SNMP

Reserved Object Identifier (OID)

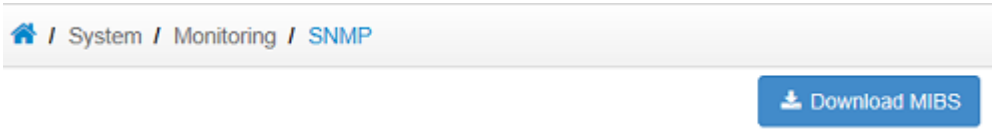
The OID .1.3.6.1.4.1.27880 has been reserved for SBC.

The following are the available Objects. Currently, all attributes are read-only, and are as follows:

.1.3.6.1.4.1.27880 NSC

.1: core
  .1.1: identity
    .1: NSC version string (eg. "1.0.head (git-0cf1d54 2011-01-19 16-36-04 -0500)")
    .2: Core UUID as a string
.2: systemStats
  .1: NSC uptime as SNMP TimerTicks (hundredths of seconds)
  .2: Number of sessions since NSC was started
  .3: Currently active sessions
  .4: Maximum allowed sessions
  .5: Currently active calls
  .6: Current sessions per second
  .7: Maximum allowed sessions per second
  .8: Peak sessions per second
  .9: Peak sessions per second Last Five Minutes
  .10: Peak sessions
  .11: Peak sessions Last Five Minutes

The above MIBS can be downloaded from link at **"System"** -> **"Monitoring"** -> **"SNMP"**:



The following is a sample full list of MIB objects available on a SBC appliance, this includes all Linux MIBs:

Some OIDs may change. We suggest using the MIB and object names, rather than hard-code OIDs in your NMS (eg. MRTG, Cacti etc) configuration.

Once you completed your SBC SNMP setup in this document, you can obtain the same list as above by snmpwalk all the MIBs as follow:

- ssh to your SBC and run the command:

  $ snmpwalk -v 1 -c public localhost .1

As an example, to get the value of ifPromiscuousMode in the IF-MIB:

```
$ snmpwalk -v 1 -c public localhost IF-MIB::ifPromiscuousMode

IF-MIB::ifPromiscuousMode.1 = INTEGER: false(2)
IF-MIB::ifPromiscuousMode.2 = INTEGER: false(2)
IF-MIB::ifPromiscuousMode.3 = INTEGER: false(2)
IF-MIB::ifPromiscuousMode.4 = INTEGER: false(2)
IF-MIB::ifPromiscuousMode.5 = INTEGER: false(2)
```

To translate the MIB object name IF-MIB::ifPromiscuousMode to OID:

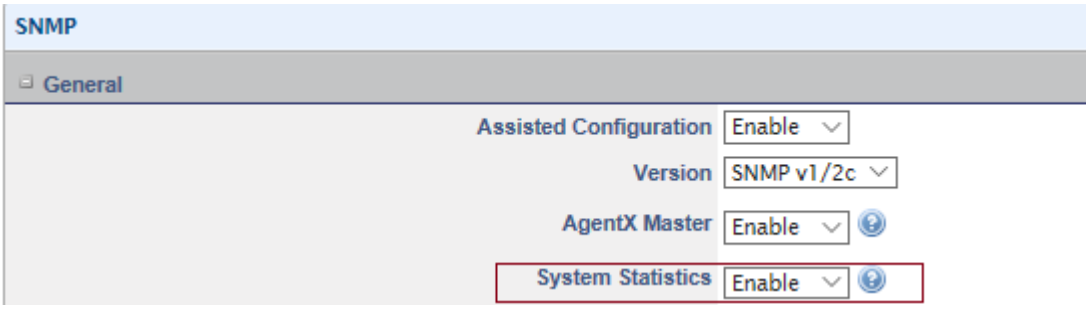
```
$ snmptranslate -On IF-MIB::ifPromiscuousMode
.1.3.6.1.2.1.31.1.1.1.16
```

Configurations

Enabling NSC SNMP module for System Statistics

Go to **"System"** -> **"Monitoring"** -> **"SNMP"**:

Select "**Enable**" in System Statistics dropdown.



AgentX Master should be enabled before enabling System statistics.

The module acts as a Agent X subagent. This means it registers with the existing SNMP server (SNMPD in the SBC) to handle a specific OID, so can monitor your system and NSC with a single daemon.

Configuring SNMPD for AgentX Subagent Support

This is currently a two steps process and must be done in the following order:

1) Expose root of SNMP tree

Most default configurations of SNMPD only allow a restricted view of the whole tree.

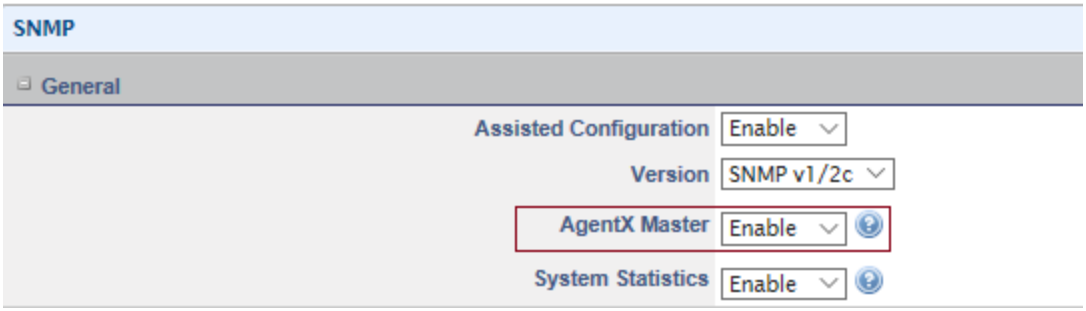
Please follow this Wiki to expose the root of the SNMP tree, this Wiki is also available under the SBC FAQ:

How do you expose a root of the SNMP tree?

2) Enabling AgentX Master from Web UI

Go to **"System"** -> **"Monitoring"** -> **"SNMP"**:

Select "**Enable**" in AgentX Master dropdown.



Testing with snmpwalk

You can test the setup by ssh to the SBC and run the following commands:

To test the NSC SNMP module:

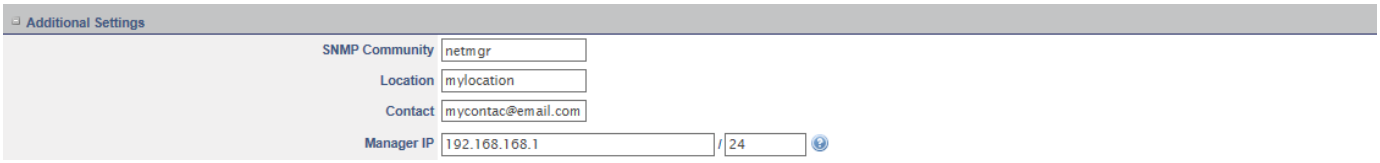
```
$ snmpwalk -v 1 -c sangoma localhost .1.3.6.1.4.1.27880
```

To snmpwalk all the MIBs in the machine:

```
$ snmpwalk -v 1 -c sangoma localhost .1
```

Additional Configuration Settings

- **SNMP Community**: string used in SNMP servers to group servers together. Server Monitor sends the community string along with all SNMP requests.
- **SNMP Location:** configure with the location of the device.
- **SNMP Contact:** contact information of who is responsible for managing the device.
- **SNMP Manger IP:** configure to restrict SNMP services only to this IP address.



To test the SNMP additional settings module:

```
$ snmpwalk -v 1 -c netmgr localhost syscontact
```

```
$ snmpwalk -v 1 -c netmgr localhost syslocation
```