

OidViEW 6.0

User's Manual



OidView SNMP MIB Browser is a network management analysis tool that uses the SNMP protocol to talk to various agents and devices on a computer network

Licensing OiDViEW

OiDViEW can be used for a total of 7 days in full evaluation mode, at which point it will automatically convert itself into the FREE version. In addition, the FREE version of OiDViEW has the following handicaps:

- ◆ Limit of 2 simultaneous MIB Browsers
- ◆ Limit of 1500 MIBs compiled or loaded into the database
- ◆ Limit of graphing and polling 2 OIDs at one time
- ◆ SNMP SETs are disabled
- ◆ No enterprise modules will work (i.e. Cisco QoS Browser, SNMP Tester, etc.)

At the moment the MIB limit or time limit expires (whichever comes first), a license must be purchased to continue use of the OiDViEW tool. There are no refunds once a license is purchased. The evaluation period should suffice as enough of a time period to make an accurate assessment of software capabilities. If bugs are found, please report them via the email tech support form and ByteSphere will make every attempt to fix bugs deemed to truly be bugs (and can be verifiably reproduced), and will deliver patches with said bug fixes free of charge to licensed customers.

OiDViEW's registration system uses a unique HARDWARE-ID for each computer. This ID will have to be sent to ByteSphere in order to license OiDViEW on your computer.

- ◆ While using OiDViEW, Click: Help -> ByteSphere On The Web -> Purchase OiDViEW OnLine.

OR:

- ◆ In a browser, <http://www.OiDViEW.com/sales.html>

At this point, you should have been directed to the ByteSphere Sales Page.

- ◆ Click the OiDViEW ADD TO CART button for the right version and number of users.
- ◆ You should now be looking at your shopping cart. When finished adding to your cart, CHECKOUT.
- ◆ Fill in the required fields, credit card, email, etc. and click *Make Secure Purchase*

Activating OiDViEW

To use OiDViEW past the trial period, you will be able to use it in FREE mode. If you prefer to remove limitations to its functionality, an OiDViEW license must be purchased and it must be registered for each machine that it is installed on. To get the HARDWARE-ID for a machine, within OiDViEW, from the menus select Help -> Show Hardware ID. A window will appear that will look like this:

To purchase online with your HARDWARE-ID, you can select Help -> ByteSphere on the Web -> Purchase OiDViEW Online. This will launch a web browser and send your HARDWARE-ID to our website for use during the purchase process.

Another way of getting the HARDWARE-ID is to drop to a command line, change into the OiDViEW directory, and type "OiDViEW REGISTER". This will also give you your HARDWARE-ID, and any other related registration information.

Licenses can be purchased online: <http://www.oidview.com/sales-oidview.html>

Once you purchase a license. If you include your HARDWARE-ID during the online sale, you will automatically be sent an activation CODE and a license.key file.

If you did not include your HARDWARE-ID during the sale, you can use our online activation system with your ORDER# and your HARDWARE-ID to retrieve an activation CODE and a license.key.

Our online activation center is located here: <http://www.oidview.com/key-request-main.html>

All that is left to do is to save the license.key attachments (included in the ZIP file) to your OiDViEW program directory and restart OiDViEW. If you installed OiDViEW using the default location, that directory would be C:\Program Files\OiDViEW, or in some cases, C:\OiDViEW

To find out more about ByteSphere's activation system, please consult our online FAQ:

<http://www.oidview.com/akeyinfo.html>

Contents

Licensing OidView.	ii		
Activating OidView	iii		
<hr/>			
1	Console	1	
	The OidView Console.	1	
	The OidView Toolbar	3	
	The Session QuickBar	3	
	The System Module Toolbar.	4	
	Session Feature Toolbar	4	
	Session Tabs	4	
	StatusBar.	5	
2	Browser Sessions	6	
	Session Overview	6	
	Creating a session	7	
	Session Creation Dialog	7	
	Session Fields - SNMP Agent	8	
	SNMPv3 Configuration Dialog.	10	
	Session Fields - Mibwalk	13	
	Session Fields - Other	14	
	Session Detail	15	
	Session Feature Bar	16	
	Configuring Sessions.	17	
	Loading an old session	18	
	Removing a session	19	
3	MIBs (Management information Bases)	20	
	MIBs	20	
	Compile New MIBs.	21	
	Profile Overview.	22	
	MIB Management Screen.	24	
	MIB Module List.	26	
	MIB Module List Actions	27	
	Pre-Compiled MIBs	29	
	Session MIBs	30	
	Unloading MIBs.	30	
<hr/>			
4	Modules	31	
	Modules	31	
	MIB BROWSER	34	
	Default MIB Browser.	34	
	General Capabilities of MIB Browser:	36	
	JumpBar	37	
	Analysis / Browser NavBar Commands	38	
	Session Toolbars.	40	
	Variable Bookmarks	44	
	Browser Window Layout	44	
	WMI BROWSER	47	
	Intro to WMI Browser	47	
	General Capabilities of WMI Browser:	48	
	WMI Browser Window Layout.	49	
	Window Layout Dialog	50	
	DISCOVER	51	
	Discover Subnet	51	

ENTITY	53	Trap Filter Manager	83
ENTITY Module	53	Trap Filter Builder	85
iGRID	55	Trap Condition Builder	87
iGRID Module	55	NOTIFIER	89
iGRID Customization	56	Notifier Module	89
Layers and Subinterfaces	56	SNMTP TESTER	91
iGRID Toolbar	57	SNMP Agent Testing Module	91
PDUtrace	58	<hr/>	
PDUtrace Module	58	5 Analysis	99
PDUtrace HEX Decode	60	Agent Examination and Analysis	99
PDUtrace Toolbar	61	<hr/>	
PDU Search	62	6 Configuration	101
PDUtrace Trace List	64	Configuring OidView	101
PDUtrace Tree Decode	66	Configuring the Database	103
PERFORMANCE	67	Helper Apps.	104
Performance Module	67	Configuring Paths	104
Performance DataGrid	68	Trap Manager - Forwarding.	104
Main Display	71	Trap Manager - Deduplication	106
Performance Profiles.	73	Trap Manager - Filters	107
Performance Toolbar.	74	Trap Manager - Status/Storage	107
CISCO BROWSER	76	Trap Manager - Miscellaneous	109
Cisco CBQ Browser	76	Trap Manager - Display.	111
TRAP MANAGER.	77	Trap Manager - Logging	112
Trap Administration	78	Trap Manager - Transport.	113
Trap Deduplication	80	<hr/>	
Trap Display Options	81	7 Miscellaneous	114
Trap Forwarding.	82	Adjusting Polling Intervals	114
		Column Grouping	116
		Index Types	118

LiveGrid Actions	119
MIB Tree Actions.	121
Profile Overview.	123
MIB Index Extraction.	124
MibWalk	125
Defining SMI and other important information.	127
SNMP Dialog	129
SNMPv3 Configuration Dialog.	130
MIB Variable Grid Actions.	133
Vendor MIB Registration	133
OidView Data Window	134
Data Window Toolba	135

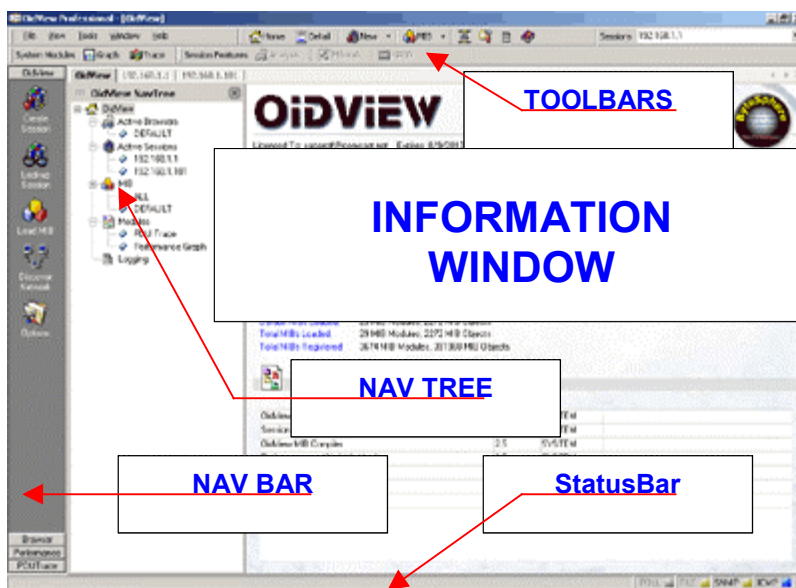
The logo for ByteSphere is a large, light blue watermark centered on the page. It features the word "ByteSphere" in a bold, italicized sans-serif font. The "B" and "S" are significantly larger than the other letters. A thin, light blue arc is positioned above the "S" and below the "P", resembling a stylized sphere or a smile.

ByteSphere

1 Console

The general layout of the OidView Console contains a number of Navigational Trees, Toolbars, and Tabs.

The OidView Console



The File Menu is located on the uppermost left part of the screen. This menu contains several options File, View, Options, Windows, and Help

Nav Bar

This is a Microsoft Outlook™ style Listbar. The Nav Bar is separated into several groups (usually one for each system module). The top group, OidView, allows one to get back to the Session Detail screen. Buttons are different in each group, according to the functionality of each module.

📁 To show / hide the OidView Nav Bar, click on **File -> View -> NavBar**.

Nav Tree

This is a standard TreeView that organizes the functionality, modules, and sessions of OidView into a simple, hierarchical tree-like structure. Sessions and other functions may be activated by double-clicking, or selected by single-clicking. The major categories of the Nav Tree are:

- ◆ OidView: clicking on this will bring you to the OidView Console Homepage, which lists general information such as the open sessions, the number of MIBs registered by the database, and hyperlinks to active sessions.
- ◆ Default MIB Browser – double click the DEFAULT node to activate the Default MIB Browser
- ◆ Sessions : list active sessions, create a new session, lookup an old session, MIB Manager, Bookmarks
- ◆ MIB Browsers: lists active MIB Browsers
- ◆ Modules : lists System Modules
- ◆ Logging: displays OidView's application logging

Main Information Window (not shown here)

This area displays Session Detail information, MIB Module Lists , Logging Information, or a Session or System Module (like Analysis/Browse, Performance, PDUtrace, etc).

The OidView Toolbar



The OidView Toolbar allows navigation to the following parts of OidView:

- ♦ Home – transfers the user to the OidView Overview screen, full of hyperlinks and information
- ♦ Detail – changes the screen to the Session Detail screen.
- ♦ New – this dropdown allows adding, configuration, removal of sessions
- ♦ MIB – Clicking will open up the MIB Manager. Dropdown will display either the Default or All Loaded MIBs
- ♦ Discover Subnet – will open up the Discover Subnet dialog .
- ♦ Tools – will open the configuration window
- ♦ Log – will change the screen to display the active logging facility
- ♦ Help – will display the online help (this file)

📄 To show / hide the OidView Toolbar, click on File -> View -> Toolbars -> OidView.

The Session QuickBar



The Session QuickBar allows one to easily change active sessions by simply clicking the combo box and choosing a new one. This is handy if the Session Tabs are OFF and one is currently browsing a MIB or not on the Console or Session Detail screen.

The System Module Toolbar



The System Module Toolbar contains buttons that launch OidView system modules, currently the Performance Graphing OID Poller and the PDUTrace Facility .

Session Feature Toolbar



The Session Feature Toolbar shows the available features for any given session. Clicking on Analysis launches a MIB Browser that will first analyze the agent. Also shown here are buttons for MibWalk , iGRID , and ENTITY-MIB .

Session Tabs



Session Tabs is located on the top or the bottom of the screen (user configurable), which when selected will change the active session.

 To show / hide the Session Tabs or change alignment, click on **File -> View -> Tabs**.

StatusBar



The StatusBar is located on the bottom part of the screen. By default, it is OFF. The left-hand side displays informational messages, and the right-hand side is split-up into different sections:

POLL

The SNMP Poller indicator light for the Performance Module. Green when polling, RED when not.

FILE

The MibWalk search indicator light. This will light when using a Mibwalk Session, and there is File I/O.

SNMP

The SNMP indicator light for MIB Browsers, Analysis Module. Activated when a PDU is on the wire.

ICMP

The ICMP indicator light for MIB Browsers, Analysis Module. Activated when a response to PING is received.

🔗 To show / hide the StatusBar, click on **File -> View -> StatusBar**.

2 Browser Sessions

Session Overview

A session is a conversation between OidView and the SNMP agent or SNMP mibwalk. OidView can handle up to 10 active sessions at once. Creating a session is the first step in the analysis process. Once the session has been created, any number of loaded analysis tools may be launched.

Each session has a separate memory space, yet can share MIB definitions with other sessions, thereby saving in OidView's overall memory footprint. In addition, they all share the Default Session MIBs. Active sessions will remember which variables existed and which variables were missing (after SNMP queries), and will retain this information until unloaded, in addition to having their own loaded MIB sets.

Creating a session

There are several ways to create a session:

- 📁 OidView Overview -> Create a New Session Hyperlink.
- 📁 OidView NavBar -> Create New Session button.
- 📁 OidView Overview or Session Detail File Menu: File -> Create New Session
- 📁 Double-click on the OidView -> Analysis Sessions -> Create icon in the OidView Navigation Tree
- 📁 Right-click on any active session in the OidView Navigational Tree, and left-clicking Add Session

Session Creation Dialog

The screenshot shows a 'Create a new Session' dialog box with the following fields and values:

Field	Value
IP Address / Hostname	127.0.0.1
Port	161
SNMP Protocol	Automatic
Read Community	public
Test OID for Read	System Table
Retries	2
Timeout	5
Write Community	
Test OID for Write	sysContact
Session Name	
Session Tag (optional)	

Buttons: Cancel, Create Session

Every time a new unique session is created, an entry is inserted into the database. If a new session is created which already matches an existing session, OidView will most likely re-use the record which corresponds to the existing session. This is important to know if analyzing many different agents, because old sessions can be loaded later.

Session Fields - SNMP Agent

Required Fields:

IPAddress

Enter the IP address or hostname of the SNMP agent.

Port

Enter the UDP port the agent is listening on (usually 161).

Optional Fields:

SNMP Protocol

Choose versions SNMPv1, SNMPv2c, or SNMPv3 (Professional Version only), or leave as Automatic if it is desired that OidView automatically determine Agent capabilities. Choosing SNMPv3 will automatically trigger a SNMPv3 Engine Discovery at the specified IP Address and UDP Port, at which point the SNMPv3 Configuration Dialog will be displayed.

Read Community

The default value is public, but modify as necessary.

Test OID for Read

Choose an OID with which to test communication with the agent. By default, the mib-2 system table is chosen.

Retries

The number of retries to use while communicating with an agent.

Timeout

The number of seconds OidView will wait before timing out a communication request.

Write Community

The community string needed to perform SNMP SETs.

Test OID for Write

Same as Test OID for Read, but used with SETs instead of GETs. By default, sysContact is used.

SNMPv3 Configuration Dialog

The SNMPv3 Configuration Dialog is available in the Professional Version. It allows the user to configure the parameters needed to open a SNMPv3 session with an agent.



Snm Protocol / Session Creation Dialog

To get the SNMPv3 Configuration Dialog, open up the Session Creation Dialog and select SNMPv3 for protocol: a little golden key will appear to the right. Click the key and the following dialog will appear:



SNMPv3 Configuration Dialog

This dialog will also appear when creating a new session or configuring an existing session and OidView attempts to automatically perform SNMPv3 engine discovery. Fill in the required fields for the specific agent you are going to analyze and press Test SNMPv3 Connection. If you have entered the parameters correctly, you will get a success message box and the light bulb will light up. If there is something wrong with the configuration you have entered, recheck your values and try again.

Relevant Fields:

Context Engine ID

Information Only. This is the discovered EngineID of the agent you are adding a session for.

Engine Boots

Information Only. The number of times this agent has restarted.

Engine Time

Information Only. The Engine Time represents the local time of the SNMPv3 agent. This will automatically be used to synchronize with OidView MIB Browser when analyzing this agent.

Context/Group

The SNMP Context of this agent instance. Often public. Synonymous with community for previous versions of SNMP.

SecurityName / UserName

The Security Name or User Name that will be used to access this SNMP agent.

Security Level

The Security Level used to access this agent. The three security levels available in SNMPv3 are:

- noAuthNoPriv (for no authentication and no privacy)
- AuthNoPriv (for Authentication but no privacy)
- AuthPriv (for communications using both Authentication protocol AND Privacy protocols)

Authentication Protocol

OidView currently supports MD5 and SHA protocols for SNMPv3 authentication.

Authentication Password

This is the password used to authenticate to the SNMPv3 agent.

Privacy Protocol

OidView does not currently support privacy, this will be supported in the next release.

Privacy Password

This is the password used for privacy communications.

Session Fields - Mibwalk

Required Fields:

[Mibwalk Name and Path](#)

Choose a mibwalk to analyze.

Optional Fields:

[Mibwalk Type](#)

OidView will attempt to figure out what type of mibwalk has been selected. If it cannot select one automatically chances are that it is an unsupported mibwalk or there may be something wrong with the mibwalk. Manually select the type of mibwalk if it is in the list. If it is not in the list, an XML profile may be created for your specific type of mibwalk, or you may request ByteSphere to certify a new type of mibwalk through the web support form. This service is only provided to registered OidView customers.

Session Fields - Other

UNDER THE GENERAL TAB

Required Field:

Session Name

Specify a name for the session, if desired. If one is not specified, one will be created automatically either using the IPAddress and port, the hostname of the device, or the mibwalk filename.

Optional Field:

Session Tag

This field allows any user-definable string to be entered and is completely optional. For example, if this agent was queried in regards to a certain problem or call ticket, use the ticket #.

UNDER THE AUTOLOADS AND PROFILES TAB:

AutoSearch Check Boxes

These check boxes activate MIB detection when first starting a session. If the agent understands the MIB, it is most likely that OidView will figure it out. This process only takes a couple of seconds and is well worth the wait as it enhances the analysis experience. If AutoLoad is not desired, simply uncheck all the check boxes.

1. Enterprise: All MIBS for the current vendor based on mib-2.private enterprises.{Enterprise Number}.
2. RFCs/Standards: All MIBS which are registered in the system and which do not belong to a specific vendor.
3. Default: All MIBS loaded in the Default MIB Profile.

Profile Selections

Previously Saved Profile: If desired, choose a definition profile that has been previously saved to load with this session. This feature is nice to use when needing to load large numbers of MIBS or definitions from different vendors or functional areas.

IGRID Assignment: Choose an iGRID profile to use with this session. IF-MIB is used by default.

Session Detail

On the left-hand side of the screen, the OidView NavBar and NavTree can be seen. Clicking on a session on the OidView NavTree will display the Session Detail window for that particular session.

Session Detail Window Layout:

The screenshot shows the OidView Session Detail window for IP Address 192.168.1.101. The window is divided into several sections:

- Session Feature Bar:** Located at the top, it contains icons for Graph, Trace, Session Features, Analysis, MIBwalk, GRID, and Entity-MIB.
- Session InfoGrid:** A central area displaying session details such as IP Address (192.168.1.101), Session Name (192.168.1.101-5000), and Session Date (4/5/2003 7:41:08 AM).
- MIB Module List:** A table listing loaded MIB modules with columns for Module, Base OID, Base Variable, Date, and # Objects. The table includes modules like BRIDGE-MIB, DISCO-AAA-CLIENT-MIB, and DISCO-QOS-POLICY-CONRG-MIB.
- Nav Tree:** A tree view on the left side of the main window.
- Nav Bar Session Features:** A vertical bar on the far left containing icons for Analysis, MIBwalk, GRID, and Entity-MIB.

Module	Base OID	Base Variable	Date	# Objects
BRIDGE-MIB	1.3.6.1.2.1.17	dot1dBridge		72
DISCO-AAA-CLIENT-MIB	1.3.6.1.4.1.3.3.158	ciscoAAAClientMIB	11/13/2001	31
DISCO-CATER-CROSSBAR-MIB	1.3.6.1.4.1.3.3.217	ciscoCatC_CrossbarMIB	6/25/2001	51
DISCO-CATOS-ACL-QOS-MIB	1.3.6.1.4.1.3.3.179	ciscoCatOS_AclQosMIB	10/18/2002	300
DISCO-CDP-MIB	1.3.6.1.4.1.3.3.23	ciscoCdpMIB	11/23/2001	95
DISCO-COPS-CLIENT-MIB	1.3.6.1.4.1.3.3.140	ciscoCopsClientMIB	6/11/2000	45
DISCO-ENTITY-FRU-CONTROL-MIB	1.3.6.1.4.1.3.3.117	ciscoEntityFruControlMIB	10/3/2002	79
DISCO-ENTITY-SENSOR-MIB	1.3.6.1.4.1.3.3.91	entitySensorMIB	12/18/1998 3120...	40
DISCO-FLASH-MIB	1.3.6.1.4.1.3.3.10	ciscoFlashMIB	4/1/2002	125
DISCO-INA...	1.3.6.1.4.1.3.3.26	ciscoIna...	9/2/1995	13
DISCO-MEN...				
DISCO-Pad				
DISCO-PRM				
DISCO-PRR				
DISCO-QOS-PIB-MIB	1.3.6.1.4.1.3.1.8.2.1	ciscoQosPIEMIB	5/2/2002	189
DISCO-QOS-POLICY-CONRG-MIB	1.3.6.1.4.1.3.3.159	ciscoQosPolicyConrgMIB	11/2/2000 10:30:0...	33
DISCO-RMON-CONRG-MIB	1.3.6.1.4.1.3.3.103	ciscoRmonConrgMIB	10/8/2002	44
DISCO-SM	1.3.6.1.4.1.3	cisco	1/11/2000	35
DISCO-S-TACK-MIB	1.3.6.1.4.1.3.5.1	ciscoStackMIB	6/11/2001	746
DISCO-S-TIP-EXTENSIONS-MIB	1.3.6.1.4.1.3.3.82	ciscoStpExtensionsMIB	12/6/2001	192
DISCO-SWITCH-ENGINE-MIB	1.3.6.1.4.1.3.3.97	ciscoSwitchEngineMIB	3/5/2002	295
DISCO-SYSLOG-MIB	1.3.6.1.4.1.3.3.41	ciscoSyslogMIB	3/7/1995	29
DISCO-SYSTEM-MIB	1.3.6.1.4.1.3.3.131	ciscoSystemMIB	6/22/2001	38
DISCO-TC	1.3.6.1.4.1.3.1.2.1	ciscoTcMibConventions	1/18/2001	17

- ◆ Session InfoGrid displays the type of session, any relevant session information, and is adjacent to the session log.
- ◆ Session Feature Bar contains shortcuts to supported OidView modules for the session. Click on these shortcuts to launch the analysis session or modules. These can also be launched from the OidView Nav Bar when in Session Feature Mode.
- ◆ MIB MODULE List displays the MIB modules which are loaded for the session. Includes Default MIB modules.

Session Feature Bar

This provides session specific features, and is located on the very top of the application, in the OidView-Console Toolbars area.



Features available with each session:

- ♦ [Analysis](#) : perform analysis or browse the agent

Features available as determined by OidView or agent type:

- ♦ [MibWalk](#): get a mibwalk of this particular agent (only available on live agents)
- ♦ [IGRID](#): launch the iGRID module
- ♦ [ENTITY-MIB](#): launch the ENTITY-MIB module

Configuring Sessions

To configure an active session, either:

- ✎ Click on the OidView NavBar icon, [Configure Session](#).
- ✎ Right-click on the session in the OidView NavTree, and select [Configure Session](#).

For Live SNMP Agents, the editable fields are:

- ◆ [SNMP Protocol](#)
- ◆ [Read Community / Test OID for Read](#)
- ◆ [Write Community / Test OID for Write](#)
- ◆ [Retries](#)
- ◆ [Timeout](#)

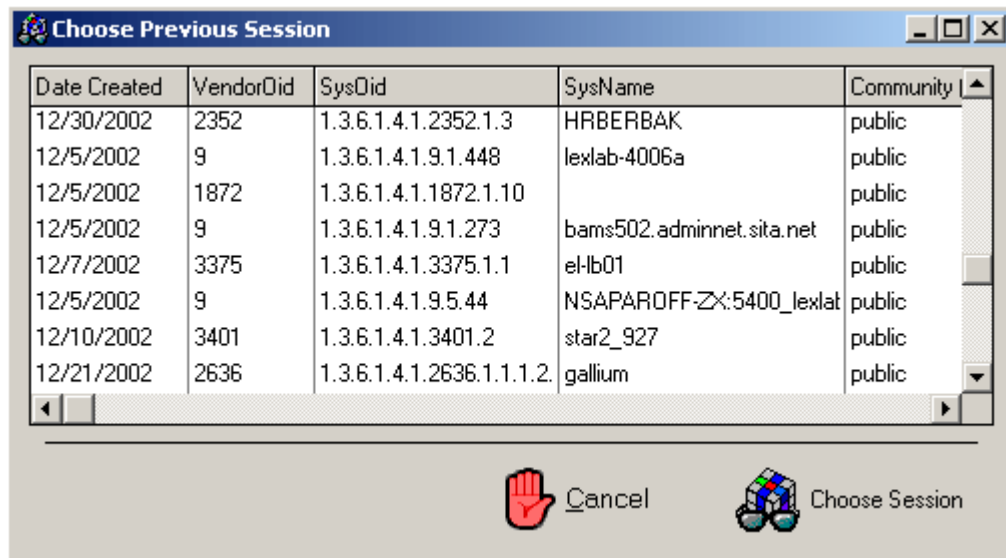
For Mibwalks, the editable fields are:

[Mibwalk Name and Path](#)

When analyzing mibwalks, reconfiguring an existing session with a different mibwalk causes the system to clear all previously 'found' variables, and set the Analysis Tree colors back to gray. This is very helpful if one needs to look at a number of similar mibwalks; the MIBs loaded for the session stay the same, and time can be saved.

Loading an old session

The advantage of loading an old session is that it saves time by not requiring the entry of session information again. Another advantage of loading old sessions is that the variable bookmarks from the previous sessions can be reused.



- ✎ Click the **OidView NavBar Lookup Old Session** icon and a window will appear listing all previous sessions in the database.
- ◆ Find the appropriate session and click on the **Choose Session** button.
- ◆ The session information will be transferred to the session create dialog.
- ◆ Make adjustments and then press **Load Session**.

Removing a session

There are several ways to remove a session.

- 📄 OidView NavBar -> Unload Session button.
- 📄 OidView Overview or Session Detail File Menu: File -> Unload Session.
- 📄 Right-clicking on any active session in the OidView NavTree, and left-clicking on Unload Session.

3 MIBs (Management information Bases)

MIBs

Some quick information about MIBs and OidView:

- ♦ MIBs provide the basis of information that OidView needs to query SNMP agents.
- ♦ OidView's capabilities are greatly enhanced by the MIBs that have been registered in the database.
- ♦ OidView can compile any SMIV1 or SMIV2 MIB, as long as all supporting IMPORT Modules are available.
- ♦ OidView can also load precompiled MIB definitions into the database.
- ♦ Assigning, Compiling, and Loading MIBs, are all performed with the MIB Management screen.

Learn how to:

- ♦ Assign MIBs to Sessions
- ♦ Compile New MIBs
- ♦ Load precompiled MIBs
- ♦ Unload MIBs

Learn more about:

- ♦ Precompiled MIBs
- ♦ MIB Module List
- ♦ Defining SMI, Enterprise Numbers, IanaIfTypes

Compile New MIBs

If looking at the MIB Management screen, this can be achieved by clicking Compile New Definitions. This will bring up the file selection dialog, which will allow selection of one to several MIBs.

If browsing the MIB Definition lists or the OidView Navigational Tree, simply right-click on the window or the tree icon and select Add or Compile New Definitions. This will bring up the MIB Management screen .

Note: If choosing several hundred MIBs at a time, please be aware that older versions of the MS Windows Operating System have limitations on how many files may be passed back through the file selection dialog. The files may have to be chosen in several blocks.

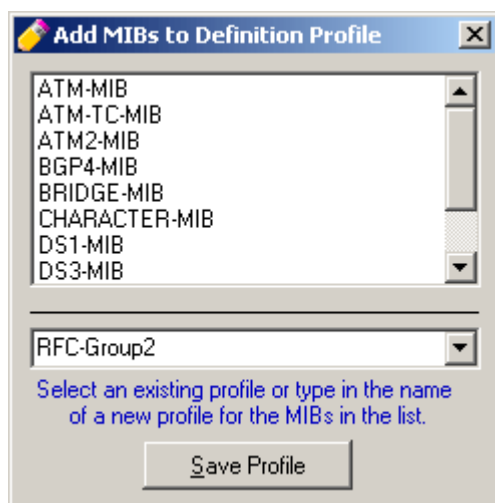
Profile Overview

What is a MIB Definition Profile?

This is simply a list of MIBs that is saved in a text file named <profile name>.txt in the /profiles/module subdirectory. A MIB Definition Profile can enable a quick determination of supported MIBs on an agent.

How is a Definition Profile created?

MIBs can be selected from the MIB Module List and saved to a MIB Definition Profile.



- ♦ If MIBs are saved to an existing definition profile, they will simply be added to it. Duplicates will be removed.
- ♦ If this is going to be a new profile, simply type in the new name.
- ♦ When finished, press Save Profile.

How is it used?

When creating a new session, the AutoLoads and Profiles Tab will display a ComboBox which allows the choice of a profile. If you were in need of determining if an agent supported any QoS (Quality of Service) MIBS over a variety of vendors, and you had created a MIB Definition profile which listed several QoS MIBs, then you could select that particular profile for use with your analysis. During the initial analysis phase, the agent will be queried for each MIB listed in the profile. If the agent responds to the query, that particular MIB will be loaded.

This is also useful when certain vendors have purchased other vendors. If a particular device has a SysOid saying it belongs to the new vendor, yet the MIBs loaded on the device belong to the old vendor, one may construct vendor profiles to accommodate for these vendor buyouts.

MIB Management Screen

Bring up the MIB Management Screen by either:

- ♦ Clicking on the MIB Management hyperlink on the OidView Overview page.
- ♦ Clicking on the MIB Manager icon on the OidView NavBar.

The screenshot shows the MIB Manager application window. The main area displays a table of Cisco MIBs registered in the local database. The table has columns for Enterprise, Vendor Name, Module, Size, DID, TopView, and R Objects. The 'Cisco-ITP-GACT-MIB' module is highlighted in blue.

Enterprise	Vendor Name	Module	Size	DID	TopView	R Objects
N/A	All Modules	CISCO-ITP-ACL-CAPABILITY		1.3.6.1.4.1.9.7.214	ciscoItpAcCapability	2
0	RFC/Standards	CISCO-ITP-ACL-MIB		1.3.6.1.4.1.9.2.27	ciscoItpAcMib	47
1	Networks	CISCO-ITP-ACT-CAPABILITY		1.3.6.1.4.1.9.219	ciscoItpActCapability	2
2	IBM	CISCO-ITP-ACT-MIB		1.3.6.1.4.1.9.230	ciscoItpActMib	33
4	Univ	CISCO-ITP-GACT-CAPABILITY		1.3.6.1.4.1.9.304	ciscoItpGactCapability	3
		CISCO-ITP-GACT-MIB		1.3.6.1.4.1.9.333	ciscoItpGactMib	33
5	ACC	CISCO-ITP-GRT-CAPABILITY		1.3.6.1.4.1.9.339	ciscoItpGrtCapability	3
7	CAYMAN	CISCO-ITP-GRT-MIB		1.3.6.1.4.1.9.334	ciscoItpGrtMib	63
9	cisco	CISCO-ITP-GSCP-CAPABILITY		1.3.6.1.4.1.9.305	ciscoItpGscpCapability	7
10	MSC	CISCO-ITP-GSCP-MIB		1.3.6.1.4.1.9.335	ciscoItpGscpMib	264
11	Hewlett Packard	CISCO-ITP-GSP2-CAPABILITY		1.3.6.1.4.1.9.307	ciscoItpGsp2Capability	5
12	Epilogue					

Below the main table, there is a section titled "[10] MIBs to Load/Compile:" with a table showing the status of various MIB files:

Filename	Size	Date	Folder	Status
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-GSCP-MIB.jpnc	17013	3/26/2005 11:30:12 AM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-GSCP-CAPABILITY.jpnc	1347	3/26/2005 11:30:10 AM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-GRT-MIB.jpnc	9305	9/22/2003 9:59:00 PM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-GRT-CAPABILITY.jpnc	723	9/22/2003 9:59:00 PM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-GACT-MIB.jpnc	2603	9/22/2003 9:58:58 PM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-GACT-CAPABILITY.jpnc	641	9/22/2003 9:58:58 PM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-ACT-MIB.jpnc	2479	9/22/2003 9:58:58 PM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-ACT-CAPABILITY.jpnc	635	1/25/2003 10:55:22 PM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-ACL-MIB.jpnc	5493	1/25/2003 10:55:20 PM	C:\PROGRA~1\OidView\apps\private\3	Loaded
C:\PROGRA~1\OidView\apps\private\3\CISCO-ITP-ACL-CAPABILITY.jpnc	642	1/25/2003 10:55:20 PM	C:\PROGRA~1\OidView\apps\private\3	Loaded

This screen allows the user to:

- ♦ Browse registered MIBs in the following categories: Vendor, RFC, All
- ♦ Compile/Load MIBs into OidView's database (Globally or by session)
- ♦ Advanced searching for text within all MIB modules of the current category
- ♦ Ability to see modules which are Loaded and/or Unloaded in the above mentioned categories by using the Filter choices (ALL, Loaded, Unloaded)
- ♦ Launch MIB Browser for a specific MIB by right-clicking on the module and left-clicking Browse Module.

To compile new ASN.1 MIBS that are not listed in the dialog screen, click the “Compile New MIBs” button located either on the NavBar under the MIB Manager group, or the “Compile New MIBs” button located in the mid-level set of buttons on the screen.

To search compiled MIB Modules for text, enter search text in the search text box on the toolbar. To enter more than one word to search for, separate words with a comma (,). To load words from a pre-defined word profile (or to build a word profile), click the “Words” button located on the toolbar.

The Force Recompil checkbox should be checked if compiling raw ASN.1 MIBs which may be already be registered in the database and it is desired that they are compiled again. This could be for a number of reasons - you have received newer MIBs, or during the last compile something went awry. If this box is not checked, OidView will simply load precompiled MIBs (if available and registered), instead of actually compiling the selected ASN1 MIBs.

MIB Module List

The MIB Module list includes information about the loaded MIB modules.

Module	Base OID	Base Variable	Date	# Objects
CISCO-QOS-PIB-MIB	1.3.6.1.4.1.9.18.2.1	ciscoQosPIBMIB	6/16/2000	169
CISCO-QOS-POLICY-CONFIG-...	1.3.6.1.4.1.9.9.159	ciscoQosPolicyConfigMIB	11/2/2000	31
CISCO-RMON-CONFIG-MIB	1.3.6.1.4.1.9.9.103	ciscoRmonConfigMIB	12/1/1998	21
CISCO-SMI	1.3.6.1.4.1.9	cisco	1/11/2000	35

When looking at the Session Detail screen, this list will show all MIBs that were loaded with a particular session. This includes Default MIB Definitions as well.

The Default Definitions and All MIBs Module lists are available from the OidView NavTree underneath the MIB Manager icon. The Default Definitions list shows MIB Modules that were loaded automatically as defaults or those MIBs that were loaded manually by the user into the DB.

There are several actions available from the MIB Module list. Simply right-click on the list and a menu will appear. The menu changes according to how many definitions are selected. Multiple selections are allowed from the MIB Module list. Click [HERE](#) to see a list of actions.

MIB Module List Actions

Browse (Session)

This will open the session analysis window and zero in on the first MIB object in the selected MIB.

Browse (MIB)

This will open a new MIB browser and zero in on the first MIB object in the selected MIB.

Compile/Load MIBs

This will open the MIB Management Screen.

Delete Selected MIBs

Delete the selected MIBs from the Database and also remove the Precompiled MIB file (PCM).

Edit MIB

If the original MIB source is available (i.e. the MIB was compiled with OidView and the ASN.1 text is available), the MIB will be loaded into the Default MIB Editor.

Recompile Selected MIBs

If the original MIB source is available, this will clear the DB of the selected MIB, delete the PCM, and recompile the MIB Module. Use this when errors are found in the compiled MIB.

Unload Selected MIB(s)

To be used when a MIB Module is no longer needed as a Default definition, or loaded for a session. If unloading a definition which is not a default definition and is being visited by multiple sessions, all sessions will be affected. This is also true for default definitions - all open sessions will be affected.

Save to (MIB Profile)

The selected MIB Modules can be saved to a definition profile, which can be used later when creating a new session.

Show Descriptions

This can be toggled to show or hide the MIB Module description in the grid.

Export to XML

This will export the currently selected modules to SMI-compliant XML files. These files can then later be imported by any NMS that can load SMI-compliant XML files (NOTE concerning IMPORTS section: The current version of OidView does not include the name of the variable needed to import, only the module name. This may or may not be a problem with some NMSs). The XML output file will have the filename: <MODULE>.xml.

Export to HTML

This will export the currently selected modules to an HTML page (1 for each module)

Export to ASCII

This will write out simple text files (PCM files) of all selected MIB definitions. One file will be created per MIB Module selected, and the filename will be: <module>.pcm. This is handy when needing a quick list of MIB variables and OIDs. The output is similar to the following:

Pre-Compiled MIBs

What are Pre-Compiled MIBs?

Pre-Compiled MIBs are MIBs that have already been compiled by OidView and stored in a compressed format to save space and time. They are named as such: <MODULE>.bpcm. They are not readable by any application other than OidView. They can be downloaded from ByteSphere's MIB Download area which is live on the Internet - <http://www.oidview.com/mibs>. OidView comes installed with all the Standard MIBs and RFCs in Pre-Compiled format.

Where are they stored on my computer?

OidView automatically stores Pre-Compiled MIBs in a directory structure under the /PCM subdirectory by default. Pre-Compiled MIB definitions can be stored locally on the computer's hard-drive, or somewhere on a central network server in the corporate location. If they are to be stored somewhere else other than the /PCM subdirectory, OidView must be informed about this by changing the Configuration Path for BPCM files.

How can I use them with OidView?

OidView can register these Pre-Compiled MIBs in a number of ways.

- ♦ Registering Pre-Compiled MIBs on a local or shared drive

On the top file menu, click:

☞ Options -> Database -> Update DB Component -> Compiled MIB Modules

- ♦ Registering Pre-Compiled MIBs which have been downloaded from <http://www.oidview.com/mibs>

After a MIB-PAK has been installed, OidView will automatically register all new Pre-Compiled MIBs when it is next launched.

Session MIBs

What are Session MIBs?

Session MIBs are MIBs which have been loaded specifically for a particular analysis session. These sometimes can include Default MIBs.

Assigning MIBs to individual sessions:

If looking at the MIB Management screen, this can be achieved by choosing a session from the drop-down combo box in the left hand corner of the toolbar. When compiling or loading MIBs, if no session is chosen, OidView will automatically choose the Default Session.

Note: If you have compiled MIBs which are now listed as Default Definitions and it is not wished to have these as Default Definitions, simply unload the MIBs.

Unloading MIBs

To unload MIBs, follow these steps:

First, bring up the MIB Module List under MIB Manager or Session Detail.

Simply right-click on any selected modules and left-click on Unload Selected Definition(s). The MIB modules will be unloaded from OidView's database and will be removed from any assigned sessions.

4 Modules

Modules

There are two types of modules, System modules (those which are global to the system in scope), and Session modules (those displaying data which is session centric). OidView's functionality is also easily extended by plugin modules, which may be purchased separately from the OidView Professional Console.

Modules may be launched from the OidView NavBar, NavTree , or Session Feature Bar.

Modules that ship as a part of the OidView Professional Console include:

[MIB Browser \(Session\)](#)

Allows one to browse local or remote SNMP agents using the SNMP protocol. MIB Tree representation, Agent OID/Value Responses, Searchable MIB Object tables, and Object definition detail windows are all readily available on the same screen. View Layout can be modified to fit any user's needs.

[WMI Browser \(Session\)](#)

Allows one to browse local or remote Windows Hosts using the WMI protocol. MOF Tree representation, Host Instance and Property Value Responses, Searchable MOF Object tables, and Object definition detail windows are all readily available on the same screen.

[Performance \(System\)](#)

Track, graph and log variable data values. Use OidView's Advanced Performance Poller and Graphing capabilities to get to the bottom of any questionable data problem. Poll numeric values or even strings!

[IGRID \(Session\)](#)

I-GRID displays interfaces in multiple layers and allows drill-down into related interface technology groups. Administer the interface or explore even deeper to retrieve associated statistics.

ENTITY-MIB (Session)

For agents that support ENTITY-MIB, OidView can automatically generate a diagram representing the physical layout of the device.

PDUTrace (System)

OidView's PDU Trace facility is essentially an SNMP Sniffer and allows complete analysis of SNMP PDU packets. Sniff PDUs, search them for ASN.1 Tags, OIDs, values, etc.

Discover (System)

Discover a subnet by using a combination of ICMP and SNMP. OidView's discover module allows for multiple IP ranges, SNMP communities, and OID filtering. It will also determine basic device capability, if so desired.

Trap Manager (System)

This module is a viewer and administration tool for the ByteSphere Trap Manager Service (TMS). Capture and Forward V1 Traps, V2 or V3 Notifications. Look at varbind contents. Replay a captured Trap Log. Assign alarms to specific categories and buckets. Use the Notifier (purchased separately), to forward alarms or notify managers of problems. Define complex filtering to adjust display, forwarding, and notification. Can be used as a development platform to receive traps or as a dedicated management platform to manage alarms. 10-IP license comes with the professional version – allowing OidView to receive as many alarms from up to 10 different sources. To be able to receive events from more sources, an add-on license must be purchased.

Modules that do not ship as a part of the OidView Professional Console but that are easily added on by purchasing an additional plug-in module license include:

Notifier (System)

Send up to 6 different types of Notifications based on different events that are triggered within OidView. Use the Notifier Profile Manager to define notification profiles and policies. Use the Trap Manager Filters to activate a Notifier Profile.

Cisco CBQ Browser (Session)

The CISCO-CBQ Browser Module is the latest addition to our network management arsenal. Cisco leads the network management industry in its' robust and widely implemented Quality Of Service (QOS) technology. Their CISCO-CLASS-BASED-QOS-MIB uses a complex system of policies and traffic classes to define and control traffic flows. As such, implementation of these traffic flows can get sophisticated and often confusing as they are usually configured with the Cisco Command Line Interface (CLI).

SNMP Agent Test Module (Session)

Test SNMP Agents with customized or automatically generated SNMP tests exercising syntax and semantics found in the loaded MIBs for the session. Test all, some or just specific objects loaded into the session.

Please note:

OidView Basic comes with only the Default MIB Browser and Performance Poller.

OidView Enterprise comes with ALL modules enabled, including a 250 IP license pack.

MIB BROWSER

Default MIB Browser

The Default MIB Browser is the core of OidView Basic version. The Basic version does not have sessions, only the Default MIB Browser. OidView Professional of course has the capability of opening up to 10 browser analysis sessions, but you also have the option of using an unlimited number of Default MIB Browsers.

- To open up a Default Browser, click the “Open Default MIB Browser” hyperlink from the Console Overview window, or double click the OidView -> Active Browsers -> DEFAULT node in the OidView NavTree .
- To create a new MIB Browser in the Professional version, one can also click on the drop-down next to “New”, and click “New MIB Browser”.

The Default MIB Browser is similar to the Session Analysis Browser in almost all ways except the following:

Vendor Analysis and MIB Autoload

The Session Browser will determine the vendor OID of the agent, attempt to load the enterprise MIBs for that particular vendor, and determine the loaded MIBs on the agent. The Default browser does no detection but has access to ALL MIBs that are loaded in the database (not just the Default MIBs). Additional MIBs must be manually loaded for the Default Browser.

Configuration

Default MIB Browser can be configured on the fly to a different IP/port, while a Session Analysis Browser cannot.

Storage of good agent and bad agent responses

Like the session browser, the Default MIB Browser stores good and bad responses for queried variables, but these get reset when you change the agent it is pointing at. The session-based MIB Browser does not reset the agent history until the session is destroyed.

The configuration toolbars are only available for the Default MIB Browser – they do not show up in the Session Analysis Browser.

Connection Configuration Toolbar



A horizontal toolbar with four dropdown menus. From left to right: 'IP Address' with value '192.168.1.101', 'UDP Port' with value '161', 'Timeout' with value '5', and 'Retries' with value '2'. Each dropdown has a small downward arrow icon.

SNMP Configuration Toolbar



A horizontal toolbar with three dropdown menus. From left to right: 'Version' with value 'SNMPv2c', 'Read' with value 'public', and 'Write' with value 'public'. Each dropdown has a small downward arrow icon.

General Capabilities of MIB Browser:

MIB Discovery and AutoLoad

The first time a session is created and analysis is performed, OidView automatically queries the agent to find out which MIBs the agent understands using our patent-pending MIBSense technology. These queries are based on the vendor's enterprise number and the MIBs which are currently registered by OidView. When a MIB query is successful, OidView automatically loads the MIB into the Database. If the MIB is not available locally, OidView will check with ByteSphere online to see if they are available. If they are, the MIB(s) will automatically be downloaded from ByteSphere's website using our patent-pending MIBAcquire technology, and then loaded into the local OidView MIB database.

Variable and Layout Memory

OidView remembers which MIB variables were present and which were missing (or not yet queried), for each distinct session, until a session is unloaded. OidView also remembers where the analysis session last left off, and how the screen was configured.

JumpBar

The basic mechanism allows for a quick retrieval of values for a certain variable in three steps:

📁 MIB Module -> MIB Table -> MIB Variable.

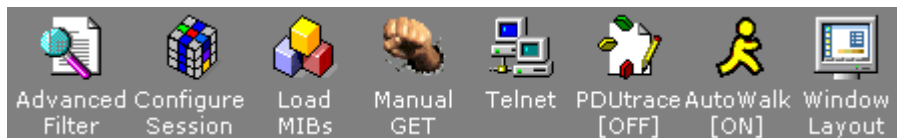
First, choose a MIB Module (here we have chosen ATM-MIB). Once, the MIB has been chosen, the Table List will be filled in automatically, and the Variable List will be filled in for the first table in the Table List:

Module ATM-MIB	Table aal5VccTable	Variable aal5VccEntry
----------------	--------------------	-----------------------

It is in this manner that data values can quickly be retrieved without browsing through the entire MIB Variable List or slowly browsing the MIB Tree.

Analysis / Browser NavBar Commands

OidView NavBar Commands for Analysis or MIB Browser:



Advanced Filter

Use the word profile dialog to adjust the variables in the MIB Variable grid.

Configure Session (N/A for non-live MIB Browsers)

Configure session communication parameters

Load MIBs (N/A for non-live MIB Browsers)

Load more MIBs into this particular session

Manual GET (Live Only)

Perform manual SNMPGet operations

Manual SET (Live Only)

Perform manual SNMPSet operations

Telnet (Live Only)

Telnet to the agent (if available), to perform administration via CLI. Configure the telnet client via the File Menu: Options -> Configure -> Helper Apps

PDUtrace (Live Only)

Trace PDUs to and from the agent for communication during this session. Toggles ON and OFF (default).

AutoWalk (N/A for non-live MIB Browsers)

Automatically send SNMP requests to the agent depending on the variable currently selected. Toggles ON (default) and OFF.

Window Layout

Adjust the window layout for this session

Session Toolbars

The Toolbars can be made visible/hidden by going to:

 **View -> Toolbars -> Browser**

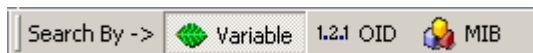
Search Toolbar



Search

Search the database for all variables, OIDs, or Modules which match the one entered in the provided text box. OidView understands simple wildcard patterns as well (e.g. tcp*, or *Conn*).

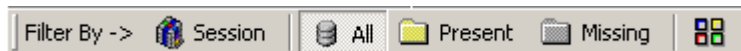
Search By Toolbar



Search By -> Variable/OID/MIB

These buttons toggle the search / sort for the MIB Variable Grid.

Filter By Toolbar



Session

When pressed, displays only those MIBs specifically loaded for that session

When unpressed (default), displays all MIBs associated with session (including defaults)

ALL

Show all MIB variables, whether they have yet been 'found' via queries or 'missing' by either unsuccessful queries or no query at all.

Present

Show only those MIB variables which have been found to be present from querying the agent.

Missing

Show only those MIB variables which have NOT been found to be present or those that have not yet been queried.

Show All Objects (ICON)

When Checked, shows all MIB Objects in the MIB Variable Grid.

When unchecked, shows only those objects defined with OIDs (default).

Command Toolbar



The command Toolbar is off by default.

Configure (ICON)

Click to configure Session

MIB Manager

Click to load new MIBs

SNMP GET (ICON)

Click to launch manual SNMP GET Dialog

SNMP SET (ICON)

Click to launch manual SNMP SET Dialog

Telnet (ICON)

Click to telnet to device / agent

PDU Trace (ICON / toggle)

Click to toggle PDU Trace ON/OFF

AutoWalk (ICON / toggle)

Click to toggle AutoWalk (ON/OFF)

Layout Toolbar



The layout toolbar is off by default.

Tree (ICON / toggle)

Click to show or hide MIB Tree

LiveGRID (ICON / toggle)

Click to show or hide the Live Grid

Variable GRID (ICON / toggle)

Click to show or hide the Variable Grid

MIB Info (ICON / toggle)

Click to show or hide MIB Info

Launch Layout Dialog (ICON / toggle)

Click to launch the layout dialog

Variable Bookmarks

Variable Bookmarks are a list of variables, OIDs, and definitions, which are saved both globally and per session. MIB variables which have been previously bookmarked can be easily accessed anytime in the future by simply clicking on the variable in this dialog, rather than having to type in the variable name or OID in the session analysis window.

To display the bookmark window:

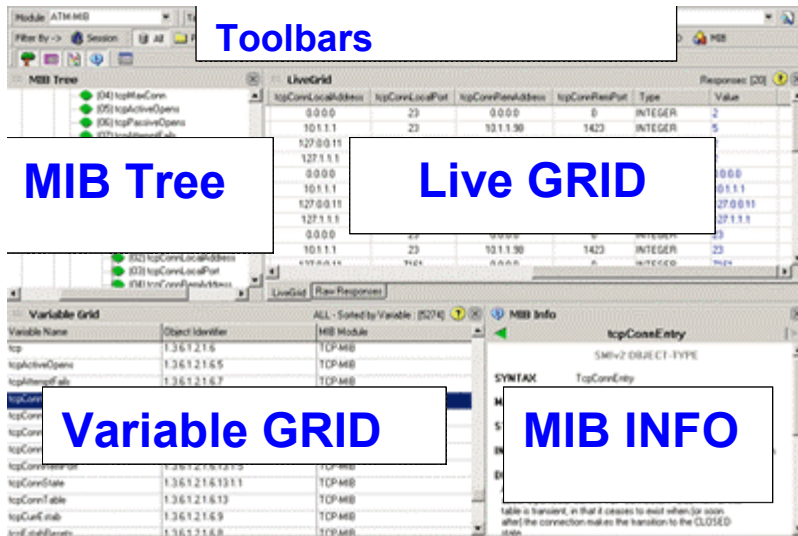
- ☞ Click on View -> Bookmarks
- ☞ In the Analysis Window -> Variable Tree, right-click on a variable, then left-click on Display Bookmarks.
- ☞ Double-click on the OidView NavTree -> Bookmarks icon

To add a variable bookmark:

- ☞ Analysis Window -> Variable Grid, right-click on the selected variables, and left-click Bookmark Selected Rows
- ☞ Analysis Window -> Variable Tree, right-click on a variable, then left click on Bookmark this variable

Browser Window Layout

MIB Browser Screen



JumpBars

Provides a quick way to jump to variables from a specific MIB Module.

Session Toolbars

Controls on these toolbars control all aspects of the MIB Browser.

MIB Variable Grid

Displays objects (variable name, object identifier, module, object type), for all loaded MIB objects from loaded MIB definitions associated with the session. This list changes depending on the values chosen by the session toolbar. Click [HERE](#) to see a list of actions.

MIB Tree

Displays all loaded MIB variables for the particular session (includes default MIB definitions and SMI). When analyzing an agent (Analysis mode), queries light-up the tree, causing the specific MIB variables which were present in the agent to be colored, and those which were not to be grey. This only applies to variables which have been queried. If a variable has not been queried, it will show as not being present, or greyed out. When in Browse mode (just browsing a MIB), all variables are colored. Click [HERE](#) to see a list of actions.

LiveGrid

Displays results from SNMP queries on the session's agent. Results are listed in the order they are received. Raw responses may be viewed by clicking the TAB underneath the LiveGrid. Click [HERE](#) to see a list of actions.

MIB Info

Displays all relevant information about a specific MIB Object. Retains a history (forwards and backwards) of 10 objects. Double-clicking on MIB objects in the text will automatically populate MIB Info with information about the clicked-on object.

WMI BROWSER

Intro to WMI Browser

The WMI Browser is a new system module that is distributed with the core OidView Product. It will be available in all versions of OidView. It uses Windows Management Interface (WMI) to talk to Windows operating systems to gather desired information, using either the simple provided tree navigation or complex WQL queries. This is useful as many Windows Machines may not have an SNMP agent running or installed. Other than being an alternate interface, WMI also provides several functions that SNMP cannot, including the capability of executing methods on remote machines.

🔗 To open up a WMI Browser, click the “WMI Browser” hyperlink from the Console Overview window, or click on the drop-down next to “New”, and click “New WMI Browser”.

Note: As this is a brand new module (1.0), it has a limited set of functionality. Please contact us to request additional functionality or to make recommendations. Also please note that WMI protocol sometimes forces the target host to use RPC calls which can often make the requesting program seem slow or unresponsive. Please give some queries up to 2 minutes to respond before assuming OidView has locked up.

MOF Files

Like the MIB browser uses SNMP MIBs as a basis for information, the WMI browser uses MOF files as a basis for information. A MOF file is a collection of information about “Classes”, “Properties” and “Methods”. The first time a WMI browser is launched, the MOF files on the local Windows machine will be read and compiled into memory. This will allow the WMI Browser to display a tree and a grid and enable the user to query MOF Classes, retrieve instances for each and view properties.

Browsing other Windows Machines

When opened the WMI Browser is pointing at localhost. To browse another machine, use the toolbars at the top of the window to enter the machine name or IP address, as well as the administrator login and password.

General Capabilities of WMI Browser:

Autodiscover Instances and Properties

As you click on nodes in the MOF tree or entries in the grid, the WMI browser will automatically discover the instances that are available on the machine being “browsed”, and place them in the MOF tree under the selected node as well as in the Live Grid. Clicking on the instance in the tree queries for the properties of the instance using WMI. Double clicking on an instance in the Live Grid does the same. Clicking on a property in the Live Grid shows information about the selected property. Clicking on a property in the MOF Tree will automatically query the host for all instances of the MOF Super Class Type.

Stored WMI Queries

In the toolbars at the top of the screen there is a drop-down with a number of popular stored queries. Simply choose one and the WMI Browser will automatically contact the target machine using WMI, retrieve the response, and populate the results in the Live Grid.

WMI Query Window

In the toolbar next to the drop-down there is a toggle button, **Query Window**. Toggling this will show or hide the WQL query window, which allows you to view and/or edit WQL to send directly to the target host. To send a WQL query, press the “EXECUTE” button on the right hand side (the Query Window must be showing).

WMI Browser Window Layout

WMI Browser Screen

The WMI Browser screen is very similar to the MIB Browser screen.

WMI Query Bars

Provides a quick way to query using stored queries and show or hide the WMI Query Window.

Connection Toolbars

Allows to connect to different hosts.

MOF Variable Grid

Displays MOF objects (Classes, Properties, References, Methods), for all loaded MOF objects from compiled MOF files in memory.

MOF Tree

Displays all loaded MOF classes, properties, and references.

LiveGrid

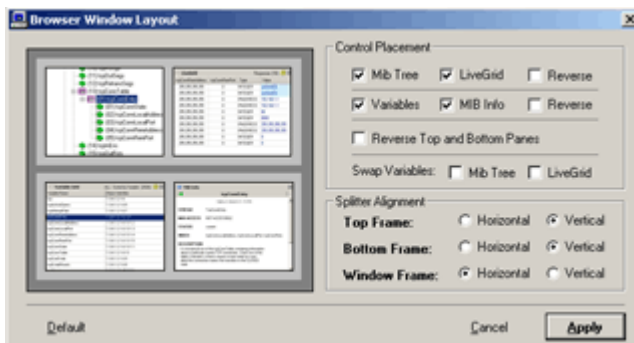
Displays results from WMI queries on the target host.

MOF Info

Displays all relevant information about a specific MOF Object.

Window Layout Dialog

Easily control the layout of your SNMP MIB Browser



The MIB Tree, LiveGrid, MIB Variable Grid (Variables), and MIB Info panes can all be swapped and reversed. Splitters can be set to Horizontal or Vertical alignment. Click OK to save your changes, Cancel to exit the dialog. Changes will be saved per session, NOT globally.

DISCOVER

Discover Subnet

To open the Discover Subnet dialog, either click the Discover Subnet icon on the NavBar, or on the Oid-View Toolbar (see OidView Console).

The Discover Subnet tool

allows a user to enter a variety of different criteria to either find as many agents as possible, or even narrow down results for only those systems and/or agents that correspond to the exact configuration desired. It uses a combination of ICMP (ping) and SNMP. If something is found to respond, the grid will list a green light. If it does not respond, a red light will be displayed.

There are two stages to discovery, Stage 1 (ICMP), and Stage 2 (SNMP). If ICMP is unchecked, there will only be one stage for discovery (Stage 2), but it will be much slower because it does not have the advantage of knowing which agents to target (as Stage 1 with ICMP helps to determine that). We recommend leaving both ICMP and SNMP checked, if possible.

Get Device Capabilities

tells Discover to look for basic device capabilities during stage 2. For example, is this a router or a switch? Is it a printer, a probe, a battery? There is a file located in the profiles subdirectory called mDiscoverRules.xml, which can be edited to modify how OidView classifies these agents. If you decide to change this file, it is best to contact ByteSphere support with your changes so we can include them in the latest distribution.

The following criteria can be used to find agents on a network:

1. ICMP and/or ICMP
2. IP Address Ranges (as many as needed)
3. Community Strings (as many as needed)
4. UDP ports (as many as needed - you are not limited to only 161)
5. OID Filters (list agents only responding to a specific OID)

To modify these parameters, simply click on the desired parameter button at the top of the dialog, and follow the simple prompts. They all work by simply pressing the Add button and entering a value. To remove a value from a listbox, simply click on that value and press the Delete Key.

To discover, simply press the discover button. A progress bar will move along and when finished, the Discover Results window will be displayed.

To launch a session on a discovered agent, simply select the agent in the grid on the discover results window, and press Start Session.

To Export discover results to XML, press the Export button and enter a filename.

To remove entries from the result window, simply select those entries and press the Delete Key.

ENTITY

ENTITY Module

General Capabilities of the ENTITY-MIB Module

Agents MUST support ENTITY-MIB in order for this icon to show up in the Session Feature Bar

OidView can automatically generate a diagram representing the physical layout of the device.

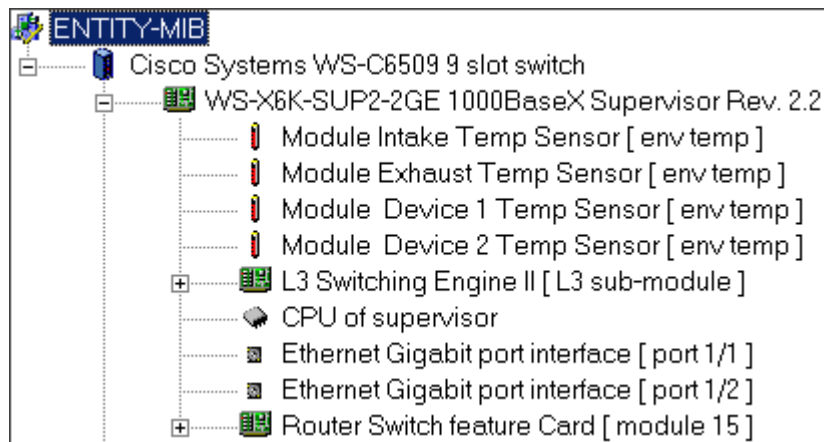


Figure 1 - Display with Small Nodes, and containers are hidden

ENTITY-MIB Module Checkbox commands

Small Nodes

Show the icons as small, or large (default).

Hide Containers

Hides the display of the container elements (off by default)

Hide Empty Containers

Only show those containers with elements (off by default)

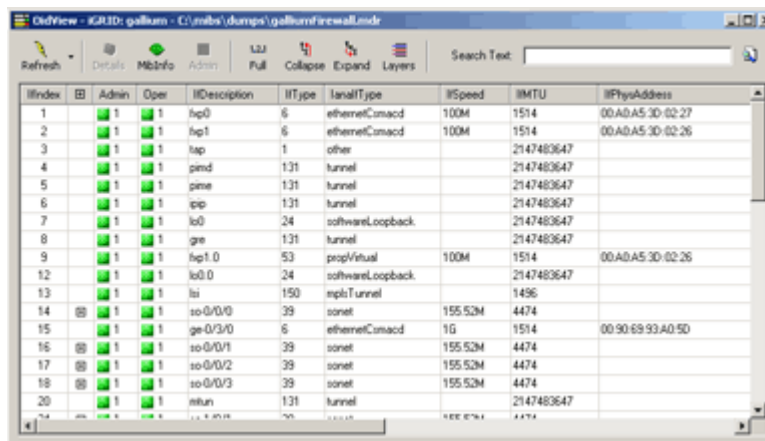
Use Relative Position

Show elements ordered by their ordinal positions in the ENTITY-MIB. This forces the display to show containers as well.

iGRID

iGRID Module

General Capabilities of the iGRID Module



The screenshot shows the iGRID module interface with a table of network interfaces. The table has columns for Index, Admin, Oper, IDescription, IType, IInterface, ISpeed, IMTU, and IPhysAddress. The data is as follows:

IIndex	Admin	Oper	IDescription	IType	IInterface	ISpeed	IMTU	IPhysAddress
1	1	1	tap0	6	ethernetCsmacd	100M	1514	00:A0:A5:3D:02:27
2	1	1	tap1	6	ethernetCsmacd	100M	1514	00:A0:A5:3D:02:26
3	1	1	tap	1	other		2147483647	
4	1	1	pin0	131	tunnel		2147483647	
5	1	1	pin1	131	tunnel		2147483647	
6	1	1	ppp	131	tunnel		2147483647	
7	1	1	lo0	24	softwareLoopback		2147483647	
8	1	1	gre	131	tunnel		2147483647	
9	1	1	tap1.0	53	propVirtual	100M	1514	00:A0:A5:3D:02:26
12	1	1	lo0.0	24	softwareLoopback		2147483647	
13	1	1	lzi	150	mplsTunnel		1496	
14	1	1	so-0/0/0	39	sonet	155.52M	4474	
15	1	1	ge-0/3/0	6	ethernetCsmacd	1G	1514	00:90:69:93:A0:5D
16	1	1	so-0/0/1	39	sonet	155.52M	4474	
17	1	1	so-0/0/2	39	sonet	155.52M	4474	
18	1	1	so-0/0/3	39	sonet	155.52M	4474	
20	1	1	stun	131	tunnel		2147483647	

Interface Layout

Get an instant inventory of all physical and logical interfaces! Delve into the interface representation on the device. See which interfaces are operationally and administratively up and down. Administer interfaces via SNMP. Dig deeper from the interface configuration layers into the individual interface's statistics using the OidView Data Window.

- ◆ About iGRID Layers
- ◆ Using the iGRID Toolbar
- ◆ Creating Custom iGRID Displays - create your own iGRID XML profile using our iGRID XML schema

iGRID Customization

Model it using our XML iGRID Schema

Just about anything with a MIB and an SNMP agent can be modeled and administered by OidView's iGRID. The default iGRID profile for any new session is IF-MIB, but feel free to create custom iGRID profiles using our XML interface and iGRID schema.

- » The schema is located in /profiles/iGRID/ mGridDefs.xsd, and specific HTML documentation is located at /doc/mGridDefs.html

Layers and Subinterfaces

iGrid can expose multiple virtual layers consisting of nested parent/child relationships. There are virtually no limits to the number of sub-layers that can be defined (i.e. ATM Port-> ATM Path-> ATM Channel, etc). Collapse and Expand layers at will.

When an interface has sublayers, the subinterface column (denoted by a +) will have a (+) in it, otherwise the cell will be empty.

IfIndex		Admin	Oper	IfDescription	IfType	IanalType	IfSpeed	IfMTU
14		1	1	so-0/0/0	39	sonet	155.52M	4474

Double-click on the (+) in the row's cell, and the interface's layers will be exposed.

GroupName	IfIndex		Admin	Oper	IfDescription	IfType
	14		1	1	so-0/0/0	39
SONET-MIB			sonetSectionCurrentStatus	sonetLineCurrentStatus	sonetPathCurrentStatus	sonetPathCurrentWidth
	14		1	1	1	sts3cSTM1(2)

- ♦ Any cell with a red triangle in the upper right hand corner denotes a special data link (a different PollOids group - see the iGRID XML schema for more details). Clicking on each of these cells will produce a Data Window which pulls different variables from the agent (possibly from a different MIB table or even a different MIB altogether).

iGRID Toolbar



Refresh

Click this to refresh the grid, or use the drop-down to refresh the state variables only.

Monitor/Details

Click this to bring up the OidView DataWindow associated with the specific interface type.

MibInfo

Toggle to show the MIB Info panel.

Admin

Use this to send an SNMP SET to the agent if the MIB variable can be administered.

Full

Toggles Full Index display.

Collapse

Collapse all subinterface layers.

Expand

Expand all subinterface layers.

Layers

Show only the layers, not all subinterfaces.

PDUtrace

PDUtrace Module

General Capabilities of the PDUtrace Module

OidView's PDU Trace facility is essentially a SNMP Sniffer and allows complete analysis of SNMP PDU packets. Sniff PDUs, search them for ASN.1 Tags, OIDs, values, etc. OidView's PDUtrace facility only works on SNMP conversations between OidView and the SNMP agent. It is not a stand alone sniffer designed to listen for SNMP conversations.

PDUtrace Window Layout

- ◆ Fields of the PDU Trace List
- ◆ Explanation for the TREE Decode
- ◆ Explanation for the HEX Decode
- ◆ Understand the NavBar commands
- ◆ PDU Search Panel

There is a JumpBar on the PDUtrace window, sandwiched between the PDU Trace List and the Decode areas. This JumpBar allows one to Jump directly to well-known SNMP sequences (like version, community string, etc), and to each OID in the selected PDU. This saves time when looking at large responses and the needed OID is known.

PDUtrace HEX Decode

Two parts of the HEX Decode window are the HEX (on the left), and the ASCII translation (on the right)

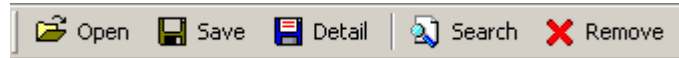
```

00: 30 82 07 39 02 01 01 04 06 70 75 62 6C 69 63 A2 |0..9.....public.
10: 82 07 2A 02 01 31 02 01 00 02 01 00 30 82 07 1D |..*..l.....0...
20: 30 14 06 0B 2B 06 01 02 01 1F 01 01 01 01 02 04 |0...+.....
30: 05 45 74 31 2F 31 30 14 06 0B 2B 06 01 02 01 1F |.Et1/10...+....
40: 01 01 01 01 03 04 05 45 74 31 2F 32 30 14 06 0B |.....Et1/20...

```

The HEX Decode window highlights the current PDU Tree selection. HEX is highlighted as blue, and ASCII text is colored RED. Clicking anywhere on either the HEX part or ASCII part will automatically highlight the appropriate PDU section in the HEX Decode window, in addition to highlighting the correct area in the PDU Tree.

PDUtrace Toolbar



Open (Trace File)

Clicking this button will read a trace file from disk and load it into the PDU Trace List.

Save (Trace File)

This will write a trace file (HEX only) to the /capture subdirectory.

Detail (Write File)

This will write a trace file which includes HEX and ASCII translation to the /capture subdirectory.

Search

Displays a search panel that enables exhaustive TAG, OID, and value searches.

Remove

This will clear the selected PDUs or ALL PDUs, depending on the response to a popup message box.



Sequence

Jump to particular sequence in the PDU.

OID

Jump to one of the specified OIDs in the PDU.

PDU Search

To display this panel, click on the Search button on the Toolbar.

TAG Match

Selected as many TAGs to search for as desired.

OID Search

Search for a specific OID in the PDU Varbinds.

Value Search

Search for specific Values in the PDU Varbinds using value operators like equals, greater than, less than.

View (Color)

Color those packets that succeed on this search.

View (Hide)

Hide those packets that do not match on this search.

Must match ALL selected parameters

If checked, all things entered in the search panel must be true in order to have a TRUE match. If unchecked, only one thing entered on this search panel will trigger a match.

Apply filter only to SELECTED packets

Search only selected PDUs for the aforementioned criteria.

Search for Version Mismatch

Check for SNMPv2c TAGs in SNMPv1 PDUs.

Search for Type/Value Discrepancies: Search for Counters going backwards or other aberrant behavior.

- ☞ Clicking the Apply Filter button will execute the search with all selected criteria.
- ☞ Clicking the Clear Filter button will clear the PDU Trace List from all coloring and/or hidden packets from previous searches.

PDUtrace Trace List

ReqId	PDU type	Length	Absolute Time	Absolute DeltaTime	PDU DeltaTime
8956	GetNextRequest	42	17:59:52.0290	00.00000000	0
8956	GetResponse	56	17:59:52.0293	00.00286622	00.00286622
8957	GetNextRequest	44	17:59:52.0295	00.00476877	00.00190255
8957	GetResponse	56	17:59:52.0296	00.00639709	00.00162832

NOTE: Not all fields are show in the image above as there is not enough room!

ReqId (Request ID)

This is the request ID for this communication stream (as read from the PDU).

Status

Error Code returned from agent (on a response), or generated by OidView (on a request).

Source Address

The name or IP Address and port of the agent sending and/or receiving the requests responses.

Community

The SNMP Community string in the PDU.

Version

The SNMP Version read from the PDU.

PDU Type

The type of SNMP PDU being decoded.

Length

The length of the PDU.

Absolute Time

The time at which the request was send / response was received.

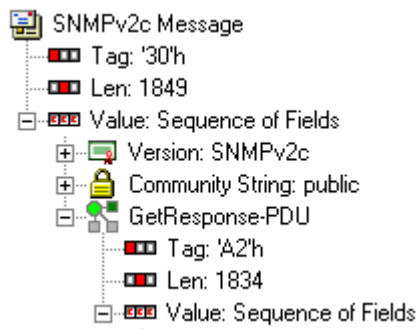
Absolute DeltaTime

The aggregate time between the first PDU request and current PDU.

PDU DeltaTime

The time between the current PDU and the last PDU. If the current PDU is a response, it would be the time between the last PDU was sent and the time when the current PDU was received (i.e. Network Time). If the current PDU is a request, it would be the time between the receipt of the last PDU and the time at which the current PDU was sent on the wire (i.e. OidView / Server Processing time).

PDUtrace Tree Decode



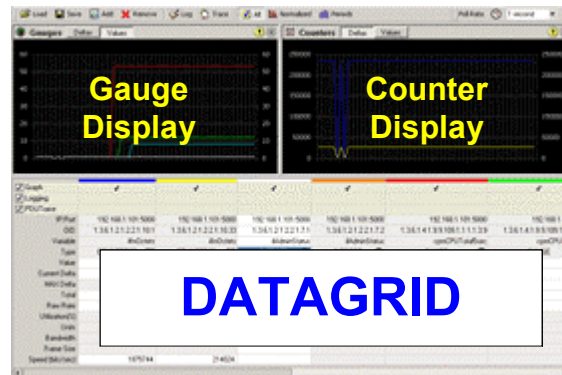
The PDU Tree Decode travels down the PDU and decodes every single part of the PDU in the exact order in which it was encoded (according to the BER or Basic Encoding Rules).

Click on any part of the PDU Tree, and the appropriate sequence will automatically be highlighted in the HEX Decode window.

PERFORMANCE

Performance Module

Performance Window Layout



General Capabilities of the Performance Module

Poll, Graph, Log OID Values in Real Time. Designed to zero-in on problems and aberrant data, the Performance Poller can capture and view data values at any interval ranging from split second polling (as many polls as the agent will handle), to one poll a minute.

- ◆ Turning Polling ON/OFF and modifying polling rates
- ◆ Using the Performance Toolbar
- ◆ Understanding the DataGrid
- ◆ Modifying the MAIN Display
- ◆ Saving and Loading Performance Poller Profiles

Performance DataGrid

Entry Specific Behavior

- ☞ To enable/disable graphing individual variable entries, double-click on the Graph Cell for that particular entry.
- ☞ To enable/disable logging for an individual entry, double-click on the Logging Cell for that entry.
- ☞ To enable/disable PDU Trace for an individual entry, double-click on the PDU Trace Cell for that entry.

<input checked="" type="checkbox"/> Graph			
<input checked="" type="checkbox"/> Logging			
<input checked="" type="checkbox"/> PDU Trace			
IP:Port	192.168.1.1:161	192.168.1.1:161	192.168.1.101:5400
OID	1.3.6.1.2.1.2.2.1.10.1	1.3.6.1.2.1.2.2.1.16.1	1.3.6.1.2.1.2.2.1.14.285
Variable	ifInOctets	ifOutOctets	ifInErrors
Type	COUNTER	COUNTER	COUNTER
Value	314474681	20134935	575844650
Current Delta	-178	204	11862
MAX Delta	15057	1012	35586
Total	5909713	4617867	275708466
Raw Rate	178.	204.	11862.
Utilization(%)	0.001	0.002	
Units	OCTETS	OCTETS	
Bandwidth	100M	100M	
Frame Size			
Speed (bits/sec)	1424.	1632.	

Attributes of the Performance Module Columns

IP:PORT

Displays the IP Address and UDP Port number requests are being sent to for this particular entry.

OID

The Object Identifier .

Variable

The Variable Name.

Type

The ASN.1 Type of object being polled.

Value

The value most recently retrieved from the last poll.

Current Delta

The difference between the Current Value and the last polled value.

MAX Delta

The largest delta recorded since polling has begun.

Total

Sum off all deltas recorded since polling has begun.

Raw Rate

This is the rate at which the value is changing per second, calculated by taking the last delta and dividing by the poll rate.

Utilization (%)

Percent Bandwidth utilization based on data arriving and the configured bandwidth of the entry.

Units (drop-down)

Valid values are OCTETS, FRAMES, CELLS.

Bandwidth (editable drop-down)

Set the bandwidth of the polled entry.

Frame Size (editable textbox)

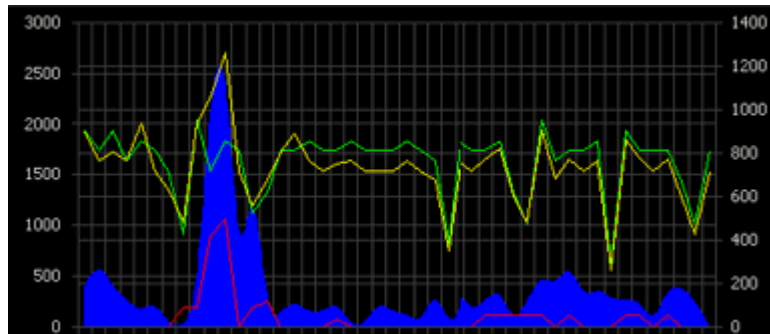
For fixed-length transmissions, set the frame size in bytes.

Speed (bits/sec)

Calculated speed in bits/second based on polled rate.

Main Display

The performance module's main graph display is capable of showing dozens of graphed entries on multiple axes. Depending on the graph mode, data will be graphed as either raw deltas (as shown below), or raw values.



Click the DELTAS or VALUES toggle buttons at the top of the display graph to choose. In addition, Counters and Gauges are displayed on different displays so the data can be more easily viewed. This has changed from earlier versions of OidView that forced you to choose only Deltas or Values and only Counters or Gauges could be seen at one time.



To modify the main display graph area, stop polling and do one of the following things:

- 🖱 Double-click on a particular series -> edit the series
- 🖱 Double-click on the graph itself -> edit the chart
- 🖱 Right-click on the graph to bring up a popup-menu -> launch the Chart Wizard, edit the Chart Data, etc.

To save the current Performance Poller configuration (OIDs being polled and graph layouts), you must save your configuration to a Performance Poller Profile.

Please Note: OidView does not automatically remember changes you make to the graphing display. When OidView is restarted, all changes made here will be reset to the defaults, unless you save your current configuration to a Performance Poller profile.

Performance Profiles

The OIDs being polled and the layout of the charts can be saved to (as well as loaded from), a configuration file on disk. This enables OidView to pick-up polling where it last left off, along with any custom chart configurations being completely restored. This is handy when there are several groups of OIDs that need to be polled habitually, as it saves the user from having to manually add those OIDs to the configuration each time OidView is started.

To save the current configuration, simply press Save Profile, and enter a filename. To load a configuration and start polling, click the Load Profile button, and select a previously saved profile from the list.

Performance Toolbar

The Performance Toolbar provides the ability to manage the Performance Poller.



Load

Load a Performance Poller profile configuration.

Save

Save the current OIDs and graphs to a Performance Poller profile configuration.

Add

Add an OID to the Performance Poller.

Remove

Remove an OID from being polled by the Performance Poller.

Log (toggle)

When toggled ON, logging will be performed for any entries that have their Logging CELL checked.

PDUTrace (toggle)

When toggled ON, tracing will occur for any entries that have their PDU Tracing CELL checked.



All (toggle)

Enabling this (default), shows all information in the Datagrid which does not change (i.e. configurable information). Disabling this hides all static information in the Datagrid.

Normalized Distribution Panel (toggle)

Enabling this will display the Normalized Distribution Graph. This is a nice way to quickly see which values are increasing or decreasing compared to others, and how much (on a comparative scale). This should be used only for a quick view and is not meant to display values of any real significance. Values are computed based on a normalized exponentially decaying scale.

Periods

Set the graph periods for the Normalized Dist. Graph and the Main Display.

CISCO BROWSER

Cisco CBQ Browser

If an agent-analysis session is created, OidView looks for the presence of the CISCO-CLASS-BASED-QOS-MIB in the agent. If it exists, the CBQ Browser button will be enabled on the session detail toolbar. This will enable the user to launch the CBQ Browser and see the current QoS configuration on the router. Once changes have been made, the visual display can be refreshed and the new configuration will be represented graphically. This is a fantastic way to quickly verify QoS configuration changes.

CBQ Browser breaks down the QoS configuration into Service Policies, Traffic Classes, and QoS objects

QoS Configuration Hierarchy				
Object Name	Object Type	Object Index	Config Index	Policy Index
- BYTESPHERE	Device			
- ATM5/0/0.201-aal5 layer-OUT	Interface			
- CBWFQ	policyMap	14427	1041	0
- LoPriority	classMap	14441	1031	14427
matchStatement	matchStatement	14445	1039	14441
queueing	queueing	14447	1043	14441
randomDetect	randomDetect	14449	1045	14441
+ BatchFQ	policyMap	14429	12353	14441
+ class-default	classMap	14453	1025	14427

PolicyMaps will be highlighted in BLUE, as the classMaps will be highlighted in yellow. The index of each object is listed in the columns to the right. Names of object types are listed in the object type column.

The hierarchical display is capable of showing multiple nested policies, enabling an administrator to view and confirm complex QoS configurations.

TRAP MANAGER

Trap Manager Overview

The OidView Trap Manager Viewer is a session module that comes with OidView by default. It is a viewer and administration tool for ByteSphere Trap Manager Service (TMS), a windows service that runs in the background. TMS receives SNMP Trap and Notification messages and this viewer will enable the user to view and manipulate each alarm in detail. The Trap Management module is incredibly powerful, versatile and offers features not found in even the top Fault Management solutions. TMS can be used for either debugging of SNMP Traps (for example, if designing an SNMP agent or troubleshooting one), as a Trap Forwarder, or as a full Fault Management solution, capable of handling tens of thousands of traps each second and storing millions of alarms. It also uses our patent-pending MIBAcquire technology to download and install MIBs when an Alarm is unknown by the system.

Licensing Options

Trap Manager comes with 10 IP licenses by default. It will accept alarms from up to 10 hosts and then it will not accept alarms from any additional hosts. To purchase addition IP licenses, please see our website for sales information. We offer several different licensing options, including an unlimited IP count per node, web-based trap-management and integration with our monitoring solution, JaguarSX.

Trap Manager has the following major features:

- ◆ Deduplication of Alarms
- ◆ Raw or post-processed forwarding
- ◆ Saving events to an access or external 3rd party database (e.g. [MYSQL](#))
- ◆ Customization of Trap Filters through the Trap Filter Manager UI or XML file
- ◆ Alerting and Notification through the Notifier
- ◆ Comprehensive administration of alarms via OidView Trap Manager UI
- ◆ Forwarding of Traps through a variety of mechanisms
- ◆ Log all incoming alarms to a text file on a global or per-matched filter basis
- ◆ Replay of a captured trap log to any IP address
- ◆ Setup Secure Users for accepting SNMPv3 Notifications
- ◆ Variety of display options
- ◆ AutoStatus daemon

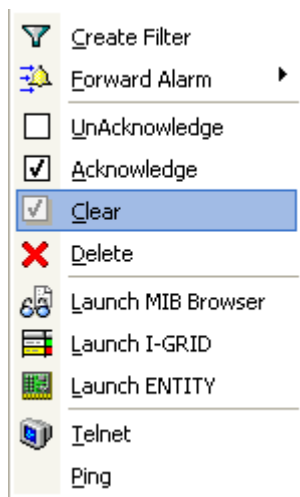
Trap Administration

Administration of Alarms

OidView's UI allows ease of administration of alarms by simply clicking on alarms and right-clicking for options.

Options include (but are not limited to):

- ♦ Creating Filters
- ♦ Forwarding alarms to a specified IP address
- ♦ UnAcknowledging Alarms
- ♦ Acknowledging Alarms
- ♦ Clearing Alarms
- ♦ Deleting Alarms
- ♦ Starting an analysis session
- ♦ Launching a MIB Browser
- ♦ Telnet
- ♦ Ping



If the Trap Detail Display options are selected in the Trap Manager Configuration, clicking on a single alarm brings up the trap specifics and Varbind detail in a nicely laid out tree structure. The MIB information is also listed on the screen in the MIB information pane.

Trap Deduplication

Trap Manager can deduplicate alarms based on:

- ♦ [Community String](#)
- ♦ [IP address](#)
- ♦ [SNMP Version](#)
- ♦ [TrapOID](#)
- ♦ [TrapType](#)
- ♦ [Varbind](#)

When OidView receives an alarm and deduplication is enabled, a trap key is created based on these properties. If a subsequent alarm is received and the same key is created for it, it is considered the same event and the existing event's count is simply incremented. If no key matches, a new event is created. This gives the administrator great flexibility on the level of detail he or she wishes to receive from managed agents. For example, if one only wants to see one alarm per unique event, all of these options should be checked. If for example, it is only wished to get one alarm per IP address, then only enable the IP dedupe filter, and disable all the rest. For fault management applications, it is highly recommended that at least some deduplication is turned on, if not all.

Deduplicating on Varbind CRC

Enabling this option will increase the number of events that would normally be registered with all other types of deduplication enabled, but it will make sure that the event is completely unique. To reduce excess noise about a particular event (i.e. collapse multiple traps with different information but describing the same event), disable this.

Trap Display Options

Alarm severity classification

Filters are the main vehicle for controlling how alarms are displayed. A filter can throw an alarm into a specific bucket, as well as assign a color-coded severity. Severities are used to classify the importance of a received alarm. The use of filters assumes that severities will be used, and the severity classification bar will be shown at the bottom of the screen. If filters are turned off, the classification bar will be removed. Likewise for alarm classification into “buckets”. If filters are turned off it is assumed that alarms will not be classified into buckets, and the classification bar will be hidden from view.

Trap Detail, Coloring and receiving non-critical Trap Types

The specific details about the received trap can be hidden or displayed. Non-critical traps classified as LOGONLY, IGNORE, or INFORMs can be displayed or hidden from view. There is also a trap manager display toolbar that can be turned on and off. This is off by default and can be turned on by going into Options -> OidView -> Trap Manager -> Display and selecting “Show Display Toolbar”.

☞ **Configurable Options** – the following options can be set in the Option Dialog located under Options -> OidView -> TrapManager -> Display

- ◆ Show Display Toolbar
- ◆ Color Grid Rows
- ◆ Store IGNORE
- ◆ Store INFORMs
- ◆ Store LOGONLY
- ◆ Show Detail Panes
- ◆ Show Detail In Grid
- ◆ Show Agent Address
- ◆ Display Update Time

Trap Forwarding

Trap Forwarding Overview

Traps can be forwarded in a variety of ways, making Trap Manager an incredibly powerful redirector of alarms. It can forward all traps (global setting), to a number of remote nodes. It can also forward traps based on a filter match or even manually by right clicking on one or more traps and choosing “Forward”. In addition, custom varbinds can be added to forwarded traps, allowing receiving management systems to identify or act accordingly. These varbinds can be defined in a custom file, set in the options.

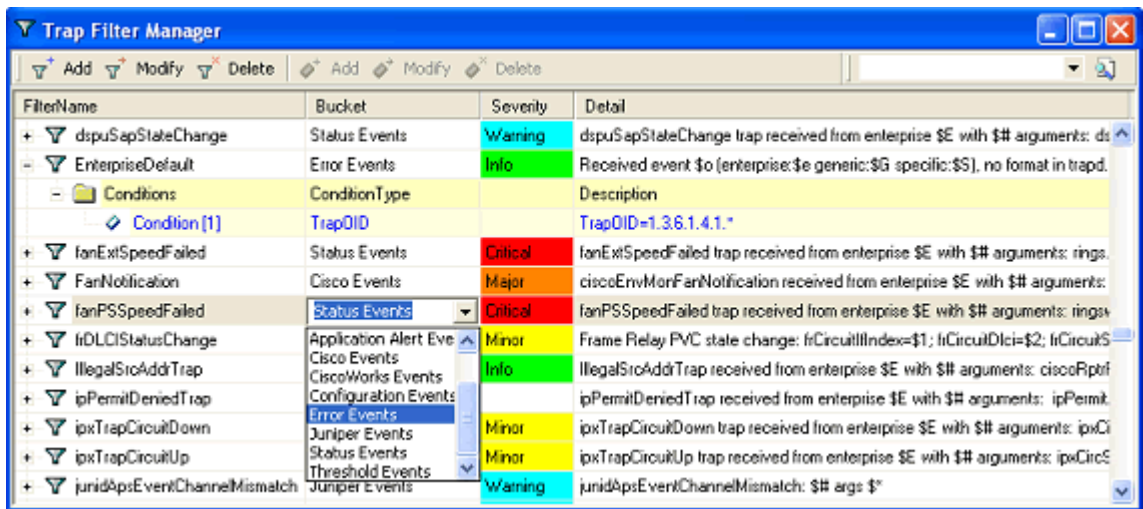
📁 **Configurable Options – the following options can be set in the Option Dialog located under Options -> OidView -> TrapManager -> Forwarding**

- ◆ Forward Traps
- ◆ Raw Forwarding
- ◆ Forward Deduped Traps
- ◆ Forward All Deduped Traps
- ◆ Forward IP Address or Hostname
- ◆ Forward UDP Port
- ◆ Send Original EngineID
- ◆ Append Varbinds
- ◆ Include Source Address
- ◆ Custom Varbind File

Trap Filter Manager

Trap Manager allows complete filter customization, showing the available filters loaded into memory in a hierarchical tree-like structure, with the filter object represented by the top-level node and Conditions nested underneath. Filters allow alarms to be classified and acted upon in numerous ways. Alarms can be categorized into buckets, assigned severities, notification profiles, etc. Filters must have one or more conditions attached to them in order for them to be enabled. A filter without conditions can exist but will do nothing. Conditions can be built using the condition builder. OidView comes with a pre-loaded trap filter configuration file “out of the box” with pre-set filters for generic events, as well as alarms from both Cisco and Juniper network gear.

Use the Filter Manager to add, modify, and delete filters:



- ☞ To add a filter, simply press “Add”.
- ☞ To modify a filter, highlight and press “Modify”.
- ☞ To delete a filter, highlight the filter and press “Delete”.

Use the Filter Manager to also change severity and bucket classifications:

- ✎ To change the bucket type for a specific filter from the filter manager, select the filter and double-click on the bucket cell for the particular filter. A drop-down list will appear, and you may select one of the available options.
- ✎ To change the severity of a particular filter from the filter manager, select the filter and double-click on the severity cell for that particular filter. A drop-down list will appear, and you may select one of the available severities

Trap Filter Builder

To get the filter builder dialog, press the “Add” or “Modify” button on the Filter Manager Dialog screen.

The screenshot shows the 'Add/Modify Filter' dialog box. It features a title bar with a close button. The main area is divided into several sections:

- File Name, Bucket, Severity:** Three dropdown menus at the top.
- Format Text:** A large text area for defining the filter's output format.
- Operation Times:** A section with six dropdown menus for 'Start Day Of Week', 'Start Day Of Month', 'Start Time Of Day', 'End Day Of Week', 'End Day Of Month', and 'End Time Of Day'.
- Time Filter:** A checkbox with a clock icon.
- Notifier Profile:** A dropdown menu with a folder icon.
- Automatically Change Status To:** A dropdown menu and a text field labeled 'Alter this many minutes->' with the value '60'.
- Forward Traps:** A checkbox with a mail icon and a 'Configure' button.
- Filter Log:** A checkbox with a document icon.
- Global Log:** A checkbox.
- Negate Filter:** A checkbox at the bottom left.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

The Filter builder allows the user to create filters with the following top-level properties:

- ◆ Classification bucket
- ◆ Assign a severity
- ◆ Format Text
- ◆ Time restrictions
- ◆ Notifier Profile
- ◆ AutoStatus
- ◆ Trap Forwarding
- ◆ Trap Logging
- ◆ Negate – apply the opposite of whatever this filter defines as a matching heuristic

After making the necessary changes, click on the OK button to save changes to the filter.

Filters also need one or more Conditions to be active.

More on Format Text

This text can be written to include tags that will substitute descriptive information into the filter's display text. A description of these tags can be found in the file: `OidView\profiles\traps\variables.txt`

Trap Condition Builder

The condition builder dialog allows one to select the type of match condition and then specify value parameters to go along with that condition.

Trap Condition Builder

Condition Type: Value: Exact Like Range RegExp

Before Time: : After Time: : Binding Index: Binding Type:

CLEAR If this condition is matched, CLEAR the trap.

SEVERITY If this condition is matched, change the trap severity.

Specify information about a value in the variable bindings. Optionally include the binding index and type.

The condition types available are:

- ♦ Source Address
- ♦ Source Port
- ♦ BindingOID
- ♦ BindingValue
- ♦ Community
- ♦ TrapOID
- ♦ Trap Name
- ♦ SNMP Version
- ♦ SNMP Agent Address
- ♦ Generic Type
- ♦ Specific Type
- ♦ Arrival Time

All of these values can be explicitly set using the condition builder UI. Values can be matched by Trap Manager using EXACT, RANGE, REGEXP, or LIKE matches, providing incredible flexibility over conditions.

There are also two special states that can be enabled for a condition – CLEAR, and SEVERITY. These two extra special states on a condition can allow for very complex filter creation.

CLEAR state can be applied if the particular condition matches. This is helpful if you can extract status information from the trap. If the information in the varbinds indicate that the trap should be cleared, you can check this in conjunction with setting the correct match values, and OidView will clear the trap.

The SEVERITY state allows control over what severity the trap is assigned. A trap can sometimes indicate in the varbinds that there should be a certain severity associated with it. OidView will change the severity based on how the condition is configured. It will also reassign an existing trap a new severity as the same trap comes in with different varbind values (if the conditions are configured to do so).

For example, a status type of Filter can be created allowing the trap to be assigned severities and cleared dynamically. A similar thing could be done with Thresholds and the RANGE operator. Instead of looking for an exact value in the varbinds, look for that value within a range, and assign it a SEVERITY or a CLEAR.

BMD GMLC Update		Status Events		STATUS: \$4
Conditions		ConditionType		Description
◆	Condition [1]	TrapOID		TrapOID=1.3.6.1.4.1.14694.1.17.2.22.2
◆	Condition [2]	BindingValue	Info	BindingValue=0 found in varbinds
◆	Condition [3]	BindingValue	Critical	BindingValue=1 found in varbinds
◆	Condition [4]	BindingValue	Major	BindingValue=2 found in varbinds
◆	Condition [5]	BindingValue	Minor	BindingValue=3 found in varbinds
◆	Condition [6]	BindingValue	Warning	BindingValue=4 found in varbinds
◆	Condition [7]	BindingValue	CLEAR	BindingValue=5 found in varbinds

NOTIFIER

Notifier Module

Very often an important event will occur that you will need notification about. The OidView Notifier module is a system module that enables notification from the OidView console without having to integrate with a third party or external Notifier application. There is an additional license cost for the Notifier but the price point and ease of use makes it an attractive addition to the OidView network management arsenal.

Alerting and Notification through the Notifier

By setting up filters, alarms can be assigned a notification profile.

Each notification profile can have a number of actions, including:

- ◆ Sending EMAIL messages
- ◆ Logging to the NT Event Log
- ◆ Sending an SMS (SMPP)
- ◆ Sending messages to an alphanumeric pager (SNPP)
- ◆ Executing an external program or script
- ◆ Sending an SNMP Trap

Status Window

The Notifier, when displayed, shows a small status window on the bottom of the OidView console. It can be enabled or disabled from here. It gives a summary of the numbers and types of events that have been sent, as well as a high-level listing of event types, times, recipients, and messages sent.

Creating a profile

Open up the Notification Profile Dialog, and click “Add”. In the textbox “Profile Name”, type in the name of the profile. Use something descriptive, like “Web Servers Down” or “Boston service not responding”. Then, choose the primary notification type for this profile by clicking on the drop-down box and choosing one of the options listed.

To add another notification type to an existing profile, just select the profile, then choose a new type, fill in the parameters, and click “Apply”. It will appear under the existing profile, along with any other notification types already defined.

To copy a notification type to a new or existing profile, simply select that type, enter the new or existing profile name in the “Profile Name” box, and press “Apply”. If the profile does not yet exist, it will automatically be created and the type will be included, otherwise it will simply be copied to a named existing profile.

To delete notification types assigned to an existing profile, simply select that type and press “Delete”

To change the order of notification types within a specified profile, use the blue up and down buttons located in the URH corner of the Notification profile tree.

☞ To rename a profile, select the profile, and click “Rename”

☞ To delete a profile, select the profile, and click “Delete”

SNMTP TESTER

SNMP Agent Testing Module

When writing an SNMP Agent, it is necessary to run comprehensive tests in order to check for compliance with the SNMP protocol standard and also compliance with the syntax of the MIB objects that will be represented. OidView now has a built-in SNMP Agent testing module (available in the Pro and Enterprise versions), that will enable the software developer to test the agent implementation and verify that it is compliant. If an agent is not compliant then it may be impossible to manage with various Network Management Systems. The result can be devastating for a new product, as users will not be able to control it or monitor it using SNMP. Agents that are fully compliant with SNMP are often more attractive to purchasers of equipment for the data center.

WARNING! Do not perform testing on a production agent or device! Doing so may cause unexpected results due to the nature of this product, as the SET tests change values that may cause undesirable results. If performing SET tests on an agent, please be sure to go through the MIB and add manual exclusions to objects that should not be tested in an automated fashion.

To use the SNMP Testing module to test an SNMP Agent, first create a session for the agent. Part of the session creation mechanism includes the automatic detection and loading of needed MIBs. If no MIBs are detected and/or loaded automatically, then the user must manually compile and/or load the MIBs desired to be tested on the agent. Once the desired MIBs are loaded in the session they will be listed in the Session MIBs grid when the session is highlighted.

Session MIBS		
Module ▾	Base OID	Base Object
EtherLike-MIB	1.3.6.1.2.1.35	etherMIB
HOST-RESOURCES-MIB	1.3.6.1.2.1.25	host
IF-MIB	1.3.6.1.2.1.31	ifMIB
IP-FORWARD-MIB	1.3.6.1.2.1.4.24	ipForward
IP-MIB	1.3.6.1.2.1.48	ipMIB

SNMP Testing Module can then be launched from the session toolbar, at the top of the screen. The button is labeled “SNMP Test”.



Once this button is clicked, OidView will launch a new window. This window will start to automatically prepare tests for use in testing the SNMP agent. Based on the MIBs loaded in the session, it will either load pre-generated MIB tests or it will dynamically create tests based on the objects defined in the loaded MIBs. Once the tests have been created for all objects, OidView will automatically write those test objects to a file named <mibName>.xml, and save it to the OidView/profiles/snmpctest directory.

The SNMP Test module has the following “Test” toolbar buttons:



Add MIBs

Manually to the test suite by clicking on the “Add MIB” button.

Build Test

If additional objects have been loaded but tests haven’t been built yet, you will need to click the “Build Test” button.

Load Test

Load a saved test suite from disk.

Save Test

Save a fully built test suite to disk, before or after it has been run.

Test Types

When a test suite is automatically built, based on the configuration options OidView will create a number of tests for each object. Creation of these test types can be controlled from the OidView Options dialog. Each of these individual tests are listed as follows:

SYNTAX

Initially performs walk on selected OIDs to get list of instances and values. Then, make sure values are within ranges and/or values that are described in the MIBs.

GET

Initially performs walk on selected OIDs to get list of instances. Then, perform individual GET operation on each index and see if response is correct.

GETNEXT

Perform GETNEXT on each OID to make sure that the response comes back in lexicographical order.

GETBULK

Performs GETBULK on each OID to make sure that the response comes back in lexicographical order and with the correct OID count and format.

GET MULTI

Initially performs walk on selected OIDs to get list of instances. Then, performs a GET with several objects and makes sure returned OIDs are the same.

SET

Initially performs walk on selected OIDs to get list of instances. Then, performs a SET with same value and checks response to make sure returned OID/value are the same.

SET POSITIVE

Initially performs walk on selected OIDs to get list of instances. Then, performs a SET with a value within accepted ranges of MIB and checks response to make sure returned OID/value are correct.

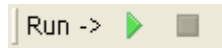
SET NEGATIVE

Initially performs walk on selected OIDs to get list of instances. Then, performs a SET with a value NOT within accepted ranges of MIB and checks response to make sure agent rejected the request.

SET MULTI

Initially performs walk on selected OIDs to get list of instances. Then, performs a multiple SET request with same OIDs and values and checks response to make sure returned OIDs/values are correct.

When a test suite is ready to be run, the “PLAY” button will be enabled on the “Run” toolbar.



Once a test suite has run, tests will be classified with status value of PASS, WARN or FAIL. A test that PASSES is one that has had no issues. A test with a WARN status means that some instances of that test passed, and some failed. A test with FAIL status means that all instances of that test failed.

All tests with one or more instances will have a (+) sign next to them and they will be expandable in the grid. Expanding a test will give much more information about each instance that runs (OID, index values, description of the failure reason, etc.)

For instance, below shows a WARNING status test with one instance that failed and the others that passed. The failed instance is because the value was 0, and the MIB specified that the value must fall between the ranges of 1 and 2147483647. Since the number 0 is not within that range, the test instance is marked as FAIL.

+	Status ▾	Object Name	OID	Index	Value	Test Type
+	FAIL	ipForwardMetric4	1.3.6.1.2.1.4.24.2.1.14			SETPOSITIVE_INTE
+	FAIL	ipForwardMetric2	1.3.6.1.2.1.4.24.2.1.12			SETPOSITIVE_INTE
+	FAIL	svPrintQName	1.3.6.1.4.1.77.1.2.29.1.1			GET_DISPLAYSTRII
+	FAIL	ipForwardMetric5	1.3.6.1.2.1.4.24.2.1.15			SETPOSITIVE_INTE
+	FAIL	hrSystemInitialLoadDevice	1.3.6.1.2.1.25.1.3			SETPOSITIVE_INTE
-	WARNING	hrStorageAllocationUnits	1.3.6.1.2.1.25.2.3.1.4			GET_INTEGER32
	PASS		1.3.6.1.2.1.25.2.3.1.4.1	1	4096	
	FAIL		1.3.6.1.2.1.25.2.3.1.4.2	2	0	
			not within range - value too small - HINT: (1 <= X <= 2147483647)			
	PASS		1.3.6.1.2.1.25.2.3.1.4.3	3	1024	
	PASS		1.3.6.1.2.1.25.2.3.1.4.4	4	65536	
	PASS		1.3.6.1.2.1.25.2.3.1.4.5	5	65536	

POP-UP MENU ITEMS

☞ **Right-clicking on a test or test instance brings up a menu.**

Run Test

Click this to re-run the selected test.

Expand Test

This expands the currently selected test's instances.

Collapse Test

This collapses the currently selected test's instances.

Add Exception

This adds an exception to the exception list.

Remove Exception

Removes an exception from the exception list.

Add Exclusion from SET Tests

Excludes this test from being included in SET tests.

Remove Exclusion from SET Tests

Removes the Exclusion.

Exceptions

There may come a time where a particular value does not match the MIB syntax but is OK and the test should PASS. In these cases, add the value as an exception by right-clicking on the instance and selecting "Add Exception". This will enable all tests with that particular OID to PASS if the specific value is seen, instead of failing it automatically. There is currently a LIMIT of 1 exception per OID.

Exclusions

OIDs can also be excluded from SET tests. For instance, one may not want to perform SET tests on a certain object like `IfAdminStatus`, because after setting a new value to the object the agent will not respond anymore (setting an interface to admin down will do that). For any of these special cases, one can add exclusions. There is currently a LIMIT of 1 SET exclusion per OID.

5 Analysis

Agent Examination and Analysis

MIB Browsing the quick and dirty way

OidView Professional is more than just a simple MIB Browser, but you have the option to use it like one. To open up a Default MIB Browser window, click the “Open Default MIB Browser” hyperlink from the Console Overview window, or double click the OidView -> Active Browsers -> DEFAULT node in the OidView NavTree .

In Depth SNMP Agent Analysis

To use OidView’s full MIB analysis capabilities, you must create a session. By creating a new session, OidView will automatically determine the agent vendor(s) (using our patent-pending MIBSense technology), download MIBs if necessary, identify the loaded MIBs on the device, and load them into OidView for use in the MIB Browser.

Once the session has been created, there are a variety of SNMP agent analysis tools at your disposal.

- ♦ Use the MIB BROWSER module to browse MIB objects and determine various properties.
- ♦ Use the iGRID module to generate a detailed interface MAP, and then query even further by polling specific interface related OIDs
- ♦ Launch the ENTITY-MIB module to determine how the device is physically laid out and how things are connected internally
- ♦ Poll OIDs and Log values with the Performance Module to monitor values or check for aberrant behavior
- ♦ Trace PDUs with the Analysis module or the Performance Module to verify proper PDU construction or load PDU trace files and perform complex searches
- ♦ Capture a MibWalk of a live agent for later analysis

- ◆ Examine the QOS configuration of a Cisco Router running the CISCO-CLASS-BASED-QOS-MIB
- ◆ Test an agent using the SNMP protocol and the MIBs loaded in the session

6 Configuration

Configuring OidView

- ☞ Click on the file menu: Tools -> Options
- ☞ Click the OidView Navigation area -> Options

Once the configuration dialog appears, changes can be made by clicking the TAB buttons on the top of the dialog.

Multiple categories will be listed in a tree like structure. Current categories include:

Database

Specify database connection and configuration information.

EMAIL

Specify email preferences.

Helper Applications

Tell OidView which applications you wish to invoke for certain actions.

Http Proxy Server

If you are behind an HTTP proxy, specify settings here

Miscellaneous

Miscellaneous

Paths

Specify paths for MIBs, compiled MIBS, etc.

SNMP Test Module

Testing preferences.

Trap Manager

Options related specifically to Trap Manager.

Configuring the Database

Prompt to compact database

Enter the maximum size desired for the database to reach. If the database reaches a size greater than the value entered (the default is 100 Megabytes), then OidView will automatically compress (and if necessary repair) the database.

Database Filename

Enter the filename of the database being used. Press the Browse button to bring up an Open File dialog box.

Backup Path

Enter the full pathname of the folder where the database will be backed up. Database backup is not automatic, it is manual. To backup your database to this folder, from the main menu press Options -> Database -> Backup Database.

Helper Apps

[TELNET application of preference](#)

Specify the favorite application used for TELNET sessions (the default is Microsoft Windows™ Telnet.exe). During an analysis session of a live SNMP Agent, it is possible to TELNET to the device (if it supports TELNET), by clicking on the TELNET button on the NavBar .

[MIB editor of preference](#)

Specify the application to use to edit MIBs. MIBs can be edited simply by right-clicking on the module in a MIB list and left-clicking Edit Definition.

[XML Editor of preference](#)

Specify a favorite editor for XML files.

Configuring Paths

[Compiled MIBs \(bPCMs\)](#)

Enter the location where compiled MIBs will be stored and accessed.

[ASN.1 MIBs](#)

Enter the location where MIBs are generally stored.

[Working Directory](#)

Enter the location that OidView can place temporary files.

Trap Manager - Forwarding

Custom Varbinds Enabled

Select this to append custom varbinds to all forwarded traps. If enabled, Trap Manager will parse a custom varbind file and append the entries to the bottom of the current trap's varbinds. This will not happen if raw forwarding is enabled.

Custom Varbind File

Specify a custom file for appended varbinds. When forwarding traps, Trap Manager will read and parse this file and append the resulting entries to the current trap.

Forward Traps

Should TrapManager forward traps? This occurs on a global scope. To forward only traps that match filters, use the Filter Manager or the Notifier.

Forward Deduped Traps

Should TrapManager forward traps that have previously been deduplicated? The default is FALSE, the behavior being that once a trap is deduplicated it will be forwarded only the first time it is received, and never forwarded again unless the event within OidView is cleared. If enabled, the trap will be forwarded once each time the trap is received per event burst (i.e. if a burst of the same trap is received 1000 times in less than 100ms, it will only be forwarded once).

Forward All Deduped Traps

Should TrapManager forward ALL traps it receives, regardless of whether deduplication is on? (i.e. if a trap is received 1000 times in a burst event, even if dedupe is ON, the trap will be forwarded 1000 times to the next event receiver).

Forward IP Address or Hostname

Specify the IP Address or HostName of the station to which the traps will be forwarded. To specify multiple addresses, use the comma “,” delimiter. This occurs on a global scope. To forward only some traps, use the Filter Manager or the Notifier.

Forward UDP Port

Specify the UDP Port of the station which will receive the forwarded traps

Include Source Address

Includes the source IP address of the host that originally sent the trap in the varbinds of the forwarded trap. This enables the receiving station to correctly identify the original source of the trap (needed for v2 traps). This is enabled by default.

Raw Forwarding

Enables RAW Forwarding for Trap Manager. In this mode, all traps are forwarded before any processing or deduplication. Normally, all forwarding is performed after traps are processed.

Send Original EngineID

If using SNMPv3 secure communications, enable this to send the original EngineID of the SNMPv3 agent that originally sent the trap. Otherwise, the localEngineID of the local machine is sent.

Trap Manager - Deduplication

Dedupe Enabled

Should deduplication filters be applied? Default is TRUE.

Dedupe Community

Deduplicate on Community String

Dedupe IPAddress

Deduplicate on IP Address

Dedupe SNMPVersion

Deduplicate on SNMP Version

Dedupe TrapOID

Deduplicate on TRAP or Notification OID

Dedupe TrapOID (Base)

Deduplicate on TRAP or Notification OID, but do not include the Generic and Specific Type.

Dedupe TrapType

Deduplicate on Trap Type (i.e. SNMP v1 TRAP, SNMPv2 Notification, SNMPv2 Inform, SNMPv3 Notification, etc.)

Dedupe VarBind

Deduplicate on Varbind CRC. Enabling this option will increase the number of events that would normally be registered during complete deduplication, but it will make sure that the event is completely unique. To reduce excess noise about a particular event (i.e. collapse multiple traps with different information but describing the same event), disable this.

Trap Manager - Filters

Filters Enabled

Are the trap filters enabled? If they are disabled, no special filter matching will occur.

Fast Match Enabled

Enable only Filters based on TrapOID. This greatly speeds up the filter process, but complex filters are not processed. Default is FALSE.

Trap Manager - Status/Storage

Alarm Clear Time

Amount in time in minutes that TrapManager will wait until automatically clearing traps that have not been updated within that amount of time. After a trap is cleared, if it is received again it is considered a completely different event. Set this value to 0 to never clear traps and force a user to clear them manually. This setting occurs on a global scale. To adjust clear times on individual traps, please use the Filter Manager.

Alarm Clear All

Enable this to apply the Alarm Clear Time to ALL traps. Disable to apply the Alarm Clear Time only to traps that DID NOT match a filter.

AutoDelete Cleared Traps

Enable this value to automatically delete all traps that are cleared.

AutoStatus Original Time

Enable this value to use the original receive time in autostatus calculations. Otherwise, the last updated time will be used (default).

Maintenance Time

The amount of time to wait in minutes between trap maintenance jobs. Any traps that need to change status according to filter rules or be cleared and/or deleted due to maximum limits are handled in this loop. The default time is set to 60 minutes but this can be set as low as 1 minute (60 seconds).

Maximum # Traps in Queue

Specify the maximum number of events that can be stored in the receive event queue before processing is launched. Valid range is between 100-10000 traps.

Maximum # Traps in DB

Specify the maximum number of traps to be stored the database. If this number is reached, 10% of the traps in the database will be deleted automatically.

Maximum # Traps in Memory

Specify the maximum number of traps to be stored in memory. If this number is reached, 10% of the traps in memory will be deleted automatically. Keeping traps in memory is handy if performing maintenance on the trap DB as traps can be manually forwarded and inspected.

Permanently Delete Traps

Check this to permanently delete traps from the database. Otherwise, deleted traps will continue to be stored in the database and they will simply be marked as deleted and retired.

Store Varbinds

Check this to store the varbinds in the database. Storing varbinds in the database will use a lot of storage. Default is FALSE.

Trap Manager - Miscellaneous

Disable Trap Processing

Disables all trap processing except RAW Forwarding mechanism. Enable only if Trap Manager is acting as a RAW forwarder.

EventLog Enabled

When enabled, ByteSphere eventLog traps will be sent to the Address and UDP port specified. An EventLog trap is sent when a trap matches a pre-defined filter, and the event type and class type parameters for the filter are defined.

EventLog Address

Specify the IP Address to send eventLog traps.

EventLog UDP Port

Specify the UDP port to send eventLog traps.

Notification - Unknown Event

Have the notifier handle any and all unknown traps with a specific named profile. For example, if you wanted Trap Manager to send emails for all unknown traps it receives, create a notification profile called NOTIFY_EMAIL and then place that name into this field.

Notification - Severity Event

Have the notifier handle all traps with a specific named profile for the default Notifier severity. For example, if you wanted Trap Manager to send emails for all critical traps it receives, create a notification profile called NOTIFY_EMAIL_CRITICAL and then place that name into this field.

Notification - Severity Value

Specify the minimum severity value (as an integer) that will trip the Severity Event Notification Profile. (1=info, 2=warning, 3=minor, 4=major, 5=critical)

Notification - MIB Lookup

Lookup MIB descriptions for trap filter events when sent through the notifier.

ODBC Connect String

To have trap manager use an ODBC datasource rather than the default DB connection, please specify the connect string here. Please bear in mind that this functionality requires an additional license. To purchase, please contact ByteSphere Sales department. For example, to connect to a local database named bytesphere with username and password 'bytesphere' using the MySQL ODBC driver, one could use the sample connect string:

```
ODBC;uid=bytesphere;pwd=bytesphere;server=127.0.0.1;driver={MySQL ODBC 3.51 Driver};database=bytesphere;dsn='';
```

Trap Sound Enabled

Play a wave file when a trap is received.

Trap Sound File

Specify Sound File to play when trap is received

Trap Buffer Size

Size of the TRAP buffers in Megabytes. Default is 1 Megabyte.

Trap Engine ID

Specify the ENGINE_ID for this Trap Manager.. Default is 0.

Trap Manager TimeZone

Specify the TimeZone for this Trap Manager.

Trap Manager - Display

Color Grid Rows

Color the entire row of a registered alarm? If unchecked, just the severity column will be colored.

Display Update Time

Amount of time in milliseconds before TMS sends a message to update the OidView Trap Manager Display. Default is 5000 (5 seconds). For slower systems or accessing TMS over a network, make this number larger.

Show Agent Address

Show the Agent Address field in the Trap Manager grid. This field is populated in V1 traps when they are forwarded via a proxy. It is intentionally left blank in this grid when the trap is received directly from the source.

Show Detail In Grid

Show trap detail in grid.

Show Detail Panes

Show all trap detail panes including trap tree showing varbinds, mib info, etc.

Show Display Toolbar

Show the visibility toolbar. This toolbar toggles many of the options available here.

Store IGNORE

Store IGNORE traps. Disabling this (recommended) causes IGNORE traps to be ignored. Enabling this causes all IGNORE traps to be logged, stored in the database, and displayed in the grid. This uses extra memory - it is advised to only use this when debugging.

Store INFORMs

Store INFORM request messages. Disabling this (recommended) causes INFORM requests to be ignored. Enabling this causes all INFORM traps to be logged, stored in the database, and displayed in the grid. This uses extra memory - it is advised to only use this when debugging.

Store LOGONLY

Store LOGONLY traps. Disabling this (recommended) causes LOGONLY traps to only be logged to the logfile if logging is enabled. Enabling this causes all LOGONLY traps to be logged, stored in the database, and displayed in the grid. This uses extra memory - it is advised to only use this when debugging.

Trap Manager - Logging

Global Logging

Log all traps received to the global trapLog.log file.

Log Duplicate Events

Log all traps received including any new duplicate events of previously received traps. This is the most accurate logfile mode but will take a large amount of space on your hard disk. Turning this off while Trap Manager is deduplicating events will result in a much smaller logfile. Please see the documentation for

more details.

Logfile Filename Format

Specify the filename format for the traplog files. Currently supports the following values:

0 = default (logs all traps to “trapLog.log”)

1 = timestamp (logs all traps to “trapLog_timestamp.log”)

Maximum Logfile Size

Specify the maximum size of a trap log file in Megabytes. When the logfile exceeds the maximum size it will be renamed to “logFileName_currentdate” and a new one will be created. Default is 100 Megabytes.

Trap Manager - Transport

SNMP Agent IPAddress

The IP Address for the interface that the SNMP Agent binds to. Only valid on machines with more than one NIC card. Currently agent is only used for sending and forwarding traps. If set to localhost or 127.0.0.1 the agent will bind to system's default IP address. If forwarding traps to an external network make sure to set to the outbound address.

SNMP Agent UDP Port

The UDP Port that the TMS SNMP Agent binds to. Currently TMS agent is only used for sending and forwarding traps.

Trap Manager Listening IPAddress

The IP Address for the interface that the Trap Manager starts listening for traps on. Only valid on machines with more than one NIC card.

Trap Manager Listening UDP Port

The UDP Port that the Trap Manager listens for traps on.

7

Miscellaneous

Adjusting Polling Intervals

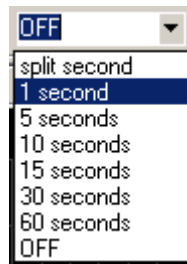
To adjust the polling interval for the Data Window or the Performance Module , double-click on the drop-down combo box in the upper right hand corner of the window:



If the StatusBar is visible at the bottom of the screen, you will see the poller status:



The drop-down combo box should open, listing several valid polling intervals:



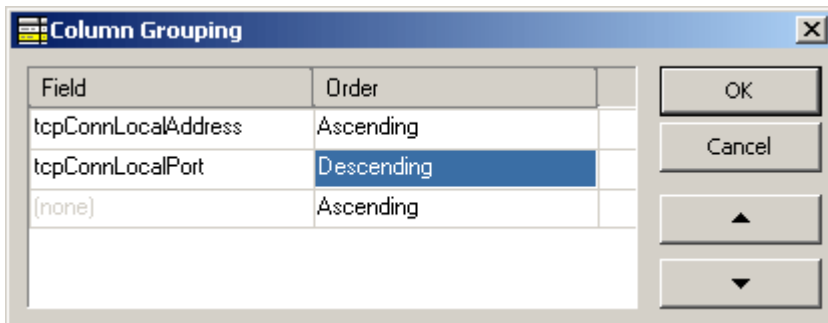
Choose the desired interval (1 second is the default), and click on something else on the screen (or TAB away from the combo box), so it loses focus. The SNMP Poller will then calibrate itself. This could take a second to a minute depending on the polling interval chosen and the number of variables currently in the poll list. If the StatusBar is visible, you will see that the poller is calibrating. After the SNMP Poller has been calibrated, it will begin polling:

The Poller status light will blink with a green color every time it is in the middle of a poll.

Column Grouping

OidView allows advanced grouping on any part of the MIB variable, OID, index, or even the resulting values from the agent.

☞ To use grouping, right-click on the LiveGrid (as long as it is full of results), and click on the **Group By** command. A dialog box will popup allowing a choice of up to 3 columns to group.



1. Select the Field from the drop-down combo box
2. Select the Order (ascending or descending) from the adjacent drop-down combo box
3. Add as many fields as needed (up to 3). Adjust the order as necessary with the up/down buttons.
4. Click OK to group result sets or Cancel to cancel the column grouping dialog.

Results:

tcpConnLocalAddress	tcpConnLocalPort	Variable	Type	Value
[-] (5) tcpConnLocalPort = 80				
192.168.1.1	80	tcpConnState	INTEGER	3
192.168.1.1	80	tcpConnLocalAddress	IPADDRESS	192.168.1.1
192.168.1.1	80	tcpConnLocalPort	INTEGER	80
192.168.1.1	80	tcpConnRemAddress	IPADDRESS	255.255.255.255
192.168.1.1	80	tcpConnRemPort	INTEGER	0
[-] (5) tcpConnLocalPort = 8080				
192.168.1.1	8080	tcpConnState	INTEGER	3
192.168.1.1	8080	tcpConnLocalAddress	IPADDRESS	192.168.1.1
192.168.1.1	8080	tcpConnLocalPort	INTEGER	8080
192.168.1.1	8080	tcpConnRemAddress	IPADDRESS	255.255.255.255
192.168.1.1	8080	tcpConnRemPort	INTEGER	0

Index Types

OidView stores learned OctetString parsing information in a file named `octetParse.ini` in the profiles subdirectory. This can be edited manually if desired. For up-to-date value definitions, please refer to the `idxTypes.txt` file in the same directory.

In most cases, with an accurate MIB, OidView should be able to automatically determine the indexing and add an entry into the `octetParse.ini` file. For those cases that it cannot determine the indexing, or figures it out incorrectly, this file can be manually edited to rectify any display problems (OidView must not be running while this file is being edited).

The entries of this file simply list the variable name, and the internal OidView type that should be mapped to it.

For example, `xtmClassName` has been given a value of 3. One can see from the table below that 3 maps to a length encoded displayString (it will be translated to ASCII text).

Modify `octetParse.ini` to add unknown or indeterminable index types to OidView.

Internal OidView Index Types

0,INTEGER	- length is 1
1,OCTETSTRING_LE	- length encoded (first octet)
2,OCTETSTRING	- not length encoded*
3,DISPLAYSTRING_LE	- length encoded (first octet) - convert to ASCII
4,DISPLAYSTRING	- not length encoded* - convert to ASCII
5,STRING	- length unknown*
6,OID	- length unknown*
7,TIMETICKS	- length is 1
8,IPADDRESS_V4	- IPV4, length of 4 octets
9,IPADDRESS_LE	- length encoded (probably 5 octets)
10,IPADDRESS_V6	- IPV6

LiveGrid Actions

In-Grid actions

Column Sort

Click on a column to sort the grid by that column

SNMP SET Value

To set a value on a live agent, simply double-click on any light blue cell to edit the value. MIB variables with enumerated values display a drop-down list box..

Right-click LiveGrid for the popup-menu:

Copy

Copies values for all / selected rows. Copies contents of the cells of LiveGrid to the clipboard. Contents of the clipboard can then be pasted into a text editor or a Microsoft Excel™ Spreadsheet.

Export Data

Export data for all / selected rows. Values can be exported to CSV, directly to Microsoft Excel™ (if installed), and XML.

Sum Numeric Cells

Sum values for all / selected rows. Sums all numeric values in the Value column and places the result in the clipboard.

Indexing

Display Indexing Information. Toggles MIB index extraction ... check/uncheck this to enable/disable index string parsing (per session)

Table Format

Display values in tabular format with columns on the top and rows going down.

Group By

Groups related columns for better/different organization of data.

Remove Grouping

Removes Groups that were created by Group By

GRAPH OID

Launches the Performance Module with this particular OID

SNMP SET

Launches the SNMP SET Dialog

SNMP GET

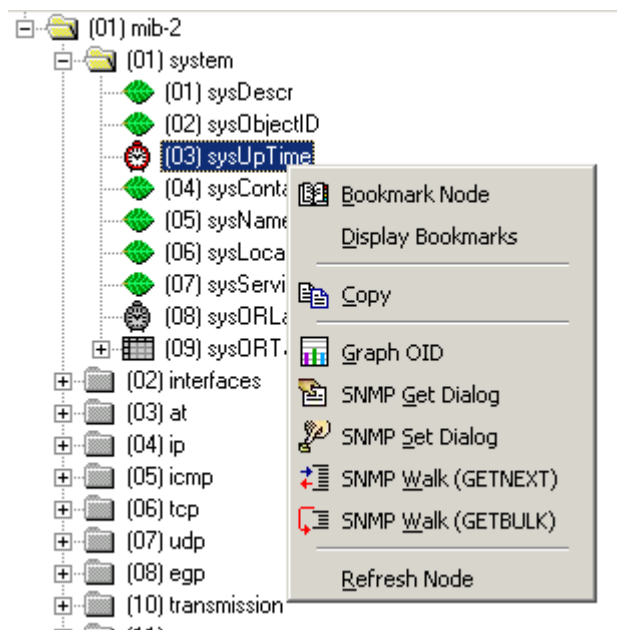
Launches the SNMP GET Dialog

Unselect

Unselects selected rows in the LiveGrid.

MIB Tree Actions

☞ Right-click the MIB Tree for the popup menu



Bookmark Node

Controls whether selected variables will be bookmarked.

Display Bookmarks

Display the Variable Bookmark dialog.

Copy

Copy the selected variable to memory.

Graph OID

Walks selected OID and if there is more than one allows the user to select the response. Then the OID will be polled and graphed by the Performance Poller.

Perform SNMP Get Operation

Display the custom SNMP GET Dialog.

Perform

Display the custom SNMP SET Dialog.

SNMP Walk (GETNEXT)

Performs a walk using SNMPv1 on the selected variable.

SNMP Walk (GETBULK)

Performs a walk using SNMPv2c GETBULK on the selected variable.

Refresh Node

Deletes and recreates the Node in the MIB Tree.

Profile Overview

What is a MIB Definition Profile?

This is simply a list of MIBs that is saved in a text file named <profile name>.txt in the /profiles/module subdirectory. A MIB Definition Profile can enable a quick determination of supported MIBs on an agent.

How is a Definition Profile created?

MIBs can be selected from the MIB Module List and saved to a MIB Definition Profile.

- ◆ If MIBs are saved to an existing definition profile, they will simply be added to it. Duplicates will be removed.
- ◆ If this is going to be a new profile, simply type in the new name.
- ◆ When finished, press Save Profile.

How is it used?

When creating a new session, the AutoLoads and Profiles Tab will display a ComboBox which allows the choice of a profile. If you were in need of determining if an agent supported any QoS (Quality of Service) MIBs over a variety of vendors, and you had created a MIB Definition profile which listed several QoS MIBs, then you could select that particular profile for use with your analysis. During the initial analysis phase, the agent will be queried for each MIB listed in the profile. If the agent responds to the query, that particular MIB will be loaded.

This is also useful when certain vendors have purchased other vendors. If a particular device has a SysOid saying it belongs to the new vendor, yet the MIBs loaded on the device belong to the old vendor, one may construct vendor profiles to accommodate for these vendor buyouts.

MIB Index Extraction

Variable	tcpConnLocalAddress	tcpConnLocalPort	tcpConnRemAddress	tcpConnRemPort
tcpConnState	0.0.0.0	23	0.0.0.0	0
tcpConnState	10.1.1.1	23	10.1.1.98	1423
tcpConnState	127.0.0.11	7161	0.0.0.0	0
tcpConnState	127.1.1.1	13006	0.0.0.0	0

OidView can automatically extract the indices out of the OID and place them into separate columns, available to the user for searching, sorting, and grouping. OidView learns how new variables are indexed as it goes, by assigning an internal index type. See how to toggle MIB Index extraction by looking under LiveGrid Actions.

MibWalk

A MibWalk is a file which contains any number of OIDs and/or variables, Types, and Values. This information can be used later by OidView by creating a MibWalk session, it can be simulated by using an SNMP simulator, or it can simply be perused by using a text editor.

- » To capture a MibWalk of an agent:



From OidView

Once a session (live agent) has been created, click on the Mibwalk button on the session feature bar. The mibwalk will be placed in the /mibwalks subdirectory.

From the Command Line

Open a command prompt, go into the \tools subdirectory.

Run walkAgent.tcl by typing: `runtcl walkagent.tcl -ip <ipaddress>`

Type `runtcl walkagent.tcl -?` to get a listing of all command line parameters...

From the Microsoft Windows™ start menu

Start -> Programs -> ByteSphere -> OidView -> WalkAgent

A window will popup, which looks similar to the create new session dialog.

Change required parameters, click TEST, and if successful, click MibWalk.

An example of a ByteSphere Format mibwalk

```
.1.3.6.1.2.1.1.1.0 OCTET-STRING 43:69:73:63:6F:20:53:79:73:74:65:6D:73:20:57:53
:2D:43:36:35:30:39:0A:43:69:73:63:6F:20:43:61:74:61:6C:79:73:74:20:4F:70:65:72:
61:74:69:6E:67:20:53:79:73:74:65:6D:20:53:6F:66:74:77:61:72:65:2C:20:56:65:72:7
3:69:6F:6E:20:36:2E:33:28:34:29:0A:43:6F:70:79:72:69:67:68:74:20:28:63:29:20:31
:39:39:35:2D:32:30:30:32:20:62:79:20:43:69:73:63:6F:20:53:79:73:74:65:6D:73:0A

.1.3.6.1.2.1.1.2.0 OID 1.3.6.1.4.1.9.5.44

.1.3.6.1.2.1.1.3.0 TIMETICKS 9377552

.1.3.6.1.2.1.1.4.0 OCTET-STRING

.1.3.6.1.2.1.1.5.0 OCTET-STRING 6C:65:78:6C:61:62:2D:36:35:30:39:62

.1.3.6.1.2.1.1.6.0 OCTET-STRING

.1.3.6.1.2.1.1.7.0 INTEGER 2

.1.3.6.1.2.1.2.1.0 INTEGER 76
```

Defining SMI and other important information.

SMI (Structured Management Information), consists of the building blocks for the base of all MIB definitions.

1	iso
1.3	org
1.3.6	dod

Iso(1).org(3).dod(6) are OIDs which are defined in SMI. The IANA (Internet Assigned Numbers Authority) keeps track of these numbers, and keeps a list of the SMI in the smi-numbers.txt file, which can be downloaded off their web site: <http://www.iana.org/assignments/smi-numbers>.

OidView can be fed this file to learn the SMI (or any updates to it). If it is desired to change the SMI in any way, simply update the file (\iana\smi-numbers.txt), and click Options -> Database -> Update DB Component -> SMI Numbers.

Enterprise Numbers

This is the list of numbers belonging to all private corporations and individuals that have registered with the IANA for a private number. This number is located under internet(1).private(4).enterprises(1). Thousands of entities have registered for these numbers. OidView understands these numbers and consequently knows which numbers belong to which vendors. Very often, the IANA updates the list of enterprise numbers: <http://www.iana.org/assignments/enterprise-numbers>.

OidView can be fed this file to learn the latest enterprise numbers. Simply save the file as \iana\enterprise-numbers.txt, and click Options -> Database -> Update DB Component -> Enterprise Numbers. Since there are so many vendors, it may be desired to trim down the file, especially if only interested in looking at network equipment from a handful of vendors. Keep in mind though that if a vendor is removed, OidView will not recognize it.

lanalTypes

These consist of the types of interfaces defined by the SMI. This list can also be found in the IANAIfType-MIB. OidView understands ifTypes, and keeps a special table in the database specifically for ifTypes.

There are two things which will cause the ifTypes to get updated:

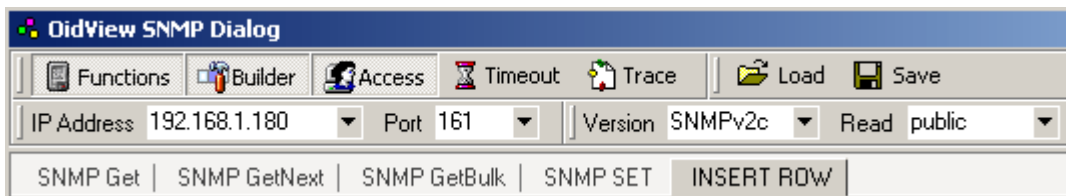
1. read in SMI
2. compile IANAIfType-MIB

SNMP Dialog

The SNMP Dialog is a tool that the administrator can use to do simple and complex SNMP operations on an SNMP Agent. It can also be used to build complex SNMP Instruction sets to be used at a later date. To launch a new SNMP Dialog, select the Drop-down on the New button on the top toolbar, then click “New SNMP Dialog”.



This will bring up a window that has a number of toolbars and TABs at the top. Simply changing the values in the IP Address, Port, Version, and Community String (Read/Write) dropdowns can change the SNMP Access parameters.



- ☞ “Functions” will show/hide the SNMP operation tabs.
- ☞ “Builder” will show/hide the PDU Builder pane.
- ☞ “Access” will show/hide the access parameter menus.
- ☞ “Timeout” will show/hide the timeout parameter menus (not shown here).
- ☞ “Trace” will trace SNMP PDUs and have them recorded into the PDU Trace Module.
- ☞ “Load” will load a set of SNMP instructions from disk
- ☞ “Save” will save a set of SNMP instructions to disk

SNMPv3 Configuration Dialog

The SNMPv3 Configuration Dialog is available in the Professional Version. It allows the user to configure the parameters needed to open a SNMPv3 session with an agent.



Snm Protocol / Session Creation Dialog

To get the SNMPv3 Configuration Dialog, open up the Session Creation Dialog and select SNMPv3 for protocol: a little golden key will appear to the right. Click the key and the following dialog will appear:



SNMPv3 Configuration Dialog

This dialog will also appear when creating a new session or configuring an existing session and OidView attempts to automatically perform SNMPv3 engine discovery. Fill in the required fields for the specific agent you are going to analyze and press Test SNMPv3 Connection. If you have entered the parameters correctly, you will get a success message box and the light bulb will light up. If there is something wrong with the configuration you have entered, recheck your values and try again.

Relevant Fields

Context Engine ID

Information Only. This is the discovered EngineID of the agent you are adding a session for.

Engine Boots

Information Only. The number of times this agent has restarted.

Engine Time

Information Only. The Engine Time represents the local time of the SNMPv3 agent. This will automatically be used to synchronize with OidView MIB Browser when analyzing this agent.

Context/Group

The SNMP Context of this agent instance. Often public. Synonymous with community for previous versions of SNMP.

SecurityName / UserName

The Security Name or User Name that will be used to access this SNMP agent.

Security Level

The Security Level used to access this agent. The three security levels available in SNMPv3 are:

- noAuthNoPriv (for no authentication and no privacy)
- AuthNoPriv (for Authentication but no privacy)
- AuthPriv (for communications using both Authentication protocol AND Privacy protocols)

Authentication Protocol

OidView currently supports MD5 and SHA protocols for SNMPv3 authentication.

Authentication Password

This is the password used to authenticate to the SNMPv3 agent.

Privacy Protocol

OidView does not currently support privacy, this will be supported in the next release.

Privacy Password

This is the password used for privacy communications.

MIB Variable Grid Actions

- ☞ Use CTRL and left mouse click to select one at a time.
- ☞ Use SHIFT and left mouse click to select multiples.

Right-click Grid for the popup menu:

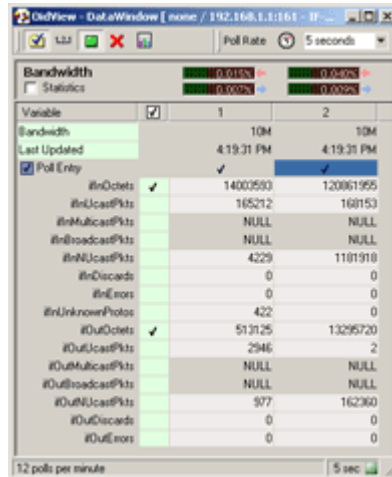
- ◆ Bookmark Selected Rows : Controls whether selected variables will be bookmarked for ALL sessions or just this session.
- ◆ Copy Selected Rows : Copy the selected variables and OIDs to the Clipboard
- ◆ DeSelect Selected Rows : Deselect the selected rows in the Variable Grid

Vendor MIB Registration

OidView will automatically determine the agent's enterprise number by querying the SysOid.

If OidView does not yet have any registered MIBS for this vendor, it will attempt to download Pre-Compiled MIBs from ByteSphere's website. If a vendor MIB-PAK exists, OidView will automatically download it and install it, and the MIBs will instantly be registered into OidView's database, providing a plethora of new information for OidView to access during analysis.

OidView Data Window



- ◆ Using the Toolbar
- ◆ Turning Polling ON/OFF and adjusting intervals
- ◆ Bandwidth BARs

Easily Drill-Down from the interface or sub-interface level into a data window which contains a pre-defined set of statistics (these can be altered in the XML profile). These statistics can be collected at almost any interval ranging from a timed poll of 1 poll per minute down to a poll every second. See which values are NULL or behaving strangely. Launch the Performance Module and log, graph, even trace PDUs for a specific variable. Collect like statistics for like interfaces in the same data window. Have ultimate control by turning polling ON or OFF for each individual interface, and even each individual variable (controlled by individual checkmark cells).

Data Window Toolbar



Show All

Displays variables which have been deprecated by newer variables (e.g. ifInMulticastPkts deprecates ifInNUcastPkts, so ifInNUcastPkts would be displayed as well if this button was pressed (default).

Show OID

Displays the OID as well as just the variable name.

Poll Entry (live agent only)

Turn polling on for this interface entry.

Remove Entry

Remove the interface entry from the Data Window.

Performance

Select a variable for a particular entry (by clicking on a cell), and toggle this button. This variable will be transferred to the Performance Module's poll list.

Index

Symbols

A

Add Exclusion from SET Tests 96
 Add MIBs 92
 Administration of Alarms 78
 Advanced Filter 38
 Alarm classification bar 81
 ASN.1 MIBs 104
 Authentication Password 132
 Authentication Protocol 131
 AutoLoads 123
 AutoWalk 39

B

Backup Path 103

C

Cisco CBQ Browser 76
 CISCO-CBQ Browser Module 33
 Collapse Test 96
 Column Sort 119
 Command Toolbar 42
 Compiled MIBs (bPCMs) 104
 Configure Session 38
 Configuring OidView 101
 Configuring the Database 103
 Connection Configuration Toolbar 35
 Context Engine ID 131

D

Database 101

Data Window 134
 Data Window Toolbar 135
 deduplication 80
 Default MIB Browser 34
 Definition Profile 123
 Discover 32
 Discover Subnet tool 51
 Display Bookmarks 121
 Drill-Down 134

E

EMAIL 89
 Engine Boots 131
 Engine Time 131
 ENTITY-MIB Module 53
 Expand Test 96

F

Filter By Toolbar 40
 Format mibwalk 126
 Forward UDP Port 82

G

GET 93
 GETBULK 93
 Get Device Capabilities 51
 GET MULTI 93
 GETNEXT 93

H

Helper Applications 101
 Helper Apps 104
 HEX Decode 60
 Hide Containers 53
 Hide Empty Containers 53
 Http Proxy Server 101

I

IanaIfTypes 128
 IGNORE 14
 IGRID Assignment 55
 iGRID Module 56
 iGRID Schema 57
 iGRID Toolbar 99
 In Depth SNMP Agent Analysis 15
 Indexing 119
 InfoGrid 81
 INFORMs 69
 In-Grid actions 119
 Internal OidView Index Types 118

J

JumpBar 37

K

L

Launch Layout Dialog 43
 Layout Toolbar 43
 LiveGrid 46, 49
 LiveGRID 43
 Live SNMP Agents 17
 loading an old session 18
 Load MIBs 38
 LOGONLY 81, 112

M

Main Information Window 2
 Manual GET 38
 Manual SET 38

- MAX Delta 69
- MIB Browser 2
- MIB Browsing 99
- MIB Definition lists 21
- MIB Definition profile 23
- MIB Definition Profile 123
- MIB detection 14
- MIB Discovery and AutoLoad 36
- MIB editor 104
- MIB Info 43
- MIB Management screen, 21
- MIB Module List 22
- MIB MODULE List 15
- MIB Tree 46
- MibWalk 125
- MOF Files 47

N

- NavBar Commands 38
- Nav Tree 2
- Normalized Distribution Panel 75
- Notifier 32
- Notifier Module 89
- NT Event Log 89

O

- octetParse.ini 118
- OctetString parsing 118
- OID 69
- OID Search 62
- OidView NavBar icon 17
- OidView NavBar Lookup Old Session icon 18

P

- Paths 102
- PDU DeltaTime 65
- PDU Search 62

- PDUtrace 38
- PDUTrace 32
- PDUtrace HEX Decode 60
- PDUtrace Module 58
- PDUtrace Toolbar 61
- PDUtrace Trace List 64
- PDU Tree Decode 66
- Performance Module 67
- Performance Module Columns 69
- Performance Poller 72
- Performance Profiles 73
- Performance Toolbar 74
- Performance Window Layout 67
- Poll Entry 135
- POP-UP MENU ITEMS 96
- Pre-Compiled MIBs 103
- Privacy Password 132
- Privacy Protocol 132

Q

R

- Registering Pre-Compiled MIBs 29
- remove a session. 19
- Remove Entry 135
- Remove Exclusion from SET Tests 96
- Run Test 96

S

- Search By Toolbar 40
- Search Toolbar 40
- Security Level 11, 131
- Security Name 11
- SecurityName 131
- Send Original EngineID 82
- Session Feature Bar 15
- Session Feature toolbar 4

- Session MIBs 30
- Session QuickBar 4
- Session Tabs 5
- SET 93
- SET MULTI 94
- SET NEGATIVE 94
- SET POSITIVE 94
- Show All Objects 41
- Small Nodes 53
- SMS 89
- SNMP Agent 8
- SNMP Agent Testing Module 91
- SNMP Agent Test Module 33
- SNMP Community 64
- SNMP Configuration Toolbar 35
- SNMP Dialog 129
- SNMP GET 120
- SNMP Get Operation 122
- SNMP PDU 64
- SNMP SET 120
- SNMP Set Operation 122
- SNMP SET Value 119
- SNMPv3 authentication 11
- SNMPv3 Configuration Dialog 10, 130
- SNMP Version 64
- SNMP Walk (GETBULK) 122
- SNMP Walk (GETNEXT) 122
- StatusBar 81
- Store IGNORE 81
- Sum Numeric Cells 119

T

- TAG Match 62
- Telnet 38
- TELNET application 104
- Test Types 93
- Trap Condition Builder 81
- Trap Detail 85

Trap Filter Builder 83
Trap Filter Manager 32
Trap Manager 77
Trap Manager Overview 43

U

UDP Port 82, 105
unload MIBs 30
Use Relative Position 54
UserName 131

V

Varbind CRC 80
Variable and Layout Memory
 36, 48
Variable Bookmarks 44
Variable GRID 43
Vendor MIB Registration 133

W

walkAgent.tcl 126
WMI BROWSER 47
WMI Queries 48
Working Directory 104

X

XML Editor 104

Y

Z

ByteSphere

ByteSphere LLC
260 Franklin Street, 11th floor
Boston, MA 02110
USA

www.oidview.com

A large, light blue watermark of the ByteSphere logo is positioned at the bottom of the page. It includes a blue arc above the word "ByteSphere", which is written in a bold, italicized, sans-serif font.