

# Managing Dell Client Systems using SNMP with Dell OMCI

*A Dell Technical White Paper*

Dell | Product Group

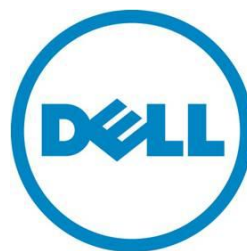
**Authors:**

**Rui An**

**Sahid Md Shaik**

**Sharmad Naik**

**Prasanna J**



**This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.**

© 2012 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

April 2012 | Rev 1.0

## Contents

Introduction .....	4
OMCI and SNMP MIB.....	4
Scope .....	4
Prerequisites .....	4
Download OMCI .....	4
Installing the Dell OMCI.....	4
Using the 10892 MIB file with the Dell OMCI to manage Dell business client systems.....	5
Monitoring alerts (SNMP traps) .....	12
Additional Resources .....	13

## Figures

Figure 1. Using a MIB browser to point to the system you want to monitor.....	5
Figure 2. Loading your MIB file .....	6
Figure 3. Walk retrieves all the data from the client systems .....	7
Figure 4. Navigate to the baseboardGroup folder .....	8
Figure 5. Checking information related to a MIB Group .....	9
Figure 6. Viewing the details of the operatingSystemGroup.....	10
Figure 7. Snapshot of the above supported groups.....	11
Figure 8. Open the Trap receiver to set up the source IP address.....	12
Figure 9. The chassis intrusion event shows up on the Trap Receiver tab .....	13

## Introduction

The Dell OpenManage Client Instrumentation (OMCI) software enables enterprise administrators to access detailed inventory, monitor status, and perform state changes like a remote shutdown on the client system. The intended audience for this white paper is enterprise administrators who plan on managing their clients using Simple Network Management Protocol (SNMP), analogous to their server management strategy.

Starting with OMCI 8.1 you can choose to enable SNMP messaging functionality to manage and monitor Dell client systems.

The Management Information Base (MIB) file is provided in the OMCI installation package for enabling the SNMP feature during installation. OMCI uses the same MIB file within OMSA (OpenManage Server Administrator).

## OMCI and SNMP MIB

### Scope

The purpose of this document is to help you use the OMCI SNMP MIB file to manage Dell client systems. This document is not intended to explain SNMP.

### Prerequisites

Below are the required system components:

- OMCI 8.1 or later installed on a system
- Windows operating system + “SNMP Service Installed and Enabled to run automatically”
- .NET 3.5 sp1 or later
- System or network administrator access
- Any MIB browser

### Download OMCI

Download the OMCI version 8.1 or later from <http://www.dell.com>.

### Installing the Dell OMCI

1. Install the Dell OMCI using the Dell Update Package (DUP).
2. Double-click the Dell OMCI 8.1 or a later version.
3. Click **Install > Next**.
4. In the License Agreement window, select **I accept the terms in the license agreement**.
5. Click **Next**.
6. In the Setup Type window, for installation type, select **Custom**, and then select **Enable SNMP**.

Note: Standard-based instrumentation is selected by default.

7. Click **Next**, and then **Install**.

The Dell OMCI with SNMP option is installed successfully on the system.

Note: Use the CLI command below to install OMCI with the SNMP option enabled.

```
<DUPNAME> /passthrough ADDLOCAL=Core,Hapi,EnableSNMP /qn
```

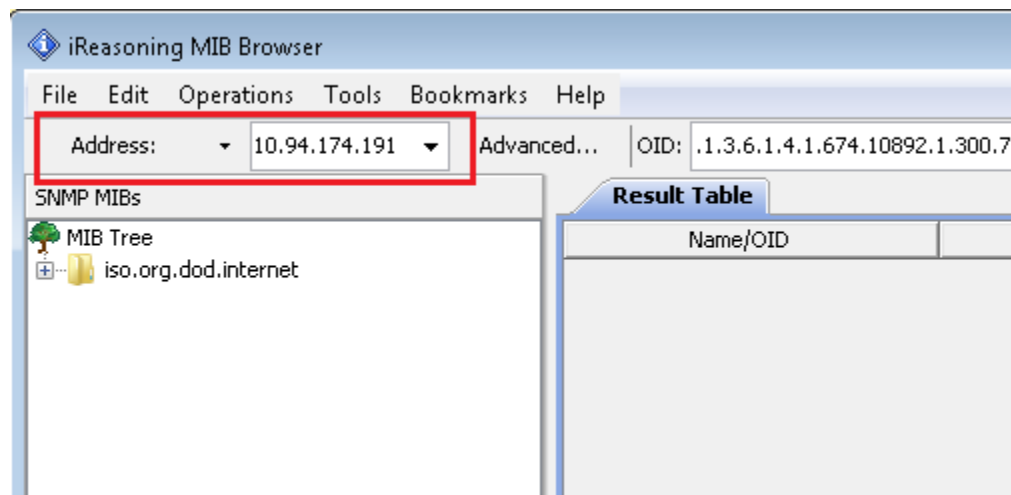
For more information on Installation, use the link:

<http://support.dell.com/support/edocs/software/smcliins/>

## Using the 10892 MIB file with the Dell OMCI to manage Dell business client systems

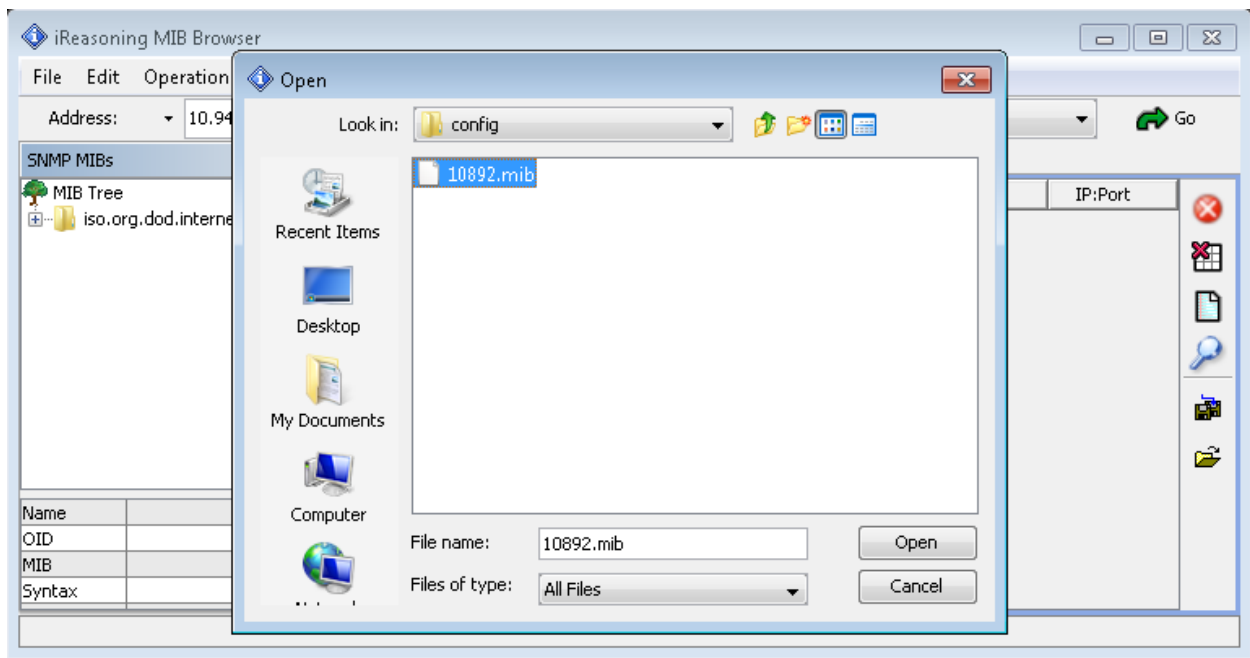
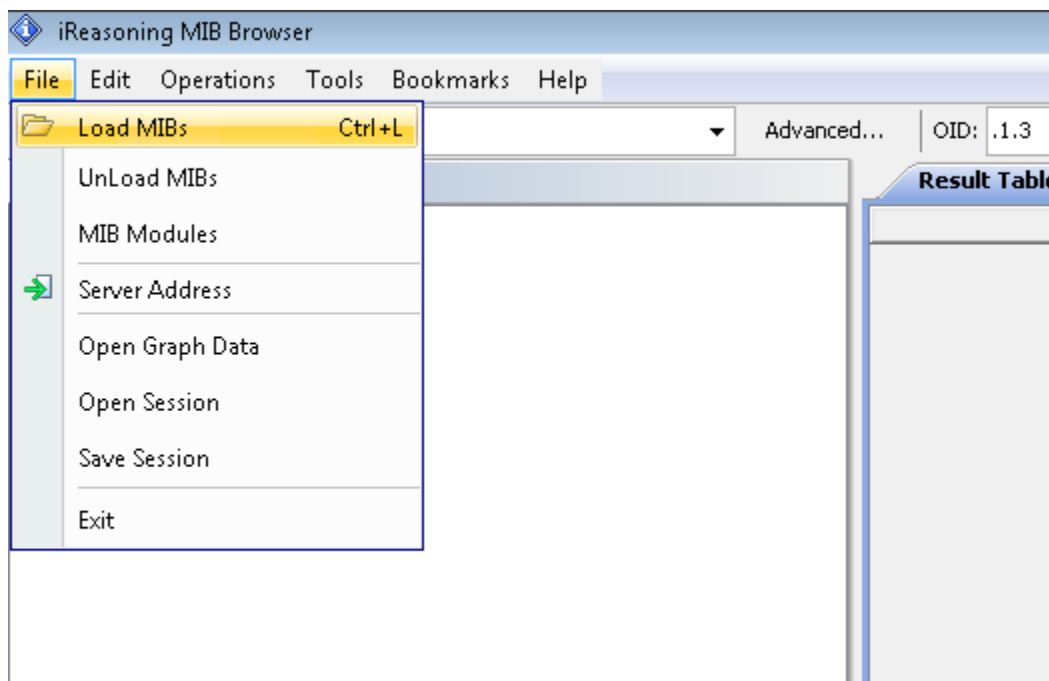
1. Enable the SNMP service. If you want to use SNMP remotely, you need to enable the SNMP service on both client and console systems.
2. Download and install a MIB browser; for example:
  - iReasoning
  - MG-SOFT
3. Launch the MIB browser and provide the IP address of the system that you want monitor.

Figure 1. Using a MIB browser to point to the system you want to monitor



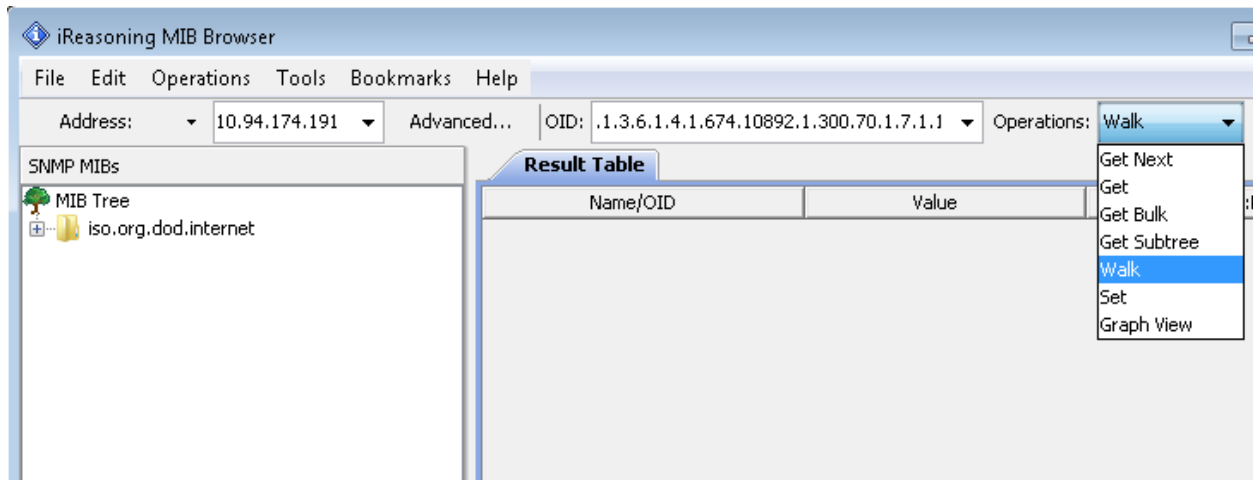
4. Load the 10892.mib file from where you saved it. If you use the same system to monitor, you can find this file under <OMCI Installed Location>\Dell\SysMgt\omsa\config.

Figure 2. Loading your MIB file



5. In the Operations drop-down list, select **Walk**. Walk retrieves all the data from the client systems using definitions in the MIB file.

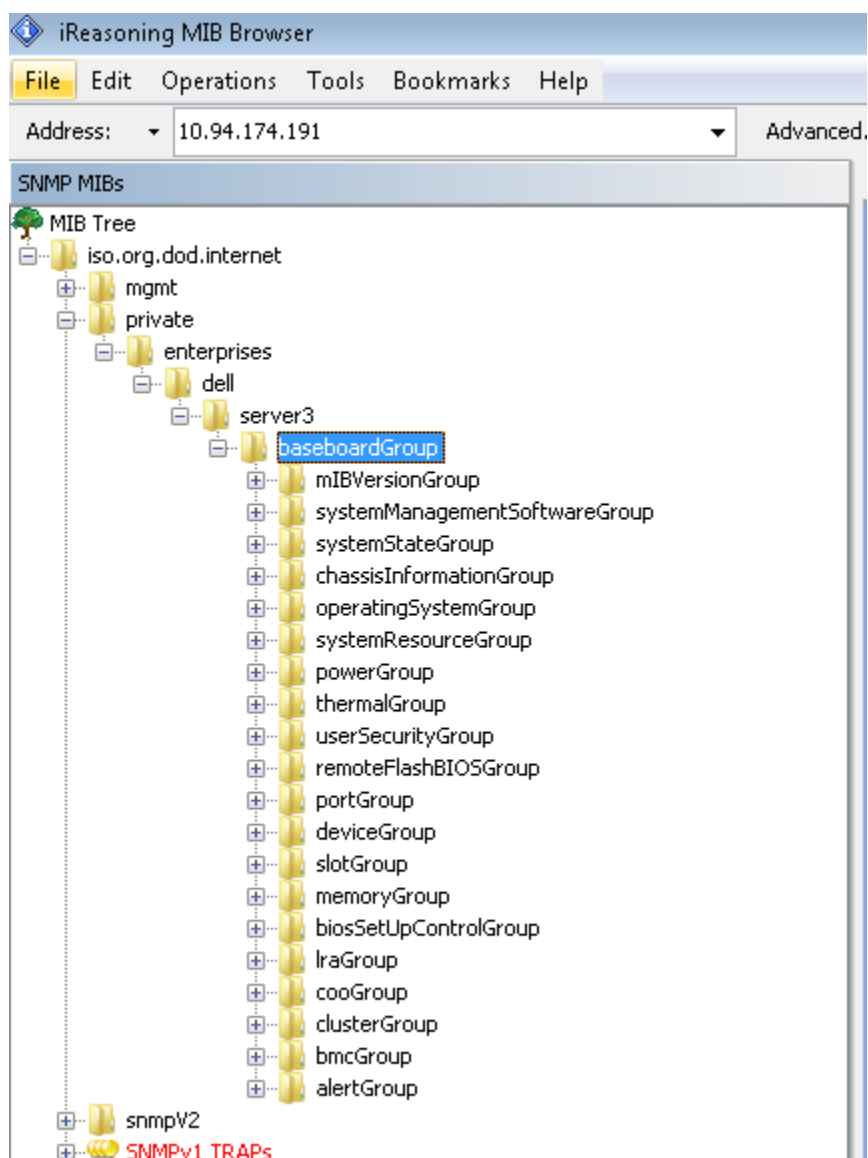
Figure 3. Walk retrieves all the data from the client systems



6. Expand the MIB tree and navigate down to dell > server3 > baseboardGroup.

Note: The Dell OMCI currently employs an Object Identifier (OID) that is traditionally used as a Dell server OID. Consoles may identify systems as servers instead of workstations, notebooks, or desktops collectively as *clients*.

Figure 4. Navigate to the baseboardGroup folder



The data is defined inside those groups.

Note: There is detail definition on each field within Group > Table > Name/OIDs in the *Dell Client SNMP Reference Guide*.

7. Click on each of the variables belonging to groups like **mIBVersionGroup** and perform **SNMP Get** operation to retrieve.

**mIBVersionGroup:**



Figure 5. Checking information related to a MIB Group

The screenshot shows the iReasoning MIB Browser interface. The top menu bar includes File, Edit, Operations, Tools, Bookmarks, and Help. The Address field is set to 10.94.174.191, and the OID field is set to 1.3.6.1.4.1.674.10892.1.2000.10.1.11.1.2. The left pane displays the SNMP MIBs tree, with the following structure:

- mibc
  - private
    - enterprises
      - dell
        - server3
          - baseboardGroup
            - mIBVersionGroup
              - mIBMajorVersionNumber (selected)
              - mIBMinorVersionNumber
              - mIBMaintenanceVersion
            - systemManagementSoftwareGroup
            - systemStateGroup
            - chassisInformationGroup
            - operatingSystemGroup
            - systemResourceGroup
            - powerGroup
            - thermalGroup
            - userSecurityGroup
            - remoteFlashBIOSGroup
            - portGroup
            - deviceGroup
            - slotGroup

The right pane displays the Result Table, which lists various MIB objects and their OIDs. The selected object, mIBMajorVersionNumber, is highlighted in the table below:

Name	mIBMajorVersionNumber
OID	.1.3.6.1.4.1.674.10892.1.1.1
MIB	MIB-Dell-10892
Syntax	DellUnsigned8BitRange
Access	read-only
Status	mandatory
DefVal	
Indexes	

Figure 6. Viewing the details of the operatingSystemGroup

The screenshot shows a network management interface with the following components:

- Address:** 10.94.174.191
- Advanced...** (button)
- OID:** .1.3.6.1.4.1.674.10892.1.400.10.1.3 (highlighted with a red box)
- SNMP MIBs:** A tree view on the left showing various MIBs. The **operatingSystemGroup** is expanded, and **operatingSystemStateSettings** is selected (highlighted with a red box).
- Result Table:** A table on the right displaying the details of the selected MIB. The table has three columns: Name/OID, Value, and a third column (likely a description or status).

Name/OID	Value	
cooOptionsState.1.1	enabled (2)	
cooOptionsLeaseInformationIndexReference.1.1	1	
cooOptionsDescriptionName.1.1	Please set the value	
cooMaintenancechassisIndex.1.1	1	
cooMaintenanceIndex.1.1	1	
cooMaintenanceState.1.1	enabled (2)	
cooMaintenanceStartDateName.1.1		
cooMaintenanceEndDateName.1.1		
cooMaintenanceProviderName.1.1	Please set the value	
cooMaintenanceRestrictionsName.1.1	Please set the value	
cooRepairchassisIndex.1.1	1	
cooRepairIndex.1.1	1	
cooRepairState.1.1	enabled (2)	
cooRepairCounter.1.1	0	
cooRepairVendorName.1.1	Please set the value	
cooSupportInformationchassisIndex.1.1	1	
cooSupportInformationIndex.1.1	1	
cooSupportInformationState.1.1	enabled (2)	
cooSupportInformationIsOutsourced.1.1	0	
cooSupportInformationType.1.1	0	
cooSupportInformationHelpDeskName.1.1	Please set the value	
cooSupportInformationFixTypeName.1.1	Please set the value	
cooTroubleTicketchassisIndex.1.1	1	
cooTroubleTicketIndex.1.1	1	
cooTroubleTicketState.1.1	enabled (2)	
cooTroubleTicketSupportInformationIndexReference.1.1	0	
cooTroubleTicketNumberName.1.1	Please set the value	
.1.3.6.1.4.1.674.10892.1.2000.10.1.1.1.1	1	
.1.3.6.1.4.1.674.10892.1.2000.10.1.1.1.2	1	
.1.3.6.1.4.1.674.10892.1.2000.10.1.2.1.1	1	
.1.3.6.1.4.1.674.10892.1.2000.10.1.2.1.2	2	
.1.3.6.1.4.1.674.10892.1.2000.10.1.3.1.1	3	
.1.3.6.1.4.1.674.10892.1.2000.10.1.3.1.2	3	
.1.3.6.1.4.1.674.10892.1.2000.10.1.4.1.1	1	
.1.3.6.1.4.1.674.10892.1.2000.10.1.4.1.2	1	
.1.3.6.1.4.1.674.10892.1.2000.10.1.5.1.1	BANK 0/ChannelA-DIMM0	
.1.3.6.1.4.1.674.10892.1.2000.10.1.5.1.2	BANK 2/ChannelB-DIMM0	

Below the table, a summary box shows:

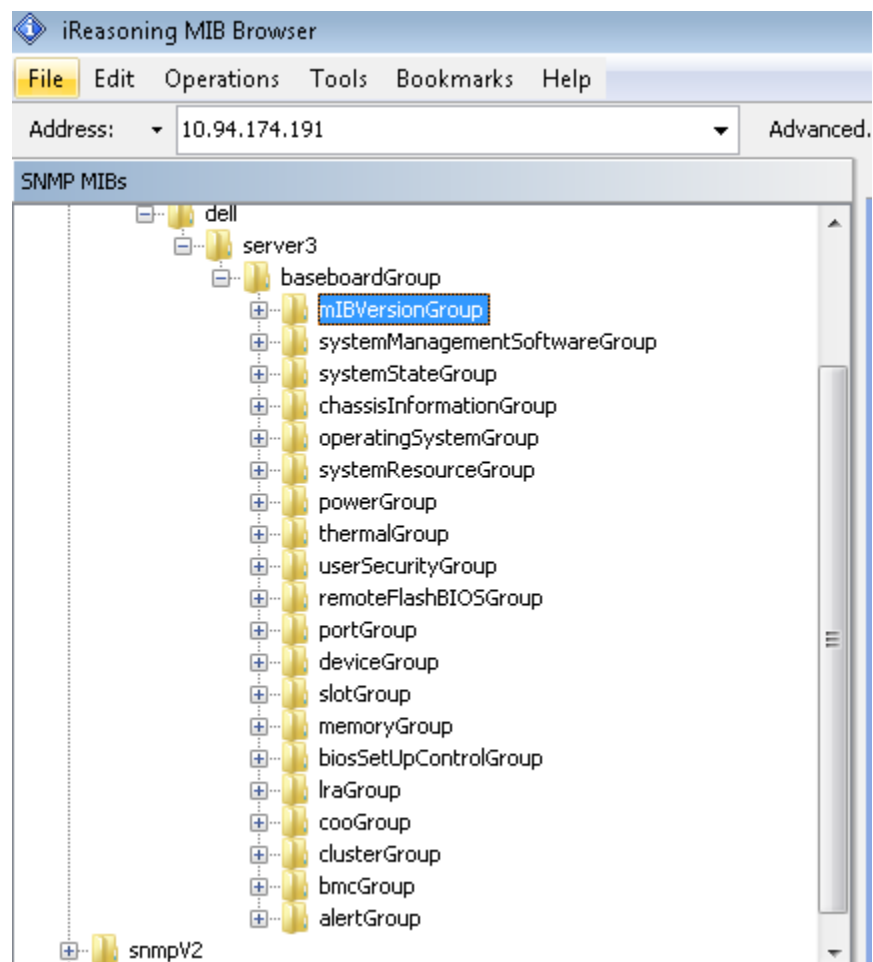
- Name:** operatingSystemStateSettings
- OID:** .1.3.6.1.4.1.674.10892.1.400.10.1.3
- MIB:** MIB-Dell-10892
- Syntax:** INTEGER {unknown(1), enabled(2), notReady...}

The other supported groups are listed here:

- systemManagementSoftwareGroup
- systemStateGroup.
- chassisInformationGroup
  - chassisInformationTable
  - systemBIOSTable
- remoteFlashBIOSGroup
- portGroup
  - pointingPortTable
  - keyboardPortTable
  - processorPortTable
  - memoryDevicePortTable
  - parallelPortTable
  - serialPortTable

- uSBPortTable
- deviceGroup
  - processorDeviceTable
  - memoryDeviceTable
  - pCIDeviceTable
  - networkDeviceTable
- slotGroup

Figure 7. Snapshot of the above supported groups

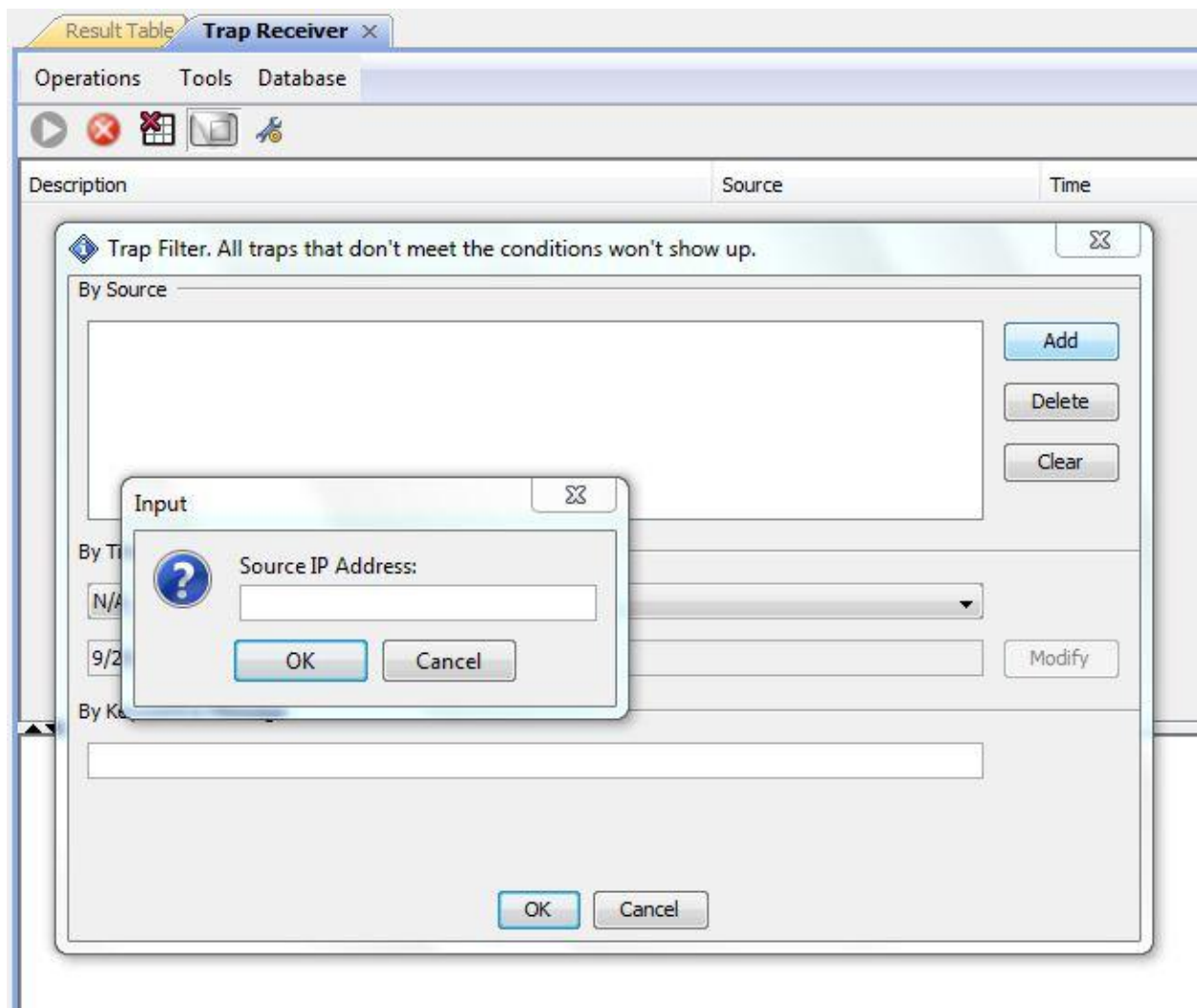


## Monitoring alerts (SNMP traps)

To monitor the chassis intrusion of various client systems in your network, use the following steps:

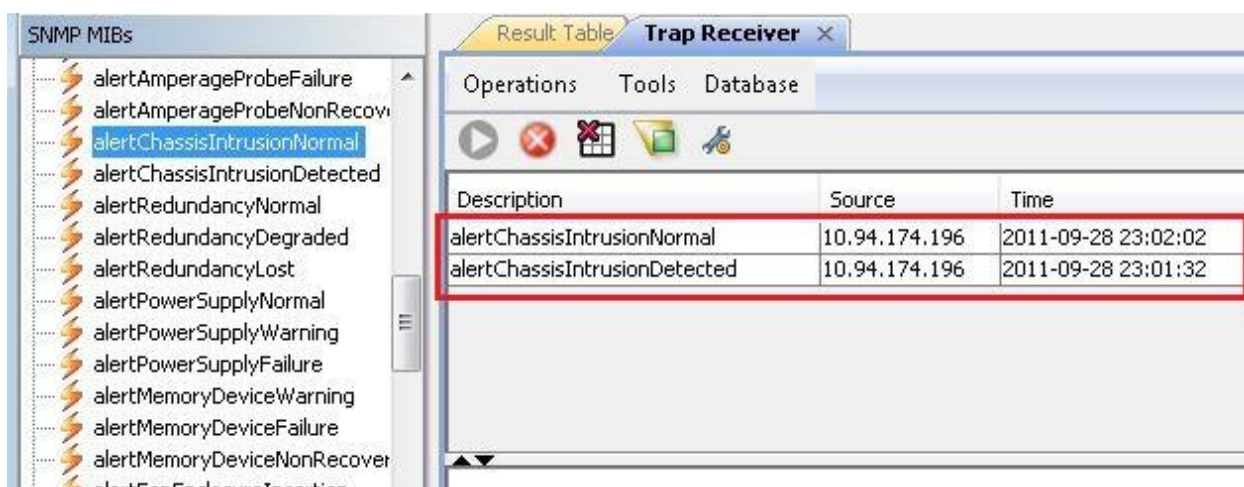
1. Invoke MIB browser and load the 10892 MIB file.
2. From the MIB browser, open the Trap receiver and set up the source IP in the Trap Filter.

Figure 8. Open the Trap receiver to set up the source IP address.



3. If a Chassis Intrusion event is triggered on the system, the event shows up in the Trap Receiver shown below.

Figure 9. The chassis intrusion event shows up on the Trap Receiver tab



Description	Source	Time
alertChassisIntrusionNormal	10.94.174.196	2011-09-28 23:02:02
alertChassisIntrusionDetected	10.94.174.196	2011-09-28 23:01:32

Example of “SNMP” Alert:

Alert from host: 10.94.174.196

Received at: 9/28/2011 23:02:02

Description: alertChassisIntrusionDetected

Note: There are also other alerts available in this MIB but most of them do not generate events because there is no support in the current Precision hardware and BIOS.

## Additional Resources

- To enable SNMP Service on a system, use the Microsoft knowledge base article: <http://support.microsoft.com/kb/324263>
- Use the *SNMP Reference Guide for Client Systems* <http://support.dell.com/>
- Additional information is available from the following sources: <http://en.community.dell.com/techcenter/systems-management/w/wiki/1773.aspx>