

Oracle® Enterprise Manager Microsoft Systems Center Operations Manager (SCOM) Event Connector User's Guide



For Enterprise Manager Cloud Control 13c Release 2

E74846-02

August 2017

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

ORACLE®

Oracle Enterprise Manager Microsoft Systems Center Operations Manager (SCOM) Event Connector User's Guide, For Enterprise Manager Cloud Control 13c Release 2

E74846-02

Copyright © 2013, 2016, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

Contents

Preface

Audience	ix
Documentation Accessibility	ix
Conventions	ix

1 Microsoft SCOM Event Connector Overview

1.1 Versions Supported	1-1
------------------------	-----

2 Installing the Microsoft SCOM Event Connector

2.1 Installation Platforms	2-2
2.2 Prerequisites for the Microsoft SCOM Event Connector	2-2
2.3 Installing the Microsoft SCOM Event Connector in Enterprise Manager	2-3
2.3.1 Installing the Connector if Enterprise Manager is in “Offline” Mode	2-5
2.4 Installing and Running the Oracle SCOM Agent	2-7
2.4.1 Preinstallation Requirements	2-7
2.4.2 Setting Up the Agent Account	2-8
2.4.2.1 System Center Operations Manager 2012 Administrator Groups	2-8
2.4.3 Installing the Oracle SCOM Agent	2-9
2.4.4 Configuring Agent Notification	2-11
2.4.5 Installing the Alert Creator Management Pack	2-13
2.4.6 Starting and Stopping the Agent	2-13
2.4.7 Uninstalling the Alert Creator Management Pack	2-13
2.4.8 Uninstalling the Oracle SCOM Agent	2-14
2.5 Exporting the Agent Installation Files	2-14
2.5.1 Exporting Agent Installation Files for Enterprise Manager 13c	2-14
2.5.1.1 Exporting Agent Installation Files to a Managed Host	2-14
2.5.1.2 Exporting Agent Installation Files to Your Workstation	2-17
2.5.2 Exporting Agent Installation Files for Enterprise Manager 12c	2-17
2.5.3 Extracting the Agent Installation Files	2-18
2.6 Installing the Microsoft SCOM Web Service	2-19
2.6.1 Installing and Running the Microsoft SCOM Web Service on UNIX	2-19

2.6.1.1	Prerequisites for UNIX	2-19
2.6.1.2	Installing the Microsoft SCOM Web Service on UNIX	2-19
2.6.1.3	Running the Microsoft SCOM Web Service on UNIX	2-21
2.6.1.4	Testing the Microsoft SCOM Web Service on UNIX	2-21
2.6.1.5	Uninstalling the Microsoft SCOM Web Service on UNIX	2-22
2.6.2	Installing and Running the Microsoft SCOM Web Service on Windows	2-22
2.6.2.1	Prerequisites for Windows	2-22
2.6.2.2	Installing the Microsoft SCOM Web Service on Windows	2-22
2.6.2.3	(Optional) Installing the Microsoft SCOM Web Services as a Windows Service	2-24
2.6.2.4	Running the Microsoft SCOM Web Service on Windows	2-25
2.6.2.5	Testing the Microsoft SCOM Web Service on Windows	2-26
2.6.2.6	Uninstalling the Microsoft SCOM Web Service on UNIX	2-26
2.6.3	Exporting the Web Service Installation File	2-26
2.7	Uninstalling the Microsoft SCOM Event Connector	2-27

3 Configuring the Microsoft SCOM Event Connector

3.1	Creating a Connector Instance	3-1
3.2	Configuring the Connector	3-2
3.3	Connector Modes of Operation	3-3
3.3.1	Switching to the Alternate Template	3-4
3.4	Enabling and Disabling the Connector	3-6
3.5	Providing General Settings	3-6
3.5.1	Connection Settings	3-7
3.5.2	Retry	3-8
3.6	Exporting the Template Files	3-8
3.7	Deleting the Microsoft SCOM Event Connector	3-9
3.8	Testing the Microsoft SCOM Event Connector	3-9

4 Forwarding Enterprise Manager Events to Microsoft SCOM

4.1	Setting Event Rules	4-1
4.2	Viewing Events in the SCOM Console	4-3

5 Working With Event Templates

5.1	Familiarization with Event Templates	5-1
5.1.1	Default Templates	5-1
5.1.1.1	Create Event Template	5-2
5.1.1.2	Update Event Template	5-3
5.1.1.3	Formatted Enterprise Manager Description Contents	5-4

5.1.1.4	Formatted Alert History Create Contents	5-5
5.1.1.5	Formatted Alert History Update Contents	5-6
5.1.1.6	Alert History Title	5-6
5.1.2	Severity Mapping	5-7
5.1.3	Priority Mapping	5-7
5.2	Customizing Event Templates	5-7
5.2.1	XML Format of Oracle Enterprise Manager Events	5-8
5.2.2	Field Descriptions for XML Format of Events	5-9
5.2.3	Managing Templates in Oracle Enterprise Manager	5-10
5.2.3.1	Edit a Template with Enterprise Manager	5-10
5.2.3.2	Viewing Template Code in Enterprise Manager	5-10
5.2.3.3	Deleting a Template with Enterprise Manager	5-11
5.2.3.4	Restoring an Updated Template with Enterprise Manager	5-11
5.2.4	Changing a Mapping	5-11
5.2.4.1	Modifying Templates	5-12
5.2.4.2	Registering Templates	5-12
5.2.4.3	Template Customization Example	5-13

6 Enabling SSL for Enterprise Manager

6.1	Configuring Enterprise Manager to Use SSL	6-1
6.2	Installing a Self-Signed Certificate	6-1
6.3	Installing a Certificate from a Certificate Authority	6-2
6.4	Importing the Web Service Certificate into Enterprise Manager	6-3

7 Troubleshooting the Microsoft SCOM Event Connector

7.1	Diagnosing the Problem	7-1
7.2	Troubleshooting Web Service Startup Errors	7-3
7.3	JVM Errors	7-4
7.4	Using the Correct URL for SCOM Web Service Operations	7-4
7.5	Troubleshooting Web Service Operation Errors	7-5
7.6	Errors from Oracle Enterprise Manager	7-6
7.6.1	Invalid Web Service Credentials	7-8
7.6.2	SSL Not Configured in Enterprise Manager	7-9
7.6.3	SCOM Web Service Down	7-9
7.6.4	Invalid IP Address	7-10
7.6.5	Invalid URL Path	7-10
7.6.6	Invalid Port Number	7-11
7.6.7	Firewall Blocking Access	7-11
7.6.8	Unknown Host	7-12

7.6.9	Invalid XML Format	7-12
7.6.10	SCOM Server Not Operational	7-12
7.6.11	Invalid SCOM API Credentials	7-13
7.6.12	Wrong SCOM API Permissions	7-14
7.6.13	SCOM Agent Not Operational	7-14
7.6.14	SCOM Agent Configuration	7-14
7.6.15	Alert Creator Management Pack Missing	7-15
7.6.16	Alert Create Timeout	7-15

A Customizing Microsoft SCOM

A.1	XML Format of Microsoft SCOM Alerts	A-1
A.1.1	Sample Create Format for Microsoft SCOM Web Service	A-1
A.1.2	Sample Update Format for Microsoft SCOM Web Service	A-2
A.1.3	Mappings Between XML Format and Alert Field Names	A-2
A.1.4	Extended Fields	A-4
A.2	Changing Default Port Numbers	A-4
A.2.1	Changing the Web Service Port (8080)	A-5
A.2.2	Changing the Web Service Port (8443)	A-5
A.3	Changing SCOM API Connection Parameters	A-5

B Enterprise Manager Event Samples

B.1	Create Sample	B-1
B.2	Update Sample	B-4
B.3	Clear Sample	B-7

C Enterprise Manager Event Format

C.1	EMEvent.xsd	C-1
C.2	connectorCommon.xsd	C-3
C.3	externalEvent.xsd	C-9

D Microsoft SCOM Web Service WSDL Format

D.1	EventService WSDL	D-1
D.2	SCOMService WSDL	D-20

E Microsoft SCOM 2007 Connector

E.1	Versions Supported by the Microsoft SCOM 2007 Connector	E-1
E.2	SCOM 2007 Installation and Customization	E-2

E.2.1	Verify Preinstallation Requirements	E-2
E.2.2	Verify Agent Account Prerequisites	E-2
E.2.3	Determine Ops Mgr Administrator Groups	E-3
E.2.4	Add Ops Mgr User Role for Oracle SCOM Agent	E-3
E.2.5	Install the Alert Creator Management Pack for Microsoft SCOM 2007	E-4
E.3	Default Templates for Microsoft SCOM 2007	E-5
E.3.1	Create Event 2007 Template	E-5
E.3.2	Update Event 2007 Template	E-6

Preface

This document provides the required information to install and configure the Microsoft System Center Operations Manager (SCOM) Event Connector that integrates Oracle Enterprise Manager with SCOM management tools and help desk systems.

Audience

This guide is written for Oracle Enterprise Manager system administrators who want to install and configure the Microsoft SCOM Event Connector to enable integration between Oracle Enterprise Manager and Microsoft SCOM.

You should already be familiar with Oracle Enterprise Manager.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/us/corporate/accessibility/support/index.html#info> or visit <http://www.oracle.com/us/corporate/accessibility/support/index.html#trs> if you are hearing impaired.

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Microsoft SCOM Event Connector Overview

There are different version-specific connectors that are used to integrate Enterprise Manager with Microsoft System Center Operations Manager (SCOM). This document provides the instructions for installing and maintaining all the different types of SCOM connectors. Most of the information contained in this document is common and applicable to all SCOM connector types. Any sections that are for a specific connector type will be clearly identified. There is one connector for integrating with SCOM 2012, and there are two different connectors for integrating with SCOM 2007:

- For SCOM 2012, the SCOM 2012 connector is for integrating Enterprise Manager with all versions of SCOM 2012.
- For SCOM 2007:
 - The SCOM 2007 pre-R2 connector is for integrating Enterprise Manager with SCOM 2007 RTM and SP1 versions.
 - The SCOM 2007 R2 connector is for integrating Enterprise Manager with SCOM 2007 R2.

There are some differences between SCOM 2007 and SCOM 2012 so there is some information that will be different for the SCOM 2007 connectors versus the SCOM 2012 connector. [Microsoft SCOM 2007 Connector](#) contains sections that are specific to SCOM 2007 that will be referenced throughout the document.

The connector monitors all events sent from Oracle Enterprise Manager and automatically updates alert information in SCOM. The connector supports the following features:

- Sharing of event information from Oracle Enterprise Manager to Microsoft SCOM.
- Customization of event to alert mappings between Oracle Enterprise Manager and Microsoft SCOM.
- Synchronization of event changes in Oracle Enterprise Manager with the alerts in Microsoft SCOM.

Once an alert is created in SCOM for an event in Enterprise Manager, for subsequent updates in event severity, there is a choice between opening a new alert in SCOM or annotating the original alert in SCOM.

1.1 Versions Supported

This connector supports the following versions of Oracle Enterprise Manager and Microsoft SCOM:

- Oracle Enterprise Manager Cloud Control:
 - 13c (13.1.0.1) and higher
 - 12c Release 2 (12.1.0.2.0) and higher

- Microsoft System Center Operations Manager (SCOM) versions including:
 - Microsoft SCOM 2012 and 2016- supported by the SCOM 2012 connector.
 - Microsoft SCOM 2007 R2 - supported by the SCOM 2007 R2 connector.
 - Microsoft SCOM 2007 RTM and SCOM 2007 SP1 - supported by the SCOM 2007 pre-R2 connector.

The base Enterprise Manager version number for the Microsoft System Center Operations Manager 2012 Connector Release 13.1.0.1.0 is Enterprise Manager 13c Release 1 (13.1.0.1) and higher.

2

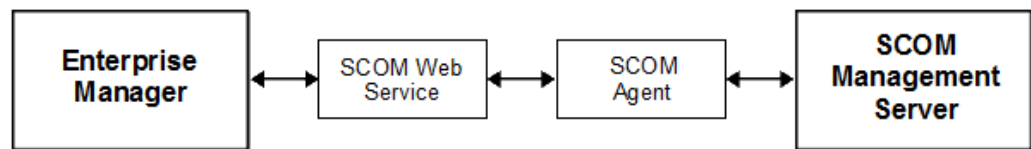
Installing the Microsoft SCOM Event Connector

The Oracle Enterprise Manager Connector Framework requires a web service interface for forwarding event information to Microsoft SCOM. To integrate with Enterprise Manager, a third-party SCOM web service front-end must be installed. In addition to the web service front-end, an Oracle SCOM Agent must also be installed. Both of these components are included in the Oracle Enterprise Manager SCOM connector installation package.

You can install the web service on any Unix or Windows system that has connectivity with the SCOM server. In addition to the SCOM web service front-end, you must also install a back-end Oracle SCOM Agent. The Oracle SCOM Agent is preconfigured and is also included in the Oracle Enterprise Manager SCOM connector installation package.

Figure 2-1 shows the communication between the various components of the SCOM Connector.

Figure 2-1 Connector Communication Between Components



The following sections in this chapter discuss these topics:

- [Installation Platforms](#)
- [Prerequisites for the Microsoft SCOM Event Connector](#)
- [Installing the Microsoft SCOM Event Connector in Enterprise Manager](#)
- [Installing and Running the Oracle SCOM Agent](#)
- [Exporting the Agent Installation Files](#)
- [Installing the Microsoft SCOM Web Service](#)
- [Uninstalling the Microsoft SCOM Event Connector](#)

 **Note:**

Unless otherwise noted, these instructions apply to the SCOM 2012 connector and to the SCOM 2007 connectors. Instructions specific to the SCOM 2007 connectors are available in [Microsoft SCOM 2007 Connector](#).

2.1 Installation Platforms

You can install the SCOM web service on the following platforms that support Oracle Java Development Kit (JDK) 6.0:

- Microsoft Windows
- Oracle Solaris
- Linux

Depending on the following SCOM connector versions, you can install the Oracle SCOM Agent on the Microsoft Windows server platform:

- For the SCOM 2012 connector, the Microsoft Windows 2008 and 2012 server platforms are supported.
- For both SCOM 2007 connectors, the Microsoft Windows 2000, 2003, and 2008 server platforms are supported.



Note:

For information, see *SCOM 2012 Connector Installing the SCOM Connector using Windows Clustering to enable HA High Availability* (Doc ID 1674577.1):

<https://support.oracle.com/rs?type=doc&id=1674577.1>

2.2 Prerequisites for the Microsoft SCOM Event Connector

Verify the following prerequisites before installing the connector:

1. A utility for unzipping .zip files is available where the SCOM Agent is to be installed.
2. Oracle Java Development Kit (JDK) 6.0 Update 11 or higher is installed on the system where the SCOM Web Service will be installed.



Note:

The web service does not support JDK 7 or 8 and must be run with JDK 6 Update 11 or higher.

3. In order to create events to Microsoft SCOM, you must import the OracleEnterpriseManager.Alert.Creator Management Pack from the Microsoft SCOM server. The Management Pack file is provided with the SCOM Agent installation binaries.
4. Verify that the connector is available in Enterprise Manager or available for download from the Self Update feature:
 - **For Oracle Enterprise Manager Cloud Control 13c:**
The latest version of the different SCOM connectors come pre-installed and do not need to be downloaded through Self Update. To determine whether the connector needs to be downloaded from self update, perform the following steps:

- a. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
- b. On the Self Update page, select **Management Connector** to display a list of available connectors.
- c. If the Microsoft SCOM connector that you need is not listed here, then you will need to set up My Oracle Support (MOS) Preferred Credentials.

 **Note:**

If the connector you wish to install is not pre-installed, the My Oracle Support (MOS) Preferred Credentials must be set to enable the download of connectors through self update.

- **For Oracle Enterprise Manager Cloud Control 12c:**
In order to install the connector, the My Oracle Support Preferred Credentials must be set to enable the download of the connector through self-update. To set the credentials, perform the following steps:
 - a. From the **Setup** menu, select **My Oracle Support**.
 - b. Select **Set Credentials**, then enter the username and password information and click **Apply**.
 - c. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
 - d. On the Self Update page, select **Check Updates** to schedule a job to collect the metadata for the connectors.

 **Note:**

Refer to the *Setting up Self Update* section in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for more details.

You can also set up Self Update in offline mode. See the *Applying an Update in Offline Mode* section for details

2.3 Installing the Microsoft SCOM Event Connector in Enterprise Manager

All connectors in the Enterprise Manager store are available on the Self Update page for downloading provided the My Oracle Support Preferred Credentials are configured. See [Prerequisites for the Microsoft SCOM Event Connector](#) for instructions. The installation files for the Oracle SCOM agent and web service are packaged with the SCOM connector. The connector must be installed first in order to gain access to the installation files.

- **For Oracle Enterprise Manager Cloud Control 13c:**
The SCOM connector is preloaded; so, in most cases you will only need to apply the connector. If you need to install an older version of the connector or the connector is inadvertently deleted, then the connector will need to be downloaded from Self Update.

To determine whether you need to download the connector, perform the following steps:

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. On the Self Update page, select **Management Connectors** to display a list of available connectors.
3. Look for the Microsoft SCOM connector that you intend to use.

If it is not listed, you will need to set up My Oracle Support Preferred Credentials as specified in [Prerequisites for the Microsoft SCOM Event Connector](#). Once the update task has completed, the connector should show up with a status of **Available**.

- For Oracle Enterprise Manager Cloud Control 12c:
None of the SCOM connectors are preloaded. To download the SCOM connectors, you will need to set up MOS Preferred Credentials as specified in [Prerequisites for the Microsoft SCOM Event Connector](#). Once the update task has completed, the SCOM connectors should show up with a status of **Available**.
If the status of the connector is **Available**, perform the following steps to download the connector.

If the status of the connector is **Available**, perform the following steps to download the connector.

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. On the Self Update page, select **Management Connectors** to display a list of available connectors.
The Microsoft SCOM connectors should be listed here with a status of Available.
3. Click the appropriate Microsoft SCOM connector to select it and then click **Download**.
The Schedule Download window will be displayed to determine when the download should be performed.
4. Click **Select** to download immediately.

 **Note:**

If you want to schedule the download for a later time, specify the date/time when the download should take place and click **Select**. You must return to finish the remainder of this procedure after the scheduled download date/time.

5. If necessary, refresh the screen until the status of the connector changes to Downloaded.

If the status of the connector is Downloaded, perform the following steps to apply the connector.

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. On the Self Update page, select **Management Connectors** to display a list of available connectors.
3. Look for the Microsoft SCOM connector that you intend to use.

4. Click the appropriate Microsoft SCOM connector to select it and then click **Apply**.
You will be prompted to confirm the operation and then a window appears that indicates the request has been submitted.
5. Refresh the screen until the status of the connector changes from **Apply Scheduled** to **Applied**.

2.3.1 Installing the Connector if Enterprise Manager is in "Offline" Mode

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

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

Note:

For Enterprise Manager 13c: All of the latest SCOM connectors come pre-installed; so, you can ignore this section if the connector that you need has been pre-installed. To determine if it is pre-installed, perform the following steps:

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. On the Self Update page, select **Management Connectors** to display a list of available connectors.
3. Look for the Microsoft SCOM connector that you intend to use. If it appears and has a status of **Downloaded**, you can skip this section.

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

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

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

4. From an Internet-enabled computer, download the catalog file using the aforementioned URL.

5. Copy the downloaded catalog file to the OMS host or the Management Agent host where you plan to import the connector.
6. Import the catalog file to Enterprise Manager:

- If the catalog file is on the OMS host:

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

Where:

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

- If the catalog file is on a different host:

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

[Example 2-1](#) shows a sample for importing the catalog archive.

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

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

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

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

Where:

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

Example 2-1 Sample for Importing Catalog Archive

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

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

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

Imports the master catalog file `p9348486_112000_Generic.zip` that is present on the host `host1.example.com`. The host must be a managed host target in Enterprise

Manager, and the Management Agent on this host must be up and running. The preferred unprivileged credentials for host host1.example.com are used to retrieve the remote file.

2.4 Installing and Running the Oracle SCOM Agent

The following sections provide procedures for installing and running the Oracle SCOM Agent:

- [Preinstallation Requirements](#)
- [Setting Up the Agent Account](#)
- [Installing the Oracle SCOM Agent](#)
- [Configuring Agent Notification](#)
- [Installing the Alert Creator Management Pack](#)
- [Starting and Stopping the Agent](#)
- [Uninstalling the Alert Creator Management Pack](#)
- [Uninstalling the Oracle SCOM Agent](#)

2.4.1 Preinstallation Requirements

 **Note:**

These requirements apply to the SCOM 2012 connector only. For the SCOM 2007 connectors, see [Verify Preinstallation Requirements in Microsoft SCOM 2007 Connector](#).

The following requirements apply to the system where the Oracle SCOM Agent is installed:

1. .NET framework 4.0 is installed.
2. ASP.NET 4.0 is installed.

After .NET framework 4.0 is installed, enter the following command to install ASP.NET 4.0:

```
%SystemRoot%\Microsoft.NET\Framework\v4.0.xxxxx\aspnet_regiis -i
```

 **WARNING:**

This command upgrades other applications running under IIS to version 4.0

3. Internet Information Services (IIS) 7.0 or higher is installed.
4. CGI and ISAPI Extensions Role Services are installed. To install the Role Services, perform the following steps:
 - a. Click **Start**, then **Administrative Tools**, and finally **Server Manager** to open the Server Manager.

- b. Expand Roles in the left panel.
 - c. Scroll down to the Web Server (IIS) section and click **Add Role Services**. This will open the Add Role Services window.
 - d. Check the check box for **CGI and ISAPI Extensions under Web Server/ Application Development**.
 - e. Click **Next** and then **Install**.
5. ISAPI and CGI Restrictions are set to allowed for ASP.NET 4.0. To enable ASP.NET 4.0, perform the following steps:
 - a. Click **Start**, then **Administrative Tools**, and finally **Internet Information Services (IIS) Manager** to open the IIS Manager.
 - b. Click the local machine name under Connections.
 - c. Select **Content View**. ISAPI and CGI Restrictions should be listed
 - d. Double click **ISAPI and CGI Restrictions**. The ISAPI and CGI Restrictions page is displayed.
 - e. Right click on the appropriate v4.0 line for your environment and select **Allow**.

 **Note:**

The path that contains Framework is for 32-bit environments, and the path that contains Framework64 is for 64-bit environments.

2.4.2 Setting Up the Agent Account

 **Note:**

These instructions apply to the SCOM 2012 connector **only**. For the SCOM 2007 connectors, see [Verify Preinstallation Requirements in Microsoft SCOM 2007 Connector](#).

Before installing the Oracle SCOM Agent, you need to set up an account for the Oracle SCOM Agent to access the SCOM API. The account must satisfy the following requirements:

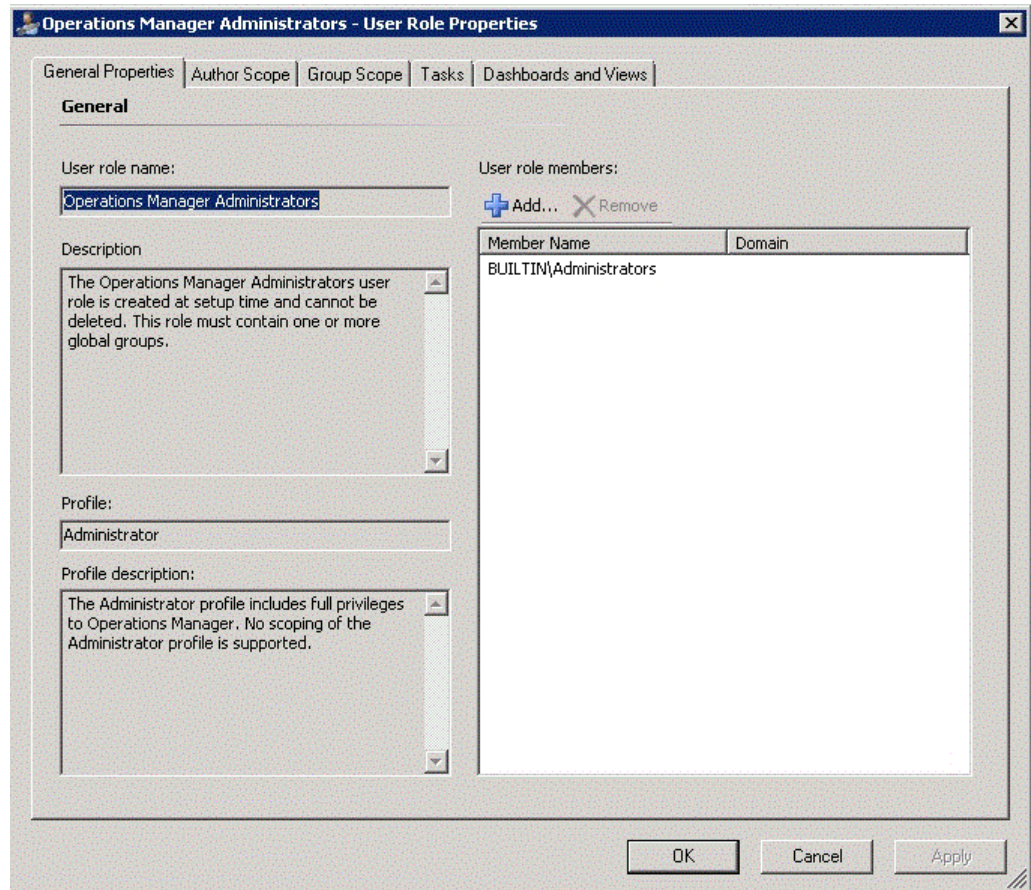
- Must be a domain account.
- Must be used exclusively by the Oracle SCOM Agent.
- Must be a member of a group designated as a System Center Operations Manager 2012 Administrator (See [System Center Operations Manager 2012 Administrator Groups](#) below)

2.4.2.1 System Center Operations Manager 2012 Administrator Groups

To determine the groups that are designated as a System Center Operations Manager 2012 Administrator, perform the following steps:

1. In the Administration pane of the System Center Operations Manager 2012 console (Figure 2-2 shows the console), select **Administration**, then **Security**, then **User Roles**. The User Roles should be displayed in the center pane.
2. Right-click on **Operations Manager Administrators** and select **Properties**. The General Properties tab lists the groups that have administrative permissions in the User Role members window. The account the Agent uses must be a member of one of the groups listed here, or you need to add one of its groups to this list.

Figure 2-2 Operations Manager Administrators Console



2.4.3 Installing the Oracle SCOM Agent

The SCOM Web Service uses the back-end Oracle SCOM Agent to access the SCOM API. The Oracle SCOM Agent must be installed on a Windows system that has connectivity to the SCOM server. The Oracle SCOM Agent is preconfigured to interface with the SCOM Web Service and requires minimal configuration.

 **Note:**

There should only be one installed instance of the Oracle SCOM Agent.

To install the Oracle SCOM Agent, perform the following steps:

1. Obtain a copy of the agent installation file from the Management Server host machine as specified in [Exporting the Agent Installation Files](#) and put the `SCOMAgent.zip` installation file into the directory where you want to install the Oracle SCOM Agent.

2. Unzip the contents of the `SCOMAgent.zip` file to any directory.

This extracts the `SCOMAgentInstaller.msi` and the `OracleEnterpriseManager.Alert.Creator.xml` files into the designated directory.

3. Navigate to the directory and run the Oracle SCOM Agent installer by double-clicking the `SCOMAgentInstaller.msi` file.

This starts the installer and displays the Welcome to the Oracle SCOM Agent Setup Wizard page.

4. Click **Next** to display the Service Type page.

5. Select the type of service to be installed under IIS. The default and recommended service type is Web Site.

This installs the service as a stand-alone web site. Selecting Virtual Directory installs the service as a Virtual Directory under an existing web site.

6. Click **Next** to display the Select Installation Folder page.

7. Enter the location to install the Agent or accept the default location of `c:\iWaveSoftware\SCOMConnectorAgent`.

8. Click **Next** to display the SCOM Agent Options page.

9. Enter the name to use when registering the connector in SCOM, or accept the default value of SCOM Agent.

10. Click **Next** to display the Confirm Installation page.

11. Click **Next** to display the SCOM Management Group Configuration page, and enter the information for the following required fields on the form:

- a. Host name or IP address of the SCOM server.
- b. Domain of the account to use when connecting to the SCOM API.
- c. User name of the account to use when connecting to the SCOM API.
- d. Password of the account to use when connecting to the SCOM API.



Note:

The information for the account from [Setting Up the Agent Account](#) should be entered in the Domain, User name, and Password fields.

12. Click **Done** to proceed. The window displayed next depends on the Service Type you selected in step 5 above:

- **If you selected Web Site:** The Web Site Configuration window appears. This window contains the Web Site Name and Port Number fields, and both have default values. Accept the default values or change them to the desired values.
- **If you selected Virtual Directory:** The Virtual Directory Configuration window appears. This window defines the name of the virtual directory to create and

the web site within which it will be installed. Accept the default values or change them to the desired values.

13. For either window, click **OK** to proceed and display the Web Service Credentials window. This window defines the credentials to specify when testing the newly installed Oracle SCOM Agent.

14. Specify valid Windows account credentials and click **OK**.

The installer now invokes the web service to verify that it is operational. A window pops up with the results of the test.

15. Close the window. The Installation Successful window appears. This window lists the URL of the Oracle SCOM Agent.

Make a note of the URL. You will need this whenever you install the SCOM Web Service.

16. Click **OK** to continue. The Installation Complete window appears.

17. Click **Close**.

The Oracle SCOM Agent installation process is complete.

2.4.4 Configuring Agent Notification

Note:

These instructions apply to the SCOM 2012 connector **only**.

If the Agent was NOT installed on the SCOM server, you must perform the following steps to configure the SCOM server to send a notification message to the SCOM agent whenever an alert is created by the SCOM 2012 connector:

1. Obtain a copy of the notification setup file from the Management Server host machine as specified in [Exporting the Agent Installation Files](#) and put the `SCOMNotification.zip` installation file into the directory where you want to install the Agent Notification utility.
2. Unzip the contents of the `SCOMNotification.zip` file to any directory. This creates the `bin\NotificationConfiguration.exe` and the `OracleEnterpriseManager.Alert.Creator.xml` files in the designated directory.
3. Right click on the `NotificationConfiguration.exe` file and select **Run** as administrator. The Agent Connection Information window will be displayed as shown in [Figure 2-3](#).
4. Enter the information required to connect to the SCOM Agent as described below:
 - a. **Agent URL:** Enter the URL that was noted when you installed the Oracle SCOM Agent. You will need to replace `localhost` with the actual hostname or IP address of the system where the Oracle SCOM Agent was installed.
 - b. **Domain:** Enter the domain of the account to use when connecting to the Oracle SCOM Agent. This field can be left blank if you are using an account that is local to the system where the Oracle SCOM Agent is installed.

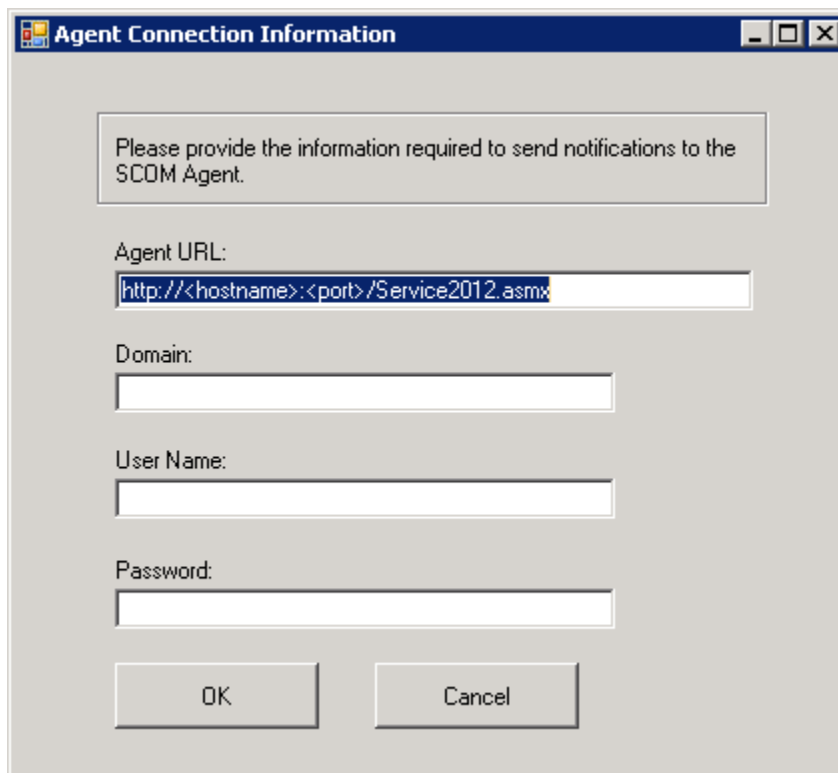
- c. **User Name:** Enter the username of the account to use when connecting to the Oracle SCOM Agent. This must be a valid user account that has permission to access the system where the Oracle SCOM Agent is installed.
- d. **Password:** Enter the password to use when connecting to the Oracle SCOM Agent. This must be the password of the account specified in the User Name field.

 **Note:**

Most likely, the Domain, User Name, and Password information will be the credentials entered in step 14 of [Installing the Oracle SCOM Agent](#).

- 5. Click **OK**.

Figure 2-3 Agent Connection Information Window



The image shows a Windows-style dialog box titled "Agent Connection Information". At the top, there is a message box that says "Please provide the information required to send notifications to the SCOM Agent." Below this, there are four input fields: "Agent URL:" with the text "http://<hostname>:<port>/Service2012.asmx", "Domain:", "User Name:", and "Password:". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

2.4.5 Installing the Alert Creator Management Pack

A management pack file named `OracleEnterpriseManager.Alert.Creator.xml` is also included in the Agent/Notification installation zip files. This management pack is required to create alerts in SCOM.

Note:

These instructions are for SCOM 2012 **only**. For instructions to install the Alert Creator Management Pack for SCOM 2007, see [Install the Alert Creator Management Pack for Microsoft SCOM 2007](#) in [Microsoft SCOM 2007 Connector](#).

Follow the steps below to import the management pack into SCOM:

1. In the Administration pane of the Operations Manager console, select **Administration**, then **Management Packs**.
2. Right-click on **Management Packs** and select **Import Management Packs...** The Select Management Packs window appears.
3. For SCOM 2012, click **Add** and select **Add from disk...**
4. Navigate to the directory where the `OracleEnterpriseManager.Alert.Creator.xml` file is located.
5. Select the `OracleEnterpriseManager.Alert.Creator.xml` file and click **Open**.
The Import Management Packs window appears.
6. Click **Install** to import the management pack.
7. Click **Close** after the management pack has been imported.

The Agent is now configured to insert alerts into SCOM.

2.4.6 Starting and Stopping the Agent

The installer automatically starts the Agent. To stop the agent, open the IIS manager, select the web site where it was installed, then click **Stop**. To start, click **Start**.

2.4.7 Uninstalling the Alert Creator Management Pack

To remove the alert creator management pack `OracleEnterpriseManager.Alert.Creator.xml`, perform the following steps:

1. In the Administration pane of the Operations Manager console, select **Administration**, then **Management Packs**.
2. In the Management Packs pane, right click the **Oracle Enterprise Manager Alert Creator** management pack and click **Delete**.
3. On the message stating that deleting the management pack might affect the scoping of some user roles, click **Yes**.

2.4.8 Uninstalling the Oracle SCOM Agent

To uninstall the Oracle SCOM Agent, perform the following steps:

1. Open the Control Panel and select **Add/Remove Programs**.
2. Find and select **SCOM Agent**. Select **Uninstall**, and click **Yes**, to confirm.
3. Manually navigate to the installation directory and remove any remaining installation files. The default installation directory is for the agent is:

C:\iWaveSoftware\

4. (Optional) Remove or disable the domain Agent Account created exclusively for the Oracle SCOM Agent.

2.5 Exporting the Agent Installation Files

The agent installation file is included in the Self Update archive that was installed in [Installing the Microsoft SCOM Event Connector in Enterprise Manager](#).

- [Exporting Agent Installation Files for Enterprise Manager 13c](#)
- [Exporting Agent Installation Files for Enterprise Manager 12c](#)
- [Extracting the Agent Installation Files](#)

2.5.1 Exporting Agent Installation Files for Enterprise Manager 13c

To export the installation files, first determine where you want to export the installation files. You can export it to a managed host machine or to your workstation:

- To export the installation files to a managed host, see [Exporting Agent Installation Files to a Managed Host](#).
- To export the installation files to your workstation, see [Exporting Agent Installation Files to Your Workstation](#).
- To extract the installation files, follow the instructions in [Extracting the Agent Installation Files](#).

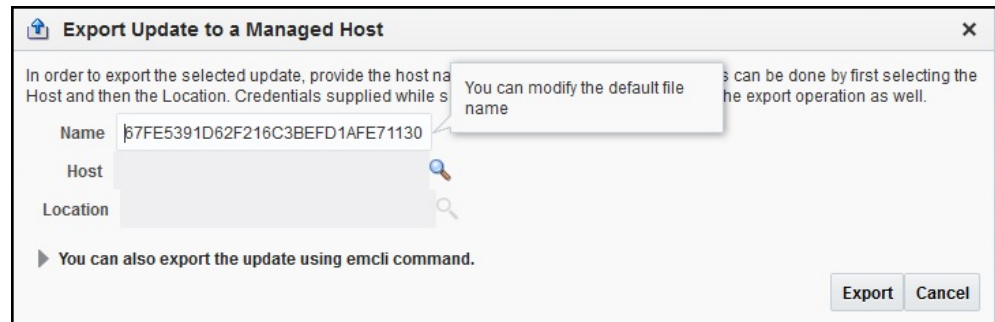
2.5.1.1 Exporting Agent Installation Files to a Managed Host

To export to a managed host machine, perform the following steps:

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. On the Self Update page, select **Management Connector** to display a list of available connectors.
3. Click the appropriate Microsoft SCOM connector name, then select **Export to->Managed Host** from the Actions list.

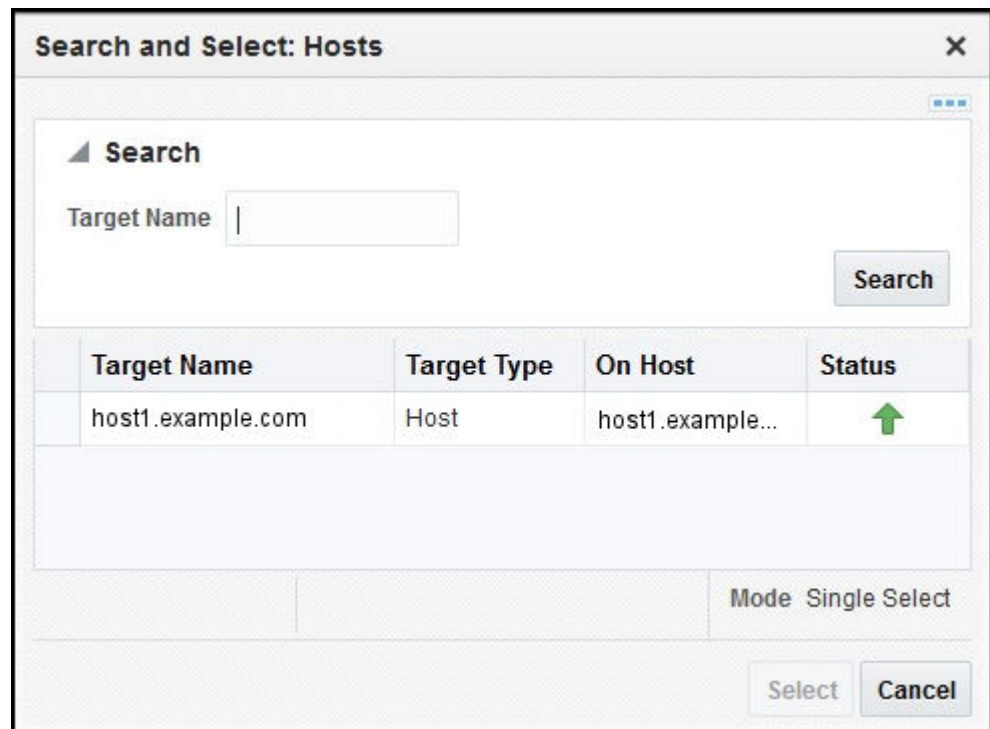
A pop-up window similar to [Figure 2-4](#) will be displayed:

Figure 2-4 Export Update to a Managed Host



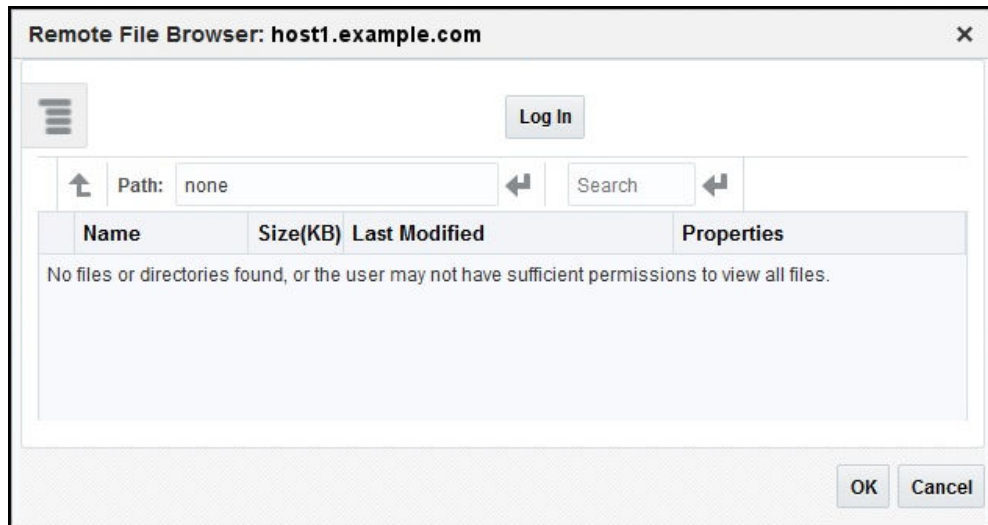
4. Enter the name of the export file name or accept the default name.
5. Click the search icon for the Host field. A pop-up window similar to [Figure 2-5](#) is displayed:

Figure 2-5 Search Hosts



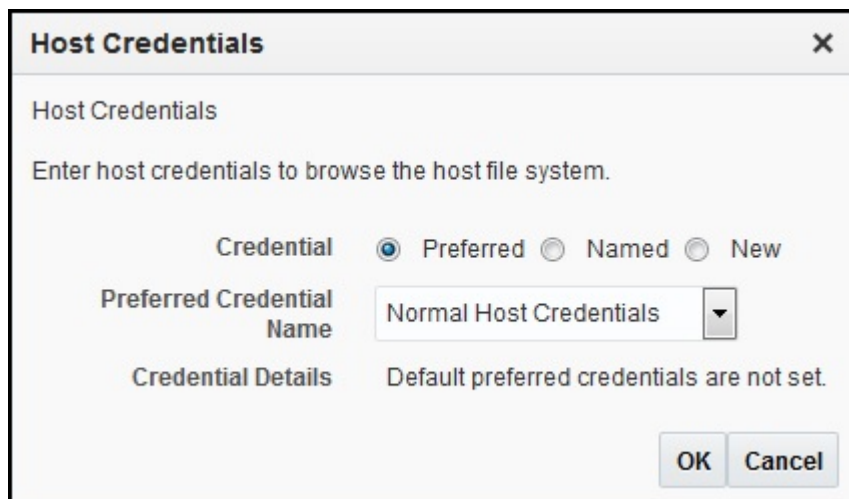
6. Select a host and click **Select**. You might need to enter a search string to narrow the results.
7. Click the search icon for the Location field. A pop-up window similar to [Figure 2-6](#) is displayed:

Figure 2-6 Host Location



8. Click **Log In**. A pop-up window similar to [Figure 2-7](#) is displayed:

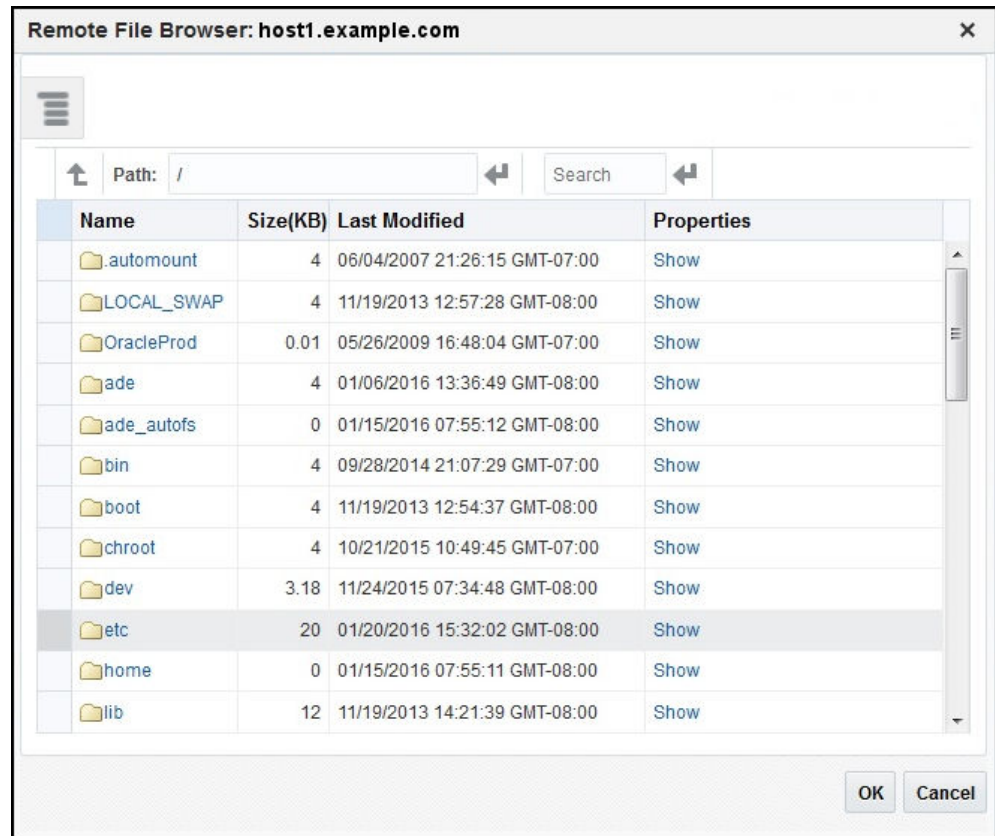
Figure 2-7 Host Credentials



9. Select existing **Preferred** or **Named** credentials or enter a **New** set of named credentials and click **OK**.

A pop-up window similar to [Figure 2-8](#) is displayed:

Figure 2-8 Select Location



10. Select the path where you want to place the export file and click **OK**.
11. The **Export Update to a Managed Host** pop-up window will be displayed with the selections listed. Click **Export**.

2.5.1.2 Exporting Agent Installation Files to Your Workstation

To export to your workstation, perform the following steps:

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. On the Self Update page, select **Management Connector** to display a list of available connectors.
3. Click the appropriate Microsoft SCOM connector name, then select **Export to->Your Workstation** from the Actions list.
4. A pop-up window will be displayed that prompts whether to open or save the file. Select **Save File** and click **OK**.
5. A pop-up window may be displayed that allows you to select the location where the file will be saved. Select the location and click **Save**.

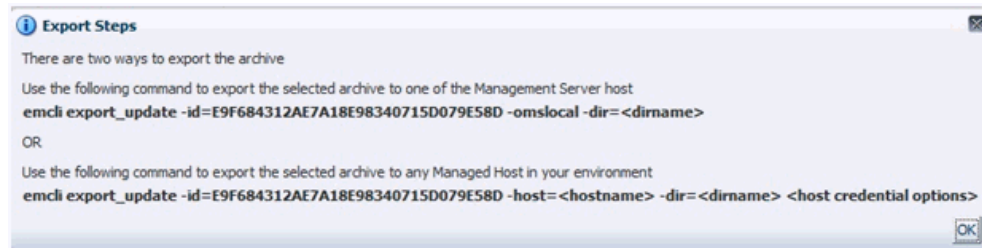
2.5.2 Exporting Agent Installation Files for Enterprise Manager 12c

The agent installation file is included in the Self Update archive that was installed in [Installing the Microsoft SCOM Event Connector in Enterprise Manager](#). To extract the installation file, perform the following steps:

1. Determine the command required to export the agent installation file. To do this, perform the following steps:
 - a. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
 - b. On the Self Update page, click the **Management Connector** link in the Type column.
 - c. Click the appropriate **Microsoft SCOM** connector name, then select **Export** from the Actions list.

A pop-up window will appear with the command required to export the file, as shown in [Figure 2-9](#):

Figure 2-9 Export Command Example



2. Open a command window on the Operations Manager host machine and navigate to a temporary directory where the file can be copied.
3. Log in to EM CLI using the following command. You will be asked to provide the password information for the Super Administrator account.

```
emcli login -username=<Super Administrator>
```

Note:

For information about using EM CLI, see the *Oracle® Enterprise Manager Command Line Interface* guide at:

http://docs.oracle.com/cd/E63000_01/EMCLI/toc.htm

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

A zip file will be created. The file name will be comprised of the ID value specified in the `export_update` command with a `.zip` extension.

5. Extract the agent installation files from the zip file using the following command:

```
unzip *.zip archives/SCOM*.zip
```

6. Continue with [Extracting the Agent Installation Files](#)

2.5.3 Extracting the Agent Installation Files

Once the zip file has been exported, perform the following steps to extract the agent installation files:

1. Open a command window on the host where the export file was copied and navigate to the directory where the file was copied.

2. Extract the agent installation files from the zip file using the following command:

```
unzip *.zip archives/SCOM*.zip
```

2.6 Installing the Microsoft SCOM Web Service

The SCOM web service acts as a front-end for all data flowing into and out of SCOM. Oracle Enterprise Manager posts calls to the web service whenever it needs to create or update an event.

You can install the SCOM web service on any UNIX or Windows system that has Oracle JDK 6.0 installed and has connectivity to the Oracle SCOM Agent and the Oracle Enterprise Manager server.

The following sections provide instructions for installing the Microsoft SCOM web service on UNIX and Windows platform:

- [Installing and Running the Microsoft SCOM Web Service on UNIX](#)
- [Installing and Running the Microsoft SCOM Web Service on Windows](#)
- [Exporting the Web Service Installation File](#)

2.6.1 Installing and Running the Microsoft SCOM Web Service on UNIX

The following sections explain how to install and then subsequently run the Microsoft SCOM Web Service on UNIX:

- [Prerequisites for UNIX](#)
- [Installing the Microsoft SCOM Web Service on UNIX](#)
- [Running the Microsoft SCOM Web Service on UNIX](#)
- [Testing the Microsoft SCOM Web Service on UNIX](#)
- [Uninstalling the Microsoft SCOM Web Service on UNIX](#)

2.6.1.1 Prerequisites for UNIX

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

1. Oracle Java Development Kit (JDK) version 6 Update 11 or higher is installed.

 **Note:**

JDK 7 and 8 are not supported; so, it must be JDK version 6 with an Update version equal to or greater than 11.

2. The `JAVA_HOME` environment variable is set to the JDK installation directory.

2.6.1.2 Installing the Microsoft SCOM Web Service on UNIX

To install the web service on a UNIX platform, perform the following steps:

1. Create a directory where you want to install the web service.
2. Obtain a copy of the web service installation file from the Management Server host machine as specified in [Exporting the Web Service Installation File](#).
3. Copy the `SCOM_webservices_adapter.jar` file to the web service installation directory.
4. Open a terminal and change the working directory to the installation directory.
5. Enter the following command to unzip and extract the .jar file:

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

 **Note:**

If the system where the SCOM web service is being installed does not have the JDK installed, you cannot extract the jar file contents. You need to copy the jar file to a system that has the JDK installed and transfer the files after they have been extracted

This creates the `adapters` directory that contains the installation files.

6. Enter the following command to change the working directory:
 - For SCOM 2012: `cd adapters/endpoints/SCOM`
 - For SCOM 2007: `cd adapters/endpoints/SCOM2007`
7. Enter the following command to run the installation script:

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

8. When the script prompts whether you want to use HTTPS:
 - If you specify **Y**, the web service is set up to use HTTPS port number **8443**.
 - If you specify **N**, the web service is set up to use HTTP port number **8080**.

 **Note:**

Refer to [Changing Default Port Numbers](#) in [Customizing Microsoft SCOM](#) for details on changing default port numbers.

9. When the script prompts for the user name of the web service, enter the user name that must be provided to access the SCOM Web Service.

The user name can be any value and is not associated with any specific OS or SCOM account. Make a note of this value and supply it when configuring the SCOM connector in Enterprise Manager.

10. When the script prompts for the password of the web service, enter the password that must be provided to access the SCOM Web Service.

The password can be any value and is not associated with any specific OS or SCOM account. Make a note of this value and supply it when configuring the SCOM connector in Enterprise Manager.

11. After the script prompts for the URL of the Oracle SCOM Agent, enter the URL that was noted when you installed the Oracle SCOM Agent. If the web service is being installed on a different machine than the Oracle SCOM Agent, the *localhost* in the URL must be replaced with the actual hostname or IP address of the machine where the Oracle SCOM Agent is installed.
12. After the script prompts for the username and password to use when accessing the Agent, enter a valid Windows username and password.

 **Note:**

If the account is a domain account, include the domain information when specifying the username. The format must follow the standard Windows format where the domain is specified first, followed by a backslash, and then the username is specified last. For example: `domain\username`

13. After the script displays the message "SCOM Web Service Complete," press **Enter** to complete the installation.
14. If the web service was configured to run using the HTTPS protocol, you must set up SSL as specified in [Configuring Enterprise Manager to Use SSL](#).

The web service framework is now installed and ready to start.

2.6.1.3 Running the Microsoft SCOM Web Service on UNIX

To run the Microsoft SCOM Web Service framework commands listed with the following tasks, first change the working directory to the following in the installation directory:

```
adapters/bin
```

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

2.6.1.4 Testing the Microsoft SCOM Web Service on UNIX

Perform the following steps to verify that the Microsoft SCOM Web Service is functional:

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

```
./testAdapter.sh
```

3. When the utility prompts for the web service password, enter the password you specified for the SCOM web service in step 10 of section [Installing the Microsoft SCOM Web Service on UNIX](#).

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

2.6.1.5 Uninstalling the Microsoft SCOM Web Service on UNIX

To uninstall the web service on UNIX:

1. Run the `service.sh status` command to determine whether the web service is running.
2. If the web service is running, run the `service.sh stop` command to stop the web service and verify it completes successfully.
3. Delete all files in the installation directory.

2.6.2 Installing and Running the Microsoft SCOM Web Service on Windows

The following sections explain how to install and then subsequently run the Microsoft SCOM Web Service on Windows:

- [Prerequisites for Windows](#)
- [Installing the Microsoft SCOM Web Service on Windows](#)
- [\(Optional\) Installing the Microsoft SCOM Web Services as a Windows Service](#)
- [Running the Microsoft SCOM Web Service on Windows](#)
- [Testing the Microsoft SCOM Web Service on Windows](#)
- [Uninstalling the Microsoft SCOM Web Service on UNIX](#)

2.6.2.1 Prerequisites for Windows

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

1. Oracle Java Development Kit (JDK) version 6 Update 11 or higher is installed.



Note:

JDK 7 and 8 are not supported; so, it must be JDK version 6 with an Update version equal to or greater than 11.

2. The `JAVA_HOME` environment variable is set to the JDK installation directory.
3. Zip utility, such as WinZip, is installed for unzipping a zip file.

2.6.2.2 Installing the Microsoft SCOM Web Service on Windows

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

1. Create a directory where you want to install the web service.
2. Obtain a copy of the web service installation file from the Management Server host machine as specified in [Exporting the Web Service Installation File](#).
3. Copy the `SCOM_webservices_adapter.jar` file to the web service installation directory.

4. Open a terminal and change the working directory to the installation directory.
5. Enter the following command to unzip and extract the .jar file:

```
%JAVA_HOME%\bin\jar xvf SCOM_webservices_adapter.jar
```

 **Note:**

If the system where the SCOM web service is being installed does not have the JDK installed, you cannot extract the jar file contents. You need to copy the jar file to a system that has the JDK installed and transfer the files after they have been extracted

This creates the adapters directory that contains the installation files.

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

- For SCOM 2012: `cd adapters\endpoints\SCOM`
- For SCOM 2007: `cd adapters\endpoints\SCOM2007`

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

```
.\install.sh
```

8. When the script prompts whether you want to use HTTPS:

- If you specify **Y**, the web service is set up to use HTTPS port number **8443**.
- If you specify **N**, the web service is set up to use HTTP port number **8080**.

 **Note:**

Refer to [Changing Default Port Numbers](#) in [Customizing Microsoft SCOM](#) for details on changing default port numbers.

9. When the script prompts for the user name of the web service, enter the user name that must be provided to access the SCOM Web Service.

The user name can be any value and is not associated with any specific OS or SCOM account. Make a note of this value and supply it when configuring the SCOM connector in Enterprise Manager.

10. When the script prompts for the password of the web service, enter the password that must be provided to access the SCOM Web Service.

The password can be any value and is not associated with any specific OS or SCOM account. Make a note of this value and supply it when configuring the SCOM connector in Enterprise Manager.

11. After the script prompts for the URL of the Oracle SCOM Agent, enter the URL that was noted when you installed the Oracle SCOM Agent. If the web service is being installed on a different machine than the Oracle SCOM Agent, the *localhost* in the URL must be replaced with the actual hostname or IP address of the machine where the Oracle SCOM Agent is installed.

12. After the script prompts for the username and password to use when accessing the Agent, enter a valid Windows username and password.

 **Note:**

If the account is a domain account, include the domain information when specifying the username. The format must follow the standard Windows format where the domain is specified first, followed by a backslash, and then the username is specified last. For example: `domain\username`

13. After the script displays the message "SCOM Web Service Complete," press **Enter** to complete the installation.
14. If the web service was configured to run using the HTTPS protocol, you must set up SSL as specified in [Configuring Enterprise Manager to Use SSL](#).


The web service framework is now installed and ready to start.

2.6.2.3 (Optional) Installing the Microsoft SCOM Web Services as a Windows Service

If you want the Microsoft SCOM web service to run as a Windows service, perform the following steps.

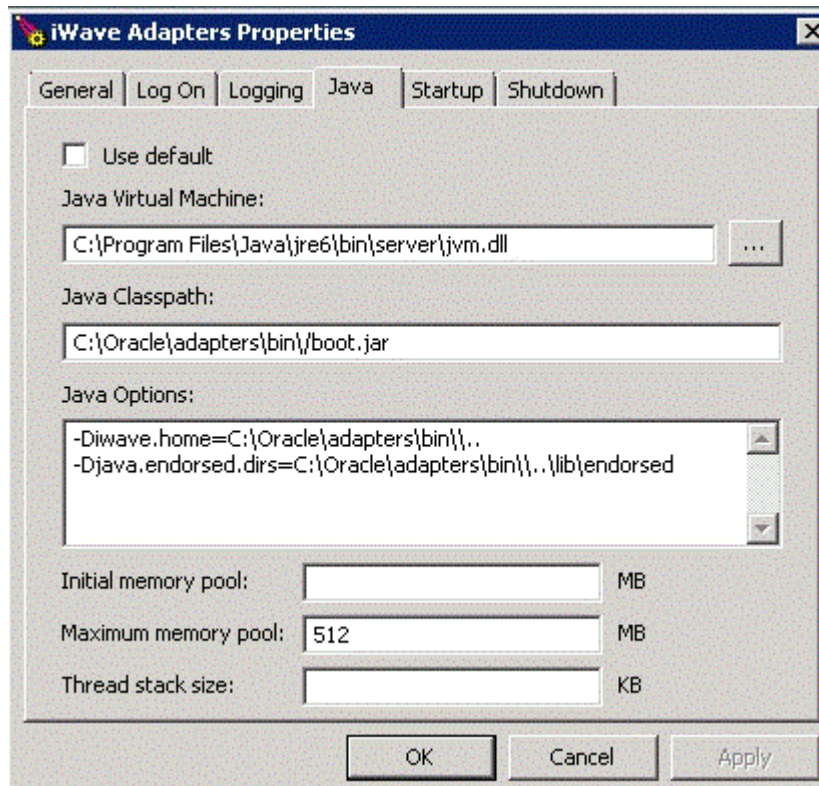
1. Change the working directory to the `adapters\bin` directory in the installation directory.
2. If the web service will be run using a 64-bit JDK, copy the `iWaveAdapters.exe` and `iWaveAdaptersw.exe` files from the `x64` directory to the current directory (`.`) overwriting the existing files.
3. Enter the following command to install the web service as a Windows service:

```
service.bat install
```

4. If the web service will be run using a 64-bit JDK, perform the following substeps to configure the service to use the 64-bit JDK:
 - a. In the `adapters\bin` directory, double click the **iWaveAdaptersw.exe** file. This will cause the iWave Adapters Properties window to be displayed.
 - b. Click the **Java** tab. The Java tab will be displayed that shows the JVM settings as shown in [Figure 2-10](#).
 - c. Uncheck the **Use default** check box if it is checked.
 - d. Click  to open the Select Java Virtual Machine DLL window.
 - e. Navigate to the `jvm.dll` file in the 64-bit JDK installation directory and click **Open**.
 - f. Click **OK**.

The web service framework is now installed and ready to start.

Figure 2-10 Java Tab on the iWave Adapters Properties Window



2.6.2.4 Running the Microsoft SCOM Web Service on Windows

Standalone Service

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

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

```
startAdapters.bat
```

To shut down the SCOM web service framework, close the window where you started the web service.

Windows Service

To start the SCOM web service framework when set up to run as a Windows service, enter the following command:

```
net start iWaveAdapters
```

To shut down the SCOM web service framework, enter the following command:

```
net stop iWaveAdapters
```

2.6.2.5 Testing the Microsoft SCOM Web Service on Windows

Perform the following steps to verify that the Microsoft SCOM Web Service is functional:

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

```
.\testAdapter.sh
```

3. When the utility prompts for the web service password, enter the password you specified for the SCOM web service in step 10 of section [Installing the Microsoft SCOM Web Service on Windows](#).

If the test completes successfully, the last line the utility displays is “Test completed successfully.”

2.6.2.6 Uninstalling the Microsoft SCOM Web Service on UNIX

To uninstall the web service on Windows, determine if the web service is installed as a Windows service:

1. If the web service is installed as a Windows service, perform the following steps:
 - a. Determine if the web service is running.
 - b. If the web service is running, run the `service.bat stop` command to stop the web service and verify it completes successfully
 - c. Run the `service.bat uninstall` command to remove it as a Windows service and verify it completes successfully.
2. If the web service is **not** installed as a Windows service, perform the following steps:
 - a. Determine if the web service is running.
 - b. If the web service is running, stop the web service by closing the Java window.
3. Delete all files in the installation directory.

2.6.3 Exporting the Web Service Installation File

The web service installation file is included in the zip file that was extracted in [Exporting the Agent Installation Files](#). To extract the installation file, perform the following steps:

1. Open a command window on the Operations Manager host machine and navigate to the temporary directory where the zip file was created.
2. Extract the web service installation file using the following command:

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

2.7 Uninstalling the Microsoft SCOM Event Connector

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

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

3

Configuring the Microsoft SCOM Event Connector

This chapter provides procedures to configure the two sub-pages of the main Configure Management Connector page, then explains how to perform other tasks to complete the configuration process.

This chapter discusses the following topics:

- [Creating a Connector Instance](#)
- [Configuring the Connector](#)
- [Connector Modes of Operation](#)
- [Enabling and Disabling the Connector](#)
- [Providing General Settings](#)
- [Exporting the Agent Installation Files](#)
- [Deleting the Microsoft SCOM Event Connector](#)
- [Testing the Microsoft SCOM Event Connector](#)

Note:

Unless otherwise noted, these instructions apply to the SCOM 2012 connector and to the SCOM 2007 connectors. Instructions specific to the SCOM 2007 connectors are available in [Microsoft SCOM 2007 Connector](#).

3.1 Creating a Connector Instance

Once the SCOM connector is installed in Enterprise Manager, you must create one or more instances of this connector type. A connector instance refers to the configured instance of the connector with specific details, such as connector name, web-service end-points, username/password, and so forth of the SCOM system.

For example, multiple connector instances for the same connector type are supported, which provides the flexibility to configure multiple SCOM systems with Enterprise Manager. That is, if the datacenter is configured with two different instances of SCOM (one for production targets and one for test targets) and you would like events from production targets to be sent to one SCOM instance and the events from test targets to be sent to the another SCOM instance, then this scenario is supported.

In another example, you could have a production database and test database that Enterprise Manager monitors, and you can create two different connector instances pointed to two different SCOM systems (one for production targets and one for test targets) with events from production targets sent to one SCOM instance and events from test targets sent to the another SCOM instance. You can associate each instance

with separate event rules. Using this setup, you can forward Enterprise Manager events generated from different targets to the appropriate SCOM system.

Follow the steps below to create a connector instance:

1. From the Enterprise Manager console, click **Setup**.
2. Select **Extensibility** in the pane.
3. Select **Management Connectors** in the left pane.
4. Select the appropriate SCOM connector type from the Create Connector drop-down list then click **Go**.
5. Enter the connector name and description on the next screen then click **OK**.
6. The connector instance shows up as unconfigured in the Connector Setup page. [Figure 3-1](#) shows an unconfigured SCOM 2012 connector instance.

Figure 3-1 Unconfigured SCOM 2012 Connector Instance

Select	Status	Name	Type	Version	Category	Description
<input type="radio"/>		SCOM 2012	SCOM 2012 Connector	12.1.0.1.0	Event Connector	SCOM 2012 Connector

3.2 Configuring the Connector

To configure the connector, follow these steps:

1. As Super Administrator from the Enterprise Manager console, click **Setup**.
2. Click **Extensibility**, then select **Management Connectors**. The Management Connectors page appears and lists all created connector instances.

Note:

The status column with a green tick mark indicates that the connector is already configured.

3. Click the name of the SCOM connector.

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

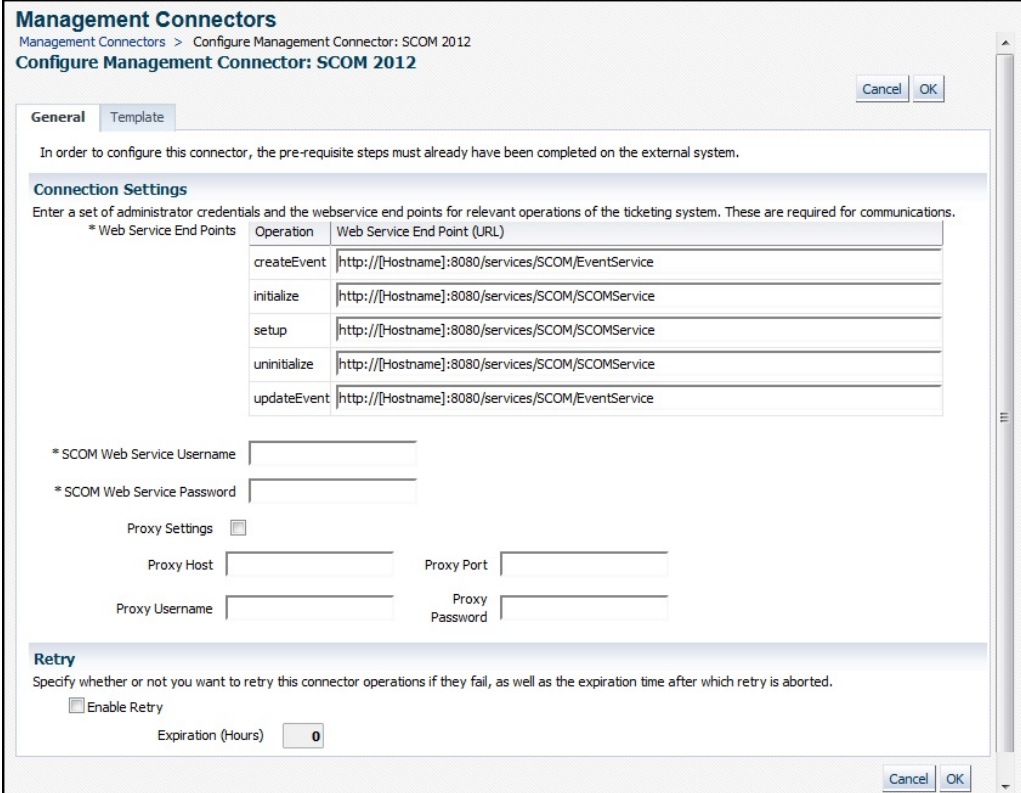
4. Provide the required settings. See [Providing General Settings](#) for details.
5. Click **OK**.

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

 **Note:**

If you chose HTTPS as the protocol to establish a connection between SCOM and Enterprise Manager, make sure you have performed the steps specified in [Configuring Enterprise Manager to Use SSL](#).

Figure 3-2 General Tab of Configure Management Connector Page



Management Connectors
Management Connectors > Configure Management Connector: SCOM 2012
Configure Management Connector: SCOM 2012

General Template

In order to configure this connector, the pre-requisite steps must already have been completed on the external system.

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

* Web Service End Points	Operation	Web Service End Point (URL)
	createEvent	http://[Hostname]:8080/services/SCOM/EventService
	initialize	http://[Hostname]:8080/services/SCOM/SCOMService
	setup	http://[Hostname]:8080/services/SCOM/SCOMService
	uninitialize	http://[Hostname]:8080/services/SCOM/SCOMService
	updateEvent	http://[Hostname]:8080/services/SCOM/EventService

* SCOM Web Service Username

* SCOM Web Service Password

Proxy Settings

Proxy Host Proxy Port

Proxy Username Proxy Password

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

Enable Retry

Expiration (Hours)

3.3 Connector Modes of Operation

 **Note:**

These modes apply to the SCOM 2012 connector **only**.

The SCOM API does not allow the severity of an alert to be changed in SCOM 2012. Because of this limitation, the connector has two modes of operation.

When the connector is operating in the Update-Only mode of operation, it creates a single alert that is updated each time an event severity change occurs in Enterprise Manager. Each time the event severity changes in Enterprise Manager, a new entry is added to the alert history log in SCOM 2012 that contains the updated information. The severity of the alert remains unchanged in SCOM 2012. This is the default mode of operation.

When the connector is operating in the Create-On-Update mode of operation, it creates a new alert in SCOM 2012 whenever a severity change occurs for the associated event in Enterprise Manager. The new alert has the correct severity and has the latest information in the description and title fields. Once the event clears in Enterprise Manager, all of the associated alerts in SCOM 2012 are closed.

To switch from the Update-Only to the Create-On-Update mode, the alternate template must be defined for the `updateEvent` operation. See [Switching to the Alternate Template](#) for instructions for switching from the Update-Only to the Create-On-Update mode.

3.3.1 Switching to the Alternate Template

There is an alternate template defined in the connector that must be installed for the `updateEvent` operation to switch from the default Update-Only mode to the Create-On-Update mode. By default, the alternate template will synchronize the history log information when a new event severity is sent from Enterprise Manager. This means that the history log in the new alert will include an entry for the original alert created and an entry for each update that has occurred up to that point in time. Also, the history log of the original alert will include an entry for the original create and one for each update as well. [Figure 3-3](#) shows an example of the history log for the new alert when the default synchronization feature is enabled.

If synchronization of the logs is not desired, the alternate template has a flag that can be changed to disable the synchronization feature. When the feature is disabled, the original alert will just have information about the original create but will not include any update entries. Also any new alerts that are created will just have a single entry for the update associated with that alert. [Figure 3-4](#) shows an example of the history log for the new alert when the synchronization feature has been disabled.

To switch the template perform the following:

1. Export the default template XSLT files from Enterprise Manager. Follow the instructions in [Exporting the Template Files](#) to obtain copies of the default template files.
2. If you want to disable the synchronization feature, perform the following substeps. Otherwise skip to the next step.
 - a. Open the `updateEvent_request_2012_alt.xml` file in a text editor.
 - b. Change the `syncHistory` flag from **true** to **false**.
 - c. Save the changes and exit.

Listed below is an example of what the flag looks like before and after the change.

syncHistory Before

```
<xsl:variable name="syncHistory">true</xsl:variable>
```

syncHistory After

```
<xsl:variable name="syncHistory">false</xsl:variable>
```

3. The last step is to register the alternate template to be used for the `updateEvent` operation. To register the alternate template, perform the following steps:
 - a. Open the `updateEvent_request_2012_alt.xml` file with a text editor.

- b. Copy the contents of the template.
- c. At the Enterprise Manager Cloud Control console, navigate to the **Template** tab of the SCOM 2012 connector configuration page.
- d. Select the **Update Event Request** template and click **Edit**.
- e. Paste the contents of the alternate template over the existing template contents and click **Save**.

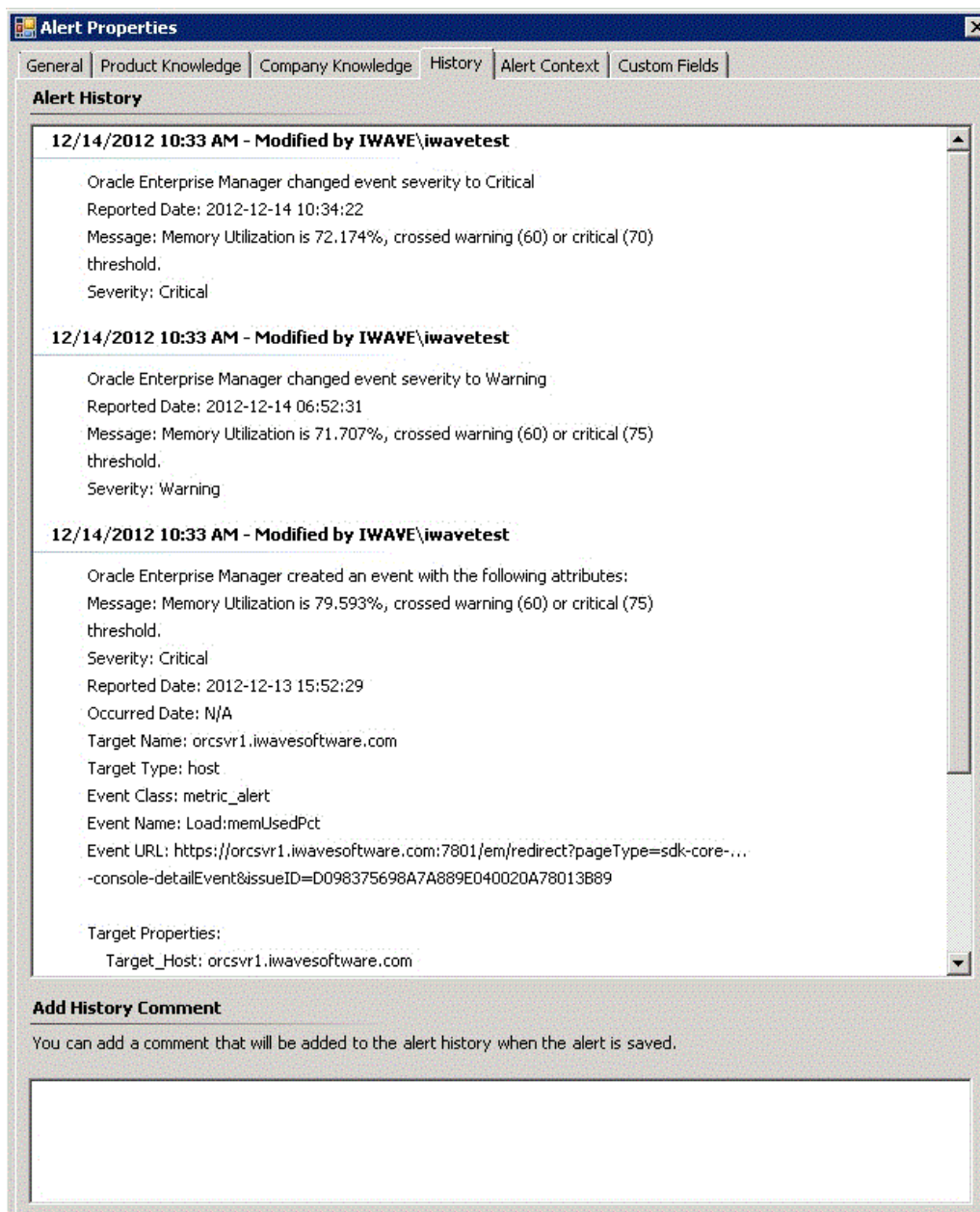
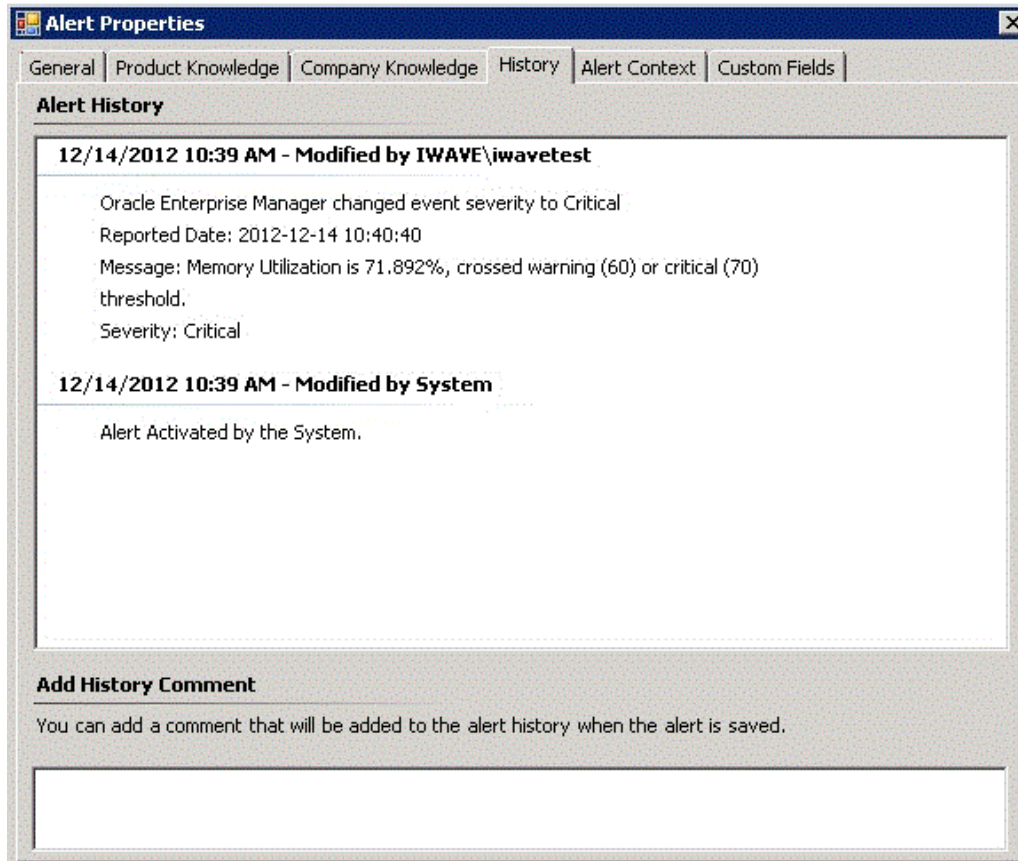
Figure 3-3 History Log with Synchronization Feature Enabled (default value)

Figure 3-4 History Log with Synchronization Feature Disabled

3.4 Enabling and Disabling the Connector

You can enable or disable a connector instance without needing to reconfigure or remove the connector from the system.

You can enable or disable a connector from the Management Connector page by selecting the connector and clicking either **Enable** or **Disable**. After a connector is disabled, a red cross icon under the Status column appears. By default, the connector instance is enabled as soon as it is configured.

Note:

Only enabled connectors are available to forward events.

3.5 Providing General Settings

The following sections explain how to provide various configuration details:

- [Connection Settings](#)
- [Retry](#)

3.5.1 Connection Settings

The SCOM connector communicates with Microsoft SCOM through the SCOM web service installed as described in [Installing the Microsoft SCOM Web Service](#). All fields are mandatory.

Web Service End Points – URL to use when performing event operations that require interaction with the SCOM web service. The web service uses two different URLs depending on the operation being performed. One URL is used for the registration of the SCOM Agent with Microsoft SCOM (setup, initialize, and uninitialize operations), and defaults to the following value:

```
http://[Hostname]:8080/services/SCOM/SCOMService
```

The other URL is used to create/update alert information in SCOM (createEvent and updateEvent operations), and defaults to the following value:

```
http://[Hostname]:8080/services/SCOM/EventService
```

Modify the URL for the operations based on whether the SCOM web service was set up using HTTP or HTTPS:

- **For HTTP:**
 - Replace [Hostname] in the URL with the hostname or IP address of the system where the SCOM web service was installed.
- **For HTTPS:**
 - Change the protocol from **http** to **https**.
 - Replace [Hostname] in the URL with the hostname or IP address of the system where the SCOM web service was installed.
 - Change the port number from **8080** to **8443**.

SCOM Web Service Username - User name that was configured for accessing the SCOM web service in step 9 of the appropriate web service installation section ([Installing the Microsoft SCOM Web Service on UNIX](#) and [Installing the Microsoft SCOM Web Service on Windows](#)).

SCOM Web Service Password - Password that was configured for accessing the SCOM web service in step 10 of the appropriate web service installation section ([Installing the Microsoft SCOM Web Service on UNIX](#) and [Installing the Microsoft SCOM Web Service on Windows](#)).

Example 3-1 Configured URLs

If the SCOM web service was installed on a system with a hostname of `scomws`, the following URLs would be configured for the `createEvent` and `updateEvent` operations.

For HTTP:

```
http://scomws:8080/services/SCOM/EventService
```

For HTTPS:

```
https://scomws:8443/services/SCOM/EventService
```

3.5.2 Retry

You can enable and disable the Retry option and configure its interval value. The Retry section, available on the connector configuration page, enables you to specify whether failed operations need to be retried within a configurable expiration time.

When you enable the Retry option, you can specify whether you want to resend a Create or Update request if the request fails the first time, and specify the time period (greater than **0**) after which you want to abandon the retry. Enterprise Manager retries every five minutes until the request is successful or the retry interval expires.

By default, the Retry is disabled. This setting applies to all events that the SCOM Connector processes. The retry period interval accepts the number of hours as any integer value. For example, **1** or **2**.

3.6 Exporting the Template Files

The web service installation file is included in the zip file that was extracted in [Exporting the Agent Installation Files](#). To extract the installation file, perform the following steps:

1. Open a command window on the machine where the zip file was exported and navigate to the temporary directory where it resides.
2. Extract the connector installation jar file from the zip file using the following command:

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

3. Extract the templates from the connector jar file using the following command:

- For SCOM 2012:

```
$JAVA_HOME/bin/jar xf archives/*.jar createEvent_request_2012.xml  
updateEvent_request_2012.xml updateEvent_request_2012_alt.xml
```

- For SCOM 2007 R2:

```
$JAVA_HOME/bin/jar xf archives/*.jar createEvent_request_R2.xml  
updateEvent_request.xml
```

- For SCOM 2007 pre-R2:

```
$JAVA_HOME/bin/jar xf archives/*.jar createEvent_request_preR2.xml  
updateEvent_request.xml
```

Note:

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

3.7 Deleting the Microsoft SCOM Event Connector

You can delete a connector from the Management Connector page by selecting the connector and clicking **Delete**. After a connector is deleted, all associated events rules are no longer configured to forward the event. Also, references to the event connector are removed from the event rules.

Additionally, if the connector deleted is the only connector instance of that connector type, the corresponding connector type is also deleted.

3.8 Testing the Microsoft SCOM Event Connector

Perform the following steps to verify that the connector is configured correctly:

1. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator permissions.
2. From the Enterprise Manager console, click **Setup**, then **Extensibility**, then **Management Connectors** from the drop-down menus.

The Management Connectors page is displayed.

3. Click the name of the SCOM connector.

The General tab of the Configure Management Connector page appears.

4. Select and copy the URL specified for the `createEvent` or `updateEvent` operation.
5. Open an internet browser on the system where the Oracle Enterprise Manager server is installed.
6. In the address window, enter the URL that was copied in step 4 above. Add **?wsdl** to the end of the URL. The URL should appear similar to the following example:

```
http://[Hostname]:8080/services/SCOM/EventService?wsdl
```

[Hostname] is the actual host name or IP address where the SCOM web service is installed.

If the WSDL is loaded, this confirms that the connector is configured correctly for sending event information to SCOM.

4

Forwarding Enterprise Manager Events to Microsoft SCOM

Events generated or updated in Oracle Enterprise Manager are not forwarded to SCOM unless you create rules to invoke the SCOM connector. A rule identifies the conditions that must be met before the connector is invoked.

The following section describes procedures that explain how to set up rules to create events and update events in SCOM based on events in Enterprise Manager:

- [Setting Event Rules](#)
- [Viewing Events in the SCOM Console](#)

Note:

Unless otherwise noted, these instructions apply to the SCOM 2012 connector and to the SCOM 2007 connectors. Instructions specific to the SCOM 2007 connectors are available in [Microsoft SCOM 2007 Connector](#).

4.1 Setting Event Rules

This section explains how to create a new rule in Enterprise Manager that invokes the SCOM connector. Log in to the Enterprise Manager console with an account that has Super Administrator permissions and then perform the following steps:

1. From the Enterprise Manager console, click **Setup**, then **Incidents**, then **Incident Rules**.
2. Determine whether you want to add the new rule to an existing rule set or whether you want to create a new rule set:
 - To update an existing rule set, click the rule set that you want to update and then click **Edit**.
 - To create a new rule set, click **Create Rule Set**, then enter the name and select the target(s) to which it applies.
3. Click the Rules tab then click **Create**. The Select Type of Rule to Create pop-up window is displayed.

As you proceed below, the wizard interface explains various rules and their usage.

For detailed information, refer to the *Incident Management* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

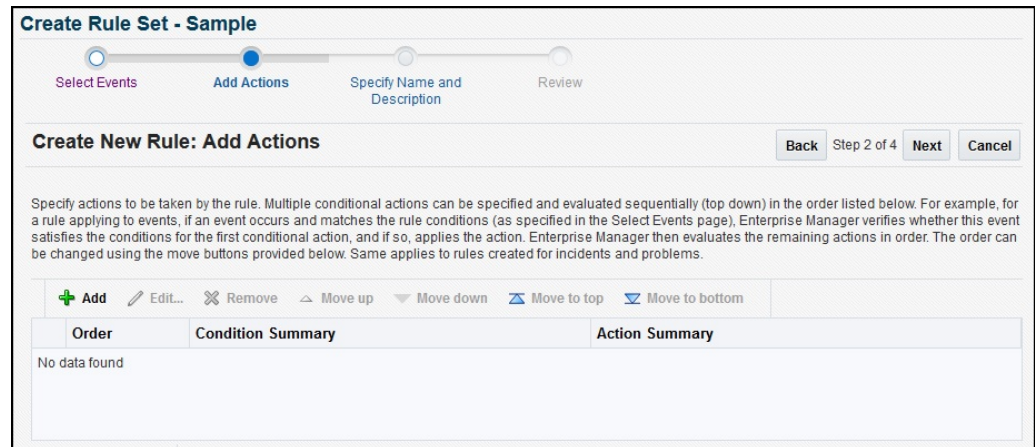
4. Select Incoming events and updates to events then click **Continue**.

The Select Events page is displayed.

5. Specify the set of events that you want to forward, then click **Next**.

The Add Actions page is displayed as shown in [Figure 4-1](#):

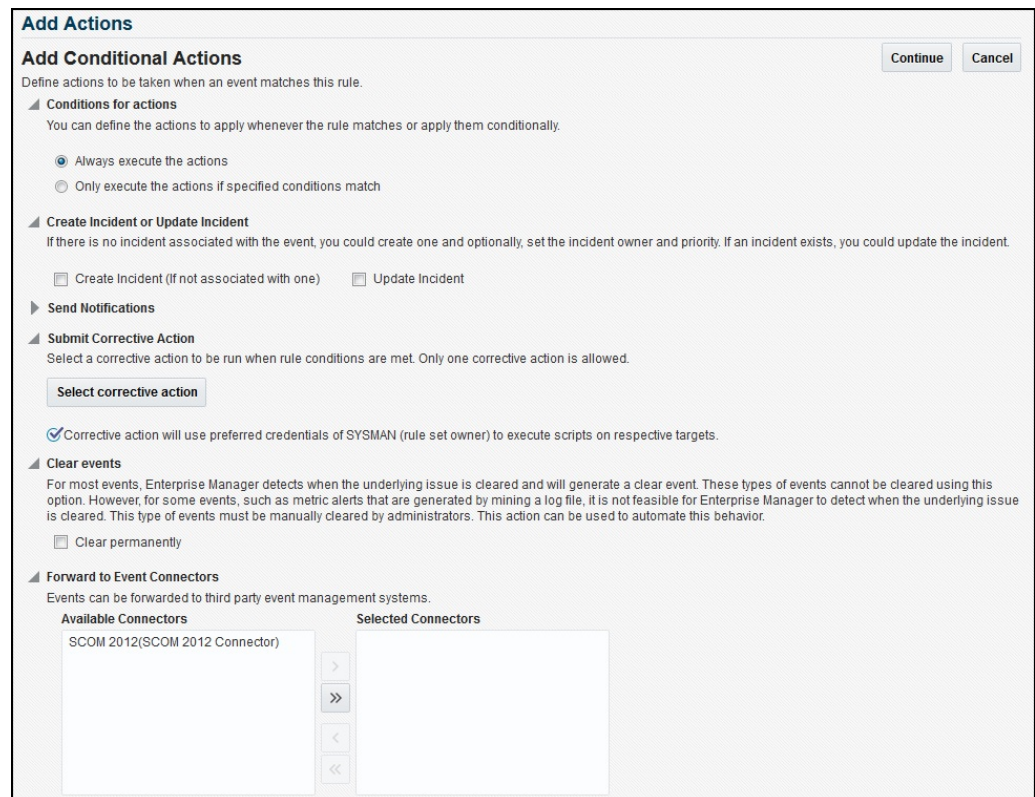
Figure 4-1 Add Actions Page



6. Click **Add**.

The Add Conditional Actions page is displayed as shown in [Figure 4-2](#):

Figure 4-2 Add Conditional Actions Page



7. Select the appropriate SCOM connector instance in the Forward to Event Connectors section then click **>**, then click **Continue**.

The Add Actions page is displayed again with the new action listed.

8. Click **Next**.

The Specify Name and Description page will be displayed.

9. Enter a name and description for the rule then click **Next**.

The Review page is displayed.

10. Click **Continue** if everything looks correct. An information popup will be displayed that says, *Rule has been successfully added to the current rule set. Newly added rules are not saved until the Save button is clicked.*

 **Note:**

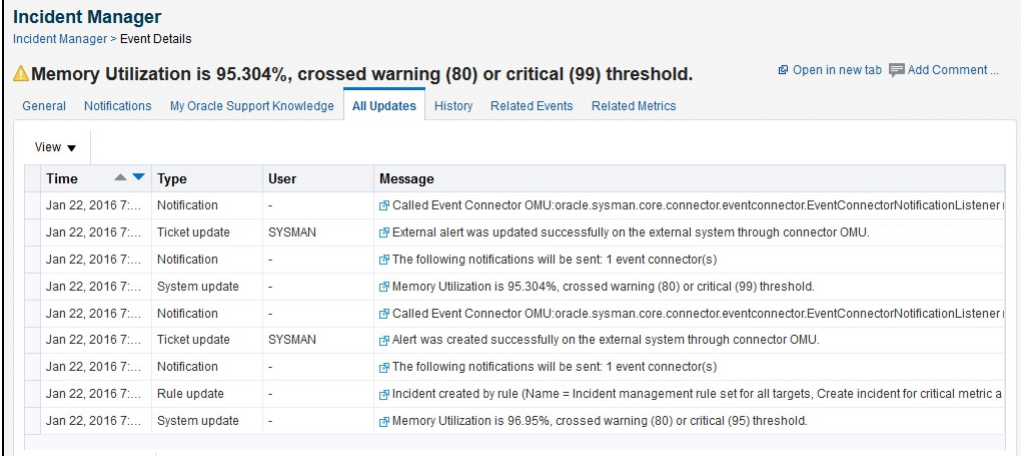
You can click **Back** and make corrections to the rule if necessary.

11. Click **Save** to save the changes to the rule set.

The following process occurs after the above created event rule is satisfied:

- A request is sent to the SCOM connector when an event is created per the criteria mentioned in the rule.
- The alert is created or updated on the SCOM console.
- In Enterprise Manager, the event is annotated with a comment on the **All Updates** tab to indicate that an event in SCOM has been created or updated as seen in [Figure 4-3](#).

Figure 4-3 Incident Manager All Updates Tab



The screenshot shows the 'Incident Manager' interface with the 'All Updates' tab selected. At the top, there is a warning message: 'Memory Utilization is 95.304%, crossed warning (80) or critical (99) threshold.' Below this, there are navigation tabs: 'General', 'Notifications', 'My Oracle Support Knowledge', 'All Updates', 'History', 'Related Events', and 'Related Metrics'. A 'View' dropdown menu is visible above the table. The table has four columns: 'Time', 'Type', 'User', and 'Message'. The messages include notifications about event connectors, ticket updates, system updates, and rule updates.

Time	Type	User	Message
Jan 22, 2016 7:...	Notification	-	Called Event Connector OMU:oracle.sysman.core.connector.eventconnector.EventConnectorNotificationListener
Jan 22, 2016 7:...	Ticket update	SYSMAN	External alert was updated successfully on the external system through connector OMU.
Jan 22, 2016 7:...	Notification	-	The following notifications will be sent: 1 event connector(s)
Jan 22, 2016 7:...	System update	-	Memory Utilization is 95.304%, crossed warning (80) or critical (99) threshold.
Jan 22, 2016 7:...	Notification	-	Called Event Connector OMU:oracle.sysman.core.connector.eventconnector.EventConnectorNotificationListener
Jan 22, 2016 7:...	Ticket update	SYSMAN	Alert was created successfully on the external system through connector OMU.
Jan 22, 2016 7:...	Notification	-	The following notifications will be sent: 1 event connector(s)
Jan 22, 2016 7:...	Rule update	-	Incident created by rule (Name = Incident management rule set for all targets, Create incident for critical metric a
Jan 22, 2016 7:...	System update	-	Memory Utilization is 96.95%, crossed warning (80) or critical (95) threshold.

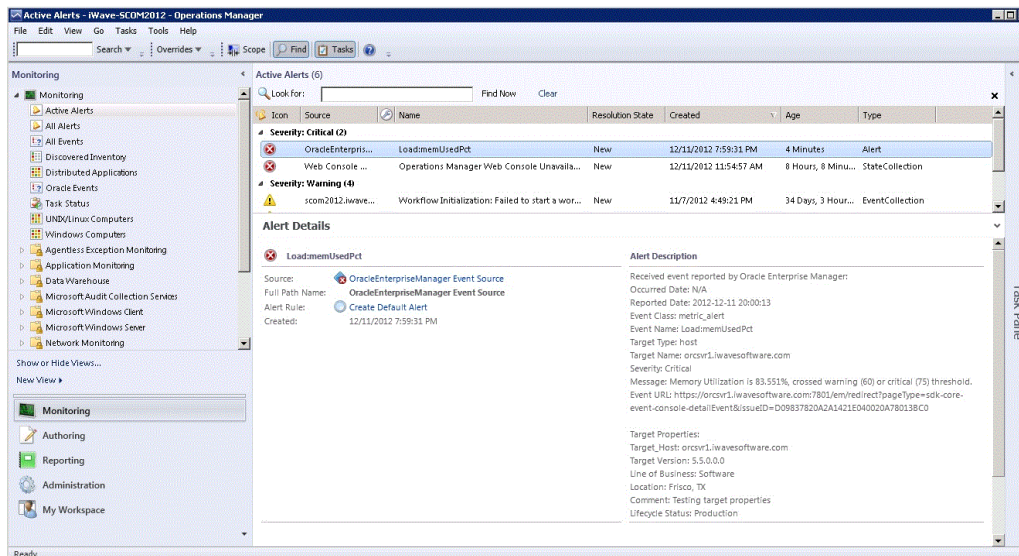
4.2 Viewing Events in the SCOM Console

After the event has been sent to SCOM, you can view it in the Microsoft SCOM console, as shown in [Figure 4-4](#). Full details of the event are sent to SCOM including:

- Event class and name.
- Target type and name.
- Message.
- Severity.

- URL to the Enterprise Manager event details page.

Figure 4-4 Event Details in the Microsoft SCOM 2012 Console



To view the event in Enterprise Manager, copy the URL listed in the event and paste in the address bar of a browser. You will be asked to log in to Oracle Enterprise Manager. After logging in, the Oracle Enterprise Manager event information is displayed.

You can change the event information sent to SCOM, or you can change the mappings between the Enterprise Manager event and Microsoft SCOM event by modifying the event templates.

See [Working With Event Templates](#) for details.

5

Working With Event Templates

This chapter provides details on the default event templates shipped along with the SCOM connectors. The event templates specify the mappings between an Enterprise Manager event attributes and SCOM web service attributes:

- [Familiarization with Event Templates](#)
- [Customizing Event Templates](#)

Note:

Unless otherwise noted, these instructions apply to the SCOM 2012 connector and to the SCOM 2007 connectors. Instructions specific to the SCOM 2007 connectors are available in [Microsoft SCOM 2007 Connector](#).

5.1 Familiarization with Event Templates

This section describes the default mappings between the Enterprise Manager event data fields and the Microsoft SCOM alert data fields.

Topics

- [Default Templates](#)
- [Severity Mapping](#)
- [Priority Mapping](#)

5.1.1 Default Templates

The event templates XML Style Sheet (XSL) files contain the mappings between the two systems. These files are located in the Self Update archive that was installed in [Installing the Microsoft SCOM Event Connector](#). To extract the installation file, perform the steps in [Exporting the Template Files](#).

[Table 5-1](#) lists the XSL files that perform the mappings for the SCOM 2012 connector and provides a summary of each. [Table E-1](#) lists the XSL files that perform the mappings for the SCOM 2007 connectors and provides a summary of each.

Table 5-1 XSL Files that Perform SCOM 2012 Mappings

File	Description
createEvent_request_2012.xsl	Transforms the Oracle Enterprise Manager event data to the Microsoft SCOM 2012 alert format for the createEvent operation.

Table 5-1 (Cont.) XSL Files that Perform SCOM 2012 Mappings

File	Description
updateEvent_request_2012.xsl	Transforms the Oracle Enterprise Manager event data to the Microsoft SCOM 2012 alert format for the <code>updateEvent</code> operation.
updateEvent_request_2012_alt.xsl	Alternate template that transforms the Oracle Enterprise Manager event data to the Microsoft SCOM 2012 alert format for the <code>updateEvent</code> operation. This template causes the connector to create a new alert in SCOM 2012 each time a status change occurs in Enterprise Manager.

The following sections provide details about the default templates:

- [Create Event Template](#)
- [Update Event Template](#)
- [Formatted Enterprise Manager Description Contents](#)
- [Formatted Alert History Create Contents](#)
- [Formatted Alert History Update Contents](#)
- [Alert History Title](#)

5.1.1.1 Create Event Template

This section identifies the default create mappings for the SCOM 2012 connector. To see the default create mappings for the SCOM 2007 connectors, refer to section [Create Event 2007 Template](#) in [Microsoft SCOM 2007 Connector](#).

The Oracle Enterprise Manager Connector Framework invokes the `createEvent` operation whenever an event is generated in Oracle Enterprise Manager and a rule is configured to invoke the SCOM 2012 connector. The `createEvent_request_2012.xsl` template is invoked during the process to transform the data from Oracle Enterprise Manager format to SCOM 2012 alert format. [Table 5-2](#) lists the default field mappings between the Microsoft SCOM alert and the Oracle Enterprise Manager event and the Microsoft SCOM 2012 alert.

Table 5-2 Create Event Template Mappings

SCOM Field Name	Required	Value
Name	Yes	Set to the event <code>EventName</code> field.
Description	Yes	Set to the formatted contents of the event as specified in Formatted Enterprise Manager Description Contents .
Priority	Yes	Set the priority based on the event priority. See Priority Mapping for details.

Table 5-2 (Cont.) Create Event Template Mappings

SCOM Field Name	Required	Value
Severity	Yes	Set the severity based on the event severity. See Severity Mapping for details.
Alert History	No	Set to the formatted contents of the event as specified in Formatted Alert History Create Contents .

5.1.1.2 Update Event Template

This section identifies the default update mappings for the SCOM 2012 connector. To see the default update mappings for the SCOM 2007 connectors, refer to [Update Event 2007 Template](#) in [Microsoft SCOM 2007 Connector](#).

The Oracle Enterprise Manager Connector Framework invokes the `updateEvent` operation whenever an event is generated in Oracle Enterprise Manager and a rule is configured to invoke the SCOM 2012 connector.

Example 5-1 Default Template

If the `updateEvent` operation is configured to use the default template, the `updateEvent_request_2102.xsl` template is invoked during the process to transform the data from Oracle Enterprise Manager format to SCOM 2012 alert format. [Table 5-3](#) lists the default field mappings between the Microsoft SCOM alert and the Oracle Enterprise Manager event and the Microsoft SCOM 2012 alert.

Table 5-3 Update Event Template Mappings

SCOM Field Name	Required	Value
ID	Yes	Set to the event <code>ExternalEventId</code> field.
Resolution State	Yes	Set to 255 (Closed) if the event severity is Clear. Otherwise, set to 0 (New).
Alert History	No	Set to "Oracle Enterprise Manager cleared alert" if the event severity is Clear. Set to "Oracle Enterprise Manager changed alert severity to warning" if the event severity is Warning. Set to "Oracle Enterprise Manager changed alert severity to critical" if the event severity is Critical. Not set for other severity values.

Example 5-2 Alternate Template

If the `updateEvent` operation has been reconfigured to use the alternate template, the `updateEvent_request_2012_alt.xsl` template is invoked during the process to transform the data from Oracle Enterprise Manager format to SCOM 2012 alert format.

[Table 5-4](#) lists the default field mappings between the Oracle Enterprise Manager event and the Microsoft SCOM 2012 alert when the status is clear.

Table 5-5 lists the default field mappings between the Oracle Enterprise Manager event and the Microsoft SCOM 2012 alert for all other status values.

Table 5-4 Clear Event Alternate Template Mappings

SCOM Field Name	Required	Value
ID	Yes	Set to the event <code>ExternalEventId</code> field.
Resolution State	Yes	Set to 255 (Closed).
Alert History	No	Set to "Oracle Enterprise Manager cleared alert"

Table 5-5 Update Event Alternate Template Mappings

SCOM Field Name	Required	Value
Name	Yes	Set to the event <code>EventName</code> field.
Description	Yes	Set to the formatted contents of the event as specified in Formatted Enterprise Manager Description Contents .
Priority	Yes	Set the priority based on the event priority. See Priority Mapping for details.
Severity	Yes	Set the severity based on the event severity. See Severity Mapping for details.
Alert History	No	<p>If the synchronization feature is enabled, entries will be added to the history log for all events leading up to and including the update. The original create entry will be formatted as specified in Formatted Alert History Create Contents. Each update entry will be formatted as specified in Formatted Alert History Update Contents.</p> <p>If the synchronization feature is disabled, an entry will be added to the alert history log that is formatted as specified in Formatted Alert History Update Contents.</p>

5.1.1.3 Formatted Enterprise Manager Description Contents

Listed below is the format used by the templates for the Description fields. Text delimited by angle brackets (< and >) designates an Enterprise Manager Event field name that will be replaced by the actual field contents. Lines marked with double asterisks indicate they will only be present if the designated event field contains data. The Notes section below contains information about some of the fields.

```
Received event reported by Oracle Enterprise Manager:
Occurred Date: <OccurredDate>
ReportedDate: <ReportedDate>
Event Class: <EventClass>
Event Name: <EventName>
```

```

Target Type: <SourceInfo/TargetInfo/TargetType>
Target Name: <SourceInfo/TargetInfo/TargetName>
Severity: <Severity>
Message: <Message>
Event URL: <EventURL>

Target Properties:**
    <TargetProperty/Name>: <TargetProperty/Value>**

Event Context:**
    <EventContextAttributes/StringAttribute/Name>: <EventContextAttributes/
StringAttribute/Value>**

```

Notes

- The Target Properties section will only be present if the event contains target property values. Listed below are some sample target property name/value pairs:
Line of business: Finance
Owner: Finance-DB Team
- The Event Context section will only be present if the event contains event context attribute values. There can be StringAttribute or NumberAttribute values that contain a name/value pair.
- Event URL is set to the URL of the event details page in Enterprise Manager. Copy the URL to a browser to directly view the event in Enterprise Manager.

5.1.1.4 Formatted Alert History Create Contents

Listed below is the format used by the templates for the Alert History field for `createEvent` operations. Text delimited by angle brackets (< and >) designates an Enterprise Manager Event field name that will be replaced by the actual field contents. Lines marked with double asterisks indicate they will only be present if the designated event field contains data. The Note section below contains information about some of the fields.

```

Oracle Enterprise Manager created an event with the following attributes:
Message: <Message>
Severity: <Severity>
Reported Date: <ReportedDate>
Occurred Date: <OccurredDate>
Target Name: <SourceInfo/TargetInfo/TargetName>
Target Type: <SourceInfo/TargetInfo/TargetType>
Event Class: <EventClass>
Event Name: <EventName>
Event URL: <EventURL>

Target Properties:**
    <TargetProperty/Name>: <TargetProperty/Value>**

Event Context:**
    <EventContextAttributes/StringAttribute/Name>: < EventContextAttributes/
StringAttribute /Value>**

```

 **Note:**

1. The Target Properties section will only be present if the event contains target property values. Listed below are some sample target property name/value pairs:
 - Line of business: Finance
 - Owner: Finance-DB Team
2. The Event Context section will only be present if the event contains event context attribute values. There can be `StringAttribute` or `NumberAttribute` values that contain a name/value pair.

5.1.1.5 Formatted Alert History Update Contents

Listed below is the format used by the templates for the Alert History field for `updateEvent` operations. The Title used is specified in [Alert History Title](#). Text delimited by angle brackets (< and >) designates an Enterprise Manager Event field name that will be replaced by the actual field contents.

```
Title
Reported Date: <ReportDate>
Message: <Message>
Severity: <Severity>
```

5.1.1.6 Alert History Title

[Table 5-6](#) shows the title that is specified for the Alert History field for `updateEvent` operations. The value used is based on the severity specified in the Enterprise Manager event information.

Table 5-6 Alert History Titles

Event Severity	Title
Clear	Oracle Enterprise Manager cleared event.
Warning	Oracle Enterprise Manager changed event severity to Warning.
Critical	Oracle Enterprise Manager changed event severity to Critical.
All Others	No title is specified.

5.1.2 Severity Mapping

The SCOM alert severity is set based on the Enterprise Manager event severity value. The following table shows the values used when creating the alert in SCOM.

When the event severity is ...	Set the alert severity to ...
Fatal	Error
Critical	Error
Warning	Warning
Minor Warning	Warning
Informational	Information
Clear	Information

5.1.3 Priority Mapping

The SCOM alert priority is set based on the Enterprise Manager event priority value. The following table shows the values used when creating the alert in SCOM.

When the event priority is ...	Set the alert priority to ...
Fatal	High
Critical	High
Warning	Normal
Minor Warning	Normal
Informational	Low
Clear	Low

5.2 Customizing Event Templates

Although the default mappings are sufficient for most implementations, you can change them as needed. The following sections discuss:

- [XML Format of Oracle Enterprise Manager Events](#)
- [Field Descriptions for XML Format of Events](#)
- [Managing Templates in Oracle Enterprise Manager](#)
- [Changing a Mapping](#)

It is assumed that you already have a good understanding of XSL.

For reference information on the SCOM mappings, see [Customizing Microsoft SCOM](#).

5.2.1 XML Format of Oracle Enterprise Manager Events

The sample below shows the format that the Oracle Enterprise Manager Connector Framework provides when an event is created or updated in Oracle Enterprise Manager. For a description of the fields, see [Field Descriptions for XML Format of Events](#).

Example 5-3 XML Format of Events

```
<EMEvent xmlns="http://xmlns.oracle.com/sysman/connector">
  <ConnectorGUID/>
  <ExternalEventID/>
  <NotificationRuleOwner/>
  <NotificationRuleName/>
  <ConnectorVariable>
    <VariableName/>
    <VariableValue/>
  </ConnectorVariable>
  <ConnectorVariable>
    <VariableName/>
    <VariableValue/>
  </ConnectorVariable>
  <Property>
    <Name/>
    <Value/>
  </Property>
  <Property>
    <Name/>
    <Value/>
  </Property>
  <SystemAttributes>
    <EventClass/>
    <EventID/>
    <SequenceID/>
    <OccurredDate/>
    <ReportedDate/>
    <DisplayTZ/>
    <EventName/>
    <Severity/>
    <SeverityCode/>
    <SourceInfo>
      <SourceObjInfo>
        <ObjID/>
        <ObjName/>
        <ObjOwner/>
        <SourceObjType/>
        <SourceObjSubType/>
      </SourceObjInfo>
      <TargetInfo>
        <TargetGUID/>
        <TargetName/>
        <TargetType/>
        <TargetTypeLabel/>
        <TargetURL/>
        <TargetProperty>
          <Name/>
          <Value/>
        </TargetProperty>
        <TargetProperty>

```

```

        <Name/>
        <Value/>
    </TargetProperty>
</TargetInfo>
</SourceInfo>
<Message/>
<ActionMessage/>
<EventURL/>
<AutoClose/>
<EventCategory/>
<EventCategory/>
</SystemAttributes>
<EventClassSpecificAttributes>
    <RawAttribute>
        <Name/>
        <Value/>
    </RawAttribute>
    <StringAttribute>
        <Name/>
        <Value/>
    </StringAttribute>
</EventClassSpecificAttributes>
<EventContextAttributes>
    <NumberAttribute>
        <Name/>
        <Value/>
    </NumberAttribute>
    <NumberAttribute>
        <Name/>
        <Value/>
    </NumberAttribute>
</EventContextAttributes>
</EMEvent>

```

5.2.2 Field Descriptions for XML Format of Events

Table 5-7 provides a description of the key fields shown in [XML Format of Oracle Enterprise Manager Events](#) that are used in the default mappings:

Table 5-7 Field Descriptions for XML Format of Events

Field	Description
ExternalEventId	Unique identifier of the message in Microsoft SCOM. This will only be set for updates.
EventClass	Identifies the type of event
OccurredDate	Date/time the event occurred
ReportedDate	Date/time the event was reported by OMS
EventName	Descriptive name of the event
Severity	Severity of the event: Fatal, Critical, Warning, Minor_Warning, Informational, or Clear

Table 5-7 (Cont.) Field Descriptions for XML Format of Events

Field	Description
SeverityCode	Severity code for the event: FATAL, CRITICAL, WARNING, MINOR_WARNING, INFORMATIONAL, or CLEAR
TargetName	Target name that is a unique instance of the target type
TargetType	Display name of the target type for which the event was generated
TargetProperty	Additional target properties that do not have a specific field in the event model (name:value pair)
Message	Description of the event
EventURL	Link to the web page for the event
EventContextAttributes	Additional event properties that do not have a specific field in the event model (name:value pair)

5.2.3 Managing Templates in Oracle Enterprise Manager

Oracle Enterprise Manager includes the functionality to allow you to manage templates within Cloud Control. Templates, which are included as part of the connector installation, are automatically registered and are shown within Enterprise Manager.

Using Enterprise Manager, you can edit a template, view the XML code, delete a template, and restore a deleted template.

To begin:

1. Log in to Enterprise Manager Cloud Control.
2. From the **Setup** menu, select **Extensibility**, then **Management Connectors**.
3. On the Management Connectors page, select the appropriate Microsoft SCOM connector. Click **Configure**.
4. On the Configure Management Connector page, click the **Template** tab.

5.2.3.1 Edit a Template with Enterprise Manager

To edit an existing template:

1. Select a template and click **Edit**.
2. After you edit the Description or Template Contents fields, click **Save**. On the confirmation page, click **Yes** to complete the template save.

5.2.3.2 Viewing Template Code in Enterprise Manager

To view template code, select a template and click **View**.

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

5.2.3.3 Deleting a Template with Enterprise Manager

To delete a template:

1. Select a template and click **Delete**.
2. Click **Yes** to confirm the delete operation.

WARNING! Once you delete a default template you will no longer be able to restore to the default settings. Once deleted, the only way to reregister a template is using the emctl command as specified in [Registering Templates](#).

5.2.3.4 Restoring an Updated Template with Enterprise Manager

To restore an updated template:

1. Select a template and click **Restore**.
2. Click **Yes** in the confirmation page that appears in order to restore.

5.2.4 Changing a Mapping

This section explains how to customize the mapping between Enterprise Manager and the Microsoft SCOM web service. The procedure provides the steps required for changing a mapping.

To change a mapping:

1. Export the default template XSLT files from Enterprise Manager to use as a baseline. Follow the instructions in [Exporting the Template Files](#) to obtain copies of the default template files.
2. Create a file that holds the customized template:
 - If the template being customized is available in the Enterprise Manager Cloud Control console, then perform the following steps to get the template data:
 - a. Follow the steps in [Viewing Template Code in Enterprise Manager](#) to view the data for the template being customized.
 - b. Select the template contents and copy.
 - c. Create an empty text file to hold the template contents.
 - d. Paste the template contents into the file and save.
 - If the template you want to customize is not available from the console, you will need to perform the following steps to export the template data. You will need to do this if you are using the alternate template:
 - a. Follow the instructions in [Exporting the Template Files](#) to obtain copies of the default template files.
 - b. Copy the template XSL file being customized to a new file name.
3. Make the desired mapping changes to the custom file. See [Modifying Templates](#) for guidance on mapping changes.
4. Update the existing template using the contents of the custom template file. Perform the following steps to update the template:

- a. Follow the steps in [Edit a Template with Enterprise Manager](#) to edit the data for the template being customized.
- b. Open the custom template file in a text editor.
- c. Copy the contents of the file.
- d. Paste the contents over the existing template contents in the Enterprise Manager Cloud Control console and save.

The files are now ready for integration. You do not need to stop and start OMS. The changes will automatically be picked up. See [Template Customization Example](#) for an example of how to customize templates.

For information on customizing SCOM, see [Customizing Microsoft SCOM](#).

5.2.4.1 Modifying Templates

A template is an XSLT file that transforms an input XML format to an output XML format. To make the mapping changes, you need to understand the input XML format being transformed and the output XML being generated by the template. The input document is the XML document that contains the Enterprise Manager event information. The output document is the request being sent to the SCOM web service. The output XML document must conform to the data format specified in the SCOM EventService WSDL.

[Enterprise Manager Event Format](#) contains details on the format of the event data generated by Enterprise Manager. [Microsoft SCOM Web Service WSDL Format](#) contains details on the XML format required by the SCOM EventService web service. [Mappings Between XML Format and Alert Field Names](#) provides the mapping between the SCOM EventService web service fields and the field names in SCOM. Listed below are the steps you should follow to modify the template file.

1. Review [Mappings Between XML Format and Alert Field Names](#) and [Microsoft SCOM Web Service WSDL Format](#) to identify the names of the fields in the SCOM web service that you are planning to modify. For example if you wanted to populate the Custom1 field in SCOM, look the field up in [Mappings Between XML Format and Alert Field Names](#) and you would see that the SCOM web service expects the data in the `/create/event/extended-fields/string-field` XML path.
2. If you are planning on using data from the event, review [Enterprise Manager Event Format](#) to identify the field(s) you want to use in the mapping. [Enterprise Manager Event Samples](#) has sample transactions that are very helpful in identifying what data is present in the XML document from Enterprise Manager.
3. Open the custom template file in a text editor or a utility that can be used to build XSLT files.
4. Make the necessary changes to the custom template file and save.
5. Unless the change is very simple, you should test the changes that you have made using the sample data from [Enterprise Manager Event Samples](#). This will require a utility that performs XSLT translations.

5.2.4.2 Registering Templates

This section documents how to register connectors using the emctl command line command. Since new templates cannot be defined for event connectors, the only

reason you would need this command is to reregister a default connector that was deleted from the Enterprise Manager Cloud Control console.

This command can also be used to update an existing template, but the recommended method of updating a template is through the Cloud Control console as specified in [Edit a Template with Enterprise Manager](#).

To register a template, run the following `emctl register_template connector` command as a user with execute privilege on `emctl` and the ability to read the template:

```
$ORACLE_HOME/bin/emctl register_template connector -t <template.xml> -repos_pwd  
<reposPassword> -cname <connectorName> -iname <internalName> -tname <templateName> -  
ttype 2 [-d <description>]
```

Where:

- `<template.xml>` is the full path name of the template file.
- `<reposPassword>` is the Enterprise Manager root (Super Administrator) password.
- `<connectorName>` is the name of the connector instance installed in step 5 of [Creating a Connector Instance](#).
- `<internalName>` is the internal name to use for the template.
- `<templateName>` is the name to display for the template.
- `<description>` is the description of the template.

For example: This command could be used to reregister the `createEvent` template for the connector instance with the name of **SCOM 2012**:

```
emctl register_template connector -t /home/oracle/customized_templates/  
createEvent_request.xml -repos_pwd <password> -cname "SCOM 2012" -iname  
"createEvent" -tname "Create Event Request" -ttype 2 -d "Demo template"
```

5.2.4.3 Template Customization Example

By default, the alert name in the Microsoft SCOM 2012 alert is set to the Oracle Enterprise Manager metric column, and no custom fields are mapped.

The following example shows how to change the alert name and add mappings for custom fields. The changes made to the default mapping are:

- The alert name is modified to use a hard-coded value of Event From Oracle Enterprise Manager.
- Custom field 1 is set to the Target Type.
- Custom field 2 is set to the Target Name.

1. Navigate to the SCOM 2012 connector configuration page.
2. Go to the **Template** tab.
3. Select the **Create Event Request** template and click **View**.
4. Select the template contents and copy.
5. Click **OK**.
6. Create an empty file named `custom_createEvent_request_2012.xml`.
7. Open the file in a text editor then paste the template contents and save.

8. At the Cloud Control console, select the **Update Event Request** template and click **View**.
9. Select the template contents and copy.
10. Create an empty file named `custom_updateEvent_request_2012.xsl`.
11. Open the file in a text editor then paste the template contents and save.
12. Open the `custom_createEvent_request_2012.xsl` file in your text editor.
13. Change the appropriate sections to reflect the new mapping.

Before Changes

The code below shows the impacted sections in the file before the changes:

```
<summary>
  <xsl:value-of select="a:SystemAttributes/a:EventName"/>
</summary>
...
<extended-fields>
  <!-- SCOM alert custom fields -->
  <!-- Uncomment fields to be set and replace "VALUE" with the actual
    value -->
  <!--
  <string-field name="CustomField1">VALUE</string-field>
  <string-field name="CustomField2">VALUE</string-field>
  <string-field name="CustomField3">VALUE</string-field>
  <string-field name="CustomField4">VALUE</string-field>
  <string-field name="CustomField5">VALUE</string-field>
  <string-field name="CustomField6">VALUE</string-field>
  <string-field name="CustomField7">VALUE</string-field>
  <string-field name="CustomField8">VALUE</string-field>
  <string-field name="CustomField9">VALUE</string-field>
  <string-field name="CustomField10">VALUE</string-field>
  -->
</extended-fields>
```

After Changes

The code below shows the Extended Fields section in the file after the changes. The changes are shown in bold.

```
<!-- SCOM alert title -->
<summary>Event From Oracle Enterprise Manager</summary>
...
<extended-fields>
  <!-- SCOM alert custom fields -->
  <!-- Uncomment fields to be set and replace "VALUE" with the actual
    value -->
  <b><string-field name="CustomField1">
    <xsl:value-of select="a:SystemAttributes/a:SourceInfo/a:TargetInfo/
a:TargetType"/>
  </string-field>
  <string-field name="CustomField2">
    <xsl:value-of select="a:SystemAttributes/a:SourceInfo/a:TargetInfo/
a:TargetName"/>
  </string-field>
  <!--
  <string-field name="CustomField3">VALUE</string-field>
  <string-field name="CustomField4">VALUE</string-field>
  <string-field name="CustomField5">VALUE</string-field>
  <string-field name="CustomField6">VALUE</string-field>
```

```
<string-field name="CustomField7">VALUE</string-field>
<string-field name="CustomField8">VALUE</string-field>
<string-field name="CustomField9">VALUE</string-field>
<string-field name="CustomField10">VALUE</string-field>
-->
</extended-fields>
```

14. Save your changes after making the updates.
15. Open the `custom_updateEvent_request_2012.xsl` file and make the same changes for the custom fields. In this case, you cannot set the alert name because it is only valid for creates.
16. Save your changes after making the updates.
17. To set up for testing, create the empty files named `create.xml` and `update.xml` and open in a text editor.
18. Copy the contents of the XML document in [Create Sample](#) into the `create.xml` file and save.
19. Copy the contents of the XML document in [Update Sample](#) into the `update.xml` file and save.
20. Test the new templates using a utility that performs XSLT translations using each of the `create.xml` and `update.xml` files as the input XML document.
21. Examine the output XML document and verify the results are correct.

 **Note:**

You can also use an XML client to send the XML output document to the SCOM web service to verify that it is a format accepted by the web service.

22. If the XML document has problems, make any necessary corrections and repeat steps 17 and 18.
23. At the Cloud Control console, edit the **Create Event Request** template.
24. Copy the contents of the `custom_createEvent_request_2012.xsl` file over the existing template and save.
25. At the Cloud Control console, edit the **Update Event Request** template.
26. Copy the contents of the `custom_updateEvent_request_2012.xsl` file over the existing template and save.

6

Enabling SSL for Enterprise Manager

This section contains information used in configuring the SCOM connector to use the HTTPS protocol.

The following sections are described:

- [Configuring Enterprise Manager to Use SSL](#)
- [Installing a Self-Signed Certificate](#)
- [Installing a Certificate from a Certificate Authority](#)
- [Importing the Web Service Certificate into Enterprise Manager](#)

Note:

Unless otherwise noted, these instructions apply to the SCOM 2012 connector and to the SCOM 2007 connectors. Instructions specific to the SCOM 2007 connectors are available in [Microsoft SCOM 2007 Connector](#).

6.1 Configuring Enterprise Manager to Use SSL

If the SCOM web service was configured to run using the HTTPS protocol, you must perform the following steps to set up SSL:

1. Install a SSL certificate in the SCOM web service keystore. You must either install a self-signed certificate or install a certificate obtained from a Certificate Authority (CA):
 - To install a self-signed certificate, perform the steps specified in [Installing a Self-Signed Certificate](#).
 - To install a certificate from a CA, perform the steps specified in [Installing a Certificate from a Certificate Authority](#).

Restart the SCOM web service to pick up the certificate changes.

2. Import the SSL certificate from the SCOM web service keystore into the Enterprise Manager keystore as specified in [Importing the Web Service Certificate into Enterprise Manager](#).

6.2 Installing a Self-Signed Certificate

Perform the following steps to generate and install a self-signed SSL certificate for the SCOM web service:

1. Open a command prompt window and change the working directory to the `adapters/conf` directory in the SCOM web service installation directory.

- Execute the following command to delete the default SSL entry from the SCOM web service keystore:
 - UNIX**

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

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

 **Note:**

The host name in the certificate must match the host name or IP address used by the web service. If they do not match, a failure will occur when Enterprise Manager tries to invoke the web service.

- UNIX**

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

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

6.3 Installing a Certificate from a Certificate Authority

Perform the following steps to request and install a signed SSL certificate for the SCOM web service:

- Request a certificate for the SCOM web service from a Certificate Authority, such as VeriSign.

 **Note:**

In the certificate request, make sure to specify the host name or IP address of the system where the SCOM web service is installed. The host name in the certificate must match the host name or IP address used by the web service. If they do not match, a failure will occur when Enterprise Manager tries to invoke the web service.

- After you obtain the certificate from the Certificate Authority, perform the following steps to install the certificate:
 - Open a command prompt window and change the working directory to the `adapters/conf` directory in the SCOM web service installation directory.

- b. Enter the following command to install the certificate, where `<certificateFile>` is the full path name of the file provided by the Certificate Authority:

- **UNIX**

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

- **Windows**

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

6.4 Importing the Web Service Certificate into Enterprise Manager

Perform the following steps to import the SCOM web service SSL certificate into the Enterprise Manager keystore (for multi-OMS environments, repeat for *each* OMS):

1. Open a command prompt window and change the working directory to the `adapters/conf` directory in the SCOM web service installation directory.
2. Issue the following command to extract the SSL certificate from the SCOM web service keystore and place in the `SCOMws.cer` certificate file:

- **UNIX:**

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

- **Windows:**

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

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

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

5. Ensure that only the following is appended to the `b64LocalCertificate.txt` file (that is, do not include blank lines or comments or any other special characters):

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

6. Restart OMS by running the following commands:

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

 **Note:**

Do not run the `emctl secure oms/agent` command after adding the external certificate to the `b64LocalCertificate.txt` file. If you run the `emctl secure` command later, then repeat steps 4 through 6 to make sure the external certificate exists in the `b64LocalCertificate.txt` file.

7

Troubleshooting the Microsoft SCOM Event Connector

This chapter provides information to assist in troubleshooting integration issues with Microsoft SCOM. The chapter focuses on troubleshooting issues in the web service front-end and the back-end Agent.

Note:

Unless otherwise noted, these instructions apply to the SCOM 2012 connector and to the SCOM 2007 connectors. Instructions specific to the SCOM 2007 connectors are available in [Microsoft SCOM 2007 Connector](#).

This chapter discusses the following topics:

- [Diagnosing the Problem](#)
- [Troubleshooting Web Service Startup Errors](#)
- [JVM Errors](#)
- [Using the Correct URL for SCOM Web Service Operations](#)
- [Troubleshooting Web Service Operation Errors](#)
- [Errors from Oracle Enterprise Manager](#)

Before you start the troubleshooting steps, you must insure that you have done the following:

1. Install the SCOM connector as specified in [Installing the Microsoft SCOM Event Connector](#).
2. Install and start the Oracle SCOM Agent as specified in [Installing and Running the Oracle SCOM Agent](#).
3. Install, start, and test the SCOM Web service as specified in [Installing the Microsoft SCOM Web Service](#).
4. Create a connector instance as specified in [Creating a Connector Instance](#).
5. Configure the connector instance as specified in [Configuring the Connector](#).
6. Set up one or more rules to forward events to the connector instance.

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

7.1 Diagnosing the Problem

Follow these steps to diagnose a problem:

1. Verify that the SCOM Web Service has been successfully started and the WSDL for the SCOM Web Service can be accessed from the machine where it is installed. Performing the following steps to do this:
 - a. Perform the steps in [Using the Correct URL for SCOM Web Service Operations](#) to determine the URL used by the SCOM Web Service.
 - b. Open a browser and paste the URL from the previous step in the address window. Append **?WSDL** to the end of the URL and attempt to load the URL.
 - c. The WSDL should be loaded if the web service is operational.

 **Note:**

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

- d. If the WSDL cannot be loaded, this indicates the web service had startup issues. See [Troubleshooting Web Service Startup Errors](#) to diagnose the problem.
2. Verify that the WSDL for the SCOM Web Service can be accessed from the machine where the Enterprise Manager server is installed.
 - a. Open a browser at the Enterprise Manager server and copy the URL from step 1-b above to the address window. The hostname for the URL will be **localhost**. Change **localhost** to the actual hostname or IP address of the machine where the SCOM Web Service is installed. If you specify a hostname, you must make sure that the hostname is recognized at the Enterprise Manager server machine. This can be done using the ping command.

For example, if the Web Service is installed on the server with a hostname of SCOMServer01 and the URL listed in `framework.log` is:

```
http://localhost:8080/services/SCOM/EventService
```

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

```
http://SCOMServer01:8080/services/SCOM/EventService
```

- b. Attempt to load the WSDL by appending **?WSDL** at the end of the URL. If the WSDL cannot be loaded, either the hostname is not recognized at the Enterprise Manager machine or there is a connectivity issue between the two machines. If you specified a hostname, try using the IP address instead of the hostname in the URL. If it still will not load, you have a connectivity problem. You will need to consult with your IT department to resolve this issue.
3. Verify that the SCOM connector specifies the correct URL for the `createEvent` and `updateEvent` operations.
 - a. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator permissions.
 - b. From the **Setup** menu, select **Extensibility**, then select **Management Connectors**.
 - c. From the Management Connectors page, click the **Configure** icon associated with the SCOM connector.

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

- d. Verify that the URL identified in step 2-b is specified for the `createEvent` and `updateEvent` operations. Also verify the URLs listed for the `setup`, `initialize`, and `uninitialize` operations. The URL is basically the same as the URL listed above except it is for the `SCOMService` instead of the `EventService`. Listed below is the URL that would be used based on the previous example.

```
http://SCOMServer01:8080/services/SCOM/SCOMService
```

- e. If any of the operations are incorrect, change to the correct URL.

 **Note:**

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

- f. Click **OK**.
4. If there were no errors found in the previous steps, this rules out connectivity issues between the connector and the SCOM Web Service. The problem must lie in the SCOM Web Service or the Oracle SCOM Agent. See [Troubleshooting Web Service Operation Errors](#) for information on diagnosing errors.

7.2 Troubleshooting Web Service Startup Errors

To identify the cause of a startup failure, navigate to the `adapters/log` directory in the SCOM Web Service install directory and open the `framework.log` file in a text editor. Search for **Exception** to find any errors in the file. If the file does not exist, it indicates that there is a problem locating or executing the JVM. See [JVM Errors](#) for information about resolving JVM issues.

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

Example 7-1 `java.net.BindException: Address already in use: bind`

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

1. Another application is using a port that the web service is configured to use. If the web service is configured to use SSL, the port number is **8443**. If it is not configured to use SSL, the port number is **8080**.

There are two possible solutions to this. You can change the other application to use a different port or you can change the SCOM Web Service to use a different port. To change the SCOM Web Service to use a different port, see [Changing Default Port Numbers](#) in [Customizing Microsoft SCOM](#).

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

Example 7-2 `org.springframework.beans.factory.BeanInitializationException: Could not load properties; nested exception is java.io.FileNotFoundException: ... framework.properties (Permission denied)`

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

To solve the problem, change the permissions to give the account or group under which the SCOM Web Service runs read and execute permissions.

For any other startup errors, consult Oracle Support.

7.3 JVM Errors

The SCOM Web Service requires version 1.6 of the JVM. If there are multiple versions of the JVM installed on the machine, it is possible that an older version of the JVM is being executed whenever the web service starts.

1. On **UNIX** systems, the `JAVA_HOME` environment variable must be set to the directory where JDK 1.6 is installed in the shell where the web service is started. To properly start the web service on a UNIX platform, perform the following:
 - a. Set the `JAVA_HOME` environment variable to the JDK 1.6 install directory.
 - b. Navigate to the `adapters/bin` subdirectory in the web service install directory.
 - c. Execute the `./service.sh start` command.
2. On **Windows** systems, perform the following to insure that JDK 1.6 is used when starting the web service:
 - a. Navigate to the `adapters\bin` subdirectory in the web service install directory.
 - b. Run the `iWaveAdaptersw.exe` executable.
 - c. Click the **Java** tab.
 - d. Be sure the **Use Default** check box is not checked.
 - e. In the Java Virtual Machine box, specify the path to the `jvm.dll` file in the JDK 1.6 install directory.
 - f. Click **OK**.

7.4 Using the Correct URL for SCOM Web Service Operations

Perform the following steps to identify and configure the connector to use the correct URL for SCOM Web Service operations:

1. Open a command terminal on the system where the SCOM web service is installed.
2. Change the working directory to the `adapters/log` directory in the SCOM web service installation directory.
3. Open the `framework.log` file in a text editor.
4. Go to the bottom of the file and search backwards for the string *Setting the server's publish address to be*. Continue searching backwards until you find the URL that contains **EventService**.

 **Note:**

If you cannot find the URL information in the log file, it means the log file has rolled over. To get the URL information back in the file, stop and start the web service.

You should specify the URL listed here for the `createEvent` and `updateEvent` operations, with one exception. You must replace the host name of `localhost` in the URL with the actual host name or IP address of the system where the SCOM Web Service is installed.

5. Go to the bottom of the file and search backwards for the string *Setting the server's publish address to be*. Continue searching backwards until you find the URL that contains **SCOMService**.

You should specify the URL listed here for the `setup`, `initialize` and `uninitialize` operations, with one exception. You must replace the host name of `localhost` in the URL with the actual host name or IP address of the system where the SCOM web service is installed.

6. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator permissions.
7. From the **Setup** menu, select **Extensibility**, then select **Management Connectors**.
8. From the Management Connectors page, click the name of the SCOM connector.
The General tab of the Configure Management Connector page appears.
9. Verify that the URL identified in step 4 is specified for the `createEvent` and `updateEvent` operations.
10. Verify that the URL identified in step 5 is specified for the `setup`, `initialize` and `uninitialize` operations.
11. If any of the operations are incorrect, change to the correct URL and click **OK**.

7.5 Troubleshooting Web Service Operation Errors

Perform the following diagnostic steps if messages are not being generated or updated as expected in SCOM:

1. Verify that the event that was triggered is referenced in a rule that forwards events to the SCOM connector.
2. Verify that the `OracleEnterpriseManager.Alert.Creator` Management Pack has been imported into the SCOM server:
 - a. Open the System Center Operations Manager console window and log in.
 - b. In the Administration pane of the Operations Manager console, select **Administration**, then **Management Packs**.
 - c. Verify that the "OracleEnterpriseManager Alert Creator" Management Pack is listed.
 - d. If the pack is not listed, import it as specified in [Installing the Alert Creator Management Pack](#).

3. Determine the error that Oracle Enterprise Manager has reported. To do this you need to examine the log file for errors. Perform the following steps to locate errors in the log file:

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

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

Where, `<EM_INSTANCE_BASE>` is the OMS Instance Base directory. By default, the OMS Instance Base directory is `gc_inst`, which is present under the parent directory of the Oracle Middleware Home.

For example, if the Oracle Middleware Home is `/u01/app/Oracle/Middleware`, then the instance base directory is `/u01/app/Oracle/Middleware/gc_inst`, and the log and trace files are available in `/u01/app/Oracle/Middleware/gc_inst/em/EMGC_OMS1/sysman/log/` directory path.

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

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

4. Diagnose the problem based on the error information. See [Errors from Oracle Enterprise Manager](#) for information on troubleshooting common error events.

7.6 Errors from Oracle Enterprise Manager

This section provides cause and solution information on troubleshooting common error messages. Find the error message in [Table 7-1](#) that matches your error message, then refer to the corresponding section(s) indicated under Possible Cause for instructions to diagnose and correct the problem.

Table 7-1 Enterprise Manager Error Messages

Error Message	Possible Cause
<pre>javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Bad response: 403 Forbidden from url ...</pre>	<p>Invalid Web Service Credentials</p>
<pre>javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target</pre>	<p>SSL Not Configured in Enterprise Manager</p>

Table 7-1 (Cont.) Enterprise Manager Error Messages

Error Message	Possible Cause
javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: Connection refused	SCOM Web Service Down
javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: No route to host	Invalid IP Address
javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Bad response: 404 Not Found from url ...	Invalid Port Number or Invalid URL Path
javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: Connection timed out	Firewall Blocking Access
javax.xml.soap.SOAPException: javax.xml.soap.SOAPException: Message send failed: hostname	Unknown Host
javax.xml.transform.TransformerConfigurationException: Could not compile stylesheet	Invalid XML Format
Unable to reconnect to server after being disconnected	SCOM Server Not Operational
ERROR - Could not connect to the server <hostname> because it is not operational	SCOM Server Not Operational
ERROR - Could not login to the server because the account was invalid or has insufficient permissions	Invalid SCOM API Credentials or Wrong SCOM API Permissions
ERROR occurred invoking SCOM connector to insert event for null	SCOM Agent Not Operational or Alert Create Timeout

Table 7-1 (Cont.) Enterprise Manager Error Messages

Error Message	Possible Cause
<pre>javax.xml.ws.WebServiceException: org.apache.cxf.service.factory.ServiceConstructionExcept ion: Failed to create service</pre>	SCOM Agent Configuration
Request failed because the specified management pack could not be found	Alert Creator Management Pack Missing

Successfully inserted the event but timed out waiting for the alert to be created	Alert Create Timeout

The following errors are described:

- [Invalid Web Service Credentials](#)
- [SSL Not Configured in Enterprise Manager](#)
- [SCOM Web Service Down](#)
- [Invalid IP Address](#)
- [Invalid Port Number](#)
- [Invalid URL Path](#)
- [Firewall Blocking Access](#)
- [Unknown Host](#)
- [Invalid XML Format](#)
- [SCOM Server Not Operational](#)
- [Invalid SCOM API Credentials](#)
- [Wrong SCOM API Permissions](#)
- [SCOM Agent Not Operational](#)
- [SCOM Agent Configuration](#)
- [Alert Creator Management Pack Missing](#)
- [Alert Create Timeout](#)

7.6.1 Invalid Web Service Credentials

Cause

The user name or password for accessing the SCOM web service is incorrect.

Solution

Verify that the port number configured for the connector is correct:

1. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator privileges.
2. From the **Setup** menu, select **Extensibility**, then select **Management Connectors**.
3. On the Management Connectors page, click the name of the appropriate SCOM connector.
This invokes edit mode, enabling you to configure the connector.
4. Correct the SCOM Web Service Username and SCOM Web Service Password fields, then click **OK**.

7.6.2 SSL Not Configured in Enterprise Manager

Cause

The SSL handshake between the Oracle Enterprise Manager Connector Framework and the SCOM web service failed. This failure occurs because Oracle Enterprise Manager is not configured correctly with the SSL certificate for the SCOM web service. The SSL certificate the SCOM web service uses must be imported into the Enterprise Manager key store. The certificate is either missing from the key store or does not match the SSL certificate provided by the SCOM web service.

Solution

Import the SSL certificate from the SCOM web service into the Enterprise Manager key store. See [Configuring Enterprise Manager to Use SSL](#) for details on setting up Oracle Enterprise Manager with the SCOM SSL certificate.

7.6.3 SCOM Web Service Down

Cause

The SCOM web service is down.

Solution

Perform the following steps to check the status of the web service and start it if necessary:

If the SCOM web service is installed on a **Unix** system:

1. Open a command terminal on the system where the SCOM web service is installed.
2. Change the working directory to the `adapters/bin` directory in the SCOM web service installation directory.
3. Enter the following command:

```
./service.sh status
```
4. If the command indicates that the service is not running, enter the following command:

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

If the SCOM web service is installed on a **Windows** system:

1. Open a command terminal on the system where the SCOM web service is installed.
2. Change the working directory to the `adapters\log` directory in the SCOM web service installation directory.
3. Open the `framework.log` file in a text editor.
4. Go to the bottom of the file and search backwards for the string **iWave Adapter Framework**. If the last occurrence found is **iWave Adapter Framework Started**, this indicates that the web service is started.
5. If the web service is not started, start the web service as specified in [Running the Microsoft SCOM Web Service on Windows](#).

7.6.4 Invalid IP Address

Cause

The IP address specified in the URL is invalid or the network is down.

Solution

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

1. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator privileges.
2. From the **Setup** menu, select **Extensibility**, then select **Management Connectors**.
3. On the Management Connectors page, click the name of the appropriate SCOM connector.

This invokes edit mode, enabling you to configure the connector.
4. Verify that the hostname/IP address specified in the URL for the `createEvent` and `updateEvent` operations are correct.
5. If the hostname/IP address is incorrect, provide the correct value, then click **OK**.

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

If the hostname/IP address appears to be correct, try to ping the system where the SCOM web service is installed using the hostname/IP address. If the ping fails, the system administrator needs to investigate why there is no connectivity.

7.6.5 Invalid URL Path

Cause

The web service received the request and rejected it because an invalid path was specified in the URL.

Solution

Perform the following steps to test the URL the connector is using:

1. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator privileges.
2. From the **Setup** menu, select **Extensibility**, then select **Management Connectors**.
3. On the Management Connectors page, click the name of the appropriate SCOM connector.
This invokes edit mode, enabling you to configure the connector.
4. Select and copy the URL specified for the `createEvent` operation.
5. Open an internet browser on the system where the Oracle Enterprise Manager server is installed.
6. In the address window, enter the URL that was copied in step 6 above. Add **?wsdl** to the end of the URL. The URL should appear similar to the following example:

```
http://[Hostname]:8080/services/SCOM/EventService?wsdl
```

[Hostname] is the actual host name or IP address where the SCOM web service is installed.

If the WSDL is loaded, this confirms that the URL is correct. If it fails to load, there is a problem with the URL. Perform the steps specified in [Using the Correct URL for SCOM Web Service Operations](#) to configure the connector to use the correct URL.

7.6.6 Invalid Port Number

Cause

The port number specified in the URL is invalid.

Solution

Verify that the port number configured for the connector is correct:

1. Log in to the Oracle Enterprise Manager console with an account that has Super Administrator privileges.
2. From the **Setup** menu, select **Extensibility**, then select **Management Connectors**.
3. On the Management Connectors page, click the name of the appropriate SCOM connector.
This invokes edit mode, enabling you to configure the connector.
4. Verify that the port number specified in the URL for the `createEvent`, `updateEvent`, `setup`, `initialize`, and `uninitialize` operations are correct.
5. If the port number is incorrect, provide the correct value and click **OK**.

7.6.7 Firewall Blocking Access

Cause

A firewall is blocking access to the system where the SCOM Web Service is installed.

Solution

Contact your IT department to give Enterprise Manager access to the port used by the SCOM Web Service. Perform the steps specified in [Using the Correct URL for SCOM Web Service Operations](#) to determine the URL used by the SCOM Web Service. The port number specified in the URL is the port number the IT department should open in the firewall..

7.6.8 Unknown Host

Cause

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

Solution

You can use the following options to address this issue:

- Coordinate with the system administrator to change the system configuration to recognize the host name.
- Specify the IP address in the URL instead of the host name. To do this, perform the following steps:
 1. Determine the IP address of the system where the SCOM web service is installed.
 2. Log in to the Oracle Enterprise Manager console by entering a user name with a Super Administrator role, entering the appropriate password, then click **Login**.
 3. From the Enterprise Manager console, click **Setup**, then **Extensibility**, and finally **Management Connectors**. The Management Connectors page appears, which shows the installed connectors.
 4. Click on the **Configure** icon associated with the Microsoft SCOM connector. This invokes edit mode, enabling you to configure the connector.
 5. Change the host name to the IP address in the URL specified for the `createEvent`, `initialize`, `setup`, `uninitialize`, and `updateEvent` operations.
 6. Click **OK**.

7.6.9 Invalid XML Format

Cause

The connector framework could not process the request because the XSL file was formatted incorrectly. This problem should not occur unless the connector has been customized.

Solution

Examine any changes made to the XSL template files for mistakes that could have caused the problem. If you can't find the problem manually, load the XSL in a utility that performs XML validation.

7.6.10 SCOM Server Not Operational

Cause

The SCOM Agent could not insert the alert into SCOM because the wrong host name is configured for SCOM or the SCOM server is down.

Solution

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

1. Verify that the host name or IP address listed in the error message is correct for the SCOM server. If the host name or IP address are incorrect, perform the following steps to correct the configuration:
 - a. Open Windows Explorer on the system where the SCOM Agent is located.
 - b. Navigate to the `bin` directory in the SCOM Agent installation directory.
 - c. Run the `SCOMAgentConfig.exe` utility to start the SCOM Agent Configuration Tool.
 - d. Click **Load** to open a directory navigation window.
 - e. Navigate to the SCOM Agent installation directory and open the `SCOMAgent.cfg` file.
 - f. Click the **Management Groups** tab, then click **Edit** to display the Edit Management Group window.
 - g. Correct the hostname/IP address in the Server field, then click **Update**.
 - h. Click **Save** to save the changes to the configuration file.
 - i. Click **Exit** to exit the utility.
 - j. Stop and restart the SCOM Agent in IIS.
2. Verify that the following OpsMgr services are running:
 - System Center Data Access
 - System Center Management
 - System Center Management Configuration

7.6.11 Invalid SCOM API Credentials

Cause

The SCOM Agent could not send the alert to the SCOM server, because the credentials configured for accessing the SCOM API are invalid.

Solution

Perform the following steps to change the credentials for accessing the SCOM API:

1. Open Windows Explorer on the system where the SCOM Agent is located.
2. Navigate to the `bin` directory in the SCOM Agent installation directory.
3. Run the `SCOMAgentConfig.exe` utility to start the SCOM Agent Configuration Tool.
4. Click **Load** to open a directory navigation window.
5. Navigate to the SCOM Agent installation directory and open the `SCOMAgent.cfg` file.

6. Click the **Management Groups** tab, then click **Edit** to display the Edit Management Group window.
7. Correct the credential information in the Domain, Username, and Password fields, then click **Update**.
8. Click **Save** to save the changes to the configuration file.
9. Click **Exit** to exit the utility.
10. Stop and restart the SCOM Agent in IIS.

7.6.12 Wrong SCOM API Permissions

Cause

The SCOM Agent could not send the alert to the SCOM server, because the credentials configured for accessing the SCOM API do not have sufficient permissions.

Solution

Refer to [Setting Up the Agent Account](#). This section provides the steps required to set up the account for accessing the SCOM API.

7.6.13 SCOM Agent Not Operational

Cause

The web service could not create an alert in SCOM because the SCOM Agent is not operational.

Solution

Open IIS Manager on the system where the SCOM Agent was installed, and start the web site for the Agent.

7.6.14 SCOM Agent Configuration

Cause

The web service could not connect to the SCOM Agent because the web service has an invalid configuration parameter. Either the URL for the SCOM Agent is incorrect or the credentials for accessing the SCOM Agent are invalid.

Solution

1. Verify that the URL for the SCOM Agent is correct. You should specify the URL that was provided at the end of the SCOM Agent installation. Note that if the host name in the URL is localhost and you are accessing it from another system, you need to replace localhost with the host name or IP address of the SCOM Agent installation machine.

If you do not know the URL, you can determine it as follows:

- If the SCOM Agent was installed as a web site, the address is:

```
http://<IP>:<port>/Service.asmx
```


... where <IP> is the IP address, and <port> is the port number specified when installing the Agent.

- If the SCOM Agent was installed as a virtual directory, the address is:

```
http://<IP>:<port>/<vdir>/Service.asmx
```

... where <IP> is the IP address, <port> is the port number for the web service where the agent was installed, and <vdir> is the virtual directory name specified for the Agent.

2. Select a user name and password that are valid on the system where the SCOM Agent was installed.
3. Open a command window and change the working directory to `adapters\endpoints\SCOM` in the SCOM web service installation directory.
4. Rerun the SCOM Web Service installer using the URL and credentials from the preceding steps. See [Installing the Microsoft SCOM Web Service on UNIX](#) or [Installing the Microsoft SCOM Web Service on Windows](#), depending on your platform, for the procedure.
5. Restart the web service as instructed in [Installing the Microsoft SCOM Web Service on UNIX](#) or [Installing the Microsoft SCOM Web Service on Windows](#).

7.6.15 Alert Creator Management Pack Missing

Cause

The web service could not create an alert in SCOM because the `OracleEnterpriseManager.Alert.Creator` management pack has not been imported into SCOM.

Solution

Refer to [Install the Alert Creator Management Pack for Microsoft SCOM 2007](#) for the steps required to import the management pack into SCOM.

7.6.16 Alert Create Timeout

Cause

The web service was able to insert an event in SCOM, but an alert was not created within the timeout period. This likely indicates that an error occurred in the alert generating rule and it was unloaded by SCOM. Whenever this occurs, the System Center Operations Manager Health Service generates an error followed by a warning in the Operations Manager log. The error entry begins with the following message:

```
A module reported an error 0x80070057 from a callback which was running as part of rule "Create.Default.Alert" running for instance "OracleEnterpriseManager Event Source" with id ...
```

The warning entry begins with the following message:

```
Summary: 1 rule(s)/monitor(s) failed and got unloaded, 1 of them reached the failure limit that prevents automatic reload ...
```

 **Note:**

This situation should not occur if the default SCOM connector configuration files are used. The only known way this can occur is if the SCOM Agent web service is directly accessed and an invalid value is passed for the Priority or Severity fields.

Solution

Restart the Windows service named "Ops Mgr Health Service" on the SCOM server.

A

Customizing Microsoft SCOM

This appendix describes the SCOM mappings and various other configuration defaults and contains the following sections:

- [XML Format of Microsoft SCOM Alerts](#)
- [Changing Default Port Numbers](#)
- [Changing SCOM API Connection Parameters](#)

A.1 XML Format of Microsoft SCOM Alerts

[Sample Create Format for Microsoft SCOM Web Service](#) represents the format that the Microsoft SCOM web service expects for creating new alerts in Microsoft SCOM.

[Sample Update Format for Microsoft SCOM Web Service](#) represents the format that the Microsoft SCOM web service expects for updating alerts in Microsoft SCOM.

Note:

Alert History information is now passed differently for SCOM 2012 than it was for SCOM 2007:

- For SCOM 2012, the history information is passed in the `logs/log/description` field.
- For SCOM 2007 the history information is passed in the `<string-field name="AlertHistory"></string-field>` field

A.1.1 Sample Create Format for Microsoft SCOM Web Service

```
<iwaveaf:create xmlns:iwaveaf="http://iwavesoftware.com/services/adapter-framework">
  <event>
    <summary></summary>
    <description></description>
    <severity></severity>
    <priority></priority>
    <logs>
      <log>
        <description></description>
      </log>
    </logs>
    <extended-fields>
      <string-field name="CustomField1"></string-field>
      ...
      <string-field name="CustomField10"></string-field>
    </extended-fields>
  </event>
</iwaveaf:create>
```

A.1.2 Sample Update Format for Microsoft SCOM Web Service

```
<iwaveaf:update xmlns:iwaveaf="http://iwavesoftware.com/services/adaptor-framework">
  <event>
    <identifier></identifier>
    <status></status>
    <logs>          <-----For SCOM 2012
      <log>
        <description></description>
      </log>
    </logs>
    <extended-fields>
      <string-field name="AlertHistory"></string-field>          <-----For SCOM 2007
      <string-field name="CustomField1"></string-field>
      ...
      <string-field name="CustomField10"></string-field>
    </extended-fields>
  </event>
</iwaveaf:update>
```

A.1.3 Mappings Between XML Format and Alert Field Names

[Table A-1](#) identifies the mappings between the Microsoft SCOM alert field names and the XML format that the Microsoft SCOM web services uses when creating an alert in SCOM. [Table A-2](#) identifies the mappings between the Microsoft SCOM alert field names and the XML format that the Microsoft SCOM web services uses when updating an alert in SCOM.

The XML document presented to the Microsoft SCOM web service must have the corresponding fields set. Fields denoted with an asterisk (*) are optional. This must be handled in the appropriate translation file identified in [Table A-1](#).

Table A-1 Create Alert Attributes and XML Path Mappings

Microsoft SCOM Field Names	XML Path	Attribute Name	Attribute Value
Name	/create/event/summary		
Description	/create/event/description		
Severity	/create/event/severity		
Priority	/create/event/priority		
Alert History	/create/event/logs/log/description		
* Owner	/create/event/owner		
* Custom Field 1	/create/event/extended-fields/string-field	name	CustomField1
* Custom Field 2	/create/event/extended-fields/string-field	name	CustomField2
* Custom Field 3	/create/event/extended-fields/string-field	name	CustomField3
* Custom Field 4	/create/event/extended-fields/string-field	name	CustomField4

Table A-1 (Cont.) Create Alert Attributes and XML Path Mappings

Microsoft SCOM Field Names	XML Path	Attribute Name	Attribute Value
* Custom Field 5	/create/event/extended-fields/string-field	name	CustomField5
* Custom Field 6	/create/event/extended-fields/string-field	name	CustomField6
* Custom Field 7	/create/event/extended-fields/string-field	name	CustomField7
* Custom Field 8	/create/event/extended-fields/string-field	name	CustomField8
* Custom Field 9	/create/event/extended-fields/string-field	name	CustomField9
* Custom Field 10	/create/event/extended-fields/string-field	name	CustomField10
* Alert Parameter 2	/create/event/extended-fields/string-field	name	AlertParameter2
* Alert Parameter 3	/create/event/extended-fields/string-field	name	AlertParameter3
* Alert Parameter 4	/create/event/extended-fields/string-field	name	AlertParameter4
* Alert Parameter 5	/create/event/extended-fields/string-field	name	AlertParameter5
* Alert Parameter 6	/create/event/extended-fields/string-field	name	AlertParameter6
* Alert Parameter 7	/create/event/extended-fields/string-field	name	AlertParameter7
* Alert Parameter 8	/create/event/extended-fields/string-field	name	AlertParameter8
* Alert Parameter 9	/create/event/extended-fields/string-field	name	AlertParameter9
* Alert Parameter 10	/create/event/extended-fields/string-field	name	AlertParameter10

Table A-2 Update Alert Attributes and XML Path Mappings

Microsoft SCOM Field Names	XML Path	Attribute Name	Attribute Value
Id	/update/event/identifier		
Resolution State	/update/event/status		
* Ticket ID	/update/event/externalIncidentIdentifier		
* Owner	/update/event/owner		

Table A-2 (Cont.) Update Alert Attributes and XML Path Mappings

Microsoft SCOM Field Names	XML Path	Attribute Name	Attribute Value
* Custom Field 1	/update/event/extended-fields/string-field	name	CustomField1
* Custom Field 2	/update/event/extended-fields/string-field	name	CustomField2
* Custom Field 3	/update/event/extended-fields/string-field	name	CustomField3
* Custom Field 4	/update/event/extended-fields/string-field	name	CustomField4
* Custom Field 5	/update/event/extended-fields/string-field	name	CustomField5
* Custom Field 6	/update/event/extended-fields/string-field	name	CustomField6
* Custom Field 7	/update/event/extended-fields/string-field	name	CustomField7
* Custom Field 8	/update/event/extended-fields/string-field	name	CustomField8
* Custom Field 9	/update/event/extended-fields/string-field	name	CustomField9
* Custom Field 10	/update/event/extended-fields/string-field	name	CustomField10
* Alert History (2012)	/update/event/logs/log/description		
* Alert History (2007)	/update/event/extended-fields/string-field	name	AlertHistory

A.1.4 Extended Fields

Extended fields pass information for fields that are not mapped to a specific field. An extended field is defined as a `<string-field/>` element that is a child of the extended-fields node. The name of the field is specified in the name attribute, and the value of the field is specified as the element value.

A.2 Changing Default Port Numbers

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

8080 is the default port number for HTTP communication, and **8443** is the default port for HTTPS communication. To change the port number, perform the steps in the appropriate subsection:

- [Changing the Web Service Port \(8080\)](#)
- [Changing the Web Service Port \(8443\)](#)

A.2.1 Changing the Web Service Port (8080)

The SCOM web service uses port **8080** as the default port for communication when the web service is configured at installation to use HTTP (no SSL). To change the port number to a different value, perform the following steps at the system where the SCOM web services are installed. Replace `<SCOM_INSTALL>` with the directory where the SCOM web services are installed.

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

```
<SCOMWS_INSTALL>/adapters/conf
```

2. Make a backup copy of the `framework.properties` file, then open the file with a text editor.
3. Replace all references to the old port number with the new port number, then save the file.
4. Restart the web service as instructed in [Running the Microsoft SCOM Web Service on UNIX](#) and [Running the Microsoft SCOM Web Service on Windows](#).
5. Perform the following steps to change the URL the SCOM connector is using:
 - a. From the **Setup** menu, select **Extensibility**, then select **Management Connectors**.
 - b. On the Management Connectors page, click the name of the SCOM connector.

The General tab of the Configure Management Connector page appears.
 - c. Change the URLs listed in the Web Service End Points section to use the new port number.
 - d. Click **OK** to save your changes.

A.2.2 Changing the Web Service Port (8443)

Contact Oracle Support for assistance in switching the default SSL port **8443** to a different port.

A.3 Changing SCOM API Connection Parameters

When installing the SCOM Agent, you must configure the connection parameters used for accessing the SCOM API. The installation includes the `SCOMAgentConfig` utility you can use to change the Agent configuration parameters.

Perform the following steps to change the connection parameters:

1. Open Windows Explorer on the system where the SCOM Agent is installed.
2. Navigate to the `bin` directory in the SCOM Agent installation directory.
3. Run the `SCOMAgentConfig.exe` utility.

This action starts the SCOM Agent Configuration Tool.

4. Click **Load**.

This action opens a directory navigation window.

5. Navigate to the SCOM Agent installation directory and open the `SCOMAgent.cfg` file.
6. Click the **Management Groups** tab and click **Edit**.

This action displays the Edit Management Group window.

7. Change the desired information in the following fields listed, then click **Update**:

Name
Server
Domain
Username
Password

8. Click **Save** to save the changes to the configuration file.
9. Click **Exit** to exit the utility.
10. Stop and restart the SCOM Agent in IIS.

B

Enterprise Manager Event Samples

This appendix contains samples that show the XML format of events from Enterprise Manager that conform to the schemas defined in [Enterprise Manager Event Format](#). These samples can be used to help identify the fields to map when customizing the event templates. They can also be used to test your customizations once they have been built.

- [Create Sample](#)
- [Update Sample](#)
- [Clear Sample](#)

B.1 Create Sample

Listed below is a sample of the XML format generated by Enterprise Manager for SCOM create operations.

```
<EMEvent xmlns="http://xmlns.oracle.com/sysman/connector">
  <ConnectorGUID>2C08969483F141F1B7482F376935C0AC</ConnectorGUID>
  <NotificationRuleOwner>Super Administrator</NotificationRuleOwner>
  <NotificationRuleName>SCOM Rule</NotificationRuleName>
  <ConnectorVariable>
    <VariableName>REGISTRATION_ID</VariableName>
    <VariableValue>Dummy</VariableValue>
  </ConnectorVariable>
  <Property>
    <Name>Notification_Method_Name</Name>
    <Value>SCOM</Value>
  </Property>
  <Property>
    <Name>AuthenticationType</Name>
    <Value>HTTPBasicAuthentication</Value>
  </Property>
  <Property>
    <Name>Registered</Name>
    <Value>yes</Value>
  </Property>
  <Property>
    <Name>IsNewTargetType</Name>
    <Value>yes</Value>
  </Property>
  <Property>
    <Name>Initialized</Name>
    <Value>yes</Value>
  </Property>
  <SystemAttributes>
    <EventClass>metric_alert</EventClass>
    <EventID>B69EC6D3F8B6A48EE040020A78016095</EventID>
    <SequenceID>B69EC6D3F8B7A48EE040020A78016095</SequenceID>
    <ReportedDate>2012-01-17T17:02:08.000-06:00</ReportedDate>
    <DisplayTZ>America/Chicago</DisplayTZ>
    <EventName>Load:cpuUtil</EventName>
  </SystemAttributes>
</EMEvent>
```

```

<Severity>Critical</Severity>
<SeverityCode>CRITICAL</SeverityCode>
<SourceInfo>
  <SourceObjInfo>
    <ObjID>D93A2E4E1622013D74D9534ECB090944</ObjID>
    <ObjName>orcsvr1.iwavesoftware.com</ObjName>
    <ObjOwner>Super Administrator</ObjOwner>
    <SourceObjType>TARGET</SourceObjType>
    <SourceObjSubType>host</SourceObjSubType>
  </SourceObjInfo>
  <TargetInfo>
    <TargetGUID>D93A2E4E1622013D74D9534ECB090944</TargetGUID>
    <TargetName>orcsvr1.iwavesoftware.com</TargetName>
    <TargetType>host</TargetType>
    <TargetTypeLabel>Host</TargetTypeLabel>
    <TargetURL>https://orcsvr1.iwavesoftware.com:7801/em/redirect?
pageType=TARGET_HOMEPAGE&targetName=orcsvr1.iwavesoftware.com&targetType=host
</TargetURL>
    <TargetProperty>
      <Name>Target_Host</Name>
      <Value>orcsvr1.iwavesoftware.com</Value>
    </TargetProperty>
    <TargetProperty>
      <Name>Target Version</Name>
      <Value>5.5.0.0.0</Value>
    </TargetProperty>
    <TargetProperty>
      <Name>Line of Business</Name>
      <Value>Software</Value>
    </TargetProperty>
    <TargetProperty>
      <Name>Location</Name>
      <Value>Frisco, TX</Value>
    </TargetProperty>
    <TargetProperty>
      <Name>Comment</Name>
      <Value>Testing target properties</Value>
    </TargetProperty>
  </TargetInfo>
</SourceInfo>
<Message>CPU Utilization is 7.777%, crossed warning (0.1) or critical (0.2)
threshold.</Message>
<EventURL>https://orcsvr1.iwavesoftware.com:7801/em/redirect?pageType=sdk-
core-event-console-detailEvent&issueID=B69EC6D3F8B7A48EE040020A78016095</
EventURL>
  <AutoClose>>true</AutoClose>
  <EventCategory>Capacity</EventCategory>
</SystemAttributes>
<EventClassSpecificAttributes>
  <StringAttribute>
    <Name>is_thresholdable</Name>
    <Value>1</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>coll_name</Name>
    <Value>LoadLinux</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>is_metric_extension</Name>
    <Value>0</Value>
  </StringAttribute>

```

```
<StringAttribute>
  <Name>metric_column_resbundle</Name>
  <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_description_resbundle</Name>
  <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
</StringAttribute>
<StringAttribute>
  <Name>unit_resbundle</Name>
  <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
</StringAttribute>
<StringAttribute>
  <Name>cycle_guid</Name>
  <Value>B69EC6D3F8B3A48EE040020A78016095</Value>
</StringAttribute>
<StringAttribute>
  <Name>is_remote</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_type</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_guid</Name>
  <Value>0C71A1AFAC2D7199013837DA35522C08</Value>
</StringAttribute>
<StringAttribute>
  <Name>num_keys</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>key_value</Name>
  <Value> </Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_description_nlsid</Name>
</StringAttribute>
<StringAttribute>
  <Name>value</Name>
  <Value>7.777</Value>
</StringAttribute>
<StringAttribute>
  <Name>is_long_running</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_group</Name>
  <Value>Load</Value>
</StringAttribute>
<StringAttribute>
  <Name>is_udm</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_description</Name>
</StringAttribute>
<StringAttribute>
  <Name>metric_column_nlsid</Name>
  <Value>host_load_cpuIdle</Value>
```

```

</StringAttribute>
<StringAttribute>
  <Name>metric_column</Name>
  <Value>cpuUtil</Value>
</StringAttribute>
<StringAttribute>
  <Name>unit_nlsid</Name>
  <Value>em_sys_standard_percent</Value>
</StringAttribute>
<StringAttribute>
  <Name>unit</Name>
  <Value>%</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_group_nlsid</Name>
  <Value>host_load</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_group_resbundle</Name>
  <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
</StringAttribute>
<StringAttribute>
  <Name>severity_guid</Name>
  <Value>B69EC6D3F8B3A48EE040020A78016095</Value>
</StringAttribute>
</EventClassSpecificAttributes>
</EMEvent>

```

B.2 Update Sample

Listed below is a sample of the XML format generated by Enterprise Manager for SCOM update operations.

```

<EMEvent xmlns="http://xmlns.oracle.com/sysman/connector">
  <ConnectorGUID>2C08969483F141F1B7482F376935C0AC</ConnectorGUID>
  <ExternalEventID>368d9bea-a659-4086-b239-0f7cf650d9df</ExternalEventID>
  <NotificationRuleOwner>Super Administrator</NotificationRuleOwner>
  <NotificationRuleName>SCOM Rule</NotificationRuleName>
  <ConnectorVariable>
    <VariableName>REGISTRATION_ID</VariableName>
    <VariableValue>Dummy</VariableValue>
  </ConnectorVariable>
  <Property>
    <Name>Notification_Method_Name</Name>
    <Value>SCOM</Value>
  </Property>
  <Property>
    <Name>AuthenticationType</Name>
    <Value>HTTPBasicAuthentication</Value>
  </Property>
  <Property>
    <Name>Registered</Name>
    <Value>yes</Value>
  </Property>
  <Property>
    <Name>IsNewTargetType</Name>
    <Value>yes</Value>
  </Property>
  <Property>
    <Name>Initialized</Name>

```

```
<Value>yes</Value>
</Property>
<SystemAttributes>
  <EventClass>metric_alert</EventClass>
  <EventID>B6A5393A91D232A0E040020A7801445B</EventID>
  <SequenceID>B69EC6D3F8B7A48EE040020A78016095</SequenceID>
  <ReportedDate>2012-01-17T17:03:49.000-06:00</ReportedDate>
  <DisplayTZ>America/Chicago</DisplayTZ>
  <EventName>Load:cpuUtil</EventName>
  <Severity>Warning</Severity>
  <SeverityCode>WARNING</SeverityCode>
  <SourceInfo>
    <SourceObjInfo>
      <ObjID>D93A2E4E1622013D74D9534ECB090944</ObjID>
      <ObjName>orcsvr1.iwavesoftware.com</ObjName>
      <ObjOwner>Super Administrator</ObjOwner>
      <SourceObjType>TARGET</SourceObjType>
      <SourceObjSubType>host</SourceObjSubType>
    </SourceObjInfo>
    <TargetInfo>
      <TargetGUID>D93A2E4E1622013D74D9534ECB090944</TargetGUID>
      <TargetName>orcsvr1.iwavesoftware.com</TargetName>
      <TargetType>host</TargetType>
      <TargetTypeLabel>Host</TargetTypeLabel>
      <TargetURL>https://orcsvr1.iwavesoftware.com:7801/em/redirect?
pageType=TARGET_HOMEPAGE&amp;targetName=orcsvr1.iwavesoftware.com&amp;targetType=host
</TargetURL>
      <TargetProperty>
        <Name>Target_Host</Name>
        <Value>orcsvr1.iwavesoftware.com</Value>
      </TargetProperty>
      <TargetProperty>
        <Name>Target_Version</Name>
        <Value>5.5.0.0</Value>
      </TargetProperty>
      <TargetProperty>
        <Name>Line of Business</Name>
        <Value>Software</Value>
      </TargetProperty>
      <TargetProperty>
        <Name>Location</Name>
        <Value>Frisco, TX</Value>
      </TargetProperty>
      <TargetProperty>
        <Name>Comment</Name>
        <Value>Testing target properties</Value>
      </TargetProperty>
    </TargetInfo>
  </SourceInfo>
  <Message>CPU Utilization is 9.68%, crossed warning (0.1) or critical (99)
threshold.</Message>
  <EventURL>https://orcsvr1.iwavesoftware.com:7801/em/redirect?pageType=sdk-
core-event-console-detailEvent&amp;issueID=B69EC6D3F8B7A48EE040020A78016095</
EventURL>
  <AutoClose>true</AutoClose>
  <EventCategory>Capacity</EventCategory>
</SystemAttributes>
<EventClassSpecificAttributes>
  <StringAttribute>
    <Name>is_thresholdable</Name>
    <Value>1</Value>
```

```
</StringAttribute>
<StringAttribute>
  <Name>coll_name</Name>
  <Value>LoadLinux</Value>
</StringAttribute>
<StringAttribute>
  <Name>is_metric_extension</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_column_resbundle</Name>
  <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_description_resbundle</Name>
  <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
</StringAttribute>
<StringAttribute>
  <Name>unit_resbundle</Name>
  <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
</StringAttribute>
<StringAttribute>
  <Name>cycle_guid</Name>
  <Value>B69EC6D3F8B3A48EE040020A78016095</Value>
</StringAttribute>
<StringAttribute>
  <Name>is_remote</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_type</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_guid</Name>
  <Value>0C71A1AFAC2D7199013837DA35522C08</Value>
</StringAttribute>
<StringAttribute>
  <Name>num_keys</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>key_value</Name>
  <Value> </Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_description_nlsid</Name>
</StringAttribute>
<StringAttribute>
  <Name>value</Name>
  <Value>9.68</Value>
</StringAttribute>
<StringAttribute>
  <Name>is_long_running</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_group</Name>
  <Value>Load</Value>
</StringAttribute>
<StringAttribute>
```

```

        <Name>is_udm</Name>
        <Value>0</Value>
    </StringAttribute>
    <StringAttribute>
        <Name>metric_description</Name>
    </StringAttribute>
    <StringAttribute>
        <Name>metric_column_nlsid</Name>
        <Value>host_load_cpuIdle</Value>
    </StringAttribute>
    <StringAttribute>
        <Name>metric_column</Name>
        <Value>cpuUtil</Value>
    </StringAttribute>
    <StringAttribute>
        <Name>unit_nlsid</Name>
        <Value>em_sys_standard_percent</Value>
    </StringAttribute>
    <StringAttribute>
        <Name>unit</Name>
        <Value>%</Value>
    </StringAttribute>
    <StringAttribute>
        <Name>metric_group_nlsid</Name>
        <Value>host_load</Value>
    </StringAttribute>
    <StringAttribute>
        <Name>metric_group_resbundle</Name>
        <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
    </StringAttribute>
    <StringAttribute>
        <Name>severity_guid</Name>
        <Value>B6A5393A91CF32A0E040020A7801445B</Value>
    </StringAttribute>
</EventClassSpecificAttributes>
</EMEvent>

```

B.3 Clear Sample

Listed below is a sample of the XML format generated by Enterprise Manager for SCOM clear operations.

```

<EMEvent xmlns="http://xmlns.oracle.com/sysman/connector">
  <ConnectorGUID>2C08969483F141F1B7482F376935C0AC</ConnectorGUID>
  <ExternalEventID>368d9bea-a659-4086-b239-0f7cf650d9df</ExternalEventID>
  <NotificationRuleOwner>Super Administrator</NotificationRuleOwner>
  <NotificationRuleName>SCOM Rule</NotificationRuleName>
  <ConnectorVariable>
    <VariableName>REGISTRATION_ID</VariableName>
    <VariableValue>Dummy</VariableValue>
  </ConnectorVariable>
  <Property>
    <Name>Notification_Method_Name</Name>
    <Value>SCOM</Value>
  </Property>
  <Property>
    <Name>AuthenticationType</Name>
    <Value>HTTPBasicAuthentication</Value>
  </Property>
  <Property>

```

```

        <Name>Registered</Name>
        <Value>yes</Value>
    </Property>
    <Property>
        <Name>IsNewTargetType</Name>
        <Value>yes</Value>
    </Property>
    <Property>
        <Name>Initialized</Name>
        <Value>yes</Value>
    </Property>
    <SystemAttributes>
        <EventClass>metric_alert</EventClass>
        <EventID>B69EDA076C5C8256E040020A780165F6</EventID>
        <SequenceID>B69EC6D3F8B7A48EE040020A78016095</SequenceID>
        <ReportedDate>2012-01-17T17:04:45.000-06:00</ReportedDate>
        <DisplayTZ>America/Chicago</DisplayTZ>
        <EventName>Load:cpuUtil</EventName>
        <Severity>Clear</Severity>
        <SeverityCode>CLEAR</SeverityCode>
        <SourceInfo>
            <SourceObjInfo>
                <ObjID>D93A2E4E1622013D74D9534ECB090944</ObjID>
                <ObjName>orcsvr1.iwavesoftware.com</ObjName>
                <ObjOwner>Super Administrator</ObjOwner>
                <SourceObjType>TARGET</SourceObjType>
                <SourceObjSubType>host</SourceObjSubType>
            </SourceObjInfo>
            <TargetInfo>
                <TargetGUID>D93A2E4E1622013D74D9534ECB090944</TargetGUID>
                <TargetName>orcsvr1.iwavesoftware.com</TargetName>
                <TargetType>host</TargetType>
                <TargetTypeLabel>Host</TargetTypeLabel>
                <TargetURL>https://orcsvr1.iwavesoftware.com:7801/em/redirect?
pageType=TARGET_HOMEPAGE&targetName=orcsvr1.iwavesoftware.com&targetType=host
</TargetURL>
                <TargetProperty>
                    <Name>Target_Host</Name>
                    <Value>orcsvr1.iwavesoftware.com</Value>
                </TargetProperty>
                <TargetProperty>
                    <Name>Target_Version</Name>
                    <Value>5.5.0.0</Value>
                </TargetProperty>
                <TargetProperty>
                    <Name>Line of Business</Name>
                    <Value>Software</Value>
                </TargetProperty>
                <TargetProperty>
                    <Name>Location</Name>
                    <Value>Frisco, TX</Value>
                </TargetProperty>
                <TargetProperty>
                    <Name>Comment</Name>
                    <Value>Testing target properties</Value>
                </TargetProperty>
            </TargetInfo>
        </SourceInfo>
        <Message>CPU Utilization is 3.75%, fallen below warning (98) and critical
(99)
        thresholds.</Message>

```



```
<EventURL>https://orcsvr1.iwavesoftware.com:7801/em/redirect?pageType=sdk-
core-event-console-detailEvent&issueID=B69EC6D3F8B7A48EE040020A78016095</
EventURL>
  <AutoClose>true</AutoClose>
  <EventCategory>Capacity</EventCategory>
</SystemAttributes>
<EventClassSpecificAttributes>
  <StringAttribute>
    <Name>is_thresholdable</Name>
    <Value>1</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>coll_name</Name>
    <Value>LoadLinux</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>is_metric_extension</Name>
    <Value>0</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>metric_column_resbundle</Name>
    <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>metric_description_resbundle</Name>
    <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>unit_resbundle</Name>
    <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>cycle_guid</Name>
    <Value>B69EC6D3F8B3A48EE040020A78016095</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>is_remote</Name>
    <Value>0</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>metric_type</Name>
    <Value>0</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>metric_guid</Name>
    <Value>0C71A1AFAC2D7199013837DA35522C08</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>num_keys</Name>
    <Value>0</Value>
  </StringAttribute>
  <StringAttribute>
    <Name>key_value</Name>
    <Value> </Value>
  </StringAttribute>
  <StringAttribute>
    <Name>metric_description_nlsid</Name>
  </StringAttribute>
  <StringAttribute>
    <Name>value</Name>
    <Value>3.75</Value>
```

```
</StringAttribute>
<StringAttribute>
  <Name>is_long_running</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_group</Name>
  <Value>Load</Value>
</StringAttribute>
<StringAttribute>
  <Name>is_udm</Name>
  <Value>0</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_description</Name>
</StringAttribute>
<StringAttribute>
  <Name>metric_column_nlsid</Name>
  <Value>host_load_cpuIdle</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_column</Name>
  <Value>cpuUtil</Value>
</StringAttribute>
<StringAttribute>
  <Name>unit_nlsid</Name>
  <Value>em_sys_standard_percent</Value>
</StringAttribute>
<StringAttribute>
  <Name>unit</Name>
  <Value>%</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_group_nlsid</Name>
  <Value>host_load</Value>
</StringAttribute>
<StringAttribute>
  <Name>metric_group_resbundle</Name>
  <Value>oracle.sysman.eml.rsc.gen.hostMsg</Value>
</StringAttribute>
<StringAttribute>
  <Name>severity_guid</Name>
  <Value>B69EDA076C5A8256E040020A780165F6</Value>
</StringAttribute>
</EventClassSpecificAttributes>
</EMEvent>
```

C

Enterprise Manager Event Format

Templates translate the XML format of Enterprise Manager events to the XML format required for the endpoint application's web service. To customize your templates, you need to understand the format of both ends so that you know how to map the data. This appendix provides detailed information on the format of the XML document that contains event information from Enterprise Manager.

A schema file defines the structure of an XML document. The `EMEvent.xsd` schema file defines the main structure of the event data. This file also imports structure information from other schema files. The following sections provide information from the schema files that define the `EMEvent` XML format:

- [EMEvent.xsd](#)
- [connectorCommon.xsd](#)
- [externalEvent.xsd](#)

C.1 EMEvent.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns="http://xmlns.oracle.com/sysman/connector"
            targetNamespace="http://xmlns.oracle.com/sysman/connector"
            elementFormDefault="qualified"
xmlns:jaxb="http://java.sun.com/xml/ns/jaxb"
jaxb:version="2.0"
xmlns:xjc="http://java.sun.com/xml/ns/jaxb/xjc"
jaxb:extensionBindingPrefixes="xjc">

  <xsd:annotation>
    <xsd:appinfo>
      <jaxb:globalBindings>
        <xjc:simple />
      </jaxb:globalBindings>
    </xsd:appinfo>
  </xsd:annotation>
  <xsd:include schemaLocation="connectorCommon.xsd"/>
  <xsd:element name="EMEvent" type="EMEventType" />
  <xsd:complexType name="EMEventType">
    <xsd:sequence>
      <xsd:element name="ConnectorGUID" type="xsd:string"/>
      <xsd:element name="ExternalEventID" type="xsd:string"
        minOccurs="0"/>
      <xsd:element name="NotificationRuleOwner" type="xsd:string"/>
      <xsd:element name="NotificationRuleName" type="xsd:string"/>
      <xsd:element name="ConnectorVariable" type="VariableType"
        minOccurs="0" maxOccurs="50"/>
      <xsd:element name="Property" type="PropertyType" minOccurs="0"
        maxOccurs="50"/>
      <xsd:element name="SystemAttributes"
        type="EventSystemAttributesType"/>
      <xsd:element name="EventClassSpecificAttributes">
```

```
<xsd:complexType>
  <xsd:sequence>
    <xsd:choice minOccurs="0" maxOccurs="200">
      <xsd:element name="StringAttribute" type="StringValue"/>
      <xsd:element name="NumberAttribute" type="StringValue"/>
      <xsd:element name="RawAttribute" type="StringValue"/>
      <xsd:element name="DateAttribute" type="DateValue"/>
    </xsd:choice>
  </xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="EventContextAttributes">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:choice minOccurs="0" maxOccurs="200">
        <xsd:element name="StringAttribute" type="StringValue"/>
        <xsd:element name="NumberAttribute" type="StringValue"/>
      </xsd:choice>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="EventSystemAttributesType">
  <xsd:sequence>
    <xsd:element name="EventClass" type="xsd:string"/>
    <xsd:element name="EventID" type="xsd:string"/>
    <xsd:element name="SequenceID" type="xsd:string"/>
    <xsd:element name="OccurredDate" type="xsd:dateTime" minOccurs="0"/>
    <xsd:element name="ReportedDate" type="xsd:dateTime"/>
    <xsd:element name="DisplayTZ" type="xsd:string"/>
    <xsd:element name="EventName" type="xsd:string"/>
    <xsd:element name="Severity" type="xsd:string"/>
    <xsd:element name="SeverityCode" type="xsd:string"/>
    <xsd:element name="SourceInfo" type="SourceInfoType"/>
    <xsd:element name="Message" type="xsd:string" minOccurs="0"/>
    <xsd:element name="ActionMessage" type="xsd:string" minOccurs="0"/>
    <xsd:element name="EventURL" type="xsd:string"/>
    <xsd:element name="AutoClose" type="xsd:boolean"/>
    <xsd:element name="EventCategory" type="xsd:string" minOccurs="0"
      maxOccurs="50"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="StringValue">
  <xsd:sequence>
    <xsd:element name="Name" type="xsd:string"/>
    <xsd:element name="Value" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="DateValueType">
  <xsd:sequence>
    <xsd:element name="Name" type="xsd:string"/>
    <xsd:element name="Value" type="xsd:dateTime"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

C.2 connectorCommon.xsd

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns="http://xmlns.oracle.com/sysman/connector"
            targetNamespace="http://xmlns.oracle.com/sysman/connector"
            elementFormDefault="qualified">
<xsd:include schemaLocation="externalEvent.xsd"/>
<xsd:complexType name="SourceInfoType">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a complex type for Source Information.
        </xsd:documentation>
    </xsd:annotation>
<xsd:sequence>
    <xsd:element name="SourceObjInfo" type="SourceObjInfoType" minOccurs="0">
        <xsd:annotation>
            <xsd:documentation>
                This element defines the data structure for the source object, the EM
                subsystem or component, that raises an EM event or an incident.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="TargetInfo" type="TargetInfoType" minOccurs="0">
        <xsd:annotation>
            <xsd:documentation>
                The element defines the data structure for an EM target as related
                to the connector framework.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="SourceObjInfoType">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a complex type for Source Object Information.
        </xsd:documentation>
    </xsd:annotation>
<xsd:sequence>
    <xsd:element name="ObjID" type="xsd:string">
        <xsd:annotation>
            <xsd:documentation>
                The unique ID to identify the source object.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="ObjName" type="xsd:string">
        <xsd:annotation>
            <xsd:documentation>
                The name of the source object.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="ObjOwner" type="xsd:string" minOccurs="0">
        <xsd:annotation>
            <xsd:documentation>
                The owner of the source object.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
</xsd:sequence>
</xsd:complexType>

```

```
    </xsd:annotation>
  </xsd:element>
  <xsd:element name="SourceObjType" type="xsd:string">
    <xsd:annotation>
      <xsd:documentation>
        The type of the source object.
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>
  <xsd:element name="SourceObjSubType" type="xsd:string" minOccurs="0">
    <xsd:annotation>
      <xsd:documentation>
        The subtype of the source object.
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="TargetInfoType">
  <xsd:annotation>
    <xsd:documentation>
      This section defines a complex type for target information.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="TargetGUID" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>
          A unique GUID for the target.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="TargetName" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>
          Name of the target.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="TargetType" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>
          Type of the target.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="TargetTypeLabel" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>
          The display label of the target type.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="TargetURL" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>
          The URL of the target.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="TargetProperty" type="PropertyType" minOccurs="0"
```

```
        maxOccurs="50">
      <xsd:annotation>
        <xsd:documentation>
          An optional list of properties for the target.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="PropertyType">
  <xsd:annotation>
    <xsd:documentation>
      This section defines a complex type for a property attribute.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="Name" type="xsd:string">
      <xsd:annotation>
        <xsd:documentation>
          A string name defining a property attribute.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="Value" type="xsd:string" nillable="true">
      <xsd:annotation>
        <xsd:documentation>
          A non-null string value.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="VariableType">
  <xsd:annotation>
    <xsd:documentation>
      This section defines a complex type for a general variable.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="VariableName" type="StringStrictT32">
      <xsd:annotation>
        <xsd:documentation>
          Name of the variable. It has to be a string containing 1 or upto
          32 upper case or lower case letters or numbers.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="VariableValue" type="StringT2048">
      <xsd:annotation>
        <xsd:documentation>
          Value of the variable. It has to be a string containing 1 or upto
          2048 characters.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="GetAlertsResponse">
  <xsd:annotation>
    <xsd:documentation>
      This section defines a complex type for responses to a getAlerts request.
```



```
        <xsd:maxLength value="64"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringT128">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a simple type for a String with maximum length of
            128 bytes.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:minLength value="1"/>
        <xsd:maxLength value="128"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringT256">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a simple type for a String with maximum length of
            256 bytes.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:minLength value="1"/>
        <xsd:maxLength value="256"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringT512">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a simple type for a String with maximum length of
            512 bytes.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:minLength value="1"/>
        <xsd:maxLength value="512"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringT2048">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a simple type for a String with maximum length of
            2048 bytes.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:minLength value="1"/>
        <xsd:maxLength value="2048"/>
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringStrictT16">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a simple type for a String with maximum length of
            16 bytes. The String can only contain lower or upper case letters,
            numbers,
            and the underscore characters.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
```

```
<xsd:minLength value="1"/>
<xsd:maxLength value="16"/>
<xsd:pattern value="([a-zA-Z0-9_]*)" />
</xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringStrictT32">
  <xsd:annotation>
    <xsd:documentation>
      This section defines a simple type for a String with maximum length of
      32 bytes. The String can only contain lower or upper case letters,
numbers,
      and the underscore characters.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1"/>
    <xsd:maxLength value="32"/>
    <xsd:pattern value="([a-zA-Z0-9_]*)" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringStrictT64">
  <xsd:annotation>
    <xsd:documentation>
      This section defines a simple type for a String with maximum length of
      64 bytes. The String can only contain lower or upper case letters,
numbers,
      and the underscore characters.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1"/>
    <xsd:maxLength value="64"/>
    <xsd:pattern value="([a-zA-Z0-9_]*)" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringStrictT128">
  <xsd:annotation>
    <xsd:documentation>
      This section defines a simple type for a String with maximum length of
      128 bytes. The String can only contain lower or upper case letters,
numbers,
      and the underscore characters.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1"/>
    <xsd:maxLength value="128"/>
    <xsd:pattern value="([a-zA-Z0-9_]*)" />
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="StringStrictT256">
  <xsd:annotation>
    <xsd:documentation>
      This section defines a simple type for a String with maximum length of
      256 bytes. The String can only contain lower or upper case letters,
numbers,
      and the underscore characters.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1"/>
```

```

        <xsd:maxLength value="256"/>
        <xsd:pattern value="([a-zA-Z0-9_]*)" />
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="VersionT">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a simple type for a String with maximum length of
            20 bytes. The String can only contain numbers and the period characters.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:minLength value="1"/>
        <xsd:maxLength value="20"/>
        <xsd:pattern value="([0-9.]*)" />
    </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

C.3 externalEvent.xsd

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://xmlns.oracle.com/sysman/connector"
    targetNamespace="http://xmlns.oracle.com/sysman/connector"
    elementFormDefault="qualified">
    <xsd:element name="ExternalEvent">
        <xsd:annotation>
            <xsd:documentation>
                This section defines the attribute requirement of an external event
                for the connector framework to process it.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name="SystemAttributes"
                    type="ExternalEventSystemAttributesType">
                    <xsd:annotation>
                        <xsd:documentation>
                            Attributes to capture general information about the external event
                            system. These attributes are system-specific, with all events from
                            the same external system sharing the same system attributes.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:element>
                <xsd:element name="EventClassAttributes"
                    type="ExternalEventClassAttributesType">
                    <xsd:annotation>
                        <xsd:documentation>
                            Attributes to capture specific information required for the event
                            as defined in the event class.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:element>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:complexType name="ExternalEventSystemAttributesType">
        <xsd:annotation>
            <xsd:documentation>

```

```
        This section defines a complex type for system attributes required for
        all external events.
    </xsd:documentation>
</xsd:annotation>
<xsd:sequence>
    <xsd:element name="eventName" type="xsd:string"
minOccurs="0">
        <xsd:annotation>
            <xsd:documentation>
                Name of the event.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="category" type="xsd:string" minOccurs="0" maxOccurs="50">
        <xsd:annotation>
            <xsd:documentation>
                The event category to which the event belongs.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="targetName" type="xsd:string">
        <xsd:annotation>
            <xsd:documentation>
                Name of the target on which event was generated. It refers
                to an entity in external systems simillar to an EM target.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="targetType" type="xsd:string">
        <xsd:annotation>
            <xsd:documentation>
                The type of the target. Target types defined for event connectors
                are used. See connectorDeploy.xsd.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="occurrenceDate" type="xsd:dateTime">
        <xsd:annotation>
            <xsd:documentation>
                Date when the event occured.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="detectedDate" type="xsd:dateTime">
        <xsd:annotation>
            <xsd:documentation>
                Date when the event was last detected.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="autoClose" type="xsd:boolean">
        <xsd:annotation>
            <xsd:documentation>
                A flag indicating if an event is auto closed by the system, or it
                has to be manually closed by users.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:element name="message" type="xsd:string">
        <xsd:annotation>
            <xsd:documentation>
```

```

        A description of the event.
    </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="severity" type="xsd:string">
    <xsd:annotation>
        <xsd:documentation>
            Severity level of the event.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="ExternalEventClassAttributesType">
    <xsd:annotation>
        <xsd:documentation>
            This section defines a complex type for class specific attributes
required
            for all external events in the class.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
        <xsd:element name="external_event_id" type="xsd:string">
            <xsd:annotation>
                <xsd:documentation>
                    ID used in external system to identify the event.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="external_rule_id" type="xsd:string" minOccurs="0">
            <xsd:annotation>
                <xsd:documentation>
                    Optional rule ID that delivered the event in the external system.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="external_host" type="xsd:string" minOccurs="0">
            <xsd:annotation>
                <xsd:documentation>
                    Optional host information from external system where event was
generated.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="external_source" type="xsd:string" minOccurs="0">
            <xsd:annotation>
                <xsd:documentation>
                    Optional source information from the external system.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="external_severity" type="xsd:string">
            <xsd:annotation>
                <xsd:documentation>
                    Severity level of the event on external system.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="external_status" type="xsd:string" minOccurs="0">
            <xsd:annotation>
                <xsd:documentation>

```

```
        Status of the event on extenal system.
    </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="custom_field1" type="xsd:string" minOccurs="0">
    <xsd:annotation>
        <xsd:documentation>
            An optional field.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:element name="custom_field2" type="xsd:string" minOccurs="0">
    <xsd:annotation>
        <xsd:documentation>
            An optional field.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:element name="custom_field3" type="xsd:string" minOccurs="0">
    <xsd:annotation>
        <xsd:documentation>
            An optional field.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:element name="custom_field4" type="xsd:string" minOccurs="0">
    <xsd:annotation>
        <xsd:documentation>
            An optional field.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:element name="custom_field5" type="xsd:string" minOccurs="0">
    <xsd:annotation>
        <xsd:documentation>
            An optional field.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

D

Microsoft SCOM Web Service WSDL Format

Templates translate the XML format of Enterprise Manager events to the XML format required for the endpoint application's web service. To customize your templates, you need to understand the format of both ends so that you know how to map the data. This appendix provides detailed information on the format of the XML document that is required by the SCOM web service.

A WSDL file defines the interface that must be used to call a web service. The WSDL defines the structure of the XML document that it accepts and how the web service is to be called. The contents of the WSDL file are listed in the following sections:

- [EventService WSDL](#)
- [SCOMService WSDL](#)

D.1 EventService WSDL

```
<wsdl:definitions name="EventService"
  targetNamespace="http://iwavesoftware.com/services/adapter-framework"
  xmlns:ns1="http://schemas.xmlsoap.org/soap/http"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://iwavesoftware.com/services/adapter-framework"
  xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/
XMLSchema">
  <wsdl:types>
    <xs:schema attributeFormDefault="unqualified"
  elementFormDefault="unqualified"
    targetNamespace="http://iwavesoftware.com/services/adapter-framework"
    xmlns:tns="http://iwavesoftware.com/services/adapter-framework"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <xs:element name="Class" type="tns:eventClass"/>
      <xs:element name="ITObject" type="tns:itObject"/>
      <xs:element name="Object" type="tns:eventObject"/>
      <xs:element name="acknowledge" type="tns:acknowledge"/>
      <xs:element name="acknowledgeResponse" type="tns:acknowledgeResponse"/>
      <xs:element name="assignment" type="tns:assignment"/>
      <xs:element name="categorization" type="tns:categorization"/>
      <xs:element name="change" type="tns:change"/>
      <xs:element name="ci" type="tns:ci"/>
      <xs:element name="ciRef" type="tns:ciRef"/>
      <xs:element name="ciRelationship" type="tns:ciRelationship"/>
      <xs:element name="classification" type="tns:classification"/>
      <xs:element name="clear" type="tns:clear"/>
      <xs:element name="clearResponse" type="tns:clearResponse"/>
      <xs:element name="client-object" type="tns:clientDefinedObject"/>
      <xs:element name="complex-field" type="tns:complexField"/>
      <xs:element name="compliance" type="tns:compliance"/>
      <xs:element name="contact" type="tns:contact"/>
      <xs:element name="container" type="tns:container"/>
      <xs:element name="create" type="tns:create"/>
      <xs:element name="createResponse" type="tns:createResponse"/>
```

```

<xs:element name="data" type="tns:data"/>
<xs:element name="date-field" type="tns:dateField"/>
<xs:element name="diary-list-field" type="tns:diaryListField"/>
<xs:element name="diary-value" type="tns:diaryValue"/>
<xs:element name="escalation" type="tns:escalation"/>
<xs:element name="event" type="tns:event"/>
<xs:element name="find" type="tns:find"/>
<xs:element name="findResponse" type="tns:findResponse"/>
<xs:element name="get" type="tns:get"/>
<xs:element name="getResponse" type="tns:getResponse"/>
<xs:element name="group" type="tns:group"/>
<xs:element name="incident" type="tns:incident"/>
<xs:element name="knowledge" type="tns:knowledge"/>
<xs:element name="log" type="tns:log"/>
<xs:element name="metric" type="tns:metric"/>
<xs:element name="number-field" type="tns:numberField"/>
<xs:element name="objectReference" type="tns:objectReference"/>
<xs:element name="problem" type="tns:problem"/>
<xs:element name="product" type="tns:product"/>
<xs:element name="resolution" type="tns:resolution"/>
<xs:element name="source" type="tns:source"/>
<xs:element name="string-field" type="tns:stringField"/>
<xs:element name="update" type="tns:update"/>
<xs:element name="updateResponse" type="tns:updateResponse"/>
<xs:element name="vendor" type="tns:vendor"/>
<xs:complexType name="clear">
  <xs:sequence>
    <xs:element minOccurs="0" name="destination" type="xs:string"/>
    <xs:element minOccurs="0" name="event" type="tns:event"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="event">
  <xs:complexContent>
    <xs:extension base="tns:itObject">
      <xs:sequence>
        <xs:element default="1970-01-01T00:00:00.0-00:00"
minOccurs="0"
          name="createDate" type="xs:dateTime"/>
        <xs:element minOccurs="0" name="description"
type="xs:string"/>
        <xs:element minOccurs="0" name="escalation"
type="tns:escalation"/>
        <xs:element minOccurs="0" name="eventClass"
type="tns:eventClass"/>
        <xs:element minOccurs="0" name="externalEventIdentifier"
          type="xs:string"/>
        <xs:element minOccurs="0"
name="externalIncidentIdentifier"
          type="xs:string"/>
        <xs:element minOccurs="0" name="group" type="tns:group"/>
        <xs:element minOccurs="0" name="impact"
type="xs:string"/>
        <xs:element minOccurs="0" name="knowledgeRoot">
          <xs:complexType>
            <xs:sequence>
              <xs:element maxOccurs="unbounded"
minOccurs="0"
                name="knowledge" type="tns:knowledge"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```



```

minOccurs="0"
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
                                name="lastModified" type="xs:dateTime"/>
type="xs:string"/>
                                <xs:element minOccurs="0" name="lastModifiedBy"
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
                                name="lastModifiedNonConnector" type="xs:dateTime"/>
minOccurs="0"
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
                                name="lastRepeatDate" type="xs:dateTime"/>
minOccurs="0" name="log"
                                <xs:element minOccurs="0" name="logs">
                                    <xs:complexType>
                                        <xs:sequence>
                                            <xs:element maxOccurs="unbounded"
                                                type="tns:log"/>
                                        </xs:sequence>
                                    </xs:complexType>
                                </xs:element>
minOccurs="0"
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
                                name="maintenanceModeLastModified"
                                type="xs:dateTime"/>
type="tns:metric"/>
                                <xs:element minOccurs="0" name="metric"
                                <xs:element name="monitorEvent" type="xs:boolean"/>
                                <xs:element minOccurs="0" name="object"
                                <xs:element minOccurs="0" name="owner" type="xs:string"/>
                                <xs:element minOccurs="0" name="priority"
                                <xs:element default="-2147483648" minOccurs="0"
                                type="xs:int"/>
                                <xs:element minOccurs="0" name="resolvedBy"
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
                                name="resolvedDate" type="xs:dateTime"/>
                                <xs:element minOccurs="0" name="severity"
                                <xs:element minOccurs="0" name="source"
                                <xs:element minOccurs="0" name="status"
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
                                name="statusLastModified" type="xs:dateTime"/>
                                <xs:element minOccurs="0" name="summary"
                                <xs:element minOccurs="0" name="type" type="xs:string"/>
                                <xs:element minOccurs="0" name="urgency"
                                </xs:sequence>
                                </xs:extension>
                                </xs:complexContent>
                                </xs:complexType>
                                <xs:complexType name="itObject">
                                    <xs:sequence>
                                        <xs:element minOccurs="0" name="extended-fields">

```

```

        <xs:complexType>
          <xs:sequence>
            <xs:choice maxOccurs="unbounded" minOccurs="0">
              <xs:element name="string-field"
type="tns:stringField"/>
              <xs:element name="date-field"
type="tns:dateField"/>
              <xs:element name="number-field"
type="tns:numberField"/>
              <xs:element name="diary-list-field"
type="tns:diaryListField"/>
              <xs:element name="complex-field"
type="tns:complexField"/>
            </xs:choice>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element minOccurs="0" name="identifier" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="escalation">
    <xs:sequence>
      <xs:element name="escalated" type="xs:boolean"/>
      <xs:element minOccurs="0" name="escalatedBy" type="xs:string"/>
      <xs:element minOccurs="0" name="server" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="eventClass">
    <xs:sequence>
      <xs:element minOccurs="0" name="container" type="tns:container"/>
      <xs:element minOccurs="0" name="description" type="xs:string"/>
      <xs:element minOccurs="0" name="displayName" type="xs:string"/>
      <xs:element minOccurs="0" name="identifier" type="xs:string"/>
      <xs:element minOccurs="0" name="name" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="container">
    <xs:sequence>
      <xs:element minOccurs="0" name="description" type="xs:string"/>
      <xs:element minOccurs="0" name="displayName" type="xs:string"/>
      <xs:element minOccurs="0" name="identifier" type="xs:string"/>
      <xs:element minOccurs="0" name="name" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="group">
    <xs:sequence>
      <xs:element minOccurs="0" name="identifier" type="xs:string"/>
      <xs:element minOccurs="0" name="name" type="xs:string"/>
      <xs:element minOccurs="0" name="version" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="knowledge">
    <xs:sequence>
      <xs:element minOccurs="0" name="content" type="xs:string"/>
      <xs:element default="1970-01-01T00:00:00.0-00:00" minOccurs="0"
name="dateCreated" type="xs:dateTime"/>
      <xs:element minOccurs="0" name="description" type="xs:string"/>
      <xs:element minOccurs="0" name="displayName" type="xs:string"/>
      <xs:element minOccurs="0" name="identifier" type="xs:string"/>
      <xs:element minOccurs="0" name="languageCode" type="xs:string"/>
      <xs:element default="1970-01-01T00:00:00.0-00:00" minOccurs="0"
name="dateCreated" type="xs:dateTime"/>
    </xs:sequence>
  </xs:complexType>

```

```

        name="lastModified" type="xs:dateTime"/>
        <xs:element minOccurs="0" name="name" type="xs:string"/>
        <xs:element minOccurs="0" name="status" type="xs:string"/>
        <xs:element minOccurs="0" name="summary" type="xs:string"/>
        <xs:element minOccurs="0" name="type" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="log">
    <xs:sequence>
        <xs:element minOccurs="0" name="extended-fields">
            <xs:complexType>
                <xs:sequence>
                    <xs:choice maxOccurs="unbounded" minOccurs="0">
                        <xs:element name="string-field"
type="tns:stringField"/>
                        <xs:element name="date-field"
type="tns:dateField"/>
                        <xs:element name="number-field"
type="tns:numberField"/>
                        <xs:element name="diary-list-field"
type="tns:diaryListField"/>
                        <xs:element name="complex-field"
type="tns:complexTypeField"/>
                    </xs:choice>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element minOccurs="0" name="description" type="xs:string"/>
        <xs:element minOccurs="0" name="identifier" type="xs:string"/>
        <xs:element minOccurs="0" name="source" type="xs:string"/>
        <xs:element default="1970-01-01T00:00:00.0-00:00" minOccurs="0"
name="submitDate" type="xs:dateTime"/>
        <xs:element minOccurs="0" name="submitter" type="xs:string"/>
        <xs:element minOccurs="0" name="summary" type="xs:string"/>
        <xs:element minOccurs="0" name="type" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="stringField">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="name" type="xs:string" use="required"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="dateField">
    <xs:simpleContent>
        <xs:extension base="xs:dateTime">
            <xs:attribute name="name" type="xs:string" use="required"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="numberField">
    <xs:simpleContent>
        <xs:extension base="xs:decimal">
            <xs:attribute name="name" type="xs:string" use="required"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="diaryListField">
    <xs:sequence>
        <xs:element maxOccurs="unbounded" minOccurs="0" name="diary-

```

```

value"
    type="tns:diaryValue"/>
</xs:sequence>
<xs:attribute name="name" type="xs:string" use="required"/>
</xs:complexType>
<xs:complexType name="diaryValue">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="author" type="xs:string"/>
      <xs:attribute name="timestamp" type="xs:dateTime"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="complexField">
  <xs:sequence>
    <xs:choice maxOccurs="unbounded" minOccurs="0">
      <xs:element name="string-field" type="tns:stringField"/>
      <xs:element name="date-field" type="tns:dateField"/>
      <xs:element name="number-field" type="tns:numberField"/>
      <xs:element name="diary-list-field"
type="tns:diaryListField"/>
      <xs:element name="complex-field" type="tns:complexField"/>
    </xs:choice>
  </xs:sequence>
  <xs:attribute name="name" type="xs:string" use="required"/>
</xs:complexType>
<xs:complexType name="metric">
  <xs:sequence>
    <xs:element minOccurs="0" name="category" type="xs:string"/>
    <xs:element minOccurs="0" name="keyValues">
      <xs:complexType>
        <xs:sequence>
          <xs:element maxOccurs="unbounded" minOccurs="0"
name="string"
          type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element minOccurs="0" name="subCategory" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="eventObject">
  <xs:sequence>
    <xs:element minOccurs="0" name="computerName" type="xs:string"/>
    <xs:element minOccurs="0" name="displayName" type="xs:string"/>
    <xs:element minOccurs="0" name="identifier" type="xs:string"/>
    <xs:element minOccurs="0" name="inMaintenanceMode"
type="xs:boolean"/>
    <xs:element minOccurs="0" name="name" type="xs:string"/>
    <xs:element minOccurs="0" name="state" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="source">
  <xs:sequence>
    <xs:element minOccurs="0" name="computerName" type="xs:string"/>
    <xs:element minOccurs="0" name="container" type="tns:container"/>
    <xs:element minOccurs="0" name="description" type="xs:string"/>
    <xs:element minOccurs="0" name="displayName" type="xs:string"/>
    <xs:element minOccurs="0" name="domain" type="xs:string"/>
    <xs:element minOccurs="0" name="identifier" type="xs:string"/>
    <xs:element minOccurs="0" name="name" type="xs:string"/>

```

```
        <xs:element minOccurs="0" name="type" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="clearResponse">
    <xs:sequence/>
</xs:complexType>
<xs:complexType name="update">
    <xs:sequence>
        <xs:element minOccurs="0" name="destination" type="xs:string"/>
        <xs:element minOccurs="0" name="event" type="tns:event"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="updateResponse">
    <xs:sequence>
        <xs:element minOccurs="0" name="return" type="tns:event"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="acknowledge">
    <xs:sequence>
        <xs:element minOccurs="0" name="destination" type="xs:string"/>
        <xs:element minOccurs="0" name="event" type="tns:event"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="acknowledgeResponse">
    <xs:sequence>
        <xs:element minOccurs="0" name="return" type="tns:event"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="get">
    <xs:sequence>
        <xs:element minOccurs="0" name="destination" type="xs:string"/>
        <xs:element minOccurs="0" name="identifier" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="getResponse">
    <xs:sequence>
        <xs:element minOccurs="0" name="return" type="tns:event"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="find">
    <xs:sequence>
        <xs:element minOccurs="0" name="destination" type="xs:string"/>
        <xs:element minOccurs="0" name="query" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="findResponse">
    <xs:sequence>
        <xs:element maxOccurs="unbounded" minOccurs="0" name="return"
type="tns:event"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="create">
    <xs:sequence>
        <xs:element minOccurs="0" name="destination" type="xs:string"/>
        <xs:element minOccurs="0" name="event" type="tns:event"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="createResponse">
    <xs:sequence>
        <xs:element minOccurs="0" name="return" type="tns:event"/>
    </xs:sequence>
</xs:complexType>
```

```

</xs:complexType>
<xs:complexType mixed="true" name="clientDefinedObject">
  <xs:sequence>
    <xs:any maxOccurs="unbounded" minOccurs="0" namespace="##other"
      processContents="skip" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="incident">
  <xs:complexContent>
    <xs:extension base="tns:itObject">
      <xs:sequence>
        <xs:element minOccurs="0" name="assignee"
type="tns:assignment" />
        <xs:element minOccurs="0" name="cis">
          <xs:complexType>
            <xs:sequence>
              <xs:element maxOccurs="unbounded"
minOccurs="0" name="ci"
                type="tns:ciRef" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element minOccurs="0" name="classification"
          type="tns:classification" />
        <xs:element minOccurs="0" name="customer"
type="tns:contact" />
        <xs:element minOccurs="0" name="description"
type="xs:string" />
        <xs:element minOccurs="0" name="direct"
type="tns:contact" />
        <xs:element minOccurs="0" name="impact"
type="xs:string" />
        <xs:element minOccurs="0" name="log-data">
          <xs:complexType>
            <xs:sequence>
              <xs:element maxOccurs="unbounded"
minOccurs="0" name="log"
                type="tns:log" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element minOccurs="0" name="logs">
          <xs:complexType>
            <xs:sequence>
              <xs:element maxOccurs="unbounded"
minOccurs="0" name="log"
                type="tns:objectReference" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element minOccurs="0" name="owner"
type="tns:assignment" />
        <xs:element minOccurs="0" name="priority"
type="xs:string" />
        <xs:element minOccurs="0" name="relationships">
          <xs:complexType>
            <xs:sequence>
              <xs:element maxOccurs="unbounded"
minOccurs="0"
                name="relationship"
type="tns:objectReference" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```

                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element minOccurs="0" name="resolution"
type="tns:resolution"/>
        <xs:element minOccurs="0" name="severity"
type="xs:string"/>
        <xs:element minOccurs="0" name="status"
type="xs:string"/>
        <xs:element minOccurs="0" name="summary"
type="xs:string"/>
        <xs:element minOccurs="0" name="urgency"
type="xs:string"/>
        <xs:element minOccurs="0" name="vendor"
type="tns:vendor"/>
        <xs:element minOccurs="0" name="weight"
type="xs:string"/>
    </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:complexType name="assignment">
    <xs:sequence>
        <xs:element minOccurs="0" name="company" type="xs:string"/>
        <xs:element minOccurs="0" name="organization" type="xs:string"/>
        <xs:element minOccurs="0" name="owner" type="xs:string"/>
        <xs:element minOccurs="0" name="primaryGroup" type="xs:string"/>
        <xs:element minOccurs="0" name="secondaryGroup"
type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="ciRef">
    <xs:sequence>
        <xs:element minOccurs="0" name="extended-fields">
            <xs:complexType>
                <xs:sequence>
                    <xs:choice maxOccurs="unbounded" minOccurs="0">
                        <xs:element name="string-field"
type="tns:stringField"/>
                        <xs:element name="date-field"
type="tns:dateField"/>
                        <xs:element name="number-field"
type="tns:numberField"/>
                        <xs:element name="diary-list-field"
type="tns:diaryListField"/>
                        <xs:element name="complex-field"
type="tns:complexField"/>
                    </xs:choice>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element minOccurs="0" name="description" type="xs:string"/>
        <xs:element minOccurs="0" name="identifier" type="xs:string"/>
        <xs:element minOccurs="0" name="name" type="xs:string"/>
        <xs:element minOccurs="0" name="status" type="xs:string"/>
        <xs:element minOccurs="0" name="type" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="classification">
    <xs:sequence>
        <xs:element minOccurs="0" name="company" type="xs:string"/>

```

```

        <xs:element minOccurs="0" name="operational"
type="tns:categorization"/>
        <xs:element minOccurs="0" name="product" type="tns:product"/>
        <xs:element default="1970-01-01T00:00:00.0-00:00" minOccurs="0"
name="reportedDate" type="xs:dateTime"/>
        <xs:element minOccurs="0" name="reportedSource"
type="xs:string"/>
        <xs:element minOccurs="0" name="serviceType" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="categorization">
    <xs:sequence>
        <xs:element minOccurs="0" name="tier1" type="xs:string"/>
        <xs:element minOccurs="0" name="tier2" type="xs:string"/>
        <xs:element minOccurs="0" name="tier3" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="product">
    <xs:complexContent>
        <xs:extension base="tns:categorization">
            <xs:sequence>
                <xs:element minOccurs="0" name="manufacturer"
type="xs:string"/>
                <xs:element minOccurs="0" name="modelVersion"
type="xs:string"/>
                <xs:element minOccurs="0" name="name" type="xs:string"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="contact">
    <xs:sequence>
        <xs:element minOccurs="0" name="company" type="xs:string"/>
        <xs:element minOccurs="0" name="department" type="xs:string"/>
        <xs:element minOccurs="0" name="emailAddress" type="xs:string"/>
        <xs:element minOccurs="0" name="firstName" type="xs:string"/>
        <xs:element minOccurs="0" name="lastName" type="xs:string"/>
        <xs:element minOccurs="0" name="middleName" type="xs:string"/>
        <xs:element minOccurs="0" name="organization" type="xs:string"/>
        <xs:element minOccurs="0" name="phoneNumber" type="xs:string"/>
        <xs:element minOccurs="0" name="site" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="objectReference">
    <xs:sequence>
        <xs:element minOccurs="0" name="identifier" type="xs:string"/>
        <xs:element minOccurs="0" name="name" type="xs:string"/>
        <xs:element minOccurs="0" name="role" type="xs:string"/>
        <xs:element minOccurs="0" name="type" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="resolution">
    <xs:complexContent>
        <xs:extension base="tns:categorization">
            <xs:sequence>
                <xs:element minOccurs="0" name="cause" type="xs:string"/>
                <xs:element minOccurs="0" name="closureSource"
type="xs:string"/>
                <xs:element minOccurs="0" name="detail"
type="xs:string"/>
                <xs:element default="1970-01-01T00:00:00.0-00:00"

```



```

minOccurs="0"
                                name="forecastResolutionDate" type="xs:dateTime"/>
                                <xs:element minOccurs="0" name="method"
type="xs:string"/>
                                <xs:element minOccurs="0" name="product"
type="tns:product"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
minOccurs="0"
                                name="requiredDate" type="xs:dateTime"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
minOccurs="0"
                                name="resolutionDate" type="xs:dateTime"/>
                                <xs:element minOccurs="0" name="satisfactionRating"
type="xs:string"/>
                                </xs:sequence>
                                </xs:extension>
                                </xs:complexContent>
                                </xs:complexType>
                                <xs:complexType name="vendor">
                                <xs:sequence>
                                <xs:element minOccurs="0" name="assignmentStatus"
type="xs:string"/>
                                <xs:element minOccurs="0" name="contact" type="tns:contact"/>
                                <xs:element minOccurs="0" name="identifier" type="xs:string"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00" minOccurs="0"
name="reportedToVendorDate" type="xs:dateTime"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00" minOccurs="0"
name="resolvedDate" type="xs:dateTime"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00" minOccurs="0"
name="respondedToVendorDate" type="xs:dateTime"/>
                                </xs:sequence>
                                </xs:complexType>
                                <xs:complexType name="ci">
                                <xs:complexContent>
                                <xs:extension base="tns:itObject">
                                <xs:sequence>
                                <xs:element minOccurs="0" name="assignee"
type="xs:string"/>
                                <xs:element minOccurs="0" name="category"
type="xs:string"/>
                                <xs:element minOccurs="0" name="className"
type="xs:string"/>
                                <xs:element minOccurs="0" name="classNameNamespace"
type="xs:string"/>
                                <xs:element minOccurs="0" name="compliance"
type="tns:compliance"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
minOccurs="0"
name="createDate" type="xs:dateTime"/>
                                <xs:element minOccurs="0" name="datasetId"
type="xs:string"/>
                                <xs:element minOccurs="0" name="description"
type="xs:string"/>
                                <xs:element minOccurs="0" name="hostName"
type="xs:string"/>
                                <xs:element minOccurs="0" name="item" type="xs:string"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
minOccurs="0"
name="lastModified" type="xs:dateTime"/>
                                <xs:element minOccurs="0" name="lastModifiedBy"
type="xs:string"/>

```

```

type="xs:string"/>
    <xs:element minOccurs="0" name="manufacturer"
    <xs:element minOccurs="0" name="model" type="xs:string"/>
    <xs:element minOccurs="0" name="name" type="xs:string"/>
    <xs:element minOccurs="0" name="relationships">
        <xs:complexType>
            <xs:sequence>
                <xs:element maxOccurs="unbounded"
minOccurs="0"
                    name="relationship"
type="tns:ciRelationship"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element minOccurs="0" name="serialNumber"
type="xs:string"/>
    <xs:element minOccurs="0" name="status"
type="xs:string"/>
    <xs:element minOccurs="0" name="submitter"
type="xs:string"/>
    <xs:element minOccurs="0" name="summary"
type="xs:string"/>
    <xs:element minOccurs="0" name="type" type="xs:string"/>
    <xs:element minOccurs="0" name="version"
type="xs:string"/>
    </xs:sequence>
    </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="compliance">
    <xs:sequence>
        <xs:element minOccurs="0" name="policyIdentifier"
type="xs:string"/>
        <xs:element minOccurs="0" name="policyName" type="xs:string"/>
        <xs:element minOccurs="0" name="status" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="ciRelationship">
    <xs:sequence>
        <xs:element minOccurs="0" name="className" type="xs:string"/>
        <xs:element minOccurs="0" name="classNamespace"
type="xs:string"/>
        <xs:element minOccurs="0" name="datasetId" type="xs:string"/>
        <xs:element minOccurs="0" name="identifier" type="xs:string"/>
        <xs:element minOccurs="0" name="name" type="xs:string"/>
        <xs:element minOccurs="0" name="sourceRole" type="xs:string"/>
        <xs:element minOccurs="0" name="targets">
            <xs:complexType>
                <xs:sequence>
                    <xs:element maxOccurs="unbounded" minOccurs="0"
name="target"
                        type="tns:objectReference"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="change">
    <xs:complexContent>
        <xs:extension base="tns:itObject">
            <xs:sequence>

```

```

minOccurs="0"
    <xs:element default="1970-01-01T00:00:00.0-00:00"
        name="actualEnd" type="xs:dateTime"/>
minOccurs="0"
    <xs:element default="1970-01-01T00:00:00.0-00:00"
        name="actualStart" type="xs:dateTime"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="businessJustification"
        type="tns:businessJustification"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="categorization"
        type="tns:categorization"/>
type="xs:dateTime"/>
    <xs:element minOccurs="0" name="company"
        type="tns:company"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="createDate"
        type="xs:dateTime"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="description"
        type="tns:description"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="impact"
        type="tns:impact"/>
minOccurs="0"
    <xs:element default="1970-01-01T00:00:00.0-00:00"
        name="lastModified" type="xs:dateTime"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="lastModifiedBy"
        type="tns:lastModifiedBy"/>
minOccurs="0" name="log"
    <xs:element minOccurs="0" name="logs">
        <xs:complexType>
            <xs:sequence>
                <xs:element maxOccurs="unbounded"
                    name="log" type="tns:objectReference"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
type="xs:string"/>
    <xs:element minOccurs="0" name="priority"
        type="tns:priority"/>
type="tns:product"/>
    <xs:element minOccurs="0" name="product"
        type="tns:product"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="reason"
        type="tns:reason"/>
minOccurs="0"
    <xs:element minOccurs="0" name="relationships">
        <xs:complexType>
            <xs:sequence>
                <xs:element maxOccurs="unbounded"
                    name="relationship" type="tns:relationship"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
type="tns:objectReference"/>
    <xs:element minOccurs="0" name="requester"
        type="tns:objectReference"/>
type="tns:contact"/>
    <xs:element minOccurs="0" name="requester"
        type="tns:contact"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="riskLevel"
        type="tns:riskLevel"/>
minOccurs="0"
    <xs:element default="1970-01-01T00:00:00.0-00:00"
        name="scheduledEnd" type="xs:dateTime"/>
minOccurs="0"
    <xs:element default="1970-01-01T00:00:00.0-00:00"
        name="scheduledStart" type="xs:dateTime"/>
type="xs:string"/>
    <xs:element minOccurs="0" name="status"
        type="tns:status"/>
    <xs:element minOccurs="0" name="summary"
        type="tns:summary"/>

```

```

type="xs:string"/>
                                <xs:element minOccurs="0" name="timing"
type="xs:string"/>
                                <xs:element minOccurs="0" name="type" type="xs:string"/>
                                <xs:element minOccurs="0" name="urgency"
type="xs:string"/>
                                </xs:sequence>
                                </xs:extension>
                                </xs:complexContent>
                                </xs:complexType>
                                <xs:complexType name="problem">
                                <xs:complexContent>
                                <xs:extension base="tns:itObject">
                                <xs:sequence>
                                <xs:element minOccurs="0" name="categorization"
                                    type="tns:categorization"/>
                                <xs:element minOccurs="0" name="company"
type="xs:string"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
minOccurs="0"
                                    name="createDate" type="xs:dateTime"/>
                                <xs:element minOccurs="0" name="description"
type="xs:string"/>
                                <xs:element minOccurs="0"
name="externalProblemIdentifier"
                                    type="xs:string"/>
                                <xs:element minOccurs="0" name="impact"
type="xs:string"/>
                                <xs:element minOccurs="0" name="investigationDriver"
type="xs:string"/>
                                <xs:element default="1970-01-01T00:00:00.0-00:00"
minOccurs="0"
                                    name="lastModified" type="xs:dateTime"/>
                                <xs:element minOccurs="0" name="lastModifiedBy"
type="xs:string"/>
                                <xs:element minOccurs="0" name="logs">
                                <xs:complexType>
                                <xs:sequence>
                                <xs:element maxOccurs="unbounded"
minOccurs="0" name="log"
                                    type="tns:objectReference"/>
                                </xs:sequence>
                                </xs:complexType>
                                </xs:element>
                                <xs:element minOccurs="0" name="priority"
type="xs:string"/>
                                <xs:element minOccurs="0" name="product"
type="tns:product"/>
                                <xs:element minOccurs="0" name="relationships">
                                <xs:complexType>
                                <xs:sequence>
                                <xs:element maxOccurs="unbounded"
minOccurs="0"
                                    name="relationship"
type="tns:objectReference"/>
                                </xs:sequence>
                                </xs:complexType>
                                </xs:element>
                                <xs:element minOccurs="0" name="requester"
type="tns:contact"/>
                                <xs:element minOccurs="0" name="rootCause"

```

```

type="xs:string"/>
type="xs:string"/>
type="xs:string"/>
type="xs:string"/>
minOccurs="0"
name="targetResolution" type="xs:dateTime"/>
type="xs:string"/>
type="xs:string"/>
type="xs:string"/>
type="xs:string"/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:complexType name="data">
  <xs:sequence>
    <xs:choice maxOccurs="unbounded" minOccurs="0">
      <xs:element name="string-field" type="tns:stringField"/>
      <xs:element name="date-field" type="tns:dateField"/>
      <xs:element name="number-field" type="tns:numberField"/>
      <xs:element name="diary-list-field"
type="tns:diaryListField"/>
      <xs:element name="complex-field" type="tns:complexType"/>
    </xs:choice>
  </xs:sequence>
</xs:complexType>
<xs:element name="UnsupportedOperationException"
type="tns:UnsupportedOperationException"/>
<xs:complexType name="UnsupportedOperationException">
  <xs:sequence/>
</xs:complexType>
<xs:element name="OperationsException" type="tns:OperationsException"/>
<xs:complexType name="OperationsException">
  <xs:sequence/>
</xs:complexType>
<xs:element name="ObjectNotFoundException"
type="tns:ObjectNotFoundException"/>
<xs:complexType name="ObjectNotFoundException">
  <xs:sequence/>
</xs:complexType>
<xs:element name="NonRecoverableOperationsException"
type="tns:NonRecoverableOperationsException"/>
<xs:complexType name="NonRecoverableOperationsException">
  <xs:sequence/>
</xs:complexType>
</xs:schema>
</wsdl:types>
<wsdl:message name="getResponse">
  <wsdl:part element="tns:getResponse" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="create">
  <wsdl:part element="tns:create" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="clearResponse">
  <wsdl:part element="tns:clearResponse" name="parameters"> </wsdl:part>

```

```

</wsdl:message>
<wsdl:message name="NonRecoverableOperationException">
  <wsdl:part element="tns:NonRecoverableOperationException"
    name="NonRecoverableOperationException"> </wsdl:part>
</wsdl:message>
<wsdl:message name="acknowledgeResponse">
  <wsdl:part element="tns:acknowledgeResponse" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="update">
  <wsdl:part element="tns:update" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="ObjectNotFoundException">
  <wsdl:part element="tns:ObjectNotFoundException"
name="ObjectNotFoundException"
  > </wsdl:part>
</wsdl:message>
<wsdl:message name="acknowledge">
  <wsdl:part element="tns:acknowledge" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="get">
  <wsdl:part element="tns:get" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="createResponse">
  <wsdl:part element="tns:createResponse" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="findResponse">
  <wsdl:part element="tns:findResponse" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="OperationException">
  <wsdl:part element="tns:OperationException" name="OperationException"> </
wsdl:part>
</wsdl:message>
<wsdl:message name="find">
  <wsdl:part element="tns:find" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="clear">
  <wsdl:part element="tns:clear" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="UnsupportedOperationException">
  <wsdl:part element="tns:UnsupportedOperationException"
name="UnsupportedOperationException"
  </wsdl:part>
</wsdl:message>
<wsdl:message name="updateResponse">
  <wsdl:part element="tns:updateResponse" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:portType name="IEventServiceDestination">
  <wsdl:operation name="clear">
    <wsdl:input message="tns:clear" name="clear"> </wsdl:input>
    <wsdl:output message="tns:clearResponse" name="clearResponse"> </
wsdl:output>
    <wsdl:fault message="tns:ObjectNotFoundException"
name="ObjectNotFoundException"> </wsdl:fault>
    <wsdl:fault message="tns:UnsupportedOperationException"
    name="UnsupportedOperationException"> </wsdl:fault>
    <wsdl:fault message="tns:OperationException"
name="OperationException"> </wsdl:fault>
    <wsdl:fault message="tns:NonRecoverableOperationException"
    name="NonRecoverableOperationException"> </wsdl:fault>
  </wsdl:operation>
  <wsdl:operation name="update">

```

```

        <wsdl:input message="tns:update" name="update"> </wsdl:input>
        <wsdl:output message="tns:updateResponse" name="updateResponse"> </
wsdl:output>
        <wsdl:fault message="tns:ObjectNotFoundException"
name="ObjectNotFoundException"> </wsdl:fault>
        <wsdl:fault message="tns:OperationsException"
name="OperationsException"> </wsdl:fault>
        <wsdl:fault message="tns:NonRecoverableOperationsException"
name="NonRecoverableOperationsException"> </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="acknowledge">
        <wsdl:input message="tns:acknowledge" name="acknowledge"> </wsdl:input>
        <wsdl:output message="tns:acknowledgeResponse"
name="acknowledgeResponse"> </wsdl:output>
        <wsdl:fault message="tns:ObjectNotFoundException"
name="ObjectNotFoundException"> </wsdl:fault>
        <wsdl:fault message="tns:UnsupportedOperationException"
name="UnsupportedOperationException"> </wsdl:fault>
        <wsdl:fault message="tns:OperationsException"
name="OperationsException"> </wsdl:fault>
        <wsdl:fault message="tns:NonRecoverableOperationsException"
name="NonRecoverableOperationsException"> </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="get">
        <wsdl:input message="tns:get" name="get"> </wsdl:input>
        <wsdl:output message="tns:getResponse" name="getResponse"> </wsdl:output>
        <wsdl:fault message="tns:ObjectNotFoundException"
name="ObjectNotFoundException"> </wsdl:fault>
        <wsdl:fault message="tns:UnsupportedOperationException"
name="UnsupportedOperationException"> </wsdl:fault>
        <wsdl:fault message="tns:OperationsException"
name="OperationsException"> </wsdl:fault>
        <wsdl:fault message="tns:NonRecoverableOperationsException"
name="NonRecoverableOperationsException"> </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="find">
        <wsdl:input message="tns:find" name="find"> </wsdl:input>
        <wsdl:output message="tns:findResponse" name="findResponse"> </
wsdl:output>
        <wsdl:fault message="tns:UnsupportedOperationException"
name="UnsupportedOperationException"> </wsdl:fault>
        <wsdl:fault message="tns:OperationsException"
name="OperationsException"> </wsdl:fault>
        <wsdl:fault message="tns:NonRecoverableOperationsException"
name="NonRecoverableOperationsException"> </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="create">
        <wsdl:input message="tns:create" name="create"> </wsdl:input>
        <wsdl:output message="tns:createResponse" name="createResponse"> </
wsdl:output>
        <wsdl:fault message="tns:OperationsException"
name="OperationsException"> </wsdl:fault>
        <wsdl:fault message="tns:NonRecoverableOperationsException"
name="NonRecoverableOperationsException"> </wsdl:fault>
    </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="EventServiceSoapBinding" type="tns:IEventServiceDestination">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/
http"/>
    <wsdl:operation name="clear">
        <soap:operation soapAction="" style="document"/>

```

```
<wsdl:input name="clear">
  <soap:body use="literal"/>
</wsdl:input>
<wsdl:output name="clearResponse">
  <soap:body use="literal"/>
</wsdl:output>
<wsdl:fault name="ObjectNotFoundException">
  <soap:fault name="ObjectNotFoundException" use="literal"/>
</wsdl:fault>
<wsdl:fault name="UnsupportedOperationException">
  <soap:fault name="UnsupportedOperationException" use="literal"/>
</wsdl:fault>
<wsdl:fault name="OperationsException">
  <soap:fault name="OperationsException" use="literal"/>
</wsdl:fault>
<wsdl:fault name="NonRecoverableOperationsException">
  <soap:fault name="NonRecoverableOperationsException" use="literal"/>
</wsdl:fault>
</wsdl:operation>
<wsdl:operation name="update">
  <soap:operation soapAction="" style="document"/>
  <wsdl:input name="update">
    <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="updateResponse">
    <soap:body use="literal"/>
  </wsdl:output>
  <wsdl:fault name="ObjectNotFoundException">
    <soap:fault name="ObjectNotFoundException" use="literal"/>
  </wsdl:fault>
  <wsdl:fault name="OperationsException">
    <soap:fault name="OperationsException" use="literal"/>
  </wsdl:fault>
  <wsdl:fault name="NonRecoverableOperationsException">
    <soap:fault name="NonRecoverableOperationsException" use="literal"/>
  </wsdl:fault>
</wsdl:operation>
<wsdl:operation name="acknowledge">
  <soap:operation soapAction="" style="document"/>
  <wsdl:input name="acknowledge">
    <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="acknowledgeResponse">
    <soap:body use="literal"/>
  </wsdl:output>
  <wsdl:fault name="ObjectNotFoundException">
    <soap:fault name="ObjectNotFoundException" use="literal"/>
  </wsdl:fault>
  <wsdl:fault name="UnsupportedOperationException">
    <soap:fault name="UnsupportedOperationException" use="literal"/>
  </wsdl:fault>
  <wsdl:fault name="OperationsException">
    <soap:fault name="OperationsException" use="literal"/>
  </wsdl:fault>
  <wsdl:fault name="NonRecoverableOperationsException">
    <soap:fault name="NonRecoverableOperationsException" use="literal"/>
  </wsdl:fault>
</wsdl:operation>
<wsdl:operation name="get">
  <soap:operation soapAction="" style="document"/>
  <wsdl:input name="get">
```



```
        <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="getResponse">
        <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="ObjectNotFoundException">
        <soap:fault name="ObjectNotFoundException" use="literal"/>
    </wsdl:fault>
    <wsdl:fault name="UnsupportedOperationException">
        <soap:fault name="UnsupportedOperationException" use="literal"/>
    </wsdl:fault>
    <wsdl:fault name="OperationsException">
        <soap:fault name="OperationsException" use="literal"/>
    </wsdl:fault>
    <wsdl:fault name="NonRecoverableOperationsException">
        <soap:fault name="NonRecoverableOperationsException" use="literal"/>
    </wsdl:fault>
</wsdl:operation>
<wsdl:operation name="find">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="find">
        <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="findResponse">
        <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="UnsupportedOperationException">
        <soap:fault name="UnsupportedOperationException" use="literal"/>
    </wsdl:fault>
    <wsdl:fault name="OperationsException">
        <soap:fault name="OperationsException" use="literal"/>
    </wsdl:fault>
    <wsdl:fault name="NonRecoverableOperationsException">
        <soap:fault name="NonRecoverableOperationsException" use="literal"/>
    </wsdl:fault>
</wsdl:operation>
<wsdl:operation name="create">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="create">
        <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="createResponse">
        <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="OperationsException">
        <soap:fault name="OperationsException" use="literal"/>
    </wsdl:fault>
    <wsdl:fault name="NonRecoverableOperationsException">
        <soap:fault name="NonRecoverableOperationsException" use="literal"/>
    </wsdl:fault>
</wsdl:operation>
</wsdl:binding>
<wsdl:service name="EventService">
    <wsdl:port binding="tns:EventServiceSoapBinding" name="EventServicePort">
        <soap:address location="http://localhost:8080/services/SCOM/
EventService"/>
    </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

D.2 SCOMService WSDL

```

<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions name="SCOMService"
  targetNamespace="http://iwavesoftware.com/services/adapter-framework"
  xmlns:ns1="http://schemas.xmlsoap.org/soap/http"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://iwavesoftware.com/services/adapter-framework"
  xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/
XMLSchema">
  <wsdl:types>
    <xs:schema attributeFormDefault="unqualified" elementFormDefault="unqualified"
      targetNamespace="http://iwavesoftware.com/services/adapter-framework"
      xmlns:tns="http://iwavesoftware.com/services/adapter-framework"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <xs:element name="deregister" type="tns:deregister"/>
      <xs:element name="deregisterResponse" type="tns:deregisterResponse"/>
      <xs:element name="register" type="tns:register"/>
      <xs:element name="registerResponse" type="tns:registerResponse"/>
      <xs:complexType name="deregister">
        <xs:sequence>
          <xs:element minOccurs="0" name="destination" type="xsd:string"/>
          <xs:element minOccurs="0" name="deleteSubscriptions" type="xsd:string"/>
        </xs:sequence>
      </xs:complexType>
      <xs:complexType name="deregisterResponse">
        <xs:sequence/>
      </xs:complexType>
      <xs:complexType name="register">
        <xs:sequence>
          <xs:element minOccurs="0" name="destination" type="xsd:string"/>
        </xs:sequence>
      </xs:complexType>
      <xs:complexType name="registerResponse">
        <xs:sequence/>
      </xs:complexType>
      <xs:element name="OperationsException" type="tns:OperationsException"/>
      <xs:complexType name="OperationsException">
        <xs:sequence/>
      </xs:complexType>
      <xs:element name="NonRecoverableOperationsException"
        type="tns:NonRecoverableOperationsException"/>
      <xs:complexType name="NonRecoverableOperationsException">
        <xs:sequence/>
      </xs:complexType>
    </xs:schema>
  </wsdl:types>
  <wsdl:message name="OperationsException">
    <wsdl:part element="tns:OperationsException" name="OperationsException"> </
wsdl:part>
  </wsdl:message>
  <wsdl:message name="registerResponse">
    <wsdl:part element="tns:registerResponse" name="parameters"> </wsdl:part>
  </wsdl:message>
  <wsdl:message name="NonRecoverableOperationsException">
    <wsdl:part element="tns:NonRecoverableOperationsException"
      name="NonRecoverableOperationsException"> </wsdl:part>
  </wsdl:message>
  <wsdl:message name="deregister">

```

```
<wsdl:part element="tns:deregister" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="register">
  <wsdl:part element="tns:register" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:message name="deregisterResponse">
  <wsdl:part element="tns:deregisterResponse" name="parameters"> </wsdl:part>
</wsdl:message>
<wsdl:portType name="ISCOMService">
  <wsdl:operation name="deregister">
    <wsdl:input message="tns:deregister" name="deregister"> </wsdl:input>
    <wsdl:output message="tns:deregisterResponse" name="deregisterResponse"> </
wsdl:output>
    <wsdl:fault message="tns:OperationsException" name="OperationsException"> </
wsdl:fault>
    <wsdl:fault message="tns:NonRecoverableOperationsException"
      name="NonRecoverableOperationsException"> </wsdl:fault>
  </wsdl:operation>
  <wsdl:operation name="register">
    <wsdl:input message="tns:register" name="register"> </wsdl:input>
    <wsdl:output message="tns:registerResponse" name="registerResponse"> </
wsdl:output>
    <wsdl:fault message="tns:OperationsException" name="OperationsException"> </
wsdl:fault>
    <wsdl:fault message="tns:NonRecoverableOperationsException"
      name="NonRecoverableOperationsException"> </wsdl:fault>
  </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="SCOMServiceSoapBinding" type="tns:ISCOMService">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="deregister">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="deregister">
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="deregisterResponse">
      <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="OperationsException">
      <soap:fault name="OperationsException" use="literal"/>
    </wsdl:fault>
    <wsdl:fault name="NonRecoverableOperationsException">
      <soap:fault name="NonRecoverableOperationsException" use="literal"/>
    </wsdl:fault>
  </wsdl:operation>
  <wsdl:operation name="register">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="register">
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="registerResponse">
      <soap:body use="literal"/>
    </wsdl:output>
    <wsdl:fault name="OperationsException">
      <soap:fault name="OperationsException" use="literal"/>
    </wsdl:fault>
    <wsdl:fault name="NonRecoverableOperationsException">
      <soap:fault name="NonRecoverableOperationsException" use="literal"/>
    </wsdl:fault>
  </wsdl:operation>
</wsdl:binding>
```

```
<wsdl:service name="SCOMService">
  <wsdl:port binding="tns:SCOMServiceSoapBinding" name="SCOMServicePort">
    <soap:address location="http://localhost:8080/services/SCOM/SCOMService"/>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

E

Microsoft SCOM 2007 Connector

The Microsoft Systems Center Operations Manager (SCOM) 2007 Connector (version 12.1.0.2.0) integrates Oracle Enterprise Manager with Microsoft SCOM 2007 (including R2) through web services. Using this connector you can create, update or close alerts on SCOM system for any event generated in Enterprise manager, which ensures an active synchronization between SCOM and Enterprise Manager. Events in Enterprise Manager are equivalent to alerts in the SCOM system.

There are two types of SCOM connectors available. You must determine which connector you want to use based on the version of SCOM being used in your environment:

- The SCOM pre R2 Connector supports the RTM and SP1 versions of SCOM 2007.
- The SCOM R2 Connector supports SCOM 2007 R2.

The SCOM 2007 connectors in the Enterprise Manager store are available on the Self Update page for downloading provided the My Oracle Support Preferred Credentials are configured. See [Installing the Microsoft SCOM Event Connector in Enterprise Manager](#) for instructions.

The following topics are presented:

- [Versions Supported by the Microsoft SCOM 2007 Connector](#)
- [SCOM 2007 Installation and Customization](#)
- [Default Templates for Microsoft SCOM 2007](#)

E.1 Versions Supported by the Microsoft SCOM 2007 Connector

The connector supports the following versions of Oracle Enterprise Manager and Microsoft SCOM:

- Oracle Enterprise Manager Cloud Control 12c Release 1.
- Microsoft Systems Center Operations Manager version 2007 (including R2).

You can install the SCOM Agent on Microsoft Windows (2000, 2003, and 2008) platform.

The base Enterprise Manager version number for the Microsoft Systems Center Operations Manager Connector Release 12.1.0.2.0 is Enterprise Manager 12c Release 1 (12.1.0.1) and higher versions.

You can install the Oracle SCOM Agent on Microsoft Windows (2000, 2003, and 2008) platform.

E.2 SCOM 2007 Installation and Customization

The SCOM 2007 and SCOM 2007 R2 connectors require additional customization for full functionality. In addition to the install directions for SCOM 2012 in this user guide, perform the following steps to complete the installation for SCOM 2007 connector instances:

- [Verify Preinstallation Requirements](#)
- [Verify Agent Account Prerequisites](#)
- [Determine Ops Mgr Administrator Groups](#)
- [Add Ops Mgr User Role for Oracle SCOM Agent](#)
- [Install the Alert Creator Management Pack for Microsoft SCOM 2007](#)

E.2.1 Verify Preinstallation Requirements

The following requirements apply to the system where the Oracle SCOM Agent is installed

1. .NET framework 2.0 is installed.
2. .NET framework 3.0 is installed.
3. ASP.NET 2.0 is installed. After .NET framework 2.0 is installed, enter the following command to install ASP.NET 2.0:

```
%SystemRoot%\Microsoft.NET\Framework\v2.0.xxxxx\aspnet_regiis -i
```

4. Internet Information Services (IIS) 5.0 or higher is installed.
5. Operations Manager 2007 Console is installed.
6. ASP.NET 2.0 extensions are enabled in IIS. To enable ASP.NET extensions, perform the following steps:
 - a. Open the IIS Manager and expand the local computer in the left pane.
 - b. Right-click on Web Service Extensions and select **Allow all Web service extensions for a specific application**.
 - c. Select **ASP.NET v2.0.0xxxxx** from the pull-down list, where **xxxxxx** is the version of the .NET framework 2.0 that is installed.
 - d. Click **OK** to enable the ASP.NET extensions.

E.2.2 Verify Agent Account Prerequisites

Before installing the Oracle SCOM Agent, you need to set up an account for the Oracle SCOM Agent to access the SCOM API. The account must satisfy the following requirements:

1. Must be a domain account.
2. Must be used exclusively by the Oracle SCOM Agent.
3. Must have local administrator permissions.
4. Must be a member of a group designated as an Ops Mgr Administrator (See [Determine Ops Mgr Administrator Groups](#) below).

5. Must be a member of an Ops Mgr role that has an Author profile (See [Add Ops Mgr User Role for Oracle SCOM Agent](#) below).

E.2.3 Determine Ops Mgr Administrator Groups

To determine the groups that are designated as an Ops Mgr Administrator, perform the following steps:

1. In the Administration pane of the Ops Mgr 2007 console, select **Administration**, then **Security**, then **User Roles**. The User Roles should be displayed in the center pane.
2. Right-click on **Operations Manager Administrators** and select **Properties**. The General tab lists the groups that have administrative permissions in the User Role member's window. The account the Agent uses must be a member of one of the groups listed here, or you need to add one of its groups to this list.

E.2.4 Add Ops Mgr User Role for Oracle SCOM Agent

To add a new Ops Mgr 2007 user role for the Oracle SCOM Agent, perform the following steps:

1. In the Administration pane of the Ops Mgr 2007 console, select **Administration**, then **Security**, then **User Roles**. Right-click on **User Roles** and select **New User Role**, then **Author**. The Create User Role wizard window appears.
2. Enter the name of the Oracle SCOM Agent in the User Role Name field.
3. Click **Add** to add a user role member. The Select Users or Groups pop-up window appears.
4. Enter the domain user account information in the Enter the object names to select dialog box. Since this is a domain user account, you need to specify the account as `<DOMAIN>\<username>`, where `<DOMAIN>` is the Windows domain where the account was created, and `<username>` is the user name of the account set up for the Oracle SCOM Agent.
5. Click **OK** to add the Oracle SCOM Agent account as a user role member.
6. Click **Next** to go to the Approve Targets page.
7. Select the targets that you want the Oracle SCOM Agent to access. These are the target types for the events that the Oracle SCOM Agent will handle. Typically, you would use the default "All targets are automatically approved, including targets in Management Packs imported in the future."
8. Click **Next** to go to the Approve Groups page.
9. Select the groups that you want the Oracle SCOM Agent to access. You would generally want to use the default of All Groups.
10. Click **Next** to go to the Approve Tasks page.
11. Click **Next** to go to the Approve Views page.
12. Click **Next** to go to the Summary page.
13. Click **Create** to create the Oracle SCOM Agent user role.

E.2.5 Install the Alert Creator Management Pack for Microsoft SCOM 2007

A management pack file named `OracleEnterpriseManager.Alert.Creator.xml` is also included in the Agent/Notification installation zip files. This management pack is required to create alerts in SCOM. Follow the steps below to import the management pack into SCOM.

1. In the Administration pane of the Operations Manager console, select **Administration**, then **Management Packs**.
2. Right-click on **Management Packs** and select **Import Management Packs**. The Select Management Packs to Import window appears.
3. Navigate to the directory where the `OracleEnterpriseManager.Alert.Creator.xml` file is located.
4. Select the **OracleEnterpriseManager.Alert.Creator.xml** file and click **Open**. The Import Management Packs window appears.

Known Issue for SCOM 2007:

Depending on the version of SCOM 2007 that you are running, you may see the following error when you attempt to open the management pack:

```
OracleEnterpriseManager Alert Creator
The OracleEnterpriseManager Alert Creator Management Pack will fail to import
because it depends on the following Management Packs:
System.Library version 6.0.6278.0
Microsoft.SystemCenter.Library version 6.0.6278.0
System.Health.Library version 6.0.6278.0
Microsoft.Windows.Library version 6.0.6278.0
Please add them to the list by clicking on the Add... button and searching in
your machine.
```

If you see this error, you need to use a text editor to change the four management packs referenced in the References section of the management pack file. The version number information must be updated to match the version numbers used in your system.

The References section that you need to edit should look like this:

```
<References>
  <Reference Alias="System">
    <ID>System.Library</ID>
    <Version>6.0.6278.0</Version>
    <PublicKeyToken>1a2b3c4d5e5f</PublicKeyToken>
  </Reference>
  <Reference Alias="SCLibrary">
    <ID>Microsoft.SystemCenter.Library</ID>
    <Version>6.0.6278.0</Version>
    <PublicKeyToken>6f5e4d3c2b1a</PublicKeyToken>
  </Reference>
  <Reference Alias="Health">
    <ID>System.Health.Library</ID>
    <Version>6.0.6278.0</Version>
    <PublicKeyToken>123abc456def</PublicKeyToken>
  </Reference>
  <Reference Alias="Windows">
    <ID>Microsoft.Windows.Library</ID>
```



```
<Version>6.0.6278.0</Version>
<PublicKeyToken>11aa22bb33cc44dd</PublicKeyToken>
</Reference>
</References>
```

5. Click **Import** to import the management pack.
6. Click **Close** after the management pack has been imported

The Agent is now configured to insert alerts into SCOM.

E.3 Default Templates for Microsoft SCOM 2007

This section identifies the default mappings for the `createEvent` and the `updateEvent` operations that are specific to the SCOM 2007 connectors.

[Table E-1](#) lists the XSL files that perform the mappings for the SCOM 2007 connector and provides a summary of each.

Table E-1 XSL Files that Perform SCOM 2007 Mappings

File	Description
<code>createEvent_request_preR2.xsl</code>	Transforms the Oracle Enterprise Manager event data to the Microsoft SCOM 2007 alert format for the <code>createEvent</code> operation for the SCOM 2007 pre-R2 connector.
<code>createEvent_request_R2.xsl</code>	Transforms the Oracle Enterprise Manager event data to the Microsoft SCOM 2007 alert format for the <code>createEvent</code> operation for the SCOM 2007 R2 connector.
<code>updateEvent_request.xsl</code>	Transforms the Oracle Enterprise Manager event data to the Microsoft SCOM 2007 alert format for the <code>updateEvent</code> operation.

E.3.1 Create Event 2007 Template

The Oracle Enterprise Manager Connector Framework invokes the `createEvent` operation whenever an event is generated in Oracle Enterprise Manager and a rule is configured to invoke a SCOM 2007 connector. The appropriate create template is invoked during the process to transform the data from Oracle Enterprise Manager format to SCOM alert format. [Table E-2](#) lists the default field mappings between the Microsoft SCOM alert and the Oracle Enterprise Manager event for `createEvent` operations.

Table E-2 Create Event 2007 Template Mappings

SCOM Field Name	Required	Value
Name	Yes	Set to the event <code>EventName</code> field.
Description	Yes	Set to the formatted contents of the event as specified in Formatted Enterprise Manager Description Contents .

Table E-2 (Cont.) Create Event 2007 Template Mappings

SCOM Field Name	Required	Value
Priority	Yes	Set the priority based on the event priority. See Priority Mapping for details.
Severity	Yes	Set the severity based on the event severity. See Severity Mapping for details.

E.3.2 Update Event 2007 Template

The Oracle Enterprise Manager Connector Framework invokes the `updateEvent` operation whenever an event is generated in Oracle Enterprise Manager and a rule is configured to invoke the SCOM connector.

The `updateEvent_request.xml` template is invoked during the process to transform the data from Oracle Enterprise Manager format to SCOM alert format. [Table E-3](#) lists the default field mappings between the Microsoft SCOM alert and the Oracle Enterprise Manager event.

Table E-3 Update Event 2007 Template Mappings

SCOM Field Name	Required	Value
ID	Yes	Set to the event <code>ExternalEventId</code> field.
Resolution State	Yes	Set to 255 (Closed) if the event severity is Clear. Otherwise, set to 0 (New).
Alert History	No	Set to "Oracle Enterprise Manager cleared alert" if the event severity is Clear. Set to "Oracle Enterprise Manager changed alert severity to warning" if the event severity is Warning. Set to "Oracle Enterprise Manager changed alert severity to critical" if the event severity is Critical. Not set for other severity values.