# Kaseya Point Paper: SNMP Monitoring Without MIB Files

**Author:** Corey Mandell
**Date:** Friday, Sept 17, 2010
**Revision:** 1

## *Overview:*

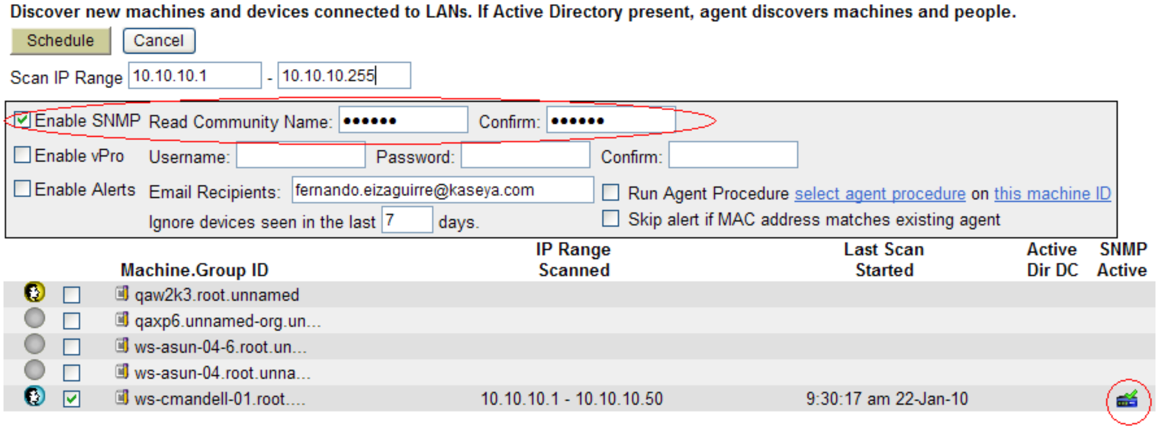
SNMP is a tricky and sometimes inconsistent standard. David Perkins, in his book 'Understanding SNMP MIBs' believes that "…RFCs defining SNMP contain definitions that are ambiguous, incomplete, internally inconsistent, incomprehensible, or are in conflict with the accepted usage." **With that in mind, this Point Paper describes the steps to follow to create a SNMP monitoring set without a MIB file.**

## *Goal*

The goal of this point paper is to allow advanced users to build their own SNMP Sets without the trouble of finding, loading and selecting MIB Objects from a less than stellar MIB Parser / Tree tool. **The focus of the following steps is to effectively work without MIB files while setting up SNMP Monitoring**.

## Step 1 – Verify "Lan Watch" with SNMP Has Been Executed

This first step is to enable Kaseya to discover each SNMP device that is found during the LanWatch scan. The administrator will select the Enable SNMP check box and include the SNMP read community string. This is the SNMP Polling string (or password) that the devices have been set up to answer SNMP polling with (the default is usually 'public').



**Discover new machines and devices connected to LANs. If Active Directory present, agent discovers machines and people.**

Scan IP Range 10.10.10.1 - 10.10.10.255

☑ Enable SNMP Read Community Name: •••••• Confirm: ••••••

□ Enable vPro Username: Password: Confirm:

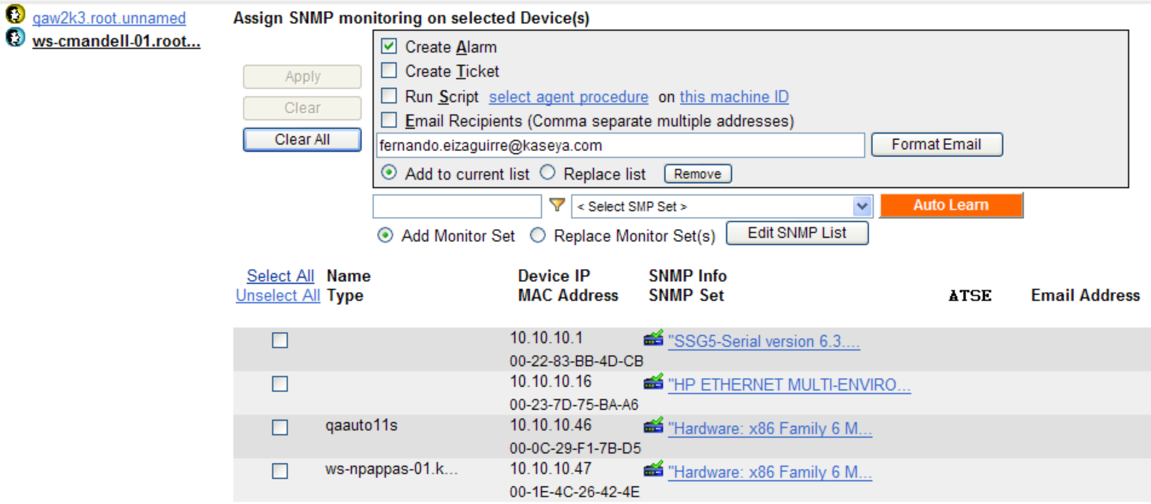
□ Enable Alerts Email Recipients: fernando.eizaguirre@kaseya.com □ Run Agent Procedure select agent procedure on this machine ID

Ignore devices seen in the last 7 days. □ Skip alert if MAC address matches existing agent

| | | Machine.Group ID | IP Range Scanned | Last Scan Started | Active Dir DC | SNMP Active |
|---|---|---|---|---|---|---|
| ● | □ | qaw2k3.root.unnamed | | | | |
| ○ | □ | qaxp6.unnamed-org.un... | | | | |
| ○ | □ | ws-asun-04-6.root.un... | | | | |
| ○ | □ | ws-asun-04.root.unna... | | | | |
| ● | ☑ | ws-cmandell-01.root.... | 10.10.10.1 - 10.10.10.50 | 9:30:17 am 22-Jan-10 | | ✓ |

## Step 2 – What do we know about the SNMP Devices returned?

Looking at the Assign SNMP function (MonitorTab), the list of Agents an administrator ran LanWatch/SNMP on is in the top left of the page. If any of them are selected, all the SNMP devices that were discovered will be displayed. Now, SNMP Sets can be assigned (Note: some may have already been assigned a SNMP Sets via an automated routine. Check your help file for descriptions of that feature). If the administrator would like to know what SNMP values are returning so far she/he will hit the SNMP Info Icon (blue and green icon next to the IP address).



qaw2k3.root.unnamed
ws-cmandell-01.root...

**Assign SNMP monitoring on selected Device(s)**

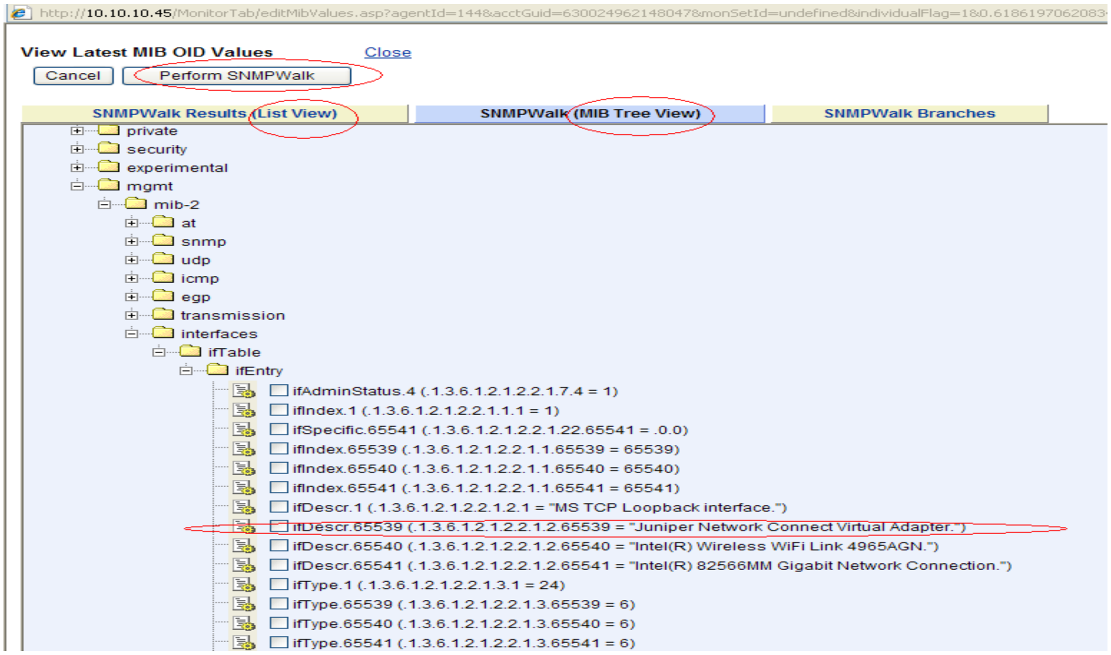
Apply
Clear
Clear All

☑ Create Alarm
□ Create Ticket
□ Run Script select agent procedure on this machine ID
□ Email Recipients (Comma separate multiple addresses)
fernando.eizaguirre@kaseya.com   Format Email
● Add to current list ○ Replace list   Remove

< Select SMP Set >   Auto Learn
● Add Monitor Set ○ Replace Monitor Set(s)   Edit SNMP List

| Select All<br>Unselect All | Name<br>Type | Device IP<br>MAC Address | SNMP Info<br>SNMP Set | ATSE | Email Address |
|---|---|---|---|---|---|
| □ |  | 10.10.10.1<br>00-22-83-BB-4D-CB | "SSG5-Serial version 6.3.... |  |  |
| □ |  | 10.10.10.16<br>00-23-7D-75-BA-A6 | "HP ETHERNET MULTI-ENVIRO... |  |  |
| □ | qaauto11s | 10.10.10.46<br>00-0C-29-F1-7B-D5 | "Hardware: x86 Family 6 M... |  |  |
| □ | ws-npappas-01.k... | 10.10.10.47<br>00-1E-4C-26-42-4E | "Hardware: x86 Family 6 M... |  |  |

This will show the SNMP information that was implicitly retrieved after the initial LanWatch discovery (via SNMPWalk scripts). This is used to either automatically or manually select the correct SNMP Set. There is a Tree and a List view of the data. The third tab will allow a master admin to change the SNMP Branches to automatically walk from that point on.



http://10.10.10.45/MonitorTab/editMibValues.asp?agentId=144&acctGuid=630024962148047&monSetId=undefined&individualFlag=1&0.6186197062083

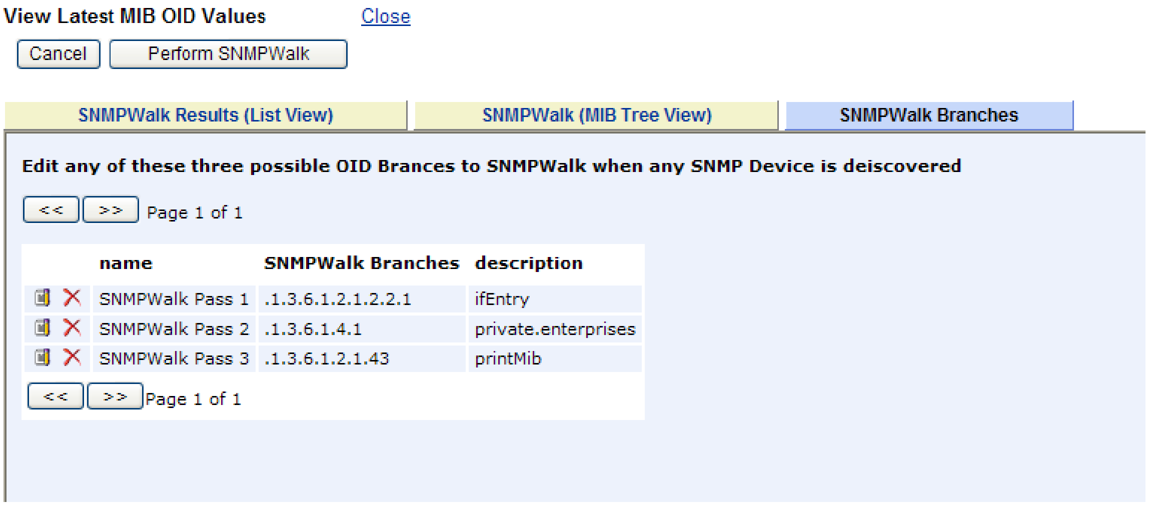
**View Latest MIB OID Values**   Close

Cancel   Perform SNMPWalk

SNMPWalk Results (List View) | SNMPWalk (MIB Tree View) | SNMPWalk Branches

```
⊞ private
⊞ security
⊞ experimental
⊟ mgmt
    ⊟ mib-2
        ⊞ at
        ⊞ snmp
        ⊞ udp
        ⊞ icmp
        ⊞ egp
        ⊞ transmission
        ⊟ interfaces
            ⊟ ifTable
                ⊟ ifEntry
                    □ ifAdminStatus.4 (.1.3.6.1.2.1.2.2.1.7.4 = 1)
                    □ ifIndex.1 (.1.3.6.1.2.1.2.2.1.1.1 = 1)
                    □ ifSpecific.65541 (.1.3.6.1.2.1.2.2.1.22.65541 = .0.0)
                    □ ifIndex.65539 (.1.3.6.1.2.1.2.2.1.1.65539 = 65539)
                    □ ifIndex.65540 (.1.3.6.1.2.1.2.2.1.1.65540 = 65540)
                    □ ifIndex.65541 (.1.3.6.1.2.1.2.2.1.1.65541 = 65541)
                    □ ifDescr.1 (.1.3.6.1.2.1.2.2.1.2.1 = "MS TCP Loopback interface.")
                    □ ifDescr.65539 (.1.3.6.1.2.1.2.2.1.2.65539 = "Juniper Network Connect Virtual Adapter.")
                    □ ifDescr.65540 (.1.3.6.1.2.1.2.2.1.2.65540 = "Intel(R) Wireless WiFi Link 4965AGN.")
                    □ ifDescr.65541 (.1.3.6.1.2.1.2.2.1.2.65541 = "Intel(R) 82566MM Gigabit Network Connection.")
                    □ ifType.1 (.1.3.6.1.2.1.2.2.1.3.1 = 24)
                    □ ifType.65539 (.1.3.6.1.2.1.2.2.1.3.65539 = 6)
                    □ ifType.65540 (.1.3.6.1.2.1.2.2.1.3.65540 = 6)
                    □ ifType.65541 (.1.3.6.1.2.1.2.2.1.3.65541 = 6)
```

r



Edit any of these three possible OID Brances to SNMPWalk when any SNMP Device is deiscovered

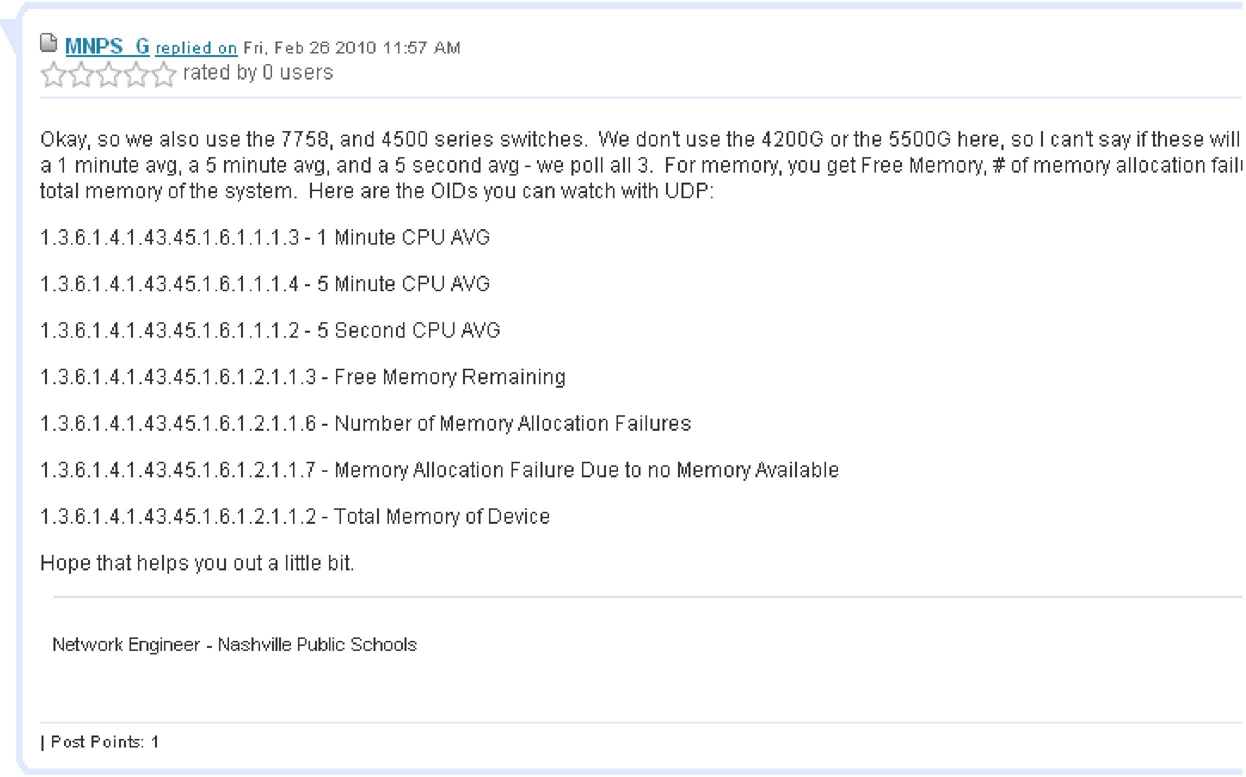
Page 1 of 1

| | name | SNMPWalk Branches | description |
|---|---|---|---|
| ✎ ✕ | SNMPWalk Pass 1 | .1.3.6.1.2.1.2.2.1 | ifEntry |
| ✎ ✕ | SNMPWalk Pass 2 | .1.3.6.1.4.1 | private.enterprises |
| ✎ ✕ | SNMPWalk Pass 3 | .1.3.6.1.2.1.43 | printMib |

Page 1 of 1

## Step 3 – Search the WEB for the SNMP Best Practice OIDs to Monitor.

From Steps 1 and 2 we have learned a bit about the SNMP Device that was discovered; now the Kaseya Administrator can Google for the discovered SNMP device and the OIDs that are the most valuable to monitor (along with suggested alarm levels). In this test case, a '3Com 4500' was discovered and our Kaseya Administrator wants to monitoring basic information so he or she 'googled' the phrase '3Com 4500 SNMP OID monitor' and received hundreds of hits. The Admin selected the first hit that was from a forum which usually has the most information on the OID topics:



MNPS_G replied on Fri, Feb 26 2010 11:57 AM

☆☆☆☆☆ rated by 0 users

Okay, so we also use the 7758, and 4500 series switches. We don't use the 4200G or the 5500G here, so I can't say if these will a 1 minute avg, a 5 minute avg, and a 5 second avg - we poll all 3. For memory, you get Free Memory, # of memory allocation faili total memory of the system. Here are the OIDs you can watch with UDP:

1.3.6.1.4.1.43.45.1.6.1.1.1.3 - 1 Minute CPU AVG

1.3.6.1.4.1.43.45.1.6.1.1.1.4 - 5 Minute CPU AVG

1.3.6.1.4.1.43.45.1.6.1.1.1.2 - 5 Second CPU AVG

1.3.6.1.4.1.43.45.1.6.1.2.1.1.3 - Free Memory Remaining

1.3.6.1.4.1.43.45.1.6.1.2.1.1.6 - Number of Memory Allocation Failures

1.3.6.1.4.1.43.45.1.6.1.2.1.1.7 - Memory Allocation Failure Due to no Memory Available

1.3.6.1.4.1.43.45.1.6.1.2.1.1.2 - Total Memory of Device

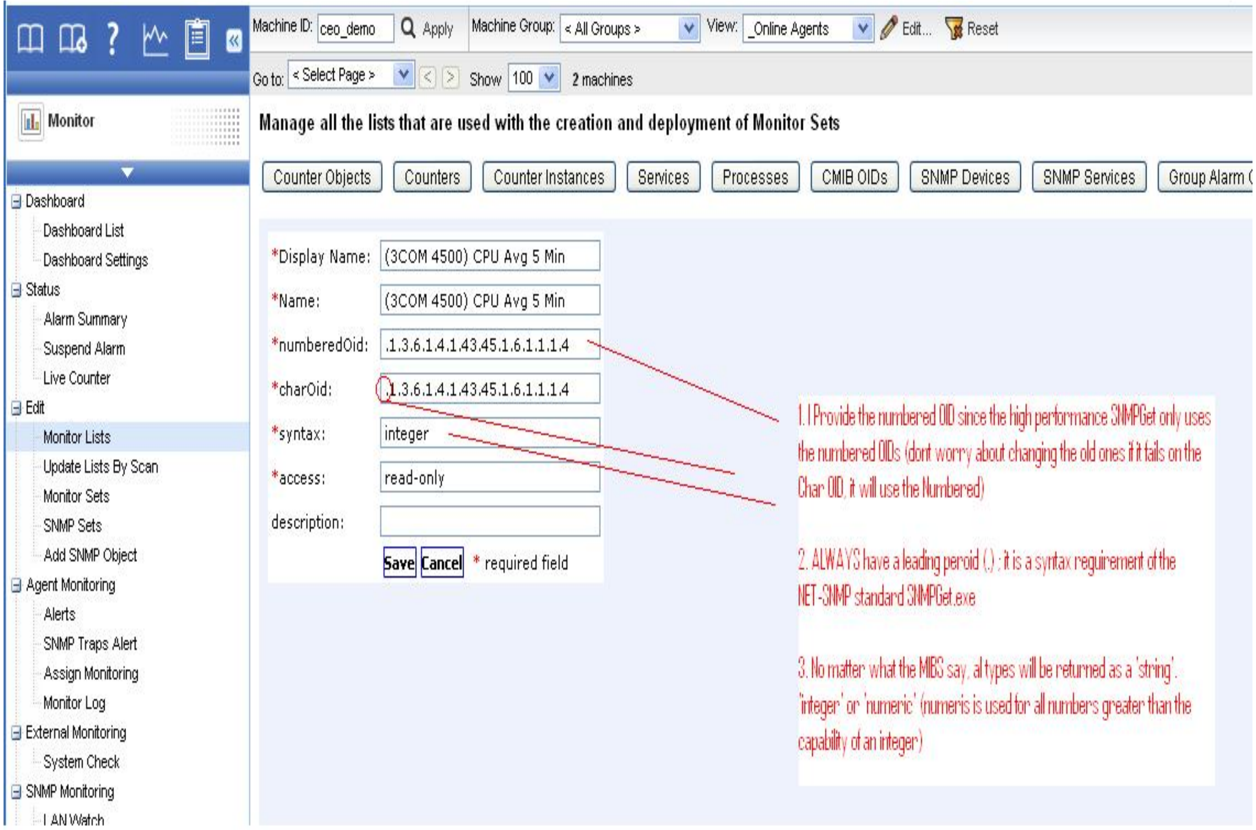
Hope that helps you out a little bit.

Network Engineer - Nashville Public Schools

| Post Points: 1

## Step 4 – Directly Add the OID into the Kaseya SNMP CMIB List

This step the Administrator allows to cut and paste most of the information into the Edit Lists->CMIB Tab function. They will add the OID directly instead of loading, selecting and adding the OID from some esoteric MIB. (per the notes in the graphic below: lead the numbered OID with a '.'  ;  syntax will always be either 'string' , 'integer' or 'float' ; access will always be 'read-only')



Manage all the lists that are used with the creation and deployment of Monitor Sets

*Display Name: (3COM 4500) CPU Avg 5 Min

*Name: (3COM 4500) CPU Avg 5 Min

*numberedOid: .1.3.6.1.4.1.43.45.1.6.1.1.1.4

*charOid: .1.3.6.1.4.1.43.45.1.6.1.1.1.4

*syntax: integer

*access: read-only

description:

* required field

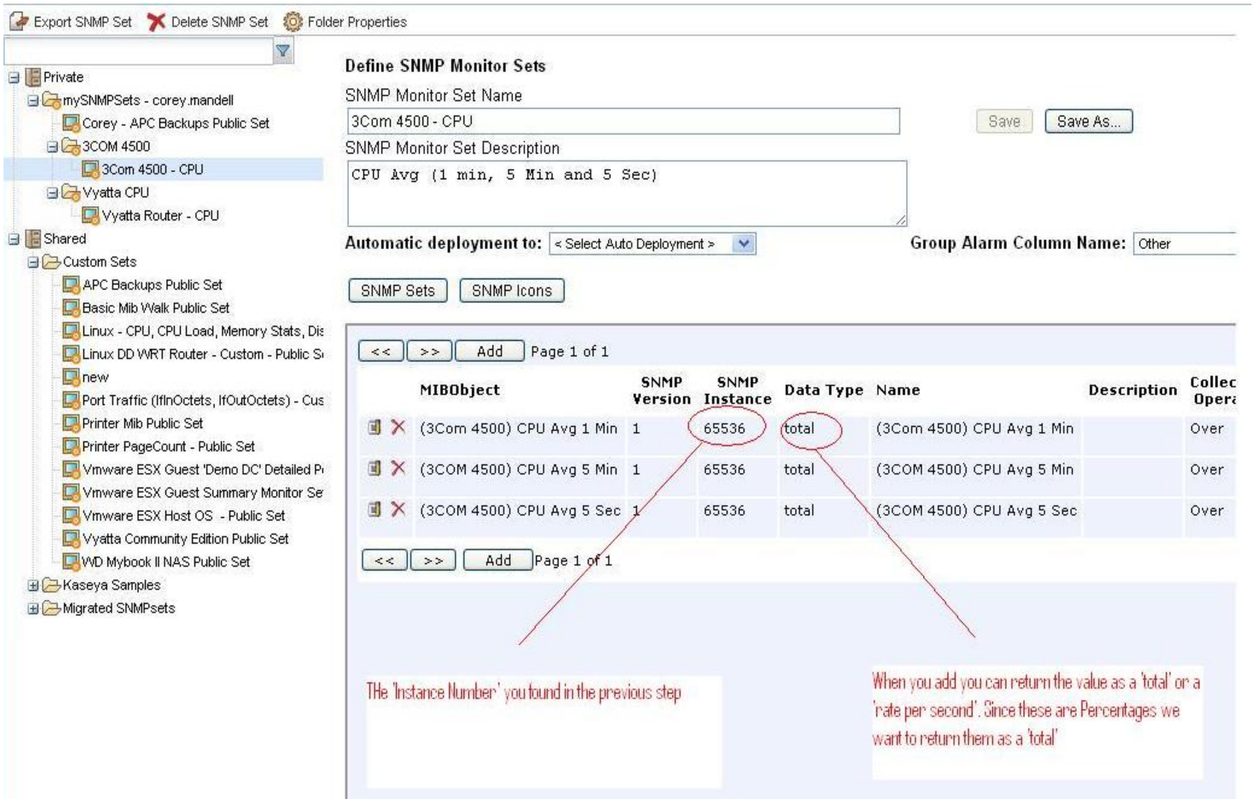
1. I Provide the numbered OID since the high performance SNMPGet only uses the numbered OIDs (dont worry about changing the old ones if it fails on the Char OID, it will use the Numbered)

2. ALWAYS have a leading peroid (.) ; it is a syntax requirement of the NET-SNMP standard SNMPGet.exe

3. No matter what the MIBS say, al types will be returned as a 'string', 'integer' or 'numeric' (numeris is used for all numbers greater than the capability of an integer)

## Step 5 - Create Your SNMP Set

The Administrator can now create a SNMP Set and select the OIDs that they just added via the Edit Lists function. Remember that the SNMP Version, unless you know it is only available in version '1' will be '2c'. The most difficult entry while creating a SNMP Set is understanding 'instances' (or interfaces which is used synonymously) .  If the value is a 'singleton' (not part of a list or table) the Instance value will be '0' (zero).  If it is part of a table ( such as there are three sensors  ... which you will have learned from the Google search), you would then enter 1-3 or 1,2,3.  In the case of a routers ports you can look at the returned data from Step 1 to see what the port numbers are. Then enter then as 'interfaces' such as 1-24, 10101 (the high port number is usually a management or loop back port).  If the OID data type is a integer or float, the Admin has the option to bring the value back as a Total (like CPU or Memory Used) or as a Rate per-second (like Bytes transfered).


Export SNMP Set
Delete SNMP Set
Folder Properties
Private
mySNMPSets - corey.mandell
Corey - APC Backups Public Set
3COM 4500
3Com 4500 - CPU
Vyatta CPU
Vyatta Router - CPU
Shared
Custom Sets
APC Backups Public Set
Basic Mib Walk Public Set
Linux - CPU, CPU Load, Memory Stats, Dis
Linux DD WRT Router - Custom - Public S
new
Port Traffic (IfInOctets, IfOutOctets) - Cus
Printer Mib Public Set
Printer PageCount - Public Set
Vmware ESX Guest 'Demo DC' Detailed P
Vmware ESX Guest Summary Monitor Se
Vmware ESX Host OS - Public Set
Vyatta Community Edition Public Set
WD Mybook II NAS Public Set
Kaseya Samples
Migrated SNMPsets
Save
Save As...
SNMP Sets
SNMP Icons
<<
>>
Add
Page 1 of 1

**Define SNMP Monitor Sets**

SNMP Monitor Set Name: 3Com 4500 - CPU

SNMP Monitor Set Description: CPU Avg (1 min, 5 Min and 5 Sec)

**Automatic deployment to:** < Select Auto Deployment >

**Group Alarm Column Name:** Other

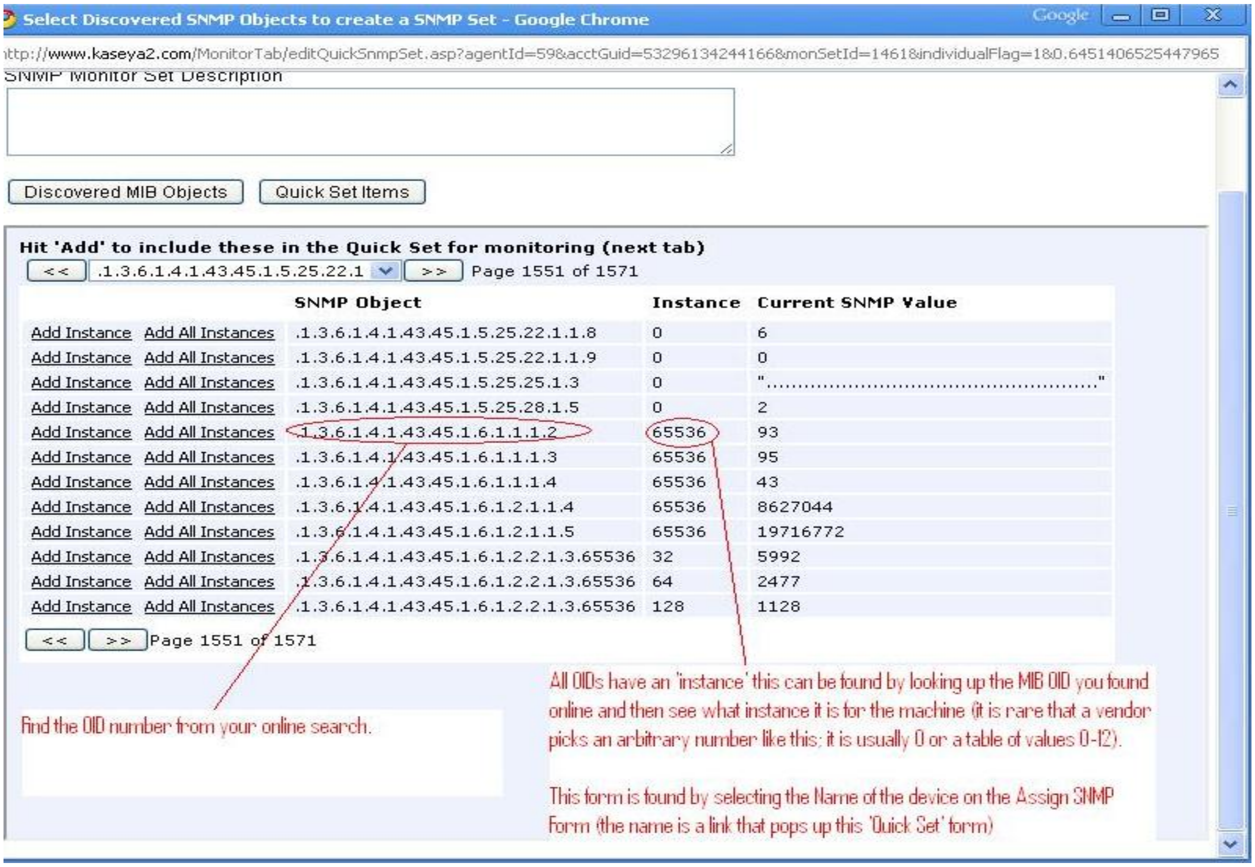
| MIBObject | SNMP Version | SNMP Instance | Data Type | Name | Description | Collec Opera |
|---|---|---|---|---|---|---|
| (3Com 4500) CPU Avg 1 Min | 1 | 65536 | total | (3Com 4500) CPU Avg 1 Min | | Over |
| (3COM 4500) CPU Avg 5 Min | 1 | 65536 | total | (3COM 4500) CPU Avg 5 Min | | Over |
| (3COM 4500) CPU Avg 5 Sec | 1 | 65536 | total | (3COM 4500) CPU Avg 5 Sec | | Over |

THe 'Instance Number' you found in the previous step

When you add you can return the value as a 'total' or a 'rate per second'. Since these are Percentages we want to return them as a 'total'

## (Alternate) Step 5 - Review the output of the Proactive SNMPWalk

The key piece of knowledge ascertained from the SNMPWalk is how many interfaces the device possesses and what those interfaces do. We can see from the results below that this NetScreen device has two interfaces (cleverly numbered 1 and 2, don't laugh, sometimes they are not in sequence. Such as 1 and 65535).



Select Discovered SNMP Objects to create a SNMP Set - Google Chrome
ıttp://www.kaseya2.com/MonitorTab/editQuickSnmpSet.asp?agentId=59&acctGuid=53296134244166&monSetId=1461&individualFlag=1&0.6451406525447965
SNMP Monitor Set Description
Discovered MIB Objects
Quick Set Items

Hit 'Add' to include these in the Quick Set for monitoring (next tab)

<< .1.3.6.1.4.1.43.45.1.5.25.22.1 >> Page 1551 of 1571

| | | SNMP Object | Instance | Current SNMP Value |
|---|---|---|---|---|
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.5.25.22.1.1.8 | 0 | 6 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.5.25.22.1.1.9 | 0 | 0 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.5.25.25.1.3 | 0 | "................................................." |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.5.25.28.1.5 | 0 | 2 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.6.1.1.1.2 | 65536 | 93 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.6.1.1.1.3 | 65536 | 95 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.6.1.1.1.4 | 65536 | 43 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.6.1.2.1.1.4 | 65536 | 8627044 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.6.1.2.1.1.5 | 65536 | 19716772 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.6.1.2.2.1.3.65536 | 32 | 5992 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.6.1.2.2.1.3.65536 | 64 | 2477 |
| Add Instance | Add All Instances | .1.3.6.1.4.1.43.45.1.6.1.2.2.1.3.65536 | 128 | 1128 |

<< >> Page 1551 of 1571

Find the OID number from your online search.

All OIDs have an 'instance' this can be found by looking up the MIB OID you found online and then see what instance it is for the machine (it is rare that a vendor picks an arbitrary number like this; it is usually 0 or a table of values 0-12).

This form is found by selecting the Name of the device on the Assign SNMP Form (the name is a link that pops up this 'Quick Set' form)

## *Summary*

The internal Engineering team has created hundreds of SNMP Sets using this method. The average time to create is about 20 minutes. It is much more efficient than searching down and loading MIB files.