDGY5yxc19O2s78o+EK9e8Wz4wM4dmUg4aSuHVVHs75W86uh7gpEFo
wssH9mtcxkqIbdPVwQoeAUTVOifNaujfxTgClvlvOjkfzvvd7SierjD9mP2rJ2pRWUbv7xR7oJmt
RXp6t22a+MKMQQR8ofAZV/WxFJcgmBR/JxLA28X+jnzmIH/yqHK/b6Agwwy7PgbJrwPI7WQ/busm
6ASeV8ZgSfAkJ83nWz4NICnH5Y8Dyu8vDtERsOQ8z/WttrBDEmcGikk09P+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.

### 4.3 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.

Now Java SSL can use this file for communication between Enterprise Manager and MOM 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)*.



---

## Connector Tips

This appendix provides various tips that might help you to resolve issues you may 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.

---

---

---

# Index

## A

---

alerts per polling, MOM Connector, A-2  
alerts, sending to external systems, 3-1

## C

---

certificate from certificate authority, MOM Connector, 4-1  
creating  
    additional target instances for MOM Connector, 2-5

## D

---

default connector target, MOM Connector, 2-5  
description of MOM Connector, 1-1, 2-1

## E

---

external systems, sending alerts to, 3-1

## G

---

generating certificate request file, MOM Connector, 4-1

## I

---

installing  
    MOM Connector, 2-1  
Internet Information Services (IIS), 2-1

## M

---

Microsoft Operations Management (MOM) Connector  
    alerts per polling, A-2  
    creating additional instances, 2-5  
    default connector target, 2-5  
    description of, 1-1, 2-1  
    general settings, 2-4  
    generating certificate request file, 4-1  
    installing, 2-1  
    polling interval, A-2  
    prerequisites, 2-1  
    recommended protocol, A-1  
    response status of targets, 2-6

    targets managed by external system, 2-5  
    targets, response status of, 2-6  
    using certificate, 4-1  
Microsoft Operations Manager 2005, 2-1  
MOM Configure Management Connector Page,  
    picture of, 2-4  
MOM Connector  
    SSL for HTTPS, 4-1  
    Wallet Manager, 4-2  
MOM Connector framework Web services, 2-1

## P

---

pictures  
    MOM Configure Management Connector Page, 2-4  
polling interval, MOM Connector and, A-2  
prerequisites  
    Internet Information Services (IIS), 2-1  
    Microsoft Operations Manager 2005, 2-1  
    MOM Connector framework Web services, 2-1

## R

---

recommended protocol  
    MOM Connector, A-1  
registering  
    re-registering removed connectors, 2-2  
removed connectors, re-registering, 2-2  
response status of targets, MOM Connector, 2-6

## S

---

settings for MOM Connector, 2-4  
SSL for HTTPS  
    MOM Connector, 4-1

## T

---

target instances and MOM Connector, 2-5  
targets  
    managed by external system, MOM Connector, 2-5  
    response status for MOM Connector, 2-6

## **U**

---

using certificate, MOM Connector, 4-1

## **W**

---

Wallet Manager  
MOM Connector, 4-2