Monitoring Cisco Standalone C-Series Servers using SNMP and iReasoning MIB Browser

September 2013

Jeff Foster (TME)
Cisco Systems

Section #1: Cisco Standalone C-Series Monitoring Overview:

Cisco Standalone C-Series servers support many communication channels including SNMP. Using SNMP communication we are able to get/read the information from the C-Series Integrated Management Controlled (IMC) – the system baseboard management controller. Additionally, the Cisco IMC can be configured to generate SNMP notifications (traps/informs) as events occur.

Cisco IMC generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap, and the initiating system cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response PDU (Protocol Data Unit). If the IMC does not receive the PDU, it can send the inform request again.

As part of this SNMP implementation, the Cisco IMC supports all three versions of SNMP i.e. SNMPv1, SNMPv2c and SNMPv3. Both SNMPv3 and SNMPv2c use a community-based form of security. We can perform SNMP get, get next, getbulk and SNMP walk on these systems. Note: SNMP v3 requires that the IMC is running v1.5 or later firmware.

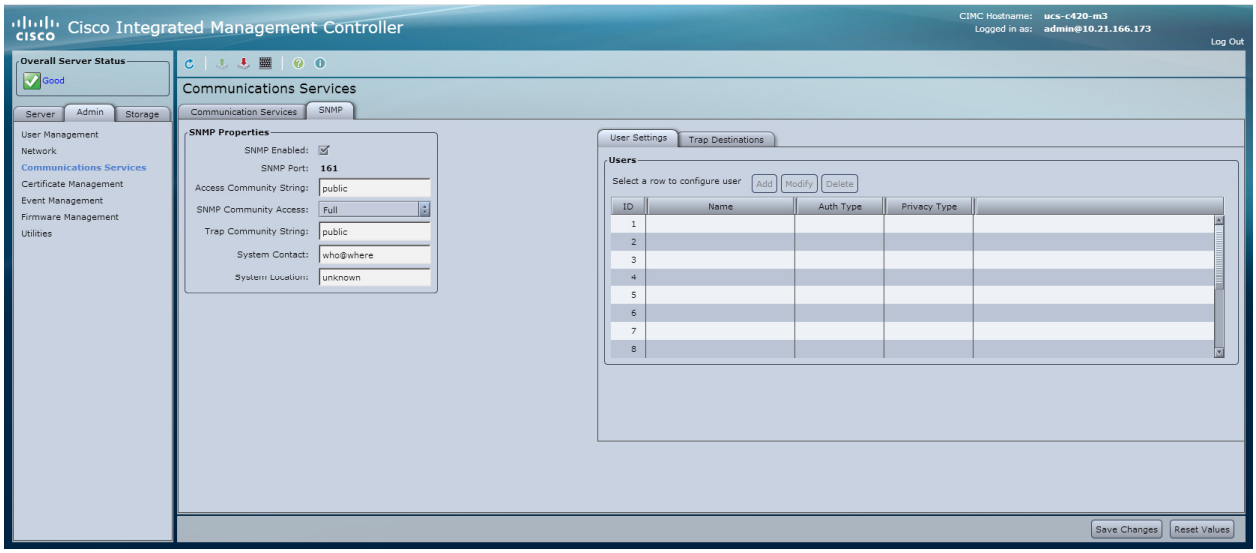
To perform any SNMP operation(s), we need to configure SNMP on the target systems. (Default SNMP is disabled on the IMC). Directions for enabling SNMP are available in Section #2.

Section #2: Configuring SNMP on Standalone C-Series Servers

SNMP Configuration Steps through GUI (WebUI):

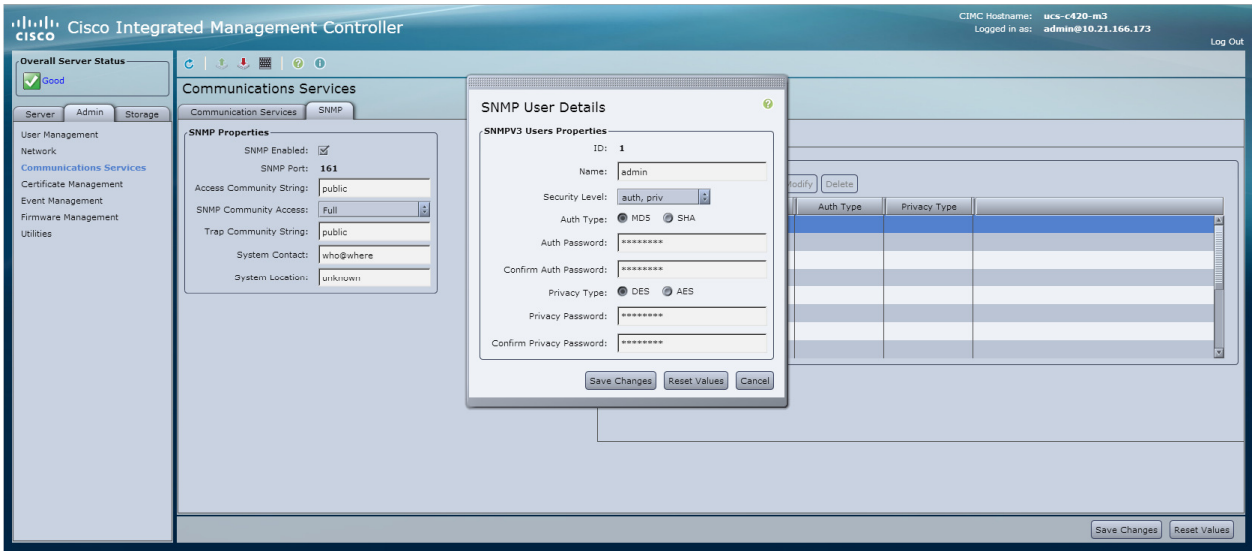
Perform the following steps in order to configure the C-Series SNMP services:

1. Open the system WebUI:
2. Select **Admin** tab and **Communication Services** page.
3. Select the **SNMP** tab in the main window:
4. Enable SNMP admin state. (Default SNMP is disabled)
5. Configure the SNMP Access/Trap community strings and select community access level from the drop-down box. After providing necessary inputs save the changes to be effective.



Configure SNMP Users (SNMPv3):

SNMPv3 supports user authentication and can be configured for up to 15 users on the Admin → Communication Services → SNMP Page.



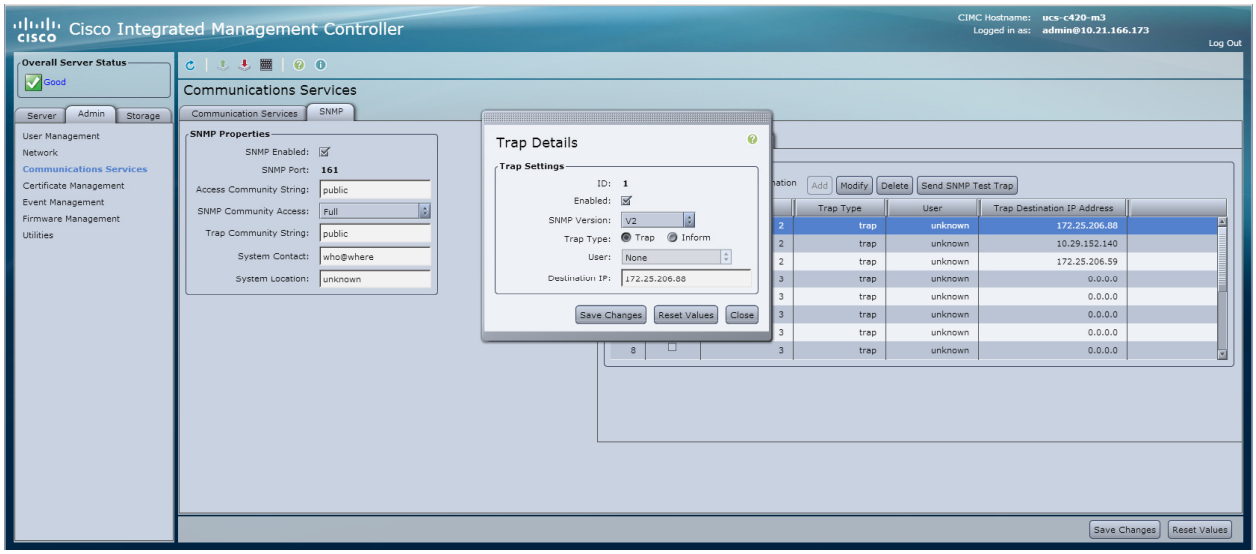
1. Select the user to be configured and then the ‘Add’’ button
2. Provide Name and Security Level along with passwords (as appropriate).

Note: Available Security Levels include “no auth, no priv”, “auth, no priv” and “auth/priv”

Configure Trap Destinations:

The Cisco IMC also supports configuration of up to 15 trap destinations. Trap destinations can be configured from the on the Admin → Communication Services → SNMP Page.

1. Select the Trap Destinations tab (located on the right side of the task pane)
2. Select a trap destination (SIM Server) line and then the ‘Add’ button
3. Provide necessary configuration details including: (Save Changes when complete)
    A. Enable
    B. SNMP Version
    C. Trap Type
    D. User (SNMPv3)
    E. Destination IP
4. Repeat as necessary and ensure that traps are being sent to the SIM Server IP.
5. To verify connectivity in later stages of the configuration, this configuration window allows you to send test traps.



User documentation for configuring communication Services in IMC v1.5 is available here: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.5/b_Cisco_UCS_C-series_GUI_Configuration_Guide.151_chapter_01010.html

Cisco IMC CLI Configuration:

Open CLI session for the IMC using proper credentials. And follow the below mentioned commands to configure SNMP. Inputs used here are to demonstrate only. Provide inputs as per your need/choice.

```
Server# scope snmp
Server /snmp # set enabled yes
Server /snmp *# commit
Server /snmp # set community-str cimcpublic
Server /snmp # set community-access Full
Server /snmp # set trap-community-str public
Server /snmp *# set sys-contact "User Name <username@example.com>"
Server /snmp *# set sys-location "San Jose, California"
Server /snmp *# commit
```

Configure Trap receiver to receive SNMP traps from Cisco IMC using CLI:

```
Server# scope snmp
Server /snmp # Scope trap-destinations 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set version 2
Server /snmp/trap-destination *# set type inform
Server /snmp/trap-destination *# set user user1
Server /snmp/trap-destination *# set v4-addr 192.2.3.4
Server /snmp/trap-destination *# commit
```

Configure SNMPv3 Users using CLI:

If you wish to use SNMPv3, you need to create SNMPv3 User in IMC to enable SNMPv3 communication.

Here is the procedure to created SNMPv3 user in CLI, Below example enables SNMP, creates an SNMPv3 user named snmp-user, specifies the use of MD5 authentication, sets the password and privacy password, and commits the transaction:

```
Server# scope snmp
Server /snmp # scope v3users 2
Server /snmp/v3users # set v3add yes
Server /snmp/v3users *# set v3security-name ucsSNMPV3user
Server /snmp/v3users *# set v3security-level authpriv
Server /snmp/v3users *# set v3proto SHA
Server /snmp/v3users *# set v3auth-key
Please enter v3auth-key:ex4mp1ek3y
Please confirm v3auth-key:ex4mp1ek3y
Server /snmp/v3users *# set v3priv-proto AES
Server /snmp/v3users *# set v3priv-auth-key
Please enter v3priv-auth-key:!1@2#3$4%5^6&7*8
Please confirm v3priv-auth-key:!1@2#3$4%5^6&7*8
Server /snmp/v3users *# commit
```

Note:

Refer to corresponding Cisco IMC CLI Configuration Guide. The v1.5 documentation is available here:
http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/cli/config/guide/1.5/b_Cisco_UCS_C-series_CLI_Configuration_Guide_151_chapter_01010.html#d45101e722a1635.

Section #3: Cisco Standalone C-Series MIB Overview:

Cisco UCS MIB files are a set of objects that are private extensions to the IETF standard MIB II. If your NMS cannot get requested information from a Standalone C-Series server or Cisco UCS, then the MIB that allows that specific data collection might be missing. Typically, if an NMS cannot retrieve a particular MIB variable, either the NMS does not recognize that MIB variable, or the agent does not support the MIB variable. If the NMS does not recognize a specific MIB variable, you might need to load the MIB into the NMS, usually with a MIB compiler. This is the case HP SIM and in Section #5 we will review the process of using the SIM MIB Compiler to Compile the required Cisco MIBs.

Prerequisite MIBS:
The MIBs in this section are required for all use cases and need to be loaded before other Cisco MIBs are loaded. You should load the MIBs in the order listed to eliminate most of the load-order issues.

- SNMPv2-SMI.my

- SNMPv2-TC.my
- SNMP-FRAMEWORK-MIB.my
- RFC1213-MIB.my
- IF-MIB.my
- CISCO-SMI.my
- CISCO-ST-TC.my
- ENTITY-MIB.my
- INET-ADDRESS-MIB
- CISCO.TC.my

Below are the MIBs required for Monitoring: (Load in the following order)
- CISCO-UNIFIED-COMPUTING-MIB.my
- CISCO-UNIFIED-COMPUTING-TC-MIB.my
- CISCO-UNIFIED-COMPUTING-FAULT-MIB.my
- CISCO-UNIFIED-COMPUTING-NOTIFS-MIB.my

Traps defined in the NOTIFS-MIB:

cucsFaultActiveNotif: This notification is generated by a Cisco UCS instance whenever a fault is raised. The OID that corresponds to this SNMP trap is .1.3.6.1.4.1.9.9.719.0.1.

cucsFaultClearNotif: This notification is generated by a Cisco UCS instance whenever a fault is cleared. The OID that corresponds to this SNMP trap is .1.3.6.1.4.1.9.9.719.0.2.

A complete list of Standalone C-Series MIBs are available for download here:
ftp://ftp.cisco.com/pub/mibs/supportlists/ucs/ucs-C-supportlist.html

The Standalone C-Series MIB Reference Guide is available here: (Complete Detail)
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.pdf

---

Section #4: Setting up iReasoning MIB Browser:

iReasoning is an intuitive, easy to use MIB Browser and trap receivers that allows administrators to query systems and receive traps without a lot of setup work. iReasoning comes in three variants (Personal Edition, Professional Edition and Enterprise Edition) and can be downloaded from their website here: http://ireasoning.com/mibbrowser.shtml

iReasoning allows customers to load their own MIBs, including MIBs downloaded from the Cisco site linked above. iReasoning can be used to issue SNMP requests that retrieve data from target systems or it can act as a trap receiver and present data received from initiator systems.

Major features highlighted by iReasoning:

- Intuitive GUI
- Complete SNMPv1, v2c and v3 (USM and VACM) support
- Complete SNMPv3 USM support, including HMAC-MD5, HMAC-SHA, CBC-DES, CFB128-AES-128, CFB128-AES-192, CFB128-AES-256 (128-bit, 192-bit and 256-bit AES) algorithms
- Robust and powerful SMIv1/SMIv2 MIB parser
- IPv6 support
- Trap Receiver
- Trap Sender
- Log window to display application log and SNMP packets exchanged between browser and agents
- Table view for MIB tables
- SNMPv3 USM user management (usmUserTable in SNMP-USER-BASED-SM-MIB)
- Performance graph tool for monitoring of numerical OID values
- Ping and traceroute tools
- SNMP Agents Comparison
- Network discovery tool
- Runs on Windows, Mac OS X, Linux and other UNIX platforms

How to use iReasoning MIB Browser to communicate with UCSM:

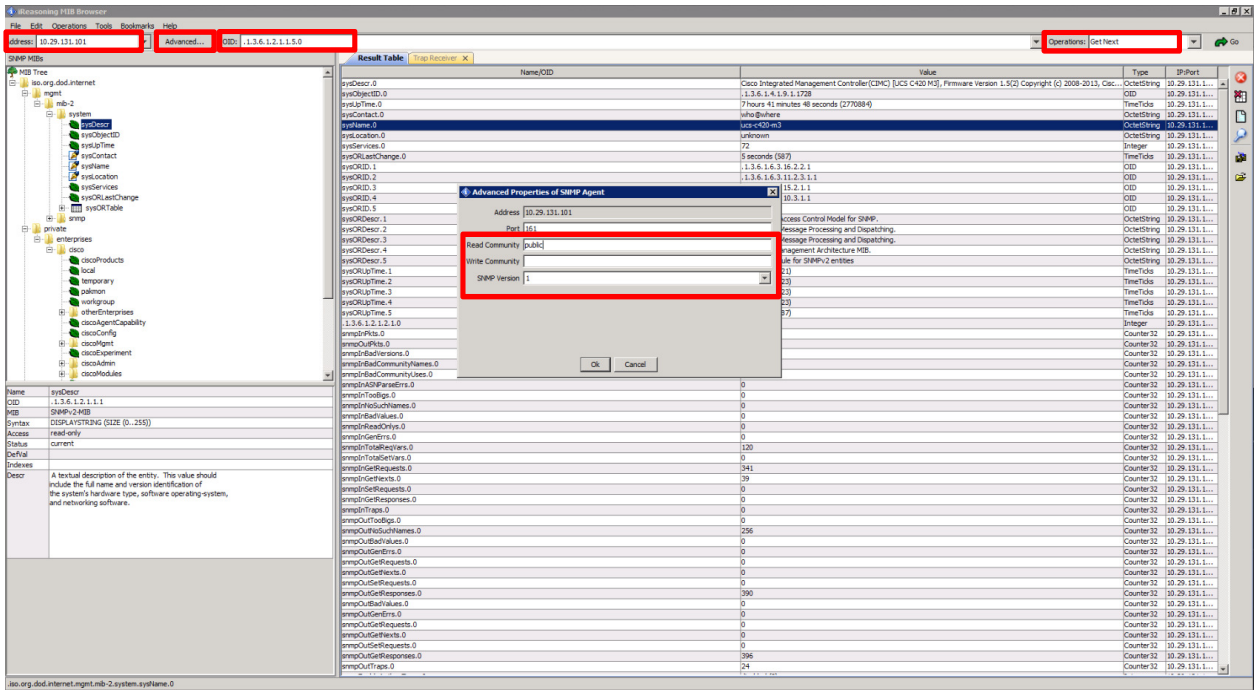
iReasoning MIB Browser should be downloaded from the iReasoning website and installed on a system that can communicate with target systems that will be monitored. Required MIBs can be downloaded from Cisco and loaded into iReasoning using the 'File → Load MIBs' Window.

SNMP should be enabled and configured on the Cisco C-Series systems as outlined in Section #2 of this document using the IP of the system where iReasoning has been installed as the Destination IP in the Cisco IMC.

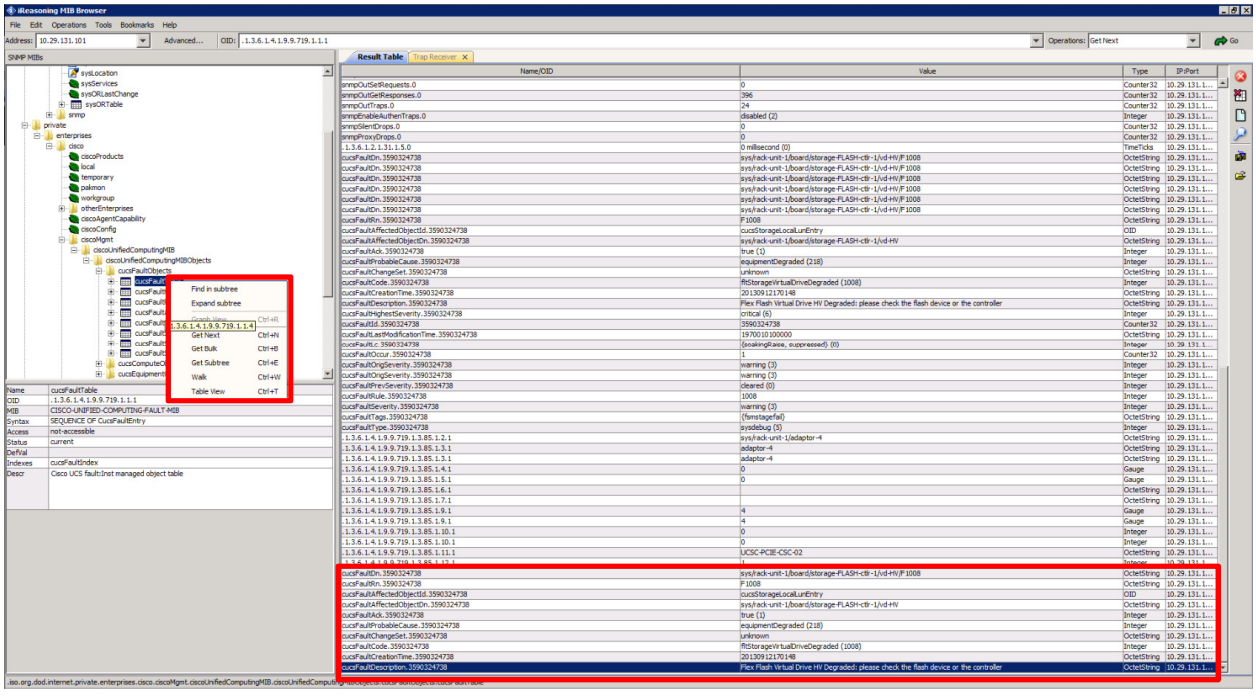
How to Browse MIB Tables and Query target system using iReaonsing:
Launch MIB Browser Window by using Start -> Programs -> iReasoning -> MIB Browser -> MIB Browser

1. After launching the application, you need to specify IP address of the C-Series node on which SNMP operations need to be performed in the address field of iReasoning.
2. Click on 'Advanced…' Properties Button to configure SNMP parameters of the node – SNMP Read community and version. The port number is always fixed to 161.
3. Specify OID in the OID – A Cisco OID follows the following syntax: .1.3.6.1.4.1.9.9.719.x.x.x.
   Use different operations in the MIB Browser to perform SNMP get, get next and get bulk.

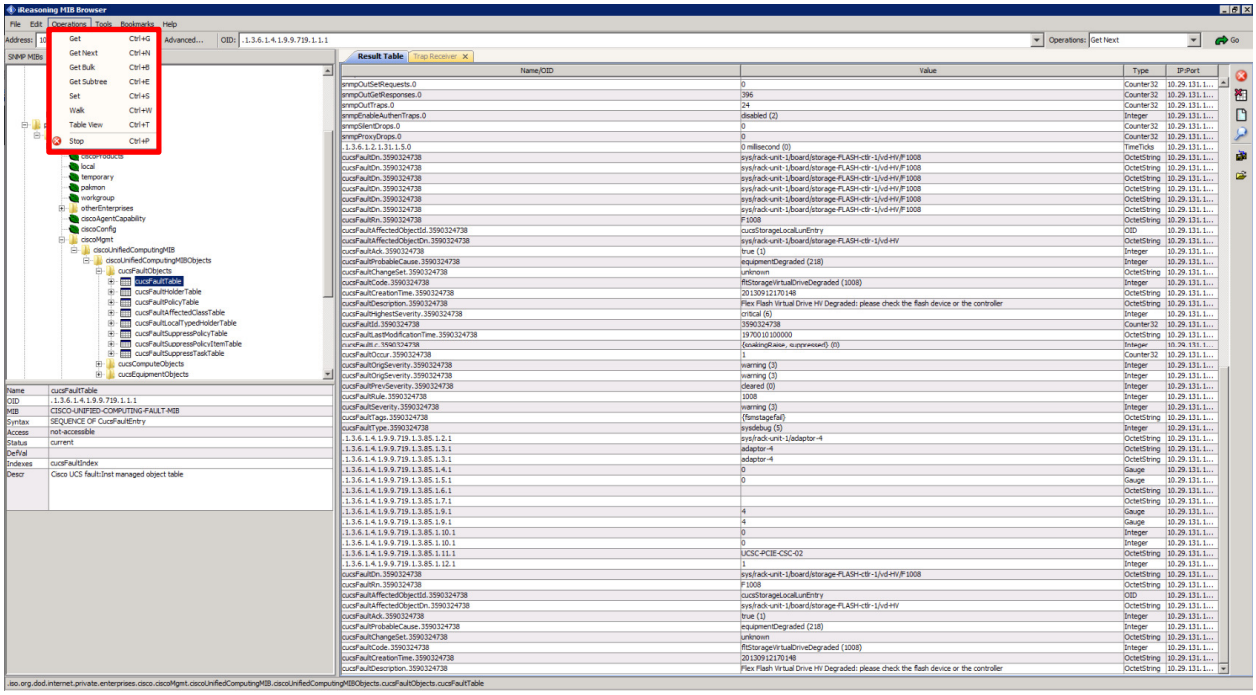
If you have provided a valid OID correctly, the MIB Browser will fetch the current value of this OID using an SNMP Get. A MIB Tree can be walked using 'Get Next', 'Get Bulk', 'Get Subtree' and other options provided in the dropdown box. These options provide a good solution if the OID of the target object you would like to query is unknown.



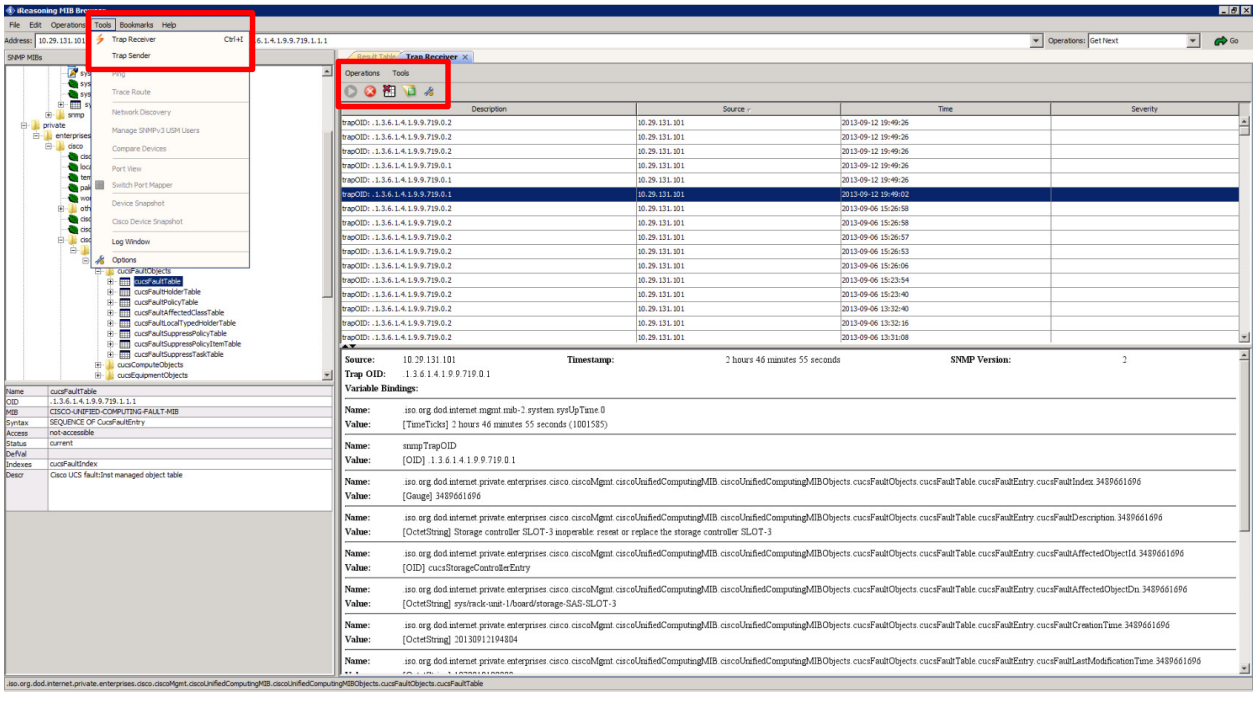
SNMP walk will fetch all OIDs with their current value in the target system. (Refer the provided pictures below)



SNMP Get Bulk can be used to collect the data from a specified MIB table and current OID and property values are returned.



iReasoning can also be used as a trap receiver to capture traps that are sent from the Cisco IMC. To start the Trap Receiver select 'Tools → Trap Receiver' and Click the green 'Start' button.



Traps will be displayed in the main screen with VarBind data populated in the bottom window. See the graphic above for a reference to a fault received using the iReasoning Trap Receiver.