

HP OpenView Internet Services

SNMP Integration with HP Operations Manager for Windows White Paper

Version: 1.00



Overview	2
Prerequisites	2
For HPOM Management Server	2
For OVIS	2
Configuration	2
Adding OVIS Server as Node in HPOM Management Server	2
Configuring OVIS to Send SNMP Traps	3
OV Message	3
OVIS Management Information Base (MIB)	3
Writing and Deploying SNMP Interceptor Policy on HPOM Management Server	4
To Create a Policy for OV Message SNMP Trap	4
To Create a Policy for OVIS MIB SNMP Trap	7
Troubleshooting	9
Cannot See Messages on the HPOM Console	9

Overview

This Whitepaper describes the process of configuring OpenView Internet Services (OVIS) for sending SNMP Traps to HP Operations Manager (HPOM) for Windows. This document also describes the method of writing SNMP Interceptor policy to display messages on HPOM console.

OVIS and HPOM for Windows can be integrated in the following two ways:

1. Using HP Operations agent: In this type of integration, the HP Operations agent is installed on the OVIS server. Whenever there is a violation, OVIS sends alarms to the Operations agent which in turn forwards it to the HPOM management server.
2. Sending SNMP Traps to HPOM console: In this type of integration, OVIS sends SNMP Traps to the HPOM server whenever a violation occurs. There is no need to install any agent on the OVIS server.

NOTE

You can configure OVIS to send SNMP traps to HP Operations Manager for UNIX in the same way.

Prerequisites

For HPOM Management Server

- HP OpenView Operations for Windows 7.50 with the patch OVOW_00247 or HP Operations Manager for Windows 8.00.
- HP OpenView Operations for UNIX 8.00 and higher.

For OVIS

- OVIS 6.10 with the latest available patch
- OVIS 6.11J with the latest available patch
- OVIS 6.20

NOTE

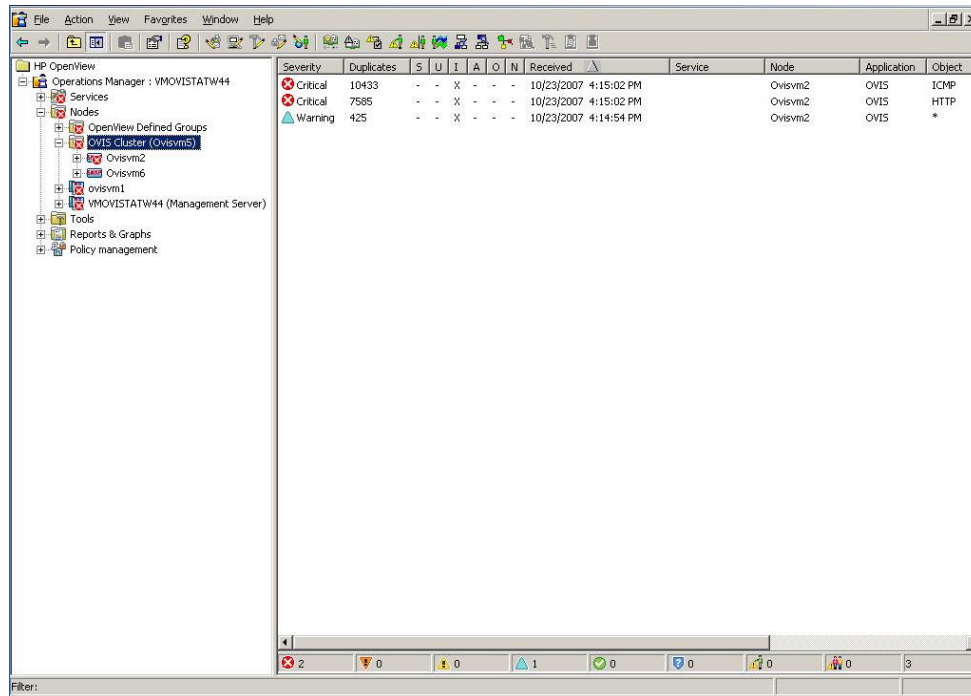
Presently only OVIS 6.10 is recommended for clusters.

Configuration

Adding OVIS Server as Node in HPOM Management Server

If the OVIS server is not added as a node in the HPOM Node Group, add it to the SNMP Node Group.

In case of OVIS cluster setup; add all the OVIS cluster nodes to the SNMP node group. You can also create a new node group and add all the OVIS cluster nodes.



Configuring OVIS to Send SNMP Traps

OVIS can send two types of SNMP (Service Network Management Protocol) traps:

OV Message

You can configure OVIS server to send each alarm event as a general SNMP trap. Any program registered to receive SNMP traps can receive this message and process it.

OVIS Management Information Base (MIB)

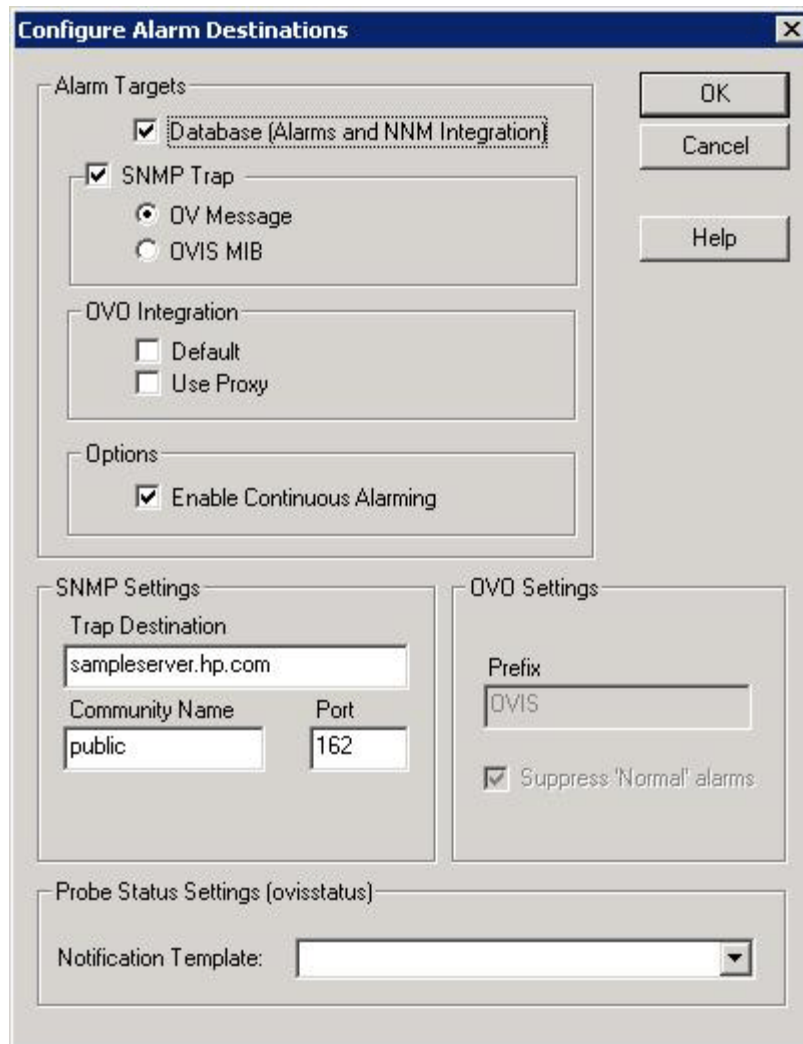
You can configure OVIS server to send an SNMP trap defined in the OVIS MIB. The OVIS MIB is located in the <install dir>\contrib directory of OVIS.

To enable SNMP Traps, go to **File** → **Configure** → **Alarm Destinations** from the OVIS Configuration Manager GUI.

In the Configure Alarm Destinations window, select OV Message or OVIS MIB SNMP Trap depending on your requirement. In the SNMP setting field, mention the name of the HPOM for Windows management server (see the following image).

NOTE

OVIS MIB provides more information compared to the OV Message. OVIS MIB also gives you the link to OVIS Dashboard for viewing target details.

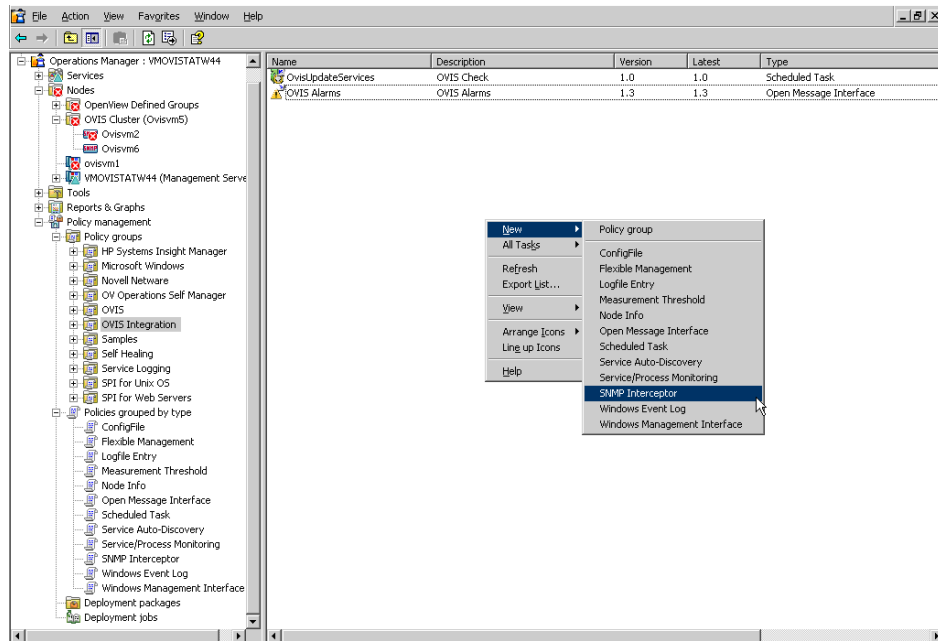


Writing and Deploying SNMP Interceptor Policy on HPOM Management Server

To view the OVIS events in the HPOM console you must create policies. The SNMP Interceptor policy catches the SNMP traps sent to the HPOM server and displays them in the console window.

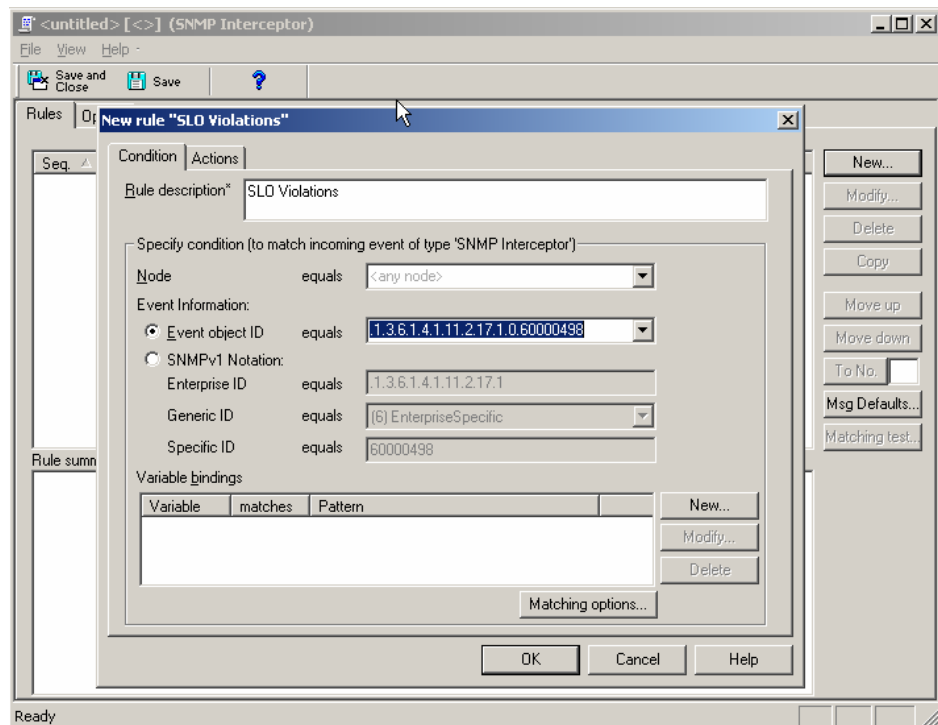
To Create a Policy for OV Message SNMP Trap

1. In the HPOM console, go to **Policy Management** → **Policy Groups**.
2. Create a new policy group OVIS Integration.
 - a) Right-click Policy Groups and select **New** → **Policy group**. A policy group named “New Group” is created.
 - b) Right-click “New Group” and rename it as OVIS Integration.
3. Select the newly created OVIS Integration policy group and right-click in the right pane of the console window.



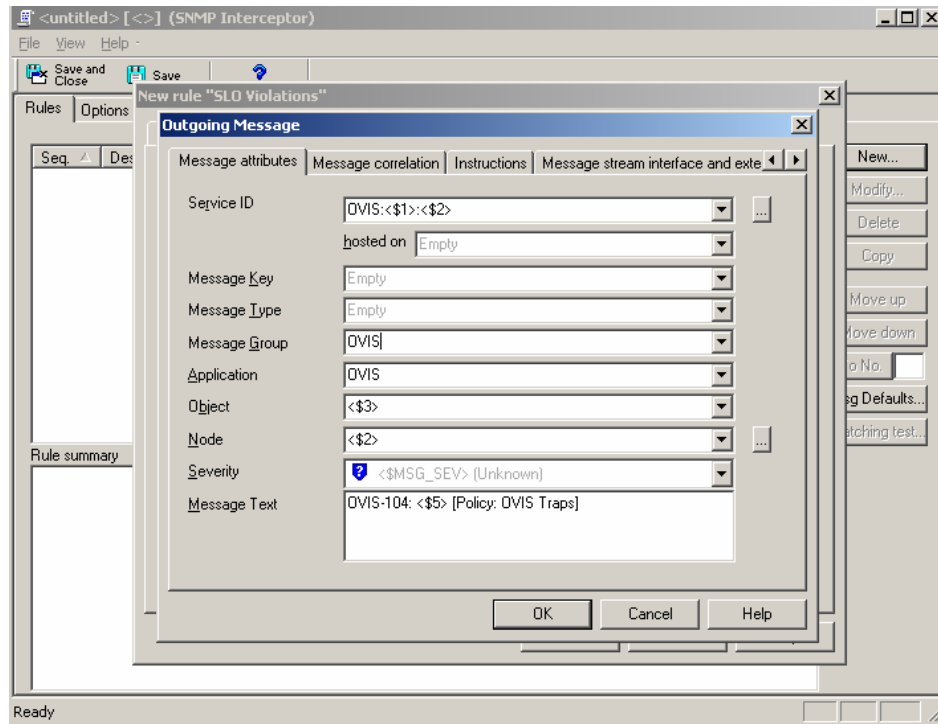
4. Select **New** → **SNMP Interceptor**. The Policy Editor window opens.
5. In the Policy Editor, click **New**. The New Rule window (Rule Editor) opens.
6. Select the **Condition** tab.
7. In the Rule Description field type "SLO Violations." In the Event Object ID field type the event ID for OV Message SNMP Trap.

For "OV Message" SNMP Trap the event ID is 1.1.3.6.1.4.1.11.2.17.1.0.60000498

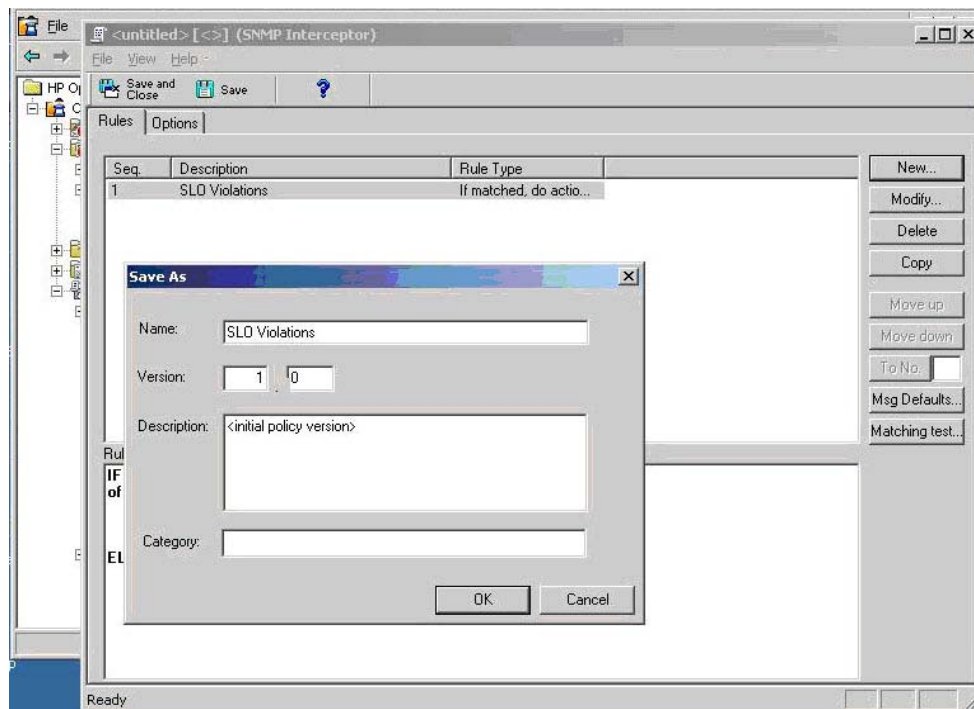


8. Select the **Actions** tab and click on **Message**. The Outgoing Message window opens.
9. Type the Service ID, Application Name, Message Group details.

The messages will now be forwarded to the HPOM console based on the conditions set in **Conditions** Tab.



10. Click **OK**, and then click **Save and Close**. The Save As window opens. In the Name field type "SLO Violations."



11. Deploy the policy on the management server.

- a) Right-click the new policy "SLO Violations" in the policy group OVIS Integration and select **All Tasks → Deploy On**. The Deploy Policies On... window opens.
- b) Select the management server and click **OK**.

NOTE

You can customize the new policy based on your requirements. For more information, see the HPOM documentation.

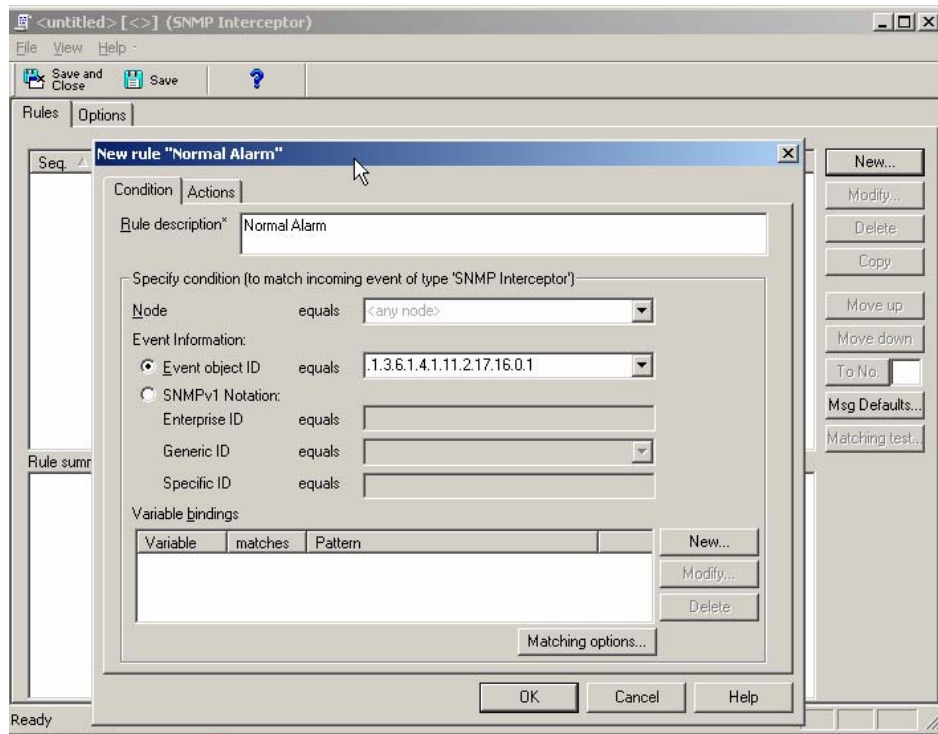
"OV Message" SNMP Trap sends limited information. It does not send a link to the dashboard along with the alarm event.

To Create a Policy for OVIS MIB SNMP Trap

1. In the HPOM console, go to **Policy Management → Policy Groups**.
2. Create a new policy group OVIS Integration.
 - a) Right-click Policy Groups and select **New → Policy group**. A policy group named "New Group" is created.
 - b) Right-click "New Group" and rename it as OVIS Integration.
3. Select the newly created OVIS Integration policy group and right-click in the right pane of the console window.
4. Select **New → SNMP Interceptor**. The Policy Editor window opens.
5. In the Policy Editor, click **New**. The New Rule window (Rule Editor) opens.
6. Select the **Condition** tab.
7. In the Rule Description field type "Normal Alarm" In the Event Object ID field type the event ID for OVIS MIB.

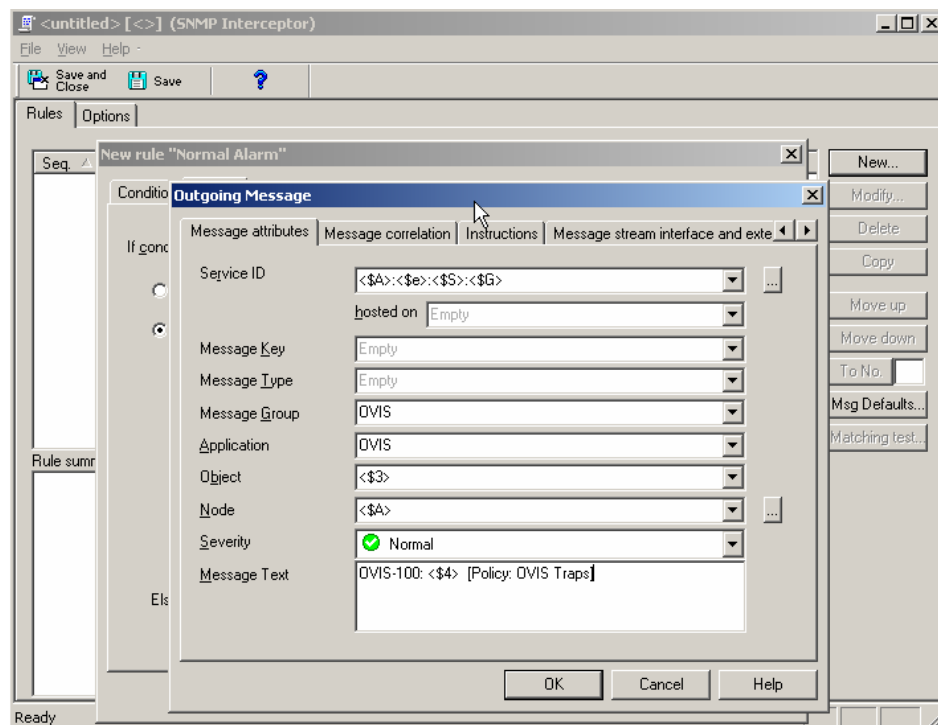
The event IDs for OVIS MIB are:

- Normal Alarm : .1.3.6.1.4.1.11.2.17.16.0.1
- Warning Alarm : .1.3.6.1.4.1.11.2.17.16.0.2
- Minor Alarm : .1.3.6.1.4.1.11.2.17.16.0.3
- Major Alarm: .1.3.6.1.4.1.11.2.17.16.0.4
- Critical Alarm: .1.3.6.1.4.1.11.2.17.16.0.5



8. Select the **Actions** tab and click on **Message**. The Outgoing Message window opens.
9. Type the Service ID, Application Name, Message Group details.

The messages will now be forwarded to the HPOM console based on the conditions set in **Conditions** Tab.



10. Click **OK** to return to the Policy Editor window.
11. Repeat steps 5-10 to create different rules for different severity alarms.
12. Click **Save and Close**. The Save As window opens. In the Name field type "SLO Violations."

13. Deploy the policy on the management server.

- a) Right-click the new policy "SLO Violations" in the policy group OVIS Integration and select **All Tasks → Deploy On**. The Deploy Policies On... window opens.
- b) Select the management server and click **OK**.

NOTE

You can customize the new policy based on your requirements. For more information, see the HPOM documentation.

Troubleshooting

Cannot See Messages on the HPOM Console

Check if the SNMP Trap service is running. If the service is not added in Windows services, install the SNMP Trap service from **Add/Remove-Windows Components → Management and Monitoring Tools**.