

Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Microsoft SQL Server

Release 8 (3.3.3.1.0)

E12776-01

August 2008

This document provides a brief description about the Oracle System Monitoring Plug-in for Microsoft SQL Server, details on the versions the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

Description

The System Monitoring Plug-in for Microsoft SQL Server extends Oracle Enterprise Manager Grid Control to add support for managing Microsoft SQL Server instances. By deploying the plug-in within your Grid Control environment, you gain the following management features:

- Monitor SQL Server instances.
- Gather configuration data and track configuration changes for SQL Server instances.
- Raise alerts and violations based on thresholds set on monitored metrics and configuration data.
- Provide rich out-of-box reports based on the gathered data.
- Support monitoring by a local or remote Agent. Local Agent is an agent running on the same host as the SQL Server. Remote Agent is an agent running on a host that is different from the host where SQL Server is running.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10.2.0.3 or higher
- Oracle Management Agent 10.2.0.1 or higher for Windows
- Standard, Enterprise, and Workgroup editions of Microsoft SQL Server 2000 and Microsoft SQL Server 2005 as detailed below:
 - Microsoft SQL Server 2000 (32-bit)
 - Microsoft SQL Server 2005 (32-bit)
 - Microsoft SQL Server 2005 (64-bit) running on x64 or Itanium-based servers
- Microsoft SQL Server 2005 Cluster (Active Passive)

Prerequisites

The following prerequisites must be met before you can deploy the plug-in:

- Install Microsoft SQL Server 2000 or Microsoft SQL Server 2005, or Microsoft SQL Server 2005 Cluster (Active-Passive).
 - Install the following components of Oracle Enterprise Manager Grid Control:
 - Oracle Enterprise Manager Grid Control 10.2.0.3 or higher
 - Oracle Management Agent for Windows 10.2.0.1 or higher

For 10.2.0.1 Agent, apply the one-off patch for bug #5587980. Refer to Metalink and Oracle bug #5587980 for more information.

For 10.2.0.2 Agent, apply the one-off patch for bug# 5587980. Refer to Metalink and Oracle bug #5587980 for more information.

You can install the Agent on the same computer as SQL Server 2000 or SQL Server 2005 (referred to as local Agent monitoring), or you can install the Agent on a different computer from SQL Server (referred to as remote Agent monitoring).
 - If you want to perform local monitoring of Microsoft SQL Server 2005 Cluster (Active-Passive), then install an Agent on each node of the cluster and also with virtual group active on each node one, after the other (this can be done by moving the group to each cluster member). Also, create or deploy a virtual agent service on the active cluster member node servicing the group. For information about configuring Grid Control Agents in Windows HA - Failover Cluster Environments, see Oracle *Metalink* note 464191.1.
- For example, for a two-node active/passive cluster, after following the steps outlined in Oracle *Metalink* note 464191.1, three Agents additionally will be listed as Agent targets in the Enterprise Manager Grid Control console - two representing the Agents installed on the cluster nodes and one representing the virtual agent service.
- As part of JDBC URL, either IP Address or host name can be provided. Ensure that the host name can be resolved consistently on the network. Standard TCP tools such as "nslookup" and "tracert" can be used to verify the host name. Validate using the following commands on Management Agent where plug-in is deployed:
 - nslookup <hostname>

This returns the IP address and fully qualified host name.

 - nslookup <IP>
- This returns the IP address and fully qualified host name.
- (For SQL Server 2000) Windows Management Instrumentation (WMI) provider of the SQL Server are installed and enabled. Enable support by running the setup.exe file located in the SQL Server Installation CD. For more information, see "[Installing and Enabling Windows Management Instrumentation](#)" on page -8.
- ```
<CD_Drive>/x86/other/wmi
```
- Windows Management Instrumentation Service is up and running.

- Preferred credentials are set and validated on all Agents where you want to deploy the plug-in. For more information, see "[Configure the Management Agent to Deploy the Plug-In](#)" on page -4.
- (For Agent running on Microsoft Windows) OS privileges for the user (set in the Preferred Credentials for the Agent) must meet the requirements documented in "Setting Credentials for the Job System to Work with Enterprise Manager" in one of the following installation guides:
  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (32-Bit) — B14316-01
  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (64-Bit) on Intel Itanium — B14317-02
  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (x64) — B15681-02

These guides are listed in the Installation Guides section of the Oracle Database Documentation Library at the following location:

<http://www.oracle.com/pls/db102/homepage>

---



---

**Note:** If you do not assign the correct privileges for users, the deployment will fail.

---



---

- Enable TCP/IP for the SQL Server instance. For more information, see "[Enabling and Finding TCP/IP Port Information](#)" on page -8 .
- Enable SQL or Mixed Authentication on the SQL Server instance. For more information, "[Enabling SQL Authentication or Mixed Authentication](#)" on page -7.
- Create a suitable DB user with 'sysadmin' fixed server role.

## Configure the Management Agent to Deploy the Plug-In

To configure the Agent, you must first ensure that the user starting the Agent service belongs to the Local Administrators Group. Also, you must set the preferred credentials on all Agents where you want to deploy the plug-in. To do so, follow the instructions given in the following sections.

### Assigning Advanced Privileges to User

To assign advanced privileges, do the following:

1. Locally on the Microsoft Windows node hosting the Agent, check that the user starting the Agent service belongs to the Local Administrators Group. If not, add it.
2. Open the Local Security Settings Windows Tool and give the following Advanced Privileges to the user starting the Agent service:
  - Act as part of the operating system
  - Adjust memory quotas for a process
  - Logon as batch job

- Replace a process level token
- 3. Restart the Agent service if it is running.
- 4. Set the Preferred Credentials for the Host and the Agent in the Grid Control. For more information, see "[Setting and Validating Preferred Credentials](#)" on page -4.
  - The OS user set in the Preferred Credentials must belong to the Local Administrators Group.
  - This OS user must have the following Advanced Privileges:
    - Act as part of the operating system
    - Adjust memory quotas for a process
    - Logon as batch job
    - Replace a process level token

## Setting and Validating Preferred Credentials

To set the preferred credentials on all Agents where you want to deploy the plug-in, do the following:

1. In Enterprise Manager Grid Control, click **Preferences**.
2. In the Preferences page, click **Preferred Credentials** in the left pane.

The Preferred Credentials page appears.
3. For the corresponding Target Type, for the Host target type, from the **Set Credentials** column, click the icon.
4. In the Host Preferred Credentials page, in the Target Credentials section, for the host that is running the Management Agent where the plug-in has to be deployed, specify the user name and password.
5. After setting the credentials, on the same page, click **Test**. If you test runs successfully, your credentials are set correctly.
6. Run the OS Command job for the Management Agent where the plug-in has to be deployed.
  - Log in to Enterprise Manager Grid Control.
  - Click the **Jobs** tab.
  - In the Job Activity page, from the Create Job list, select **OS Command**, and click **Go**.
  - Fill up the details required in the following pages, and click **Submit** to run the job. If the job runs successfully, your credentials are set correctly.

## Deploying the Plug-in

After you ensure that the prerequisites are met, follow these steps to deploy the plug-in .

---

---

**Note:** If you want to perform local monitoring of Microsoft SQL Server Clusters, then:

- Deploy the plug-in on each node of the cluster where the local Agent is running. Local Agent is the agent running on each node of the cluster. Do not deploy on the virtual host.
- Repeat step 9, 10, and 11.
- Navigate to the `bin` directory of Virtual Agent Service host and run the following command. [On this Virtual Agent Service home page, if the **Add** drop-down list does not list the target name **Microsoft SQL Server**, then refresh the home page].

```
.\emctl reload agent
```

---

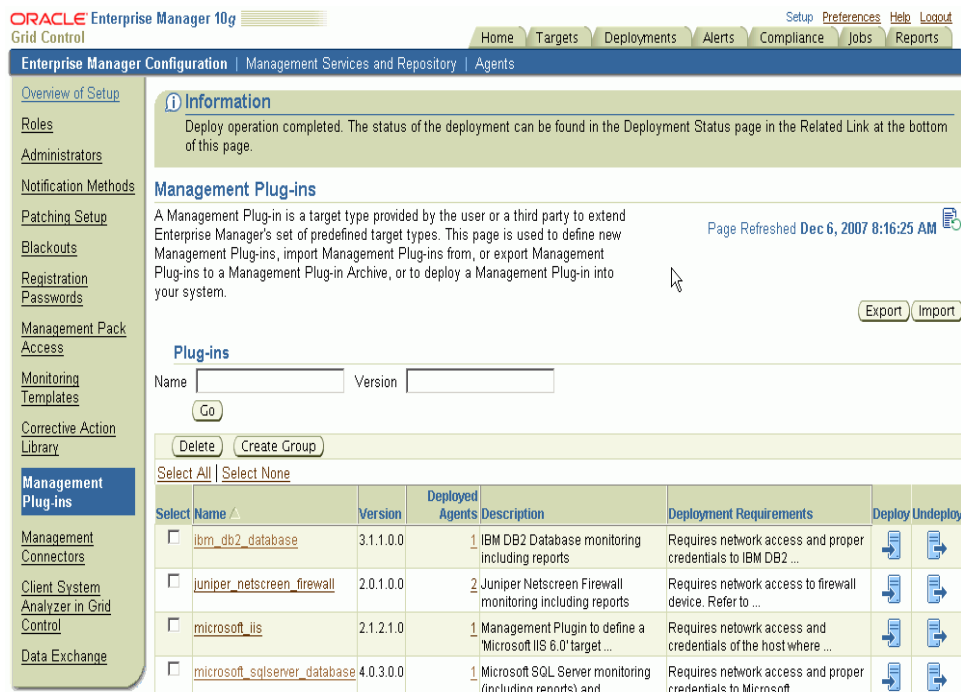
---

1. Download the SQL Server Plug-in archive to your desktop or computer on which the browser is launched. You can download the archive from the Oracle Technology Network (OTN).
2. Log into Enterprise Manager Grid Control as a Super Administrator.
3. Click the **Setup** link in the upper right corner of the Grid Control Home page, then click the **Management Plug-ins** link on the left side of the Setup page.
4. Click **Import**.
5. Click **Browse** and select the plug-in archive.
6. Click **List Archive**.
7. Select the plug-in and click **OK**.
8. Verify that you have set preferred credentials on all Agents where you want to deploy the plug-in.
9. In the Management Plug-ins page, click the icon in the **Deploy** column for the SQL Server plug-in. The Deploy Management Plug-in wizard appears.
10. Click **Add Agents**, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you selected.
11. Click **Next**, then click **Finish**.

If you see an error message stating that the preferred credential is not set up, go to the Preferences page and add the preferred credentials for the Agent target type.

If there are no errors, then you will see the following screen:

**Figure 1 Successful Deployment**



12. To check the deployment status, go to Related Links and click the link **Deployment Status**.

## Enabling and Finding TCP/IP Port Information

The following sections provide information you require to enable the TCP/IP port and to find the TCP/IP port for a particular SQL server instance.

### Enabling TCP/IP Port

#### For SQL Server 2000

1. From the SQL Server Enterprise Manager, right-click the SQL Server instance in the left panel and select **Properties**. SQL Server Properties dialog box appears.
2. In General tab, click **Network Configuration**. The SQL Server Network Utility dialog box appears.
3. Ensure that TCP/IP is listed in the Enabled protocols list.

#### For SQL Server 2005

1. From the **SQL Server Configuration Manager**, select **SQL Server 2005 Network Configuration** in the left panel and navigate to the SQL Server instance.

The right panel displays all protocols for the specified SQL Server instance and their status.

2. Ensure that TCP/IP is enabled.
3. (If TCP/IP is disabled), right-click **TCP/IP** and select **Properties**. The TCP/IP Properties dialog box appears.
4. In the Protocol tab, select **enabled**, and click **Apply**.
5. Restart the SQL Server instance.

## Finding TCP/IP Port

After enabling the TCP/IP protocol, restart the SQL Server to apply the changes. After restarting the server, follow the steps given in the previous section, that is, "[Enabling TCP/IP Port](#)" to identify the TCP/IP port number.

Alternatively, use the registry editor to find the TCP/IP port number for a particular SQL Server instance:

- (Non-default SQL Server instance) HKEY\_LOCAL\_MACHINE\Software\Microsoft\Microsoft SQL Server\\MSSQLServer\SuperSocketNetLib\Tcp
- (Default SQL Server instance) HKEY\_LOCAL\_MACHINE\Software\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp

The TCP Port provides the port number.

## Enabling SQL Authentication or Mixed Authentication

Modify the permissions for database authentication so that you enable SQL authentication or mixed authentication, and set sysadmin role for the database user that you are going to use for discovering the target and running jobs.

On the SQL Server, for the user you are going to use for monitoring and running jobs, set the write permissions by following these steps:

---

---

**Note:** If you do not have a user, then create one. To do so, from the task bar, go to Start, select **Settings**, and then **Control Panel**. In the Control Panel, double-click **Users and Passwords** and click **Add** in the Users tab.

---

---

1. In the Control Panel, double-click **Administrative Tools** and then **Computer Management**. The Computer Management screen appears.
2. In the left panel, go to Services and Applications and select the Microsoft SQL Server and navigate down to Security.
3. Double-click **Security**, and select **Logins**.
4. Right-click Logins and click NewLogin. The SQL Server Login Properties-New Login dialog box appears.
5. Click **General** tab, specify the name for the new login, select **SQL Server Authentication** and specify a unique password to use when connecting to the server using SQL Authentication.
6. Click **Server Roles** tab and ensure that **sysadmin** is selected in the Server Roles section.

7. Click **Database Access** tab, and ensure that in the Permit in Database Role section, no role is selected for any database.

---

---

**See Also:**

[http://msdn2.microsoft.com/en-us/library/aa933458\(SQL.80\).aspx](http://msdn2.microsoft.com/en-us/library/aa933458(SQL.80).aspx)

---

---

## Installing and Enabling Windows Management Instrumentation

(For SQL Server 2000) Install and enable Windows Management Instrumentation (WMI) provider of the SQL Server. Enable support by running the setup.exe file located in the SQL Server Installation CD:

```
<CD_Drive>/x86/other/wmi
```

## Modifying Permissions

Modify Windows Management Instrumentation Control permissions, registry permissions, and DCOM remote access permissions as described in the section *Modifying Permissions* in the *Enterprise Manager System Monitoring Plug-in Troubleshooting Guide* available at the following location:

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

## Adding Instances for Monitoring

Follow these steps to add the plug-in target to Grid Control for central monitoring and management:

1. From the Agent home page where the plug-in was deployed, select the Microsoft SQL Server target type from the **Add** drop-down list, then click **Go**. The Add Microsoft SQL Server page appears.

---

---

**Note:** If you are performing a local monitoring of SQL Server Cluster, then the Agent home page will be the Virtual Agent Service home page.

---

---

2. Provide the following information for the properties:

- **Name** — Unique target name across all the Grid Control targets, such as SqlServer2k\_Hostname. This is the display name in the Grid Control. It represents this SQL Server target across all user interfaces within Grid Control.

- **JDBC URL** — URL for JDBC.

For example,

```
jdbc:sqlserver://<host>:<port>
```



---

---

**Note:** You can specify either IP Address or host name. However, ensure that the host name can be resolved consistently on the network. Standard TCP tools such as "nslookup" and "tracert" can be used to verify the host name. Also, if you are monitoring a Microsoft SQL Server Cluster, then specify the IP address or host name of the virtual host of the cluster.

---

---

- **JDBC Driver** — (Optional) SQL+Driver JDBC driver class name.

For example,

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

- **Database Username** — Valid user for the database in sysadmin fixed server role.
- **Password for the Database User** — Corresponding password for the database user
- **System Username** — Valid host user name. Required only for remote Agent monitoring. For more information, see "[Configuring Remote Connections to Monitor Targets](#)".
- **System Password** — Password for the Username. Required only for remote Agent monitoring.
- **Role** — (Optional)

---

---

**Note:** For Oracle Management Service 10g Release 3 (10.2.0.3), if you do not reenter the encrypted parameters (*Database Username, Password for the Database User, System Username, System Password*) before clicking **OK**, you might encounter an error informing you that the login failed.

---

---

3. Click Test Connection to make sure the parameters you entered are correct.
4. Reenter the encrypted parameters from step 2 if the connection test was successful, then click **OK**.

**Figure 2 Add Microsoft SQL Server**

ORACLE Enterprise Manager 10g  
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports

Enterprise Manager Configuration | Management Services and Repository | Agents

### Add Microsoft SQL Server

Test Connection Cancel OK

**Properties**

\* Name:   
Type: **Microsoft SQL Server**

| Name                                                          | Value                                                                     |
|---------------------------------------------------------------|---------------------------------------------------------------------------|
| JDBC URL                                                      | <input type="text" value="jdbc:sqlserver://foo.com:1433"/>                |
| JDBC Driver                                                   | <input type="text" value="com.microsoft.sqlserver.jdbc.SQLServerDriver"/> |
| Database Username                                             | <input type="text" value="*****"/>                                        |
| Password of Database User                                     | <input type="text" value="*****"/>                                        |
| System Username (Needed when SQLServer is at remote location) | <input type="text"/>                                                      |
| System Password (Needed when SQLServer is at remote location) | <input type="text"/>                                                      |
| Role (Optional)                                               | <input type="text"/>                                                      |

**Monitoring**

Oracle has automatically enabled monitoring for this target's availability and performance, so no further monitoring configuration is necessary. You can edit the metric thresholds from the target's homepage.

Test Connection Cancel OK

---

**Important:** If you do not reenter the encrypted parameters before clicking **OK**, you might encounter an error suggesting that the login failed.

---

After you deploy and configure the plug-in to monitor one or more targets in the environment, you can customize the monitoring settings of the plug-in. This alters the collection intervals and threshold settings of the metrics to meet the particular needs of your environment. If you decide to disable one or more metric collections, this could impact the reports that the metric is a part of.

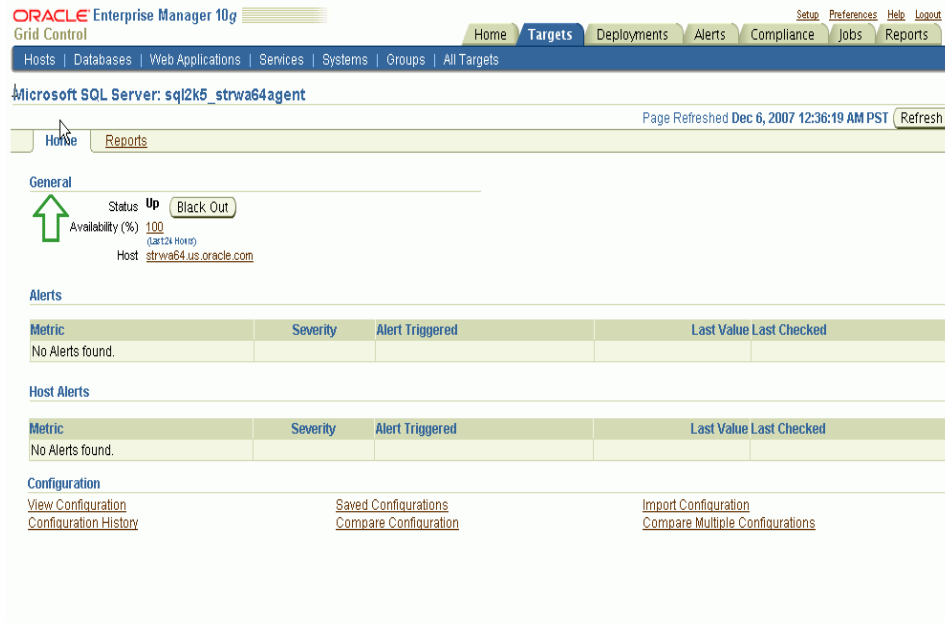
## Verifying and Validating the Plug-in

After waiting a few minutes for the plug-in to start collecting data, use the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the SQL Server target link from the Agent home page Monitored Targets table.

The Microsoft SQL Server home page appears.

**Figure 3 Microsoft SQL Server Home Page**



2. Verify that no metric collection errors are reported in the Metrics table.
3. Ensure that reports can be seen and no errors are reported by clicking the **Reports** property page.
4. Ensure that configuration data can be seen by clicking the **View Configuration** link in the Configuration section. If configuration data does not immediately appear, click **Refresh** in the View Configuration page.

## Upgrading the Plug-in

Follow these steps to upgrade the plug-in:

1. Download the SQL Server Plug-in archive to your desktop or computer on which the browser is launched. You can download the archive from the Oracle Technology Network (OTN).
2. Log into Enterprise Manager Grid Control as a Super Administrator.
3. Click the **Setup** link in the upper right corner of the Grid Control Home page, then click the **Management Plug-ins** link on the left side of the Setup page.
4. Click **Import**.
5. Click **Browse** and select the plug-in archive that you have downloaded for upgrading.
6. Click **List Archive**.
7. Select the plug-in and click **OK**.
8. Verify that preferred credentials are set on all Agents to which you want to deploy the plug-in.

9. Blackout the Microsoft SQL Server targets for agents to which you want to deploy higher version of the plug-in. Ensure that you select immediate blackout.
10. In the Management Plug-ins page, click the icon in the **Deploy** column for the SQL Server plug-in. The Deploy Management Plug-in wizard appears.
11. Click **Add Agents**, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you selected.
12. Click **Next**, then click **Finish**.

If you see an error message stating that the preferred credential is not set up, go to the Preferences page and add the preferred credentials for the Agent target type.

13. Remove blackout for the targets (required only if Step 9 applies).

## Undeploying the Plug-in

Follow these steps to undeploy the plug-in from an Agent:

1. Log in to Enterprise Manager Grid Control as a Super Administrator.
2. Select the **Targets** tab, then the **All Targets** subtab. The All Targets page appears.
3. Select the Microsoft SQL Server Plug-in target and click **Remove**. You must do this step for all targets of the specific version of the plug-in.
4. Make sure that the preferred credentials are set on the Agents where the plug-in is deployed.
5. Click the **Setup** link in the upper right corner of the All Targets page, then click the Management Plug-ins link on the left side of the Setup page. The Management Plug-ins page appears.
6. Click the icon in the **Undeploy** column for the Microsoft SQL Server Plug-in. The Undeploy Management Plug-in page appears.
7. Check all the Agents that are currently deployed with the Microsoft SQL Server Plug-in and click **OK**.

You must undeploy the plug-in from every Agent in the system to completely remove it from the enterprise.

8. Select the Microsoft SQL Server Plug-in on the Management Plug-in page and click **Delete**.

## Configuring Connections

This section provides details about configuring connections for monitoring targets and executing jobs.

### Configuring Remote Connections to Monitor Targets

If you want to monitor targets using remote Agents, then Oracle recommends that you do the following security configurations on every system where SQL Server target resides.

- Set WMI namespace security (Refer to the 'Modifying Windows Management Instrumentation Control Permissions' section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)
- Restrict access to the registry from a remote computer (Refer to the 'Modifying Registry Permissions' section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)
- Set DCOM Security to allow user to access a computer remotely (Refer to the 'Modifying DCOM Remote Access Permissions' section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)

## Configuring Connections to Execute Jobs

If you want to execute jobs using local or remote Agents, then Oracle recommends that you do the following security configurations on every system where SQL Server target resides.

- Set WMI namespace security (Refer to the 'Modifying Windows Management Instrumentation Control Permissions' section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)
- Set DCOM Security to allow user to access a computer remotely (Refer to the 'Modifying DCOM Remote Access Permissions' section of the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.)

For configuration details, refer to the following:

- Microsoft Help and Support Web site.  
To access the Web site, go to the following URL:  
<http://support.microsoft.com>
- *Oracle Enterprise Manager Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide* available at the following URL:  
<http://www.oracle.com/technology/documentation/oem.html>
- Document 367797.1 on Oracle *Metalink* .  
To locate document 367797.1:
  1. Go to the following URL:  
<http://metalink.oracle.com>
  2. Click **Advanced** at the top of the Oracle *Metalink* page.
  3. Enter 367797.1 in the **Document ID** field and click **Submit**.

## Creating and Editing Jobs

To create and edit jobs, follow these steps:

---



---

**Note:** Currently jobs are supported only for stand-alone SQL Server instances. Jobs submitted for SQL Server 2005 cluster instances will fail.

---



---

1. In Grid Control, click the **Jobs** tab. Grid Control displays the Job Activity page.
2. Select a job type from the **Create Job** menu and click **Go**.

You can select one of these:

- Microsoft SQL Server and/or SQL Agent Start
- Microsoft SQL Server and/or SQL Agent Stop
- Microsoft SQL Server Pause or Resume

---

**Note:** If you want to edit a job, then select an existing job from the list and click **Edit**.

---

3. In the **General** tab of the Create *<Job Type>* Job page, provide a name for the job and add the individual targets or one composite target such as a Group.

---

**Note:** If you are editing a job, then modify the job name and the selected targets.

---

4. In the **Parameters** tab of the Create *<Job Type>* Job page, from the **Options** menu, select an appropriate option to make the job function accordingly when it starts.

You can select one of these options:

**Table 1 Job Parameters Options**

| Job Type                                    | Available Options                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft SQL Server and/or SQL Agent Start | <ul style="list-style-type: none"> <li>■ Start SQL Server and SQL Server Agent services<br/>(You will select this option when both, SQL Server and SQL Server Agent, are stopped or when SQL Server is running but the SQL Server Agent is stopped)</li> <li>■ Start SQL Server service<br/>(You will select this option when both, SQL Server and SQL Server Agent, are stopped and if you want to start only the SQL Server)</li> </ul>                     |
| Microsoft SQL Server and/or SQL Agent Stop  | <ul style="list-style-type: none"> <li>■ Stop SQL Server and SQL Server Agent services<br/>(You will select this option when both, SQL Server and SQL Server Agent, are running, when SQL Server is paused but the SQL Server Agent is running, when SQL Server is running/paused but the SQL Server Agent is stopped)</li> <li>■ Stop SQL Server Agent service<br/>(You will select this option when you want to stop a running SQL Server Agent)</li> </ul> |

**Table 1 (Cont.) Job Parameters Options**

| Job Type                             | Available Options                                                                                                                                                                                                                                                          |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft SQL Server Pause or Resume | <ul style="list-style-type: none"><li>■ Pause SQL Server service<br/>(You will select this option when you want to pause a running SQL Server)</li><li>■ Resume SQL Server service<br/>(You will select this option when you want to resume a paused SQL Server)</li></ul> |

Grid Control starts the SQL server and agent services according to the selection made.

---

---

**Note:** If you are editing a job, then modify the options for that job.

---

---

5. In the **Credentials** tab of the Create <Job Type> Job page, select an appropriate option for credentials.

You can choose to use the preferred credentials that are already set or override the preferred credentials with new credentials. In either case, you need to provide the credentials for agent host and database host.

To set the preferred credentials, click **Preferences** at the top-right corner of the Grid Control console. From the left-vertical navigation bar, click **Preferred Credentials**. Grid Control displays the Preferred Credentials page. On this page, you can set the preferred credentials

---

---

**Note:** If you are editing a job, then modify the credentials set for that job.

---

---

6. In the **Schedule** tab of the Create <Job Type> Job page, schedule the job.

---

---

**Note:** If you are editing a job, then modify the schedule prepared for that job.

---

---

7. In the **Access** tab of the Create <Job Type> Job page, define or modify the access you want other users to have to this job.

---

---

**Note:** If you want to edit, then modify the access levels for that job.

---

---

8. Click **Submit** to create the job.

## Troubleshooting the Plug-In

To resolve various issues that you might encounter while using the plug-in, see the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide* available at the following URL:

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

## 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, seven days a week. For TTY support, call 800.446.2398.

---

System Monitoring Plug-in Installation Guide for Microsoft SQL Server, Release 8 (3.3.3.1.0)  
E12776-01

Copyright © 2008 Oracle. All rights reserved.

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, JD Edwards, PeopleSoft, and Siebel are registered trademarks 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.