



[MG-SOFT Corporation](http://www.mg-soft.com)

MIB Browser 2018 Professional Edition

USER MANUAL

(Document Version: 8.0)

Document published on Wednesday, 20-December-2017

Copyright © 1995-2018 MG-SOFT Corporation

In order to improve the design or performance characteristics, MG-SOFT reserves the right to make changes in this document or in the software without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MG-SOFT Corporation. Permission to print one copy is hereby granted if your only means of access is electronic.

Depending on your license, certain functions described in this document may not be available in the version of the software that you are currently using.

Screenshots used in this document may slightly differ from those on your display.

MG-SOFT may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 1995-2018 MG-SOFT Corporation. All rights reserved.

TABLE OF CONTENTS

1	Introduction	13
1.1	Product Description	14
1.1.1	<i>MIB Browser Main Features</i>	<i>15</i>
1.2	About This Manual	17
1.2.1	<i>Using MIB Browser Manual</i>	<i>17</i>
2	Getting Started	20
2.1	System Requirements	20
2.1.1	<i>Windows Operating System</i>	<i>20</i>
2.1.2	<i>Linux Operating System</i>	<i>20</i>
2.1.3	<i>Mac OS X Operating System</i>	<i>21</i>
2.1.4	<i>Solaris Operating System</i>	<i>21</i>
2.2	Installing MIB Browser Professional Edition	22
2.2.1	<i>Windows Operating System</i>	<i>22</i>
2.2.2	<i>Linux Operating System</i>	<i>23</i>
2.2.3	<i>Mac OS X Operating System</i>	<i>24</i>
2.2.4	<i>Solaris Operating System</i>	<i>25</i>
2.3	Uninstalling MIB Browser Professional Edition	26
2.3.1	<i>Windows Operating System</i>	<i>26</i>
2.3.2	<i>Linux Operating System</i>	<i>27</i>
2.3.3	<i>Mac OS X Operating System</i>	<i>27</i>
2.3.4	<i>Solaris Operating System</i>	<i>28</i>
3	Start SNMP MIB Browser Professional Edition	29
3.1	Starting MIB Browser	29
3.1.1	<i>Windows Operating System</i>	<i>29</i>
3.1.2	<i>Linux Operating System</i>	<i>30</i>
3.1.3	<i>Mac OS X Operating System</i>	<i>32</i>
3.1.4	<i>Solaris Operating System</i>	<i>33</i>
3.2	MIB Browser Desktop	34
4	Apply License Key	36
5	Contact Remote SNMP Agent and Query All Its Object Instances	38
5.1	Contacting Remote SNMP Agent	38
5.1.1	<i>Using IPv4 or IPv6 Address</i>	<i>39</i>
5.1.2	<i>Selecting Binding Interface</i>	<i>41</i>
5.2	Selecting Nodes in MIB Tree	42
5.2.1	<i>Symbols Used for Different Types of MIB Nodes</i>	<i>44</i>
5.2.2	<i>Colors Used for Representing Different Access Types of MIB Nodes</i>	<i>44</i>
5.2.3	<i>Finding MIB Tree Nodes by Name or OID</i>	<i>45</i>
5.3	Retrieving All Object Instance Values with SNMP Walk Operation	46
5.3.1	<i>Performing SNMP Walk Operation</i>	<i>47</i>
5.4	Viewing MIB Node Properties	52
6	Specify SNMP Protocol Parameters	54
6.1	Using SNMPv1 Protocol	55
6.2	Using SNMPv2c Protocol	56
6.3	Using SNMPv3 Protocol with User-based Security Model (USM)	62
6.3.1	<i>Creating New SNMPv3 USM User Profile</i>	<i>64</i>
6.3.2	<i>Specifying Password or Security Key</i>	<i>66</i>

6.3.3	<i>Diffie-Hellman Key Exchange for DOCSIS-Based SNMPv3 Agents</i>	69
6.4	Using SNMPv3 Protocol with Transport Security Model (TSM)	71
6.4.1	<i>Using SNMPv3 over TLS</i>	71
6.4.2	<i>Using SNMPv3 over DTLS</i>	75
7	Configure and Use SNMP Agent Profiles	79
7.1	Creating New SNMP Agent Profiles	79
7.1.1	<i>Using SNMPv1 Protocol</i>	81
7.1.2	<i>Using SNMPv2c Protocol</i>	83
7.1.3	<i>Using SNMPv3 Protocol with User-Based Security Model</i>	86
7.1.4	<i>Using SNMPv3 Protocol with Transport Security Model (TLS/DTLS)</i>	92
7.1.5	<i>Automatically Load MIB Modules</i>	95
7.2	Using SNMP Agent Profiles to Manage SNMP Agents.....	98
7.3	Organizing SNMP Agent Profiles in Folders	99
7.4	Viewing Current Status of SNMP Agents.....	103
7.5	Exporting and Importing SNMP Agent Profiles	104
8	Load MIB Modules in MIB Browser	105
8.1	Importing MIB Files Directly into MIB Browser.....	105
8.2	Compiling MIB Files in MG-SOFT MIB Compiler	109
8.3	Manually Loading MIB Modules in MIB Browser.....	111
8.4	Searching for MIB Modules	112
8.5	Saving MIB Modules to MIB Group	114
8.5.1	<i>Loading MIB Group</i>	114
8.5.2	<i>Renaming MIB Group</i>	115
8.5.3	<i>Deleting MIB Group</i>	115
8.6	Checking MIB Module Properties	115
9	Query Object Instances by Using SNMP Get Requests	117
9.1	SNMP Get Requests for Scalar Objects	117
9.2	SNMP Get Requests for Columnar Objects.....	118
10	Query Object Instances by Using SNMP GetNext Requests	122
10.1	SNMP GetNext Request for Scalar Objects	122
10.2	SNMP GetNext Request for Columnar Objects	122
11	Query Object Instances by Using Command Line Interface	126
11.1	Using SNMP Get Command.....	126
11.2	Using SNMP GetNext Command	129
11.3	Using Walk Command.....	130
11.4	Retrieving Multiple Object Instances with One Request	131
11.4.1	<i>Using Get Command with Multiple Variable Bindings</i>	131
11.4.2	<i>Using GetNext Command with Multiple Variable Bindings</i>	131
11.4.3	<i>Using GetBulk Command with Multiple Variable Bindings</i>	132
12	Step-by-Step SNMP Walk Operation	134
12.1	Performing Step-by-Step SNMP Walk Operation	134
13	Modify Values of Object Instances in Remote SNMP Agents	137
13.1	Modifying Values of Object Instances by Using the SNMP Set Operation	137
13.1.1	<i>Specifying Value to Be Set if the SNMP Syntax is BITS</i>	139
13.2	Modifying Values of Table Object Instances Directly in Table View	141
13.3	SNMP Set Requests with Multiple Variable Bindings.....	144

13.3.1	<i>Making Multiple Variable Bindings List</i>	144
13.3.2	<i>Performing SNMP Set Operation with Multiple Variable Bindings</i>	149
13.4	Resolving Problems When Performing SNMP Set Operation	151
14	Discover Remote SNMP Agents	152
14.1	Discovering Remote SNMP Agents.....	152
14.1.1	<i>Repeating Discovery Operation on Different IP Range</i>	154
14.1.2	<i>Repeating Discovery Operation with Different SNMP Access Parameters</i>	154
14.2	Obtaining More Information About Discovered SNMP Agents	155
14.3	Example: How to Discover Only SNMP Agents Implementing a Specific OID	156
15	Monitor SNMP Agents in Info Windows	157
15.1	Monitoring SNMP Agent in Info Window.....	157
15.1.1	<i>Editing the List of Object Instances Monitored in Info Window</i>	158
15.1.2	<i>Monitoring Another SNMP Agent</i>	161
15.1.3	<i>Logging the Queried Object Instance Values</i>	161
15.2	Monitoring More SNMP Agents	161
16	Scan SNMP Agent for Implemented MIB Modules	163
16.1	Searching for Implemented MIB Modules.....	163
16.2	Loading MIB Modules Implemented in SNMP Agent	166
17	View, Poll and Modify SNMP Tables	167
17.1	Viewing and Polling SNMP Tables in Tabular Form	167
17.1.1	<i>Adjusting Tabular Column Widths</i>	168
17.1.2	<i>Copying Displayed SNMP Table</i>	169
17.2	Modifying Table Object Instance Values.....	169
17.3	Adding Row to SNMP Table.....	169
18	Graphic Representation of Object Instance Values	171
18.1	Start Graphing Operation Directly from MIB Tree	171
18.1.1	<i>Changing the Polling Interval</i>	173
18.1.2	<i>Pausing and Resuming the Graphing Operation</i>	173
18.2	Start Graphing Operation in Conventional Way	174
18.2.1	<i>Loading Graph Parameters From File</i>	174
18.2.2	<i>Adding a Variable to Performance Graph Window</i>	175
18.3	Adding Additional Variables to Graph.....	177
18.3.1	<i>Adding Variables by Using Drag&Drop Technique</i>	177
18.4	Editing Graph Settings	179
18.5	Saving Graph Settings to File.....	179
19	Receive SNMP Trap and SNMP Inform Notification Messages	181
19.1	Receiving SNMPv1 and SNMPv2c Notification Messages on Standard Ports.....	181
19.1.1	<i>Viewing Received SNMP Notification Messages</i>	181
19.1.2	<i>Identifying SNMPv1 Trap Notifications through Enterprise OID</i>	183
19.2	Receiving SNMPv3 Notification Messages	186
19.3	Sound Notification on Received SNMP Notification Messages.....	187
19.4	Acknowledging Received SNMP Notification Messages.....	187
19.5	Searching and Filtering SNMP Notification Messages	188
19.6	SNMP Notification Messages on other UDP Ports	191
19.6.1	<i>Configuring a New Listening Port</i>	191
19.7	Checking the SNMP Notification Reception Status.....	192
19.8	Copying and Saving SNMP Notification Messages	192

19.9	Information About SNMP Notification Messages	194
19.9.1	Information About SNMPv2c and SNMPv3 Notifications	194
19.9.2	Information About SNMPv1 Trap Notifications	195
19.10	Decoding SNMP Notification Messages	197
20	Send SNMP Trap and Inform Notification Messages	199
20.1	Sending SNMPv1 Generic and Specific Trap Notification Messages	199
20.1.1	Setting Parameters for SNMPv1 Generic and Specific Trap Notifications	199
20.1.2	Sending SNMPv1 Trap Messages	202
20.2	Sending SNMPv2c/v3 Trap and Inform Notification Messages	203
20.2.1	Difference between SNMP Trap and Inform Notifications	203
20.2.2	Creating Variable Binding List for SNMPv2c/v3 Notification Messages	204
20.2.3	Sending SNMPv2c/v3 Notification Messages	205
21	Take and Compare SNMP Agent Snapshots	207
21.1	Taking and Viewing SNMP Agent Snapshots	207
21.1.1	Saving and Loading Agent Snapshots	209
21.2	Comparing SNMP Agent Snapshots	210
21.2.1	Opening Compare Agent Snapshots Window	210
21.2.2	Setting Agent Snapshot Preferences	211
21.2.3	Taking SNMP Agent Snapshots	212
21.2.4	Saving and Loading SNMP Agent Snapshots	212
21.2.5	Comparing Agent Snapshots	213
21.2.6	Comparison Report	215
21.3	Saving and Loading SNMP Agent Snapshot Sessions	216
22	Manage SNMPv3 USM Users on Remote SNMP Agents	219
22.1	Managing Existing SNMPv3 Users on Remote SNMP Agent	219
22.2	Creating New SNMPv3 USM User on Remote SNMP Agent	221
23	Debug Problems in Generic SNMP Trace Window	223
23.1	Tracing Exchanged SNMP Messages	223
23.1.1	Select MIB Browser Windows to Be Recorded	223
23.1.2	Tracing and Decoding SNMP Messages	224
23.1.3	Searching and Filtering SNMP Messages	227
23.2	Troubleshooting in Generic SNMP Trace Window	229
24	Perform Multiple Operations	232
24.1	About Multiple Operations Window	232
24.2	Configuring SNMP Operations in Multiple Operations Window	233
24.2.1	Adding Operations to Multiple Operations Window	233
24.3	Running SNMP Operations in Multiple Operations window	238
25	Simulate SNMP Agent	241
Index		248
Appendix: MIB Browser File Formats		253

TABLE OF FIGURES

Figure 1: Accessing operations in MIB Browser by using menu commands	17
Figure 2: Accessing operations in MIB Browser by using pop-up menu commands	18
Figure 3: MIB Browser disk image file (DMG) on Mac OS X desktop	24
Figure 4: Double-click the “setup.pkg” icon in Finder to run the MIB Browser installer	24
Figure 5: MIB Browser installer introduction screen	25
Figure 6: Uninstalling MIB Browser on Mac OS X	28
Figure 7: About MG-SOFT MIB Browser dialog box	29
Figure 8: Starting MIB Browser from the menu in the KDE desktop environment	30
Figure 9: Starting MIB Browser from the main menu in the GNOME environment	31
Figure 10: Starting MIB Browser on Mac OS X	32
Figure 11: Starting MIB Browser on Solaris (Gnome environment)	33
Figure 12: MIB Browser desktop	34
Figure 13: Menu bar and toolbar on MIB Browser desktop	35
Figure 14: Status bar of MIB Browser desktop	35
Figure 15: Selecting the license.key file	36
Figure 16: Applying the license.key file	36
Figure 17: Applying the license.key file - restarting MIB Browser	37
Figure 18: MIB Browser displaying a response from the contacted SNMP agent	38
Figure 19: IPv6 address with scope ID in the Remote SNMP Agent input line	40
Figure 20: Selecting binding interface in the MIB Browser Preferences dialog box	41
Figure 21: Expanding the MIB tree	42
Figure 22: Expanded pop-up menu command and a displayed MIB tree in the MIB tree panel	43
Figure 23: MIB nodes of different access types (default colors)	45
Figure 24: The Find Object in MIB Tree dialog box	46
Figure 25: Terminology used for MIB tree objects and nodes	47
Figure 26: Search Compiled MIB Modules To Resolve OID dialog box	48
Figure 27: Results of the SNMP Walk operation on the <code>system</code> sub tree	49
Figure 28: Specifying SNMP GetBulk settings	50
Figure 29: MIB Node Properties window with a displayed drop-down list of MIB modules	52
Figure 30: SNMP Protocol Preferences dialog box	54
Figure 31: Specifying SNMPv1 protocol preferences	55
Figure 32: Specifying SNMPv2c protocol preferences	57
Figure 33: Multiple object instances with corresponding values returned in SNMP GetBulk packet	59
Figure 34: A list of variable bindings in the Multiple Variable Bindings window	60
Figure 35: Object instances and their values returned in response to SNMP GetBulk request with multiple variable bindings	61
Figure 36: Specifying SNMPv3 USM protocol preferences	62
Figure 37: SNMPv3 USM User Profiles window	63
Figure 38: Specifying SNMPv3 USM user parameters	64
Figure 39: Password For Authentication/Privacy Protocol dialog box	65
Figure 40: Entering password in HEX dump format	67
Figure 41: Binary Key For Privacy Protocol dialog box	68
Figure 42: Diffie-Hellman key exchange settings	69

Figure 43: Selecting the SNMPv3 TSM protocol.....	72
Figure 44: Specifying the SNMPv3 TSM security parameters	72
Figure 45: Loading the manager X.509 digital certificate for SNMPv3 over (D)TLS.....	73
Figure 46: SNMP Protocol Preferences - SNMPv3 TSM settings (SNMPv3 over TLS/TCP)	74
Figure 47: Example of a successful <i>Contact</i> operation using <i>SNMPv3 over TLS/TCP</i>	75
Figure 48: SNMP Protocol Preferences - SNMPv3 TSM settings (SNMPv3 over DTLS/UDP)	76
Figure 49: Example of a successful <i>Contact</i> operation using <i>SNMPv3 over DTLS/UDP</i>	78
Figure 50: SNMP Agent Profiles window	79
Figure 51: A new SNMP agent profile icon	80
Figure 52: Opening the Agent Profile Properties dialog box	80
Figure 53: Agent Profile Properties dialog box, General panel	81
Figure 54: Agent Profile Properties dialog box, SNMPv1 community settings	82
Figure 55: Setting the timeout and retransmit agent profile properties	82
Figure 56: Agent Profile Properties dialog box, SNMPv2c protocol selected	83
Figure 57: Agent Profile Properties dialog box, SNMPv2c community settings.....	84
Figure 58: Setting the Get-Bulk agent profile properties	84
Figure 59: Setting the timeout and retransmits agent profile properties (SNMPv2c).....	85
Figure 60: Agent Profile Properties dialog box, SNMPv3 USM protocol selected	86
Figure 61: Agent Profile Properties dialog box, SNMPv3 properties	87
Figure 62: SNMPv3 USM User Profiles window	88
Figure 63: Specifying parameters for SNMPv3 security users.....	89
Figure 64: Password For Authentication/Privacy Protocol dialog box	90
Figure 65: Agent Profile Properties dialog box, SNMPv3 properties (new USM user selected).....	91
Figure 66: Agent Profile Properties dialog box, SNMPv3 TSM/DTLS protocol selected	92
Figure 67: Agent Profile Properties dialog box, SNMPv3 TSM (TLS/DTLS) properties - empty	93
Figure 68: Loading an X.509 digital certificate for SNMPv3 over (D)TLS	94
Figure 69: Agent Profile Properties dialog box, SNMPv3 TSM (TLS/DTLS) properties - specified	95
Figure 70: Agent Profile Properties dialog box, Load MIB Modules properties - empty	96
Figure 71: Selecting MIB modules to be loaded with the agent profile	96
Figure 72: Agent Profile Properties dialog box, Load MIB Modules properties - modules specified	97
Figure 73: SNMP Agent Profiles window	98
Figure 74: Creating a new folder in the SNMP Agent Profiles window	99
Figure 75: A new folder created in the SNMP Agent Profiles window	100
Figure 76: A new SNMP agent profile added to the SNMP Agent Profiles window.....	100
Figure 77: Creating SNMP agent profiles for discovered SNMP agents	101
Figure 78: SNMP agent profiles created for discovered SNMP agents	102
Figure 79: Manually refreshing the SNMP agent status.....	103
Figure 80: Imported SNMP agent profiles configuration	104
Figure 81: Selecting MIB files for import	105
Figure 82: The Import MIB Module(s) window - pre-scanning MIB file(s).....	106
Figure 83: The Imported MIB Not Found dialog box lets you resolve missing imports issues	107
Figure 84: The Error Compiling MIB dialog box appears in case a compilation error occurs	108
Figure 85: Viewing the final results of a MIB import operation.....	108
Figure 86: Viewing the structure and nodes of the imported MIB modules	109
Figure 87: Compiling MIB files with MG-SOFT MIB Compiler	110
Figure 88: Loading MIB modules	111

Figure 89: Setting the Live search options in the MIB tab of the main window.....	112
Figure 90: Viewing the search results in the MIB tab of the main window.....	113
Figure 91: Enter New Group Name dialog box	114
Figure 92: MIB Groups view pop-up menu.....	114
Figure 93: MIB tab with loaded MIB modules and a displayed pop-up menu.....	115
Figure 94: Module Database Properties window.....	116
Figure 95: Selecting the SNMP Get command on a scalar object in the MIB tree	117
Figure 96: Viewing the SNMP Get operation request and response in the Query results panel	118
Figure 97: Selecting a columnar object in the MIB tree	119
Figure 98: SNMP Get command and its sub menu.....	119
Figure 99: Selecting a columnar object instance in the Select Table Instance(s) window	120
Figure 100: Specifying a columnar object instance in the Instance To Query dialog box	120
Figure 101: Number of octets received on the selected device displayed in the Query Results panel ...	121
Figure 102: Selecting a scalar object	122
Figure 103: SNMP GetNext command and its sub menu	123
Figure 104: SNMP GetNext request and response.....	123
Figure 105: SNMP Get and SNMP GetNext operation on the <code>sysName</code> node.....	124
Figure 106: Entering a get command into the Command line drop-down list	127
Figure 107: Viewing results of a get command into the Query results window panel.....	127
Figure 108: Using the get command while object is selected in the MIB tree.....	128
Figure 109: Running the Walk command on the selected subtree	130
Figure 110: Specifying the SNMP GetBulk parameters for a specific purpose.....	132
Figure 111: Prompt For OID dialog box	134
Figure 112: Specifying the OID of an object by selecting it in the MIB tree	135
Figure 113: Step-by-Step SNMP Walk operation on the <code>ifTable</code>	136
Figure 114: Selecting the Set command from the context menu (notice writable object names in blue).....	138
Figure 115: Set dialog box.....	138
Figure 116: Selecting a pre-defined value (integer-enumeration) to be set.....	139
Figure 117: Select Bits Value dialog box.....	140
Figure 118: Specifying a new value to be set in the SNMP agent	140
Figure 119: An SNMP table (e.g., <code>ifTable</code>) displayed in a tabular form in the Table View window.....	141
Figure 120: Colored instance values of a writable table object (i.e., <code>ifAdminStatus</code>)	142
Figure 121: Selecting the value to be set from the list of pre-defined values	142
Figure 122: Multiple Variable Bindings window with the selected object	144
Figure 123: Select dialog box with object OID	145
Figure 124: Specifying the instance of a scalar object in the <i>OID</i> input line	145
Figure 125: A scalar object (<code>sysContact</code>) with a specified instance (<code>sysContact.0</code>), syntax and value	145
Figure 126: Selecting a columnar object instance	146
Figure 127: A columnar object (<code>ifAdminStatus</code>) with a specified instance (<code>ifAdminStatus.2</code>), syntax and value	146
Figure 128: Select dialog box.....	147
Figure 129: A list of multiple variable bindings	148
Figure 130: Selecting the operation type.....	149
Figure 131: Setting values of object instances with one SNMP set request.....	150
Figure 132: Remote SNMP Agent Discovery window.....	152

Figure 133: A list of discovered SNMP agents	153
Figure 134: Viewing the discovery log file	154
Figure 135: Remote SNMP Agent Discovery window status bar	155
Figure 136: Info window displaying more information about a discovered SNMP agent	155
Figure 137: A list of discovered SNMP agents that implement a specific OID	156
Figure 138: Info window with a list of repeatedly queried object instances	157
Figure 139: Info Window Properties dialog box	158
Figure 140: Select OID To Query dialog box	159
Figure 141: Info window with a new set of OIDs	160
Figure 142: All opened Info windows arranged in ascending order	162
Figure 143: Scan Agent For Implemented MIB Modules window	163
Figure 144: Scan Agent For Implemented MIB Modules window with a list of MIB modules implemented in the scanned SNMP agent	164
Figure 145: Scan Agent For Implemented MIB Modules Preferences dialog box	164
Figure 146: Loading MIB modules from the Scan Agent For Implemented MIB Modules window	166
Figure 147: Table View window	167
Figure 148: Mirrored contents of the Table View window	168
Figure 149: Editing values of table object instances directly in the table view	169
Figure 150: Add New Table Instance dialog box	170
Figure 151: Selecting the instances of a columnar object to be plotted in the same graph	172
Figure 152: Monitoring values of 4 SNMP variables in the Performance Graph window	173
Figure 153: Start/pause the graphing operation and specify the polling interval	173
Figure 154: Empty Performance Graph window	174
Figure 155: Graph Properties dialog box	175
Figure 156: Retrieved values of an object instance presented in a graph chart	176
Figure 157: Using Drag&Drop technique to add a new variable to the Performance Graph window	177
Figure 158: Performance Graph window with three graph lines	178
Figure 159: Graphical presentation of the number of octets per second received in (blue line) and transmitted out (red line) of the interface	180
Figure 160: SNMP Trap Ringer Console window with received SNMP notification messages	181
Figure 161: Selected SNMP notification message displayed in a tree structure (right panel)	182
Figure 162: Trap Ringer Console Preferences panel in the MIB Browser Preferences dialog box	183
Figure 163: SNMPv1 Trap message resolved through the SNMPv1 Trap number and the Enterprise value	184
Figure 164: SNMPv1 Trap message resolved only through the SNMPv1 Trap number value	185
Figure 165: Notification SNMPv3 Security Preferences panel	186
Figure 166: SNMP Trap Ringer Console window displaying all received SNMP notification messages	188
Figure 167: Setting the Live search options in the SNMP Trap Ringer Console	189
Figure 168: Viewing the Live search results in the SNMP Trap Ringer Console	190
Figure 169: Notification Port Preferences panel	191
Figure 170: Adding a new port for dialog box	191
Figure 171: Selecting the Properties pop-up command on a NOTIFICATION-TYPE MIB tree node	194
Figure 172: Viewing the properties of a notification-type node	195
Figure 173: Selecting the Properties pop-up command on a TRAP-TYPE node	196
Figure 174: Viewing the description of an SNMPv1 Trap	196

Figure 175: SNMP notification message received into SNMP Trap Ringer Console window decoded and displayed in the Generic SNMP Trace For Trap Ringer window	198
Figure 176: Multiple Variable Bindings window	199
Figure 177: SNMPv1 Trap Protocol Parameters dialog box	200
Figure 178: Example of a variable binding for SNMPv1 linkUp Trap	201
Figure 179: Specifying the trap receiver IP address	202
Figure 180: SNMP Protocol Preferences dialog box	202
Figure 181: Selecting the Trap entry from the programmable button	203
Figure 182: A typical variable binding list used with SNMPv2c/v3 linkUp traps	204
Figure 183: Agent Snapshot Preferences dialog box	207
Figure 184: Agent Snapshot window	209
Figure 185: Compare Agent Snapshot window with a displayed Agent/File toolbar switch	211
Figure 186: SNMP Agent Snapshot window and Display Filter menu	214
Figure 187: Comparison Report window	216
Figure 188: Creating a session in the Compare Agent Snapshot window	217
Figure 189: Loading a session in the Compare Agent Snapshot window	217
Figure 190: Manage Agent SNMPv3 Users dialog box	219
Figure 191: Entering SNMPv3 user's old authentication protocol password	220
Figure 192: Entering SNMPv3 user's new authentication protocol password	220
Figure 193: Cloning an SNMPv3 USM user on remote SNMP agent	221
Figure 194: New SNMPv3 USM user created on remote SNMP agent	222
Figure 195: In Generic SNMP Trace Window Preferences panel specify MIB Browser windows to be traced	224
Figure 196: Decoded SNMP message in the Generic SNMP Trace window	225
Figure 197: Generic SNMP Trace Preferences dialog box	226
Figure 198: Selecting the Live search options in the Generic SNMP Trace window	227
Figure 199: Viewing Live search results in the Generic SNMP Trace window	228
Figure 200: SNMPv3 message parameters displayed in the Decoder panel	229
Figure 201: The contents of an SNMP message displayed in the Hex Dump panel	229
Figure 202: The contents of an SNMP message decoded and displayed in the Decoder panel	230
Figure 203: SNMPv3 message parameters displayed in the Decoder panel	231
Figure 204: Empty Multiple Operations window	232
Figure 205: Adding a new operation to the Multiple Operations window	233
Figure 206: Selecting the operation type	234
Figure 207: Adding a new binding to selected operation in the Multiple Operations window	235
Figure 208: Select dialog box	235
Figure 209: A new variable binding in the Multiple Operations window (Send panel)	236
Figure 210: Selecting the <i>Multiple Operations</i> command from the MIB tree pop-up menu	236
Figure 211: Operation for retrieving the scalar object instances of the MIB-2 'system' group	237
Figure 212: Operations for retrieving object instances form the MIB-2 subtree	238
Figure 213: Performing operations in the Multiple Operations window	239
Figure 214: SNMP Agent Simulator window (simulation is not running)	241
Figure 215: Selecting a binding interface in the SNMP Agent Simulator window	242
Figure 216: Setting the agent simulator protocol preferences	243
Figure 217: Selecting a SNMPv3 USM user profile for the agent simulator	244
Figure 218: Specifying SNMPv3 TSM details for the agent simulator	244

Figure 219: SNMP Agent Simulator window - simulation is running	246
Figure 220: SNMP Agent Simulator Status Report window	247

1 INTRODUCTION

Thank you for using MG-SOFT MIB Browser Professional Edition with MIB Compiler.

MG-SOFT Corporation, established in 1990, is the world's leading supplier of SNMP, SMI, NETCONF, YANG and general network management applications, toolkits and solutions for Windows, Linux, Mac OS X and Solaris platforms. MG-SOFT provides major IT companies worldwide with network management applications as well as with toolkits implementing core network management technologies. Furthermore, MG-SOFT provides customers with consulting services, custom made turn-key software products, solutions and/or services and network management integration solutions based on our extensive know-how and vast experience in network management technologies.

MG-SOFT has developed the world's first 32-bit SNMP protocol stack implementation for MS Windows operating systems and one of the first SNMPv3 implementations for Win32 platforms. As of today, MG-SOFT's [SNMP stack implementation](#) provides a solid base for all MG-SOFT's SNMP applications (as well as for thousands of third-party applications, built by our clients who licensed MG-SOFT WinSNMP API implementation) running on a number of operating system platforms: MS Windows (32-bit, 64-bit, embedded CE), Linux (32-bit and 64-bit), Mac OS X (PPC and Intel platforms, 32-bit and 64-bit), Mac iOS (iPad) and Solaris (Sparc and Intel platforms).

MG-SOFT is also active in the network configuration management area and offers a full range of NETCONF and YANG software products, ranging from a graphical YANG and YIN model explorer, over Visual YANG Designer, to full-blown NETCONF configuration manager and NETCONF/YANG Python scripting framework for automated testing and configuring of NETCONF devices.

For additional information about MG-SOFT Corporation, please contact the following address:

MG-SOFT Corporation
Strma ulica 8
2000 Maribor
Slovenia

Phone: +386 2 2506565
Fax: +386 2 2506566
E-mail: info@mg-soft.com
URL: <http://www.mg-soft.com/>

1.1 Product Description

MG-SOFT MIB Browser Professional with MIB Compiler is powerful, flexible and user-friendly general-purpose software for SNMP network management. It is available for Windows, Linux, Mac OS X and Solaris operating systems.

The software is available in the following editions:

- ❑ **MIB Browser Professional SNMPv1/v2c Edition**
This edition supports SNMPv1 and SNMPv2c protocols and is available only in the Windows version of the software.
- ❑ **MIB Browser Professional SNMPv3 Edition**
This edition supports SNMPv1, SNMPv2c and SNMPv3 USM protocols.
- ❑ **MIB Browser Professional DOCSIS/DH Edition**
This edition supports SNMPv1, SNMPv2c and SNMPv3 USM protocols and the Diffie-Hellman key exchange extension to USM for managing DOCSIS-based SNMPv3 agents. This edition support also SNMPv3 TSM with TLS and DTLS transports. Besides, this edition supports IPv6 protocol.
- ❑ **MIB Browser Professional Developer's Edition**
This edition supports SNMPv1, SNMPv2c and SNMPv3 USM protocols and the Diffie-Hellman key exchange extension to USM for managing DOCSIS-based SNMPv3 agents. This edition support also SNMPv3 TSM with TLS and DTLS transports, as well as IPv6 protocol. Besides, this edition includes the Generic SNMP Trace debugging feature.
- ❑ **MIB Browser Professional Simulator Edition**
This edition supports SNMPv1, SNMPv2c and SNMPv3 USM protocols, the Diffie-Hellman key exchange extension to USM for managing DOCSIS-based SNMPv3 agents, SNMPv3 TSM with TLS and DTLS transports, the Generic SNMP Trace feature, and IPv6 protocol. Furthermore, this edition incorporates the SNMP Agent Simulator.

MG-SOFT MIB Browser can monitor and manage any SNMP device on the network by using the standard SNMPv1, SNMPv2c and SNMPv3 protocols over UDP or TCP in IPv4 and IPv6 networks. MIB Browser supports also Diffie-Hellman key exchange model, so that DOCSIS-based SNMPv3 agents (i.e. cable modems, cable modem termination systems, set-top boxes etc.) can be seamlessly contacted and managed. Furthermore, in addition to the standard User-based Security Model (USM), MG-SOFT MIB Browser implements also the Transport Security Model (TSM) for SNMP, and supports SNMPv3 over TLS over TCP and SNMPv3 over DTLS over UDP protocol, as specified in RFC 6353. Moreover, the software supports also HMAC-SHA-2 authentication protocols (RFC 7860) and AES-192, AES-256 and 3DES privacy protocols for SNMPv3 USM.

Due to its intuitive user interface and numerous features MIB Browser is suitable both for beginners as well as for SNMP experts. It allows you to perform SNMP Get, GetNext, GetBulk and Set operations and lets you receive and send SNMP Trap and Inform notification messages.

Besides the basic SNMP operations, MIB Browser offers a number of advanced features (briefly introduced in the next section; [MIB Browser Main Features](#) section) that make management and monitoring of SNMP devices most effective and easy.

1.1.1 MIB Browser Main Features

Here is a brief introduction of MIB Browser features that are presented and described in this manual:

- ❑ SNMP Get, GetNext, GetBulk and Set operations

To retrieve object instance values from a remote SNMP agent, you can use either the SNMP Get, SNMP GetNext or SNMP GetBulk operation. Or, to modify values of writable object instances in the agent, use the SNMP Set operation.

- ❑ SNMP Walk and Step-by-Step SNMP Walk operation

The SNMP Walk operation lets you quickly retrieve all values of management information from an SNMP agent in just one step. For more controlled query, you can use the Step-by-Step SNMP Walk operation and traverse all object instances implemented in an SNMP agent manually.

- ❑ SNMP Table Viewer, Table Editor and Add Row Feature

In the Table View window, you can view and monitor all object instances of an SNMP table in a tabular form. You can also edit writable object instance values of the displayed SNMP table and if the table supports it, add a new row to the table.

- ❑ Graphic Representation of Values

The Performance Graph window lets you concurrently monitor numerical values in any number of SNMP agents and displays the retrieved values in a real-time graph chart. A number of Performance Graph windows can be used at the same time.

- ❑ SNMP Requests with Multiple Variable Bindings in PDUs

In the Multiple Variable Bindings window you can create a list of desired variable bindings and send it in a single SNMP packet to a remote SNMP agent. In this way you can retrieve or modify any number of values in SNMP agents with a single operation. You can also use the Multiple Variable Bindings window for sending SNMP Trap or Inform notification messages.

- ❑ Receiving and Sending SNMP Notification Messages

The MIB Browser's Trap Ringer Console feature lets you receive SNMPv1, v2c and v3 Trap and Inform notification messages sent from arbitrary SNMP devices on any UDP/IPv4 and UDP/IPv6 port. As mentioned above, the SNMP notifications can also be sent to SNMP devices by using the Multiple Variable Bindings window.

- ❑ Discovering SNMP Agents

With this feature you can discover all remote SNMP agents on the network within a selected range of IP addresses.

- ❑ Scanning SNMP Agents for MIB Modules

This feature lets you scan an SNMP agent for its implemented MIB modules and automatically load all discovered MIB modules into MIB Browser.

- ❑ Monitoring SNMP Agents in Info Windows

You can use Info windows to simultaneously monitor arbitrary sets of object instance values in one or more SNMP agents. The monitored values can be logged to files in the CSV format and then imported to spreadsheet or database applications for further processing.

- ❑ Comparing SNMP Agent Snapshots

MIB Browser lets you take snapshots of SNMP agents and compare them side-by-side. An agent snapshot is a MIB tree-like presentation of MIB object instances together with their syntax and values, as retrieved from the SNMP agent at the given time. The comparison of SNMP agent snapshots shows matches and mismatches between object instance values, 'orphaned' MIB tree nodes and syntax differences.

- ❑ Managing SNMPv3 USM User Configuration on Remote SNMP Agents

MIB Browser provides a convenient and user-friendly interface for managing SNMPv3 USM user configuration on remote SNMPv3 agents. The USM user management operations include 'cloning' SNMPv3 USM users, changing their secret authentication and privacy keys, as well as enabling, disabling and deleting USM users.

- ❑ Tracing and Decoding SNMP Messages

The Generic SNMP Trace window can be configured to trace SNMP messages, including SNMP Trap and Inform notifications, sent from or received into any MIB Browser window. Traced SNMP messages are displayed in raw hexadecimal dump format as well as in the decoded, human-readable format. This feature is particularly useful for debugging when developing an SNMP agent and for resolving problems when MIB Browser cannot properly query an SNMP agent.

- ❑ Performing Multiple SNMP Operations

The Multiple Operations window can automatically perform an arbitrary sequence of SNMP operations with one or more variable binding against a selected SNMP agent. This is useful, for example, when testing or configuring SNMP agents, etc.

- ❑ Simulating SNMP Agents

The software lets you take or create a snapshot of an SNMP agent and then simulate this agent on the computer where MIB Browser runs. Simulating means that MIB Browser runs a separate process, which listens for SNMP queries on a selected network interface and port and responds to queries by returning the OIDs and values specified in a given agent snapshot file.

- ❑ Importing and Loading MIB Files

While the standard MIB files come bundled in MIB Browser package, vendor specific MIB files can be imported into MIB Browser using the convenient Import MIB feature that requires minimal user intervention. This functionality lets you select desired MIB definition files on disk and it automatically compiles and loads compiled MIB modules in MIB Browser.

1.2 About This Manual

This manual contains instructions for completing basic operations that can be undertaken by using MG-SOFT MIB Browser Professional for Windows, Linux, Mac OS X and Solaris. Task-based instructions in this manual and many illustrative examples will help you understand how MIB Browser works and how to use it effectively.

Note: MIB Browser Professional is available in five editions (briefly introduced in the [Product Description](#) section) supporting different features. Depending on your license, some features presented in this manual might not be available in your edition of the software.

1.2.1 Using MIB Browser Manual

It is supposed that you are familiar with basic actions in a graphical desktop environment such as choosing a main menu command or a pop-up command, dragging and dropping icons, etc.

To find and access a topic of your interest in this manual, go through the table of contents and click the heading of the section that you wish to read. Or, use the [Index](#) at the end of the manual.

Accessing Operations in MIB Browser

Almost all operations in MG-SOFT MIB Browser can be accessed or started in several possible ways, either by using command selections listed in menus, toolbar buttons or keyboard shortcuts.

Possible ways of accessing operations in MIB Browser:

- ❑ Menu commands (e.g., **SNMP** / **Contact**. This is a short form of the instruction that means: To contact an SNMP agent, expand the **SNMP** menu in the main window and select the **Contact** command, see [Figure 1](#)).

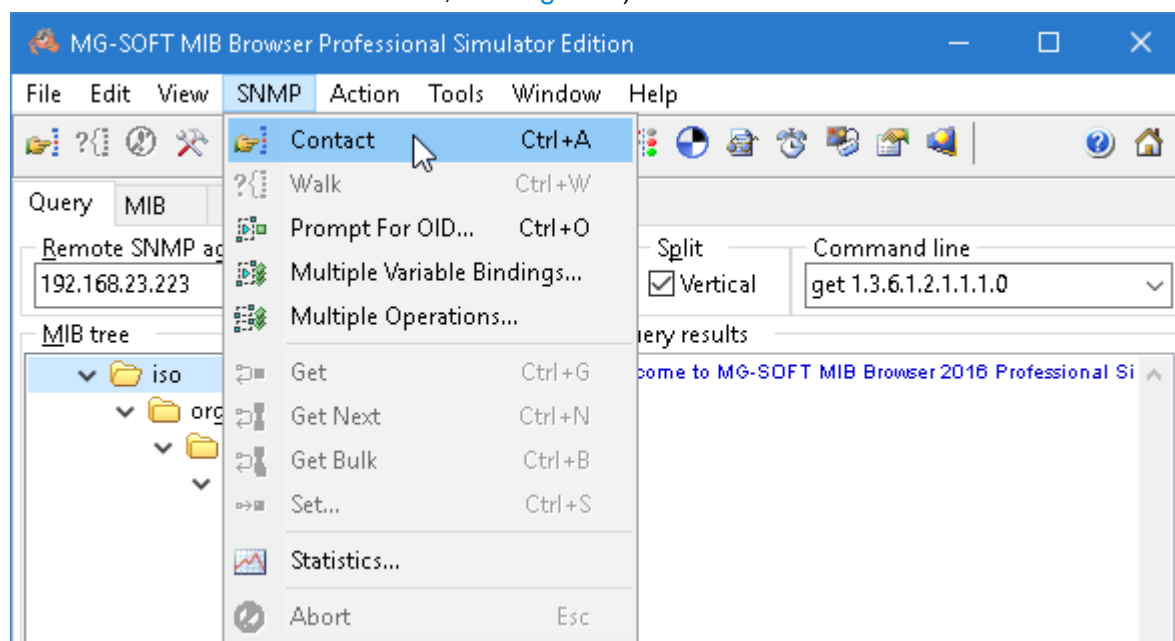




Figure 1: Accessing operations in MIB Browser by using menu commands

- ❑ Toolbar buttons (e.g., to contact an SNMP agent, click the  **Contact Remote SNMP Agent** toolbar button).
- ❑ Keyboard shortcuts (e.g., **Ctrl+A**. Which means: to contact an SNMP agent, hold down the **Ctrl** key on the keyboard and at the same time press the **A** key.).

Note: On **Mac OS X** use the **Command** key () available on the Apple Macintosh keyboards instead of the **Ctrl** key.

- ❑ Pop-up menu commands (e.g., to contact an SNMP agent, expand the pop-up menu by right-clicking the MIB tree and select the **Contact** command, see [Figure 2](#)).

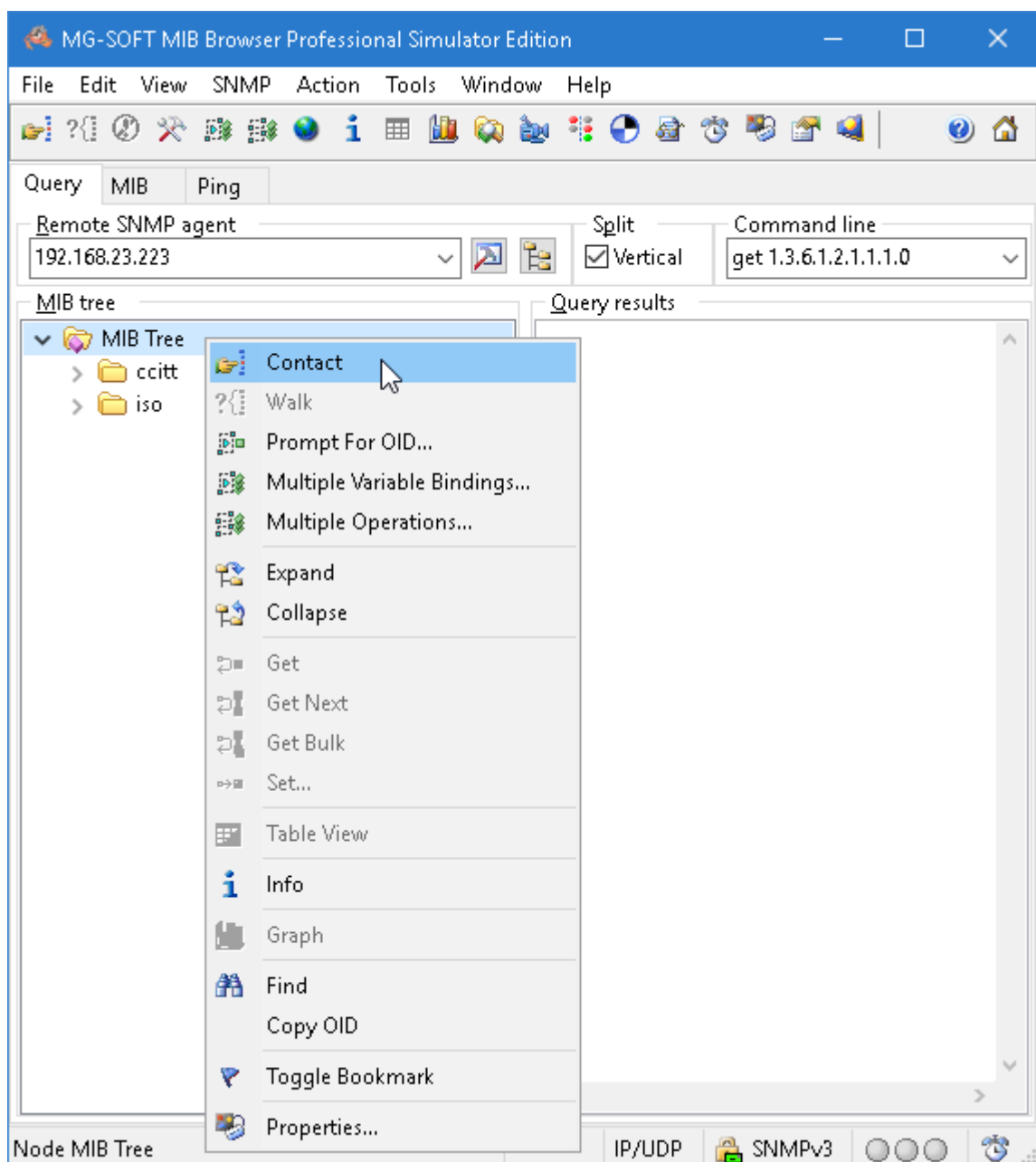


Figure 2: Accessing operations in MIB Browser by using pop-up menu commands

In this manual the access to most operations is described through the use of command selections listed in menus. However, you can also use any of the mentioned shortcuts if they are available.

Cross-References and Hyperlinks in MIB Browser Manual

While reading the manual you might come across some 'active' text. 'Active' means that a word or a phrase is a hyperlink or a cross-reference, which you can click to go to a web page or to an item appearing in another location in the manual. In this manual the active text is mainly colored with blue or red color.

In this manual hyperlinks and cross-references present mainly:

- ❑ References to related sections in the manual (e.g., a cross-reference to the [Starting MIB Browser](#) section).
- ❑ References to definitions of colored items (e.g., [retransmits](#)), which are located somewhere else in the manual.
- ❑ References to figures (e.g., [Figure 12](#)).
- ❑ Links to web pages (e.g., <http://www.mg-soft.com/>).

Tip: When you click the active text, you are taken to another location in the document. To return to the previous location, use the **Go to Previous View** toolbar button (in the Acrobat Reader).

2 GETTING STARTED

This section presents the basic system requirements your computer has to meet to install and use MG-SOFT MIB Browser Professional Edition with MIB Compiler, and it describes the installing and uninstalling procedures for MG-SOFT MIB Browser on Windows, Linux, Mac OS X and Solaris operating systems.

2.1 System Requirements

MG-SOFT MIB Browser Professional Edition with MIB Compiler is an SNMP manager application. It is available for 32-bit and 64-bit Microsoft Windows operating systems, for Linux operating systems (for Intel x86 and x86_64 architecture), for Apple Mac OS X operating systems (x86_64 platform) as well as for Solaris operating systems (for both, Intel x86 and SPARC platforms). In order to install and use the software, your computer has to meet the following system requirements:

2.1.1 Windows Operating System

The Windows version of MG-SOFT MIB Browser has been successfully tested on the following 32-bit (where available) and 64-bit Microsoft Windows operating systems:

- ❑ Windows Server 2008
- ❑ Windows 7
- ❑ Windows Server 2012
- ❑ Windows 8.x
- ❑ Windows 10
- ❑ Windows Server 2016

Note: To install the software on Windows, you need to have administrative privileges.

2.1.2 Linux Operating System

The Linux version of MG-SOFT MIB Browser has been successfully tested on the following Linux distributions running on the Intel x86 and x86_64 architecture:

- ❑ RHEL / CentOS 4 or newer
- ❑ Fedora 5 or newer
- ❑ SUSE 10 or newer
- ❑ Debian 4 or newer
- ❑ Ubuntu 6 or newer
- ❑ Slackware 12 or newer

For the most recent information about the supported distributions, please refer to the release notes (READ_ME.TXT) of the current software release.

Note: To install the software on Linux, you need to have the root user privileges.

2.1.3 Mac OS X Operating System

MG-SOFT MIB Browser for Mac release contains binaries for Intel x86_64 platform. It has been successfully tested by MG-SOFT on:

- ❑ Mac OS X v10.8.x Mountain Lion
- ❑ Mac OS X v10.9.x Mavericks
- ❑ Mac OS X v10.10.x Yosemite
- ❑ Mac OS X v10.11.x El Capitan
- ❑ Mac OS X v10.12.x Sierra
- ❑ Mac OS X v10.13.x High Sierra

For the most recent information about the supported distributions, check the release notes (READ_ME.TXT) of the current software release.

Note: To install the software on Mac OS X, you need to have admin user privileges.

2.1.4 Solaris Operating System

MG-SOFT MIB Browser for Solaris has been successfully tested on the following Solaris operating systems:

- ❑ Solaris v10 (Intel x86 and SPARC platforms)
- ❑ Solaris v11 (Intel x86)

For the most recent information about the supported distributions, check the release notes (READ_ME.TXT) of the current software release.

Note: To install the software on Solaris, you need to have the root user privileges.

2.2 Installing MIB Browser Professional Edition

Before you install MIB Browser Professional Edition with MIB Compiler on your computer, first make sure your computer meets the system requirements described in the [System Requirements](#) section.

2.2.1 Windows Operating System

Note: To install the software on Windows, you need to have administrative privileges.

1. Use Windows Explorer to locate the MG-SOFT MIB Browser software distribution (zip archive or setup files) that you have downloaded from MG-SOFT's Website or obtained on a removable medium.

Note: If MG-SOFT MIB Browser installer has been delivered to you on a USB flash card (WalletFlash), insert the card into a free USB port on your computer and allow the operating system to install the necessary drivers to use the flash drive.

2. The software distribution contains installers for 32-bit (x86) and 64-bit (x86_64) build of MG-SOFT MIB Browser Professional Edition with MIB Compiler for Windows.
 - ❑ On 32-bit Windows operating systems, double-click the **setup-32.exe** file to start installing the 32-bit version of MG-SOFT MIB Browser.
 - ❑ On 64-bit Windows operating systems, double-click the **setup-64.exe** file to start installing the 64-bit version of MG-SOFT MIB Browser.

Note: On 64-bit Windows systems, it is possible to install 64-bit or 32-bit version of MIB Browser Professional Edition. However, both versions cannot be installed on the same computer.

3. Follow the installation guidelines on screen to complete the software installation. When prompted for the license, point the dialog box to the `license.key` file you have received via e-mail or on the enclosed USB flash card in order for the installer to apply the license key to be used with the installed software.

Tip: You can install the software also without providing a `license.key` file and apply the license later, as described in the [Apply License Key](#) section.

Once the installation is complete, you can [start MG-SOFT MIB Browser](#) program.

2.2.2 Linux Operating System

Before the installation, please close all running MG-SOFT applications and uninstall any previous version of MG-SOFT MIB Browser Professional Edition with MIB Compiler from the system.

Note: To install the software on Linux, you need to have the root user privileges.

1. Put the MG-SOFT MIB Browser Professional Edition CD into your CD-ROM drive and mount the CD.
2. The software is available for two architectures (`i386` and `x86_64`) in three different package types (`.rpm`, `.deb` and `.tgz`). The complete installation procedure involves installing two components: MG-SOFT SNMP Trap daemon (`mgtrapd`) and MG-SOFT MIB Browser (`mgmibbrowser`). Depending on your Linux distribution and architecture, run the following commands in a Terminal window to install the software:

- ❑ On a Linux distribution with the RPM package manager, install the corresponding RPM packages:

```
# rpm -ivh mgtrapd-XXX.AAA.rpm
# rpm -ivh mgmibbrowser-XXX.AAA.rpm
```

- ❑ On a Linux distribution with the DPKG package manager, install the DEB packages:

```
# dpkg -i mgtrapd-XXX.AAA.deb
# dpkg -i mgmibbrowser-XXX.AAA.deb
```

- ❑ On the Slackware Linux distribution, install the TGZ packages:

```
# ./tgz-install.sh mgtrapd-XXX.AAA.tgz
# ./tgz-install.sh mgmibbrowser-XXX.AAA.tgz
```

Where **xxx** is the **version** of the software included in the tarball, and **aaa** is the **architecture**, i.e., `i386` for 32-bit systems and `x86_64` for 64-bit Linux systems.

3. To apply the license, copy your `license.key` file to the following directories:

<code>/usr/local/mg-soft/mgtrapd/bin</code>	(unlocks SNMP Trap daemon)
<code>/usr/local/mg-soft/mgmibbrowser/bin</code>	(unlocks MIB Browser, Compiler)

Note: The `license.key` file name must be specified in lower case (e.g., `LICENSE.KEY` file will not be accepted).

4. Restart the computer.

Once the installation is complete, you can [start MG-SOFT MIB Browser](#) program.

2.2.3 Mac OS X Operating System

1. Double-click the MG-SOFT MIB Browser disk image file (.dmg) that you have downloaded from MG-SOFT's Website or obtained on a removable medium (Figure 3).

Tip: Use **Finder** to navigate to the DMG file if it is not located on your desktop.

Note: You need to have administrative privileges to install the software on Mac OS X.

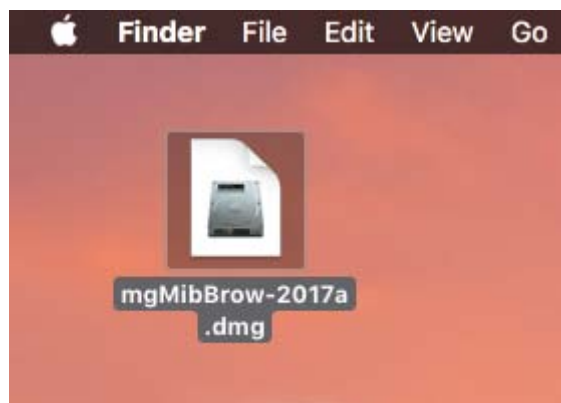


Figure 3: MIB Browser disk image file (DMG) on Mac OS X desktop

2. The contents of the double-clicked disk image displays in a Finder window (Figure 4). Double-click the MIB Browser installer package (**setup.pkg**) in the Finder to start installing the software.



Figure 4: Double-click the "setup.pkg" icon in Finder to run the MIB Browser installer

3. The wizard-driven MIB Browser installer appears ([Figure 5](#)) that guides you through the installation process. Follow the instructions displayed on the screen to finish the installation.

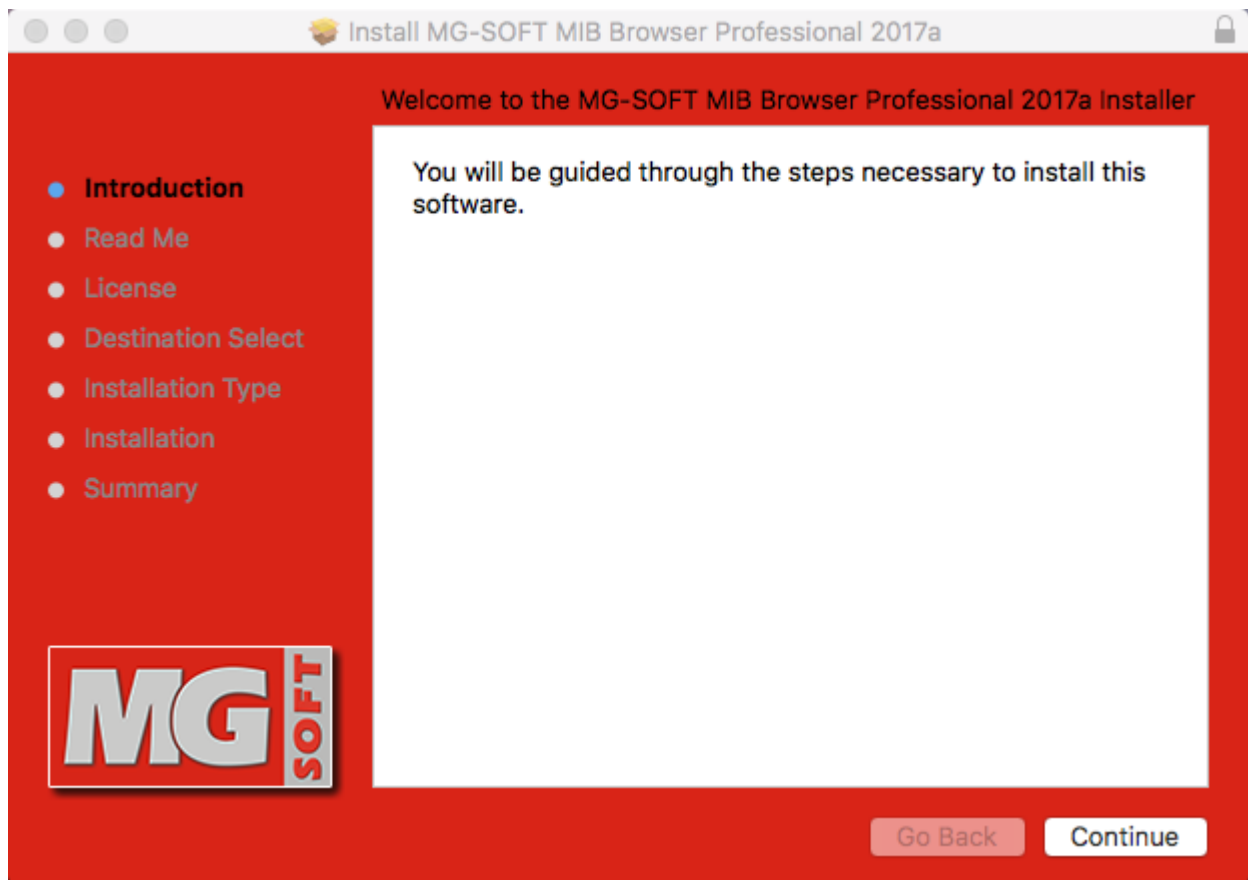


Figure 5: MIB Browser installer introduction screen

4. Eject (unmount) the MIB Browser disk image (DMG) in the Finder.

Once the installation is complete, you can [start MG-SOFT MIB Browser for Mac OS X](#) from the Finder.

2.2.4 Solaris Operating System

Before installing the software, please close all running MG-SOFT applications and uninstall any previous version of MG-SOFT MIB Browser Professional Edition with MIB Compiler from the system. The installation procedure involves installing two packages: MG-SOFT SNMP Trap daemon package and MG-SOFT MIB Browser package, as follows:

Note: To install the software, you need to have the root user privileges.

1. Depending on the platform, run the following commands in a Terminal window:

On i86pc-based systems

```
# pkgadd -d MGSOFtmgtrapd-sol10-i386-vvv.pkg
# pkgadd -d MGSOFtmgmibbrowser-sol10-i386-vvv.pkg
```

where "vvv" is the version of the software you are installing.
(accept the default installation settings for both packages)

On SPARC-based systems

```
# pkgadd -d MGSOFtmgtrapd-sol10-sparc-vvv.pkg
# pkgadd -d MGSOFtmgmibbrowser-sol10-sparc-vvv.pkg
```

where "vvv" is the version of the software you are installing.
(accept the default installation settings for both packages)

2. Copy your `license.key` file to the following directories:

```
/usr/local/mg-soft/mgtrapd/bin      (unlocks SNMP Trap daemon)
/usr/local/mg-soft/mgmibbrowser/bin (unlocks MIB Browser, Compiler)
```

3. Start MG-SOFT SNMP Trap daemon by using the following command:

```
# /etc/init.d/mgtrapd start
```

Once the installation is complete, you can [start MG-SOFT MIB Browser for Solaris](#).

2.3 Uninstalling MIB Browser Professional Edition

Administrative user privileges (administrator/root) are required to uninstall the software.

2.3.1 Windows Operating System

To uninstall MIB Browser Professional on Windows operating system:

1. Close the MIB Browser program.
2. From the Windows taskbar, select the **Start / Programs / MG-SOFT MIB Browser / Uninstall MIB Browser** command.

3. Follow the instructions displayed on the screen.

2.3.2 Linux Operating System

To uninstall MIB Browser Professional on Linux operating system:

Uninstalling MG-SOFT MIB Browser 2018

Note: For uninstalling previous versions of MIB Browser, please refer to the *Uninstalling the software* section of the `README.TXT` file, which installs with the software.

1. If the software has been installed by the RPM package manager, the following command in the command prompt will uninstall MIB Browser Professional Edition with MIB Compiler from your computer:

```
# rpm -e mgmibbrowser_2018
# rpm -e mgtrapd <if not needed by other MG-SOFT applications>
```

2. If the software has been installed by the DPKG package manager, use the following command in the command prompt to uninstall MIB Browser Professional Edition with MIB Compiler from your computer:

```
# dpkg -r mgmibbrowser-2018
# dpkg -r mgtrapd <if not needed by other MG-SOFT applications>
```

3. On Slackware Linux distribution use the following commands to uninstall MIB Browser Professional Edition with MIB Compiler from your computer:

```
# removepkg mgmibbrowser_2018
# removepkg mgtrapd <if not needed by other MG-SOFT applications>
```

2.3.3 Mac OS X Operating System

To uninstall MIB Browser Professional on Mac OS X operating system:

1. Close the MIB Browser program.
2. Open the **Finder** and select the **Applications** entry in the panel on the left.
3. Select the **MG-SOFT MIB Browser** folder (menu) in the Finder and double-click the **Uninstall MIB Browser** entry ([Figure 6](#)).
4. Follow the instructions displayed on the screen.

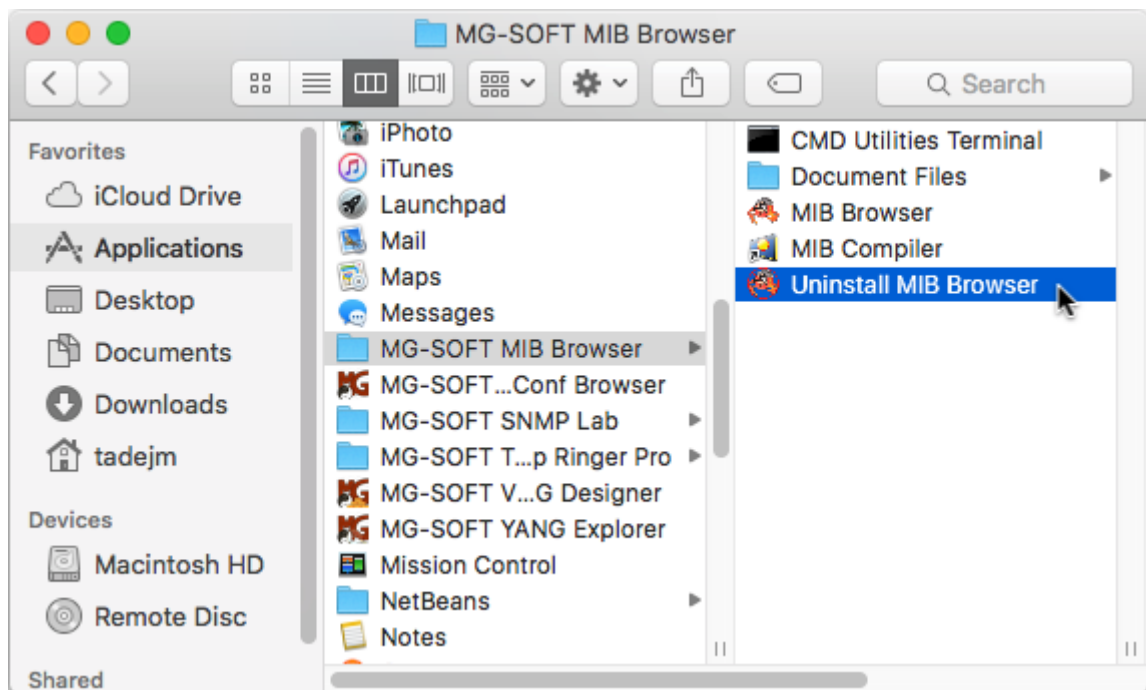


Figure 6: Uninstalling MIB Browser on Mac OS X

2.3.4 Solaris Operating System

1. To uninstall MIB Browser Professional for Solaris, run the following command in a Terminal window:

```
# pkgrm MGSOFTmgmibbrowser
```

2. If MIB Browser is the only MG-SOFT's application you are using, uninstall also MG-SOFT SNMP Trap daemon (otherwise, do **not** uninstall it, as it is required by other MG-SOFT's applications to receive SNMP traps):

```
# pkgrm MGSOFTmgtrapd
```

3 START SNMP MIB BROWSER PROFESSIONAL EDITION

3.1 Starting MIB Browser

3.1.1 Windows Operating System

1. In Windows operating systems, select the **Start / Programs / MG-SOFT MIB Browser / MIB Browser** command from the Windows taskbar.
2. As the program starts, the MIB Browser Professional Edition splash screen appears, followed by the About MG-SOFT MIB Browser dialog box (Figure 7).
3. The About MG-SOFT MIB Browser dialog box displays information about MG-SOFT MIB Browser and the license details.

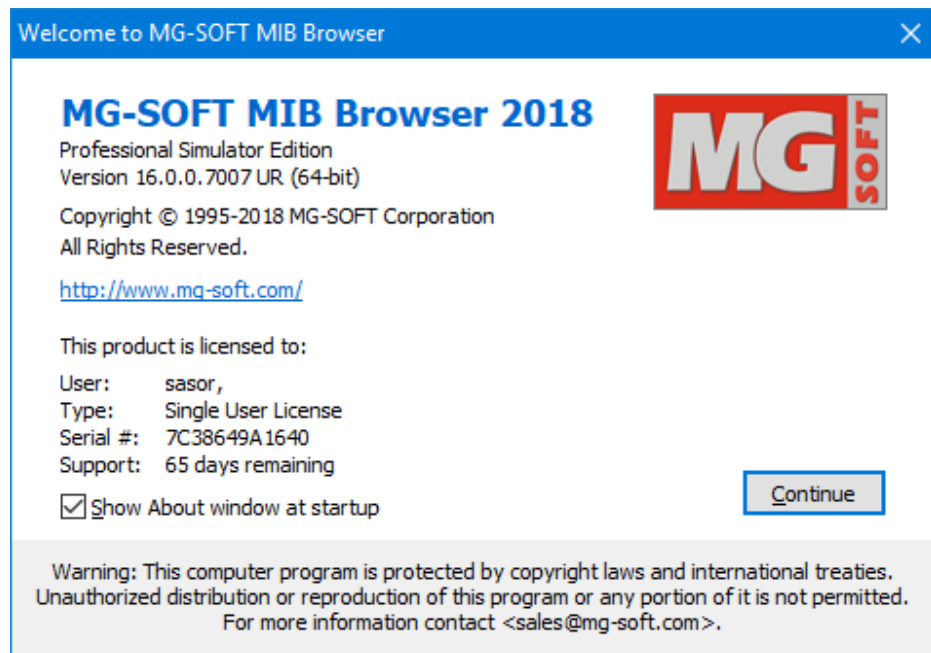


Figure 7: About MG-SOFT MIB Browser dialog box

4. Click the **Continue** button. The Tip Of The Day message box appears. After reading the recommendations, click the **Close** button.

Tip: You can open the Tip Of The Day message box at any time by selecting the **Help / Tip of the Day** command.

5. The MIB Browser desktop appears (Figure 12) and you can start using the software.

3.1.2 Linux Operating System

The easiest way to start MIB Browser under Linux operating system is to use the start menu. The start menu can be displayed from the desktop taskbar.

KDE Desktop Environment

1. If you have the KDE desktop environment installed, display the menu by clicking the application launcher button ([Figure 8](#)).
2. To start MIB Browser, select the **Applications** entry and navigate to (or search for) and select the **MG-SOFT MIB Browser / MIB Browser** menu item.

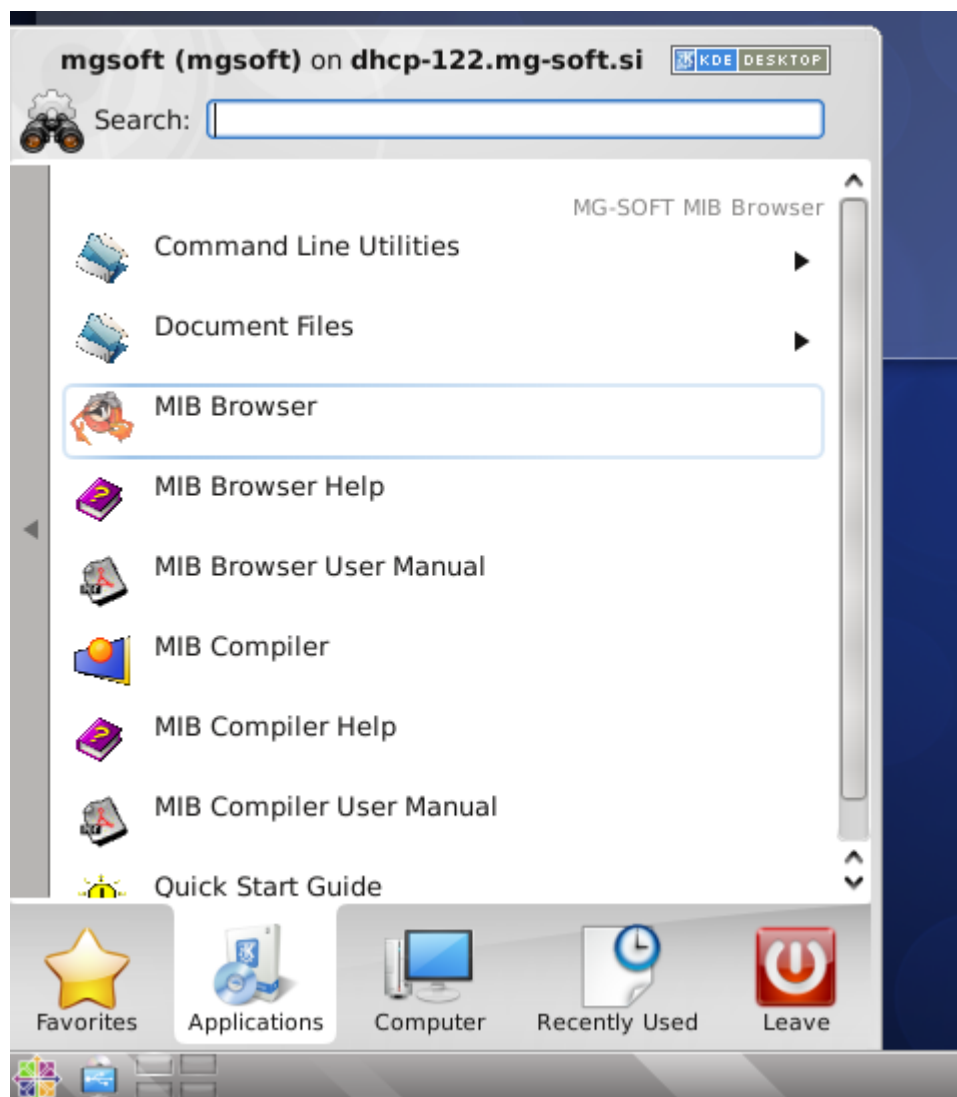


Figure 8: Starting MIB Browser from the menu in the KDE desktop environment

3. As the program starts, the MIB Browser Professional Edition splash screen appears, followed by the About MG-SOFT MIB Browser dialog box ([Figure 7](#)).

4. The About MG-SOFT MIB Browser dialog box displays information about MG-SOFT MIB Browser and MG-SOFT Corporation, and shows a list of all other MG-SOFT products.
5. To close the About MG-SOFT MIB Browser dialog box, click the **Continue** button. The Tip Of The Day message box appears. After reading the recommendations, click the **Close** button.
6. The MIB Browser desktop appears (Figure 12) and you can start using the software.

Tip: You can also start MIB Browser Professional Edition from the command prompt (xterm or compatible) by the following command:

```
# mgmibbpe
```

GNOME Desktop Environment

1. If you have the GNOME desktop installed, display the main menu by clicking the **Applications** start button (Figure 9).
2. To start MIB Browser, navigate to (or search for) and select the **MG-SOFT MIB Browser / MIB Browser** menu item.

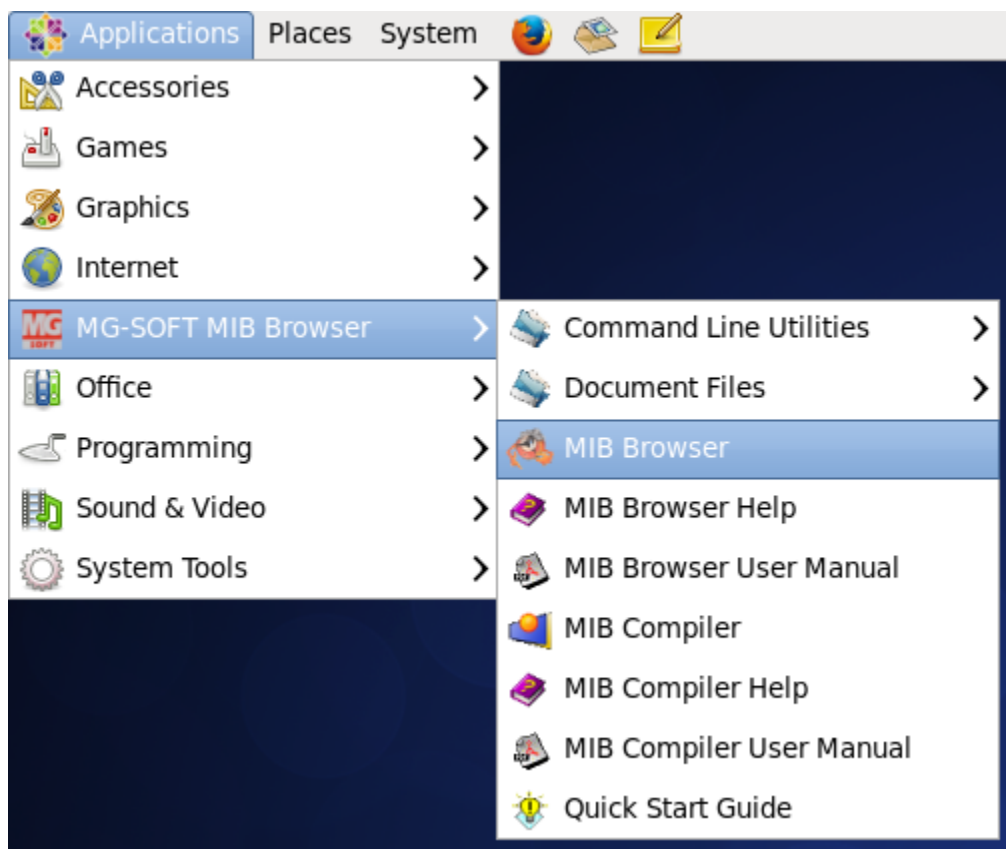


Figure 9: Starting MIB Browser from the main menu in the GNOME environment

3. As the program starts, the MIB Browser Professional Edition splash screen appears, followed by the About MG-SOFT MIB Browser dialog box (Figure 7).

4. The About MG-SOFT MIB Browser dialog box displays information about MG-SOFT MIB Browser and MG-SOFT Corporation, and shows a list of all other MG-SOFT products.
5. To close the About MG-SOFT MIB Browser dialog box, click the **Continue** button. The Tip Of The Day message box appears. After reading the recommendations, click the **Close** button.
6. The MIB Browser desktop appears (Figure 12) and you can start using the software.

3.1.3 Mac OS X Operating System

1. Open the **Finder** and select the **Applications** entry in the panel on the left.
2. Select the **MG-SOFT MIB Browser** folder (menu) in the Finder and double-click the **MIB Browser** entry (Figure 10).

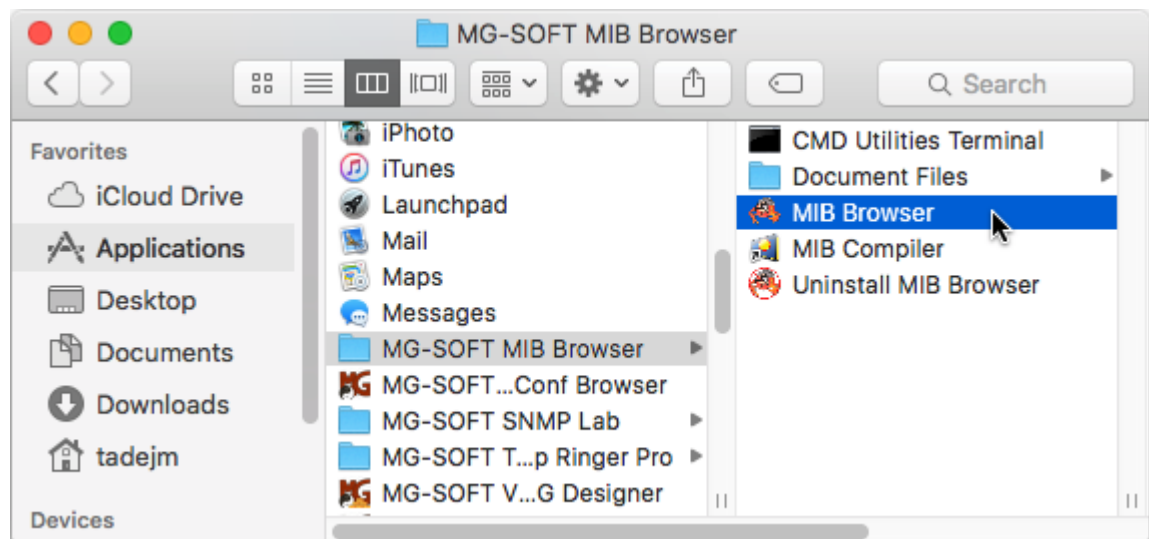


Figure 10: Starting MIB Browser on Mac OS X

3. As the program starts, the MIB Browser Professional Edition splash screen appears, followed by the About MG-SOFT MIB Browser dialog box (Figure 7). The latter displays information about MG-SOFT MIB Browser and MG-SOFT Corporation, and shows a list of all other MG-SOFT products. Click the **OK** button to close the dialog box.
4. The Tip Of The Day message box appears. After reading the recommendations, click the **Close** button.

Tip: You can open the Tip Of The Day message box at any time by selecting the **Help / Tip of the Day** command.

5. The MIB Browser desktop appears (Figure 12) and you can start using the software.

3.1.4 Solaris Operating System

The easiest way to start MIB Browser under Sun Solaris 10 operating system is to use the Sun Java Desktop System (JDS) Launch menu. In the CDE desktop environment, MIB Browser and other bundled applications can only be launched from a command line. Starting MIB Browser under Solaris 11 is similar, using the Gnome desktop environment.

1. If using JDS desktop environment, display the **Launch** menu by clicking the taskbar **Launch** button.
2. If using Gnome desktop environment, display the **Applications** menu from the taskbar.
3. To start MIB Browser, select the **MG-SOFT MIB Browser / MIB Browser menu** item (Figure 11).

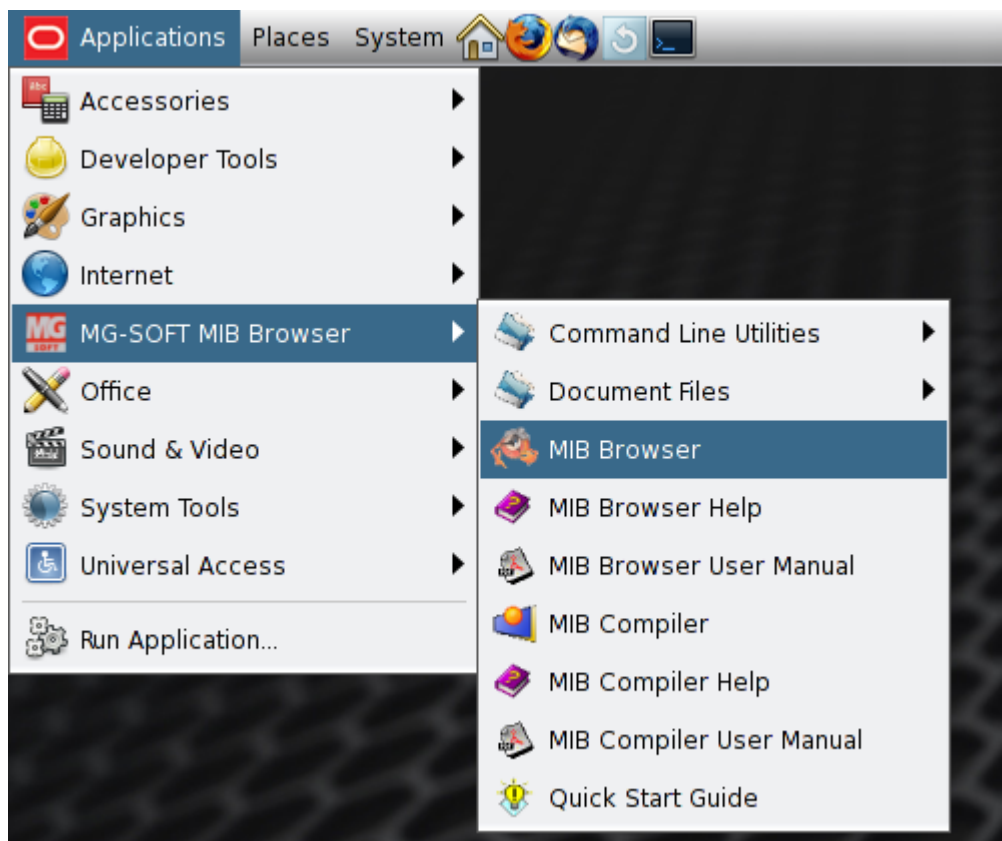


Figure 11: Starting MIB Browser on Solaris (Gnome environment)

4. As the program starts, the MIB Browser Professional Edition splash screen appears, followed by the About MG-SOFT MIB Browser dialog box (Figure 7). The latter displays information about MG-SOFT MIB Browser and MG-SOFT Corporation, and shows a list of all other MG-SOFT products. Click the **OK** button to close the dialog box.
5. The Tip Of The Day message box appears. After reading the recommendations, click the **Close** button.

Tip: You can open the Tip of The Day message box at any time by selecting the *Help / Tip of the Day* command.

6. The MIB Browser desktop appears (Figure 12) and you can start using the software.

Tip: You can also start MIB Browser from a terminal window by using the following command:

```
# /usr/local/mg-soft/mgmibbrowser/bin/mgmibbrowser.sh
```

In the CDE desktop environment, MIB Browser can be launched only from a command line.

3.2 MIB Browser Desktop

The design of MIB Browser appearance and functionality follows the conventions of the general Windows-based application. The MIB Browser desktop (Figure 12) has a title bar, menu bar, toolbar, status bar, minimize, maximize and close buttons and some areas specific only to MIB Browser.

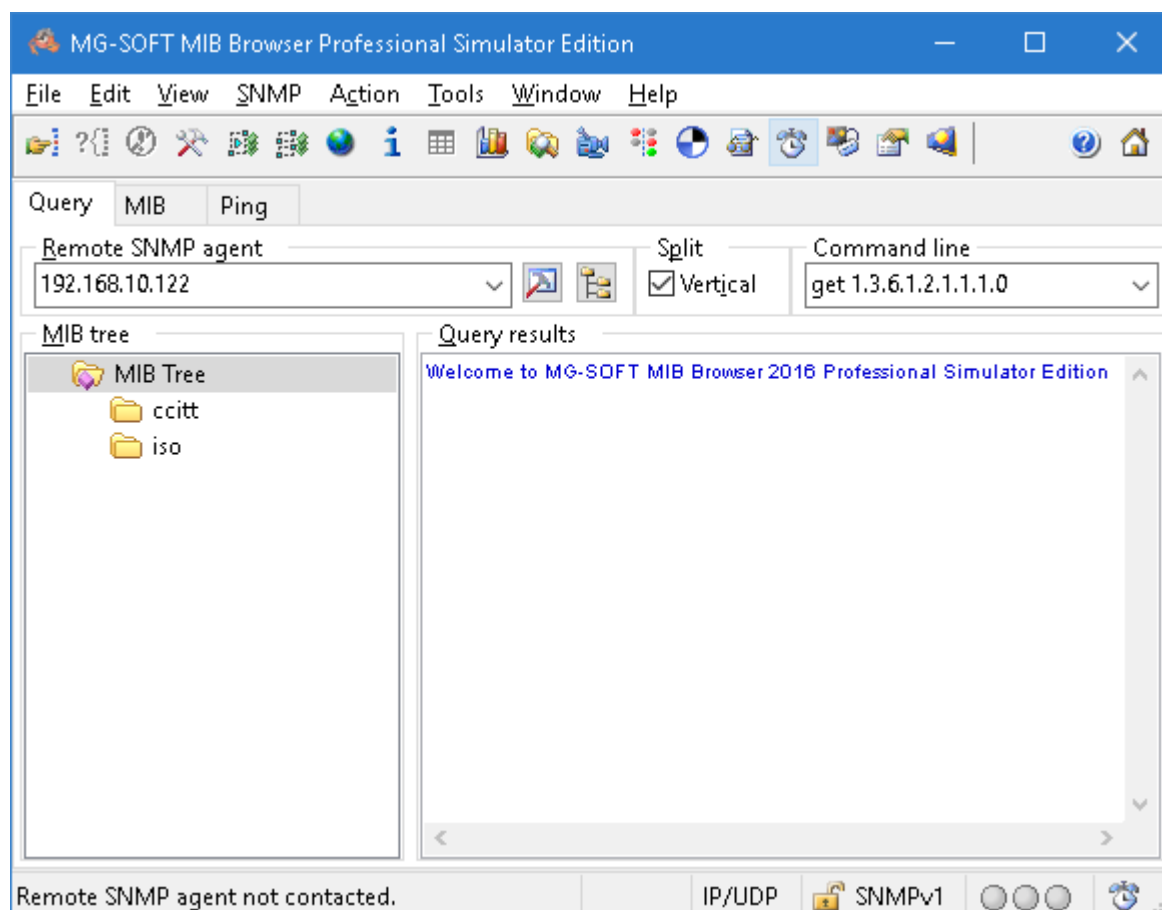


Figure 12: MIB Browser desktop

In MIB Browser desktop, you can switch between three general tabs, the Query tab, MIB tab and Ping tab. The displayed tab views consist of panels, frames or tabs, which

contain either the MIB tree structure, results of performed SNMP operations, a list of MIB groups and of loaded or unloaded MIB modules, and Ping operation results.

For detailed description of these areas, please see the MIB Browser Help file (**Help / Help Topics**).

Menu bar

The bar near the top of MIB Browser desktop ([Figure 13](#)) that contains menus, such as File, Edit, View, SNMP, Action etc. Menus can be expanded to show a list of command selections, which are used to access various features of the program and to perform different operations.

Toolbar

The toolbar near the top of MIB Browser desktop ([Figure 13](#)) that contains buttons that open most of MIB Browser windows or provide a quick access to some commands in MIB Browser.

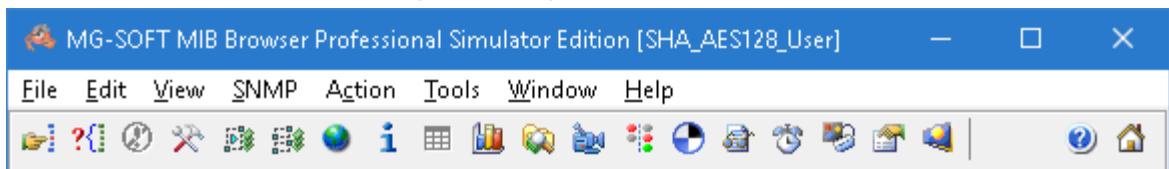


Figure 13: Menu bar and toolbar on MIB Browser desktop

Working area

The area placed between the toolbar and the status bar, in which you can choose between the **Query**, **MIB** and **Ping** tab. Controls available in these tabs allow you to perform basic SNMP operations on selected MIB tree nodes and view the results of SNMP operations (Query tab), to load and unload compiled MIB modules (MIB tab), and to query remote devices by means of ICMP Ping requests (Ping tab).

Status bar

A bar at the bottom of MIB Browser desktop with six fields displaying different types of information ([Figure 14](#)).



Figure 14: Status bar of MIB Browser desktop

The first field informs you about the last change or action performed in MIB Browser (e.g., it informs you whether a query of an SNMP agent has been successful or timed out, or which MIB node has been selected etc.). The second field shows the number of SNMP packets sent from MIB Browser. This value is reset each time the Query Results panel is cleared. The third field shows the currently used transport protocols (e.g., IP/UDP), the fourth field displays the currently used SNMP version (e.g., SNMPv1), the fifth field is the last operation status indicator (semaphore), and the last field shows an alarm clock that notifies you with a ringing animation when a new SNMP Trap or Inform notification message is received. The ringing animation continues until you acknowledge notifications in the SNMP Trap Ringer Console window.

4 APPLY LICENSE KEY

Without a valid `license.key` file in place MIB Browser will operate in restricted mode. To apply a `license.key` file after the software has been installed, proceed as follows:

1. If you have received your `license.key` file on a USB flash card (WalletFlash), insert the card into a free USB port on your computer and allow the operating system to install the necessary drivers to use the flash drive.
2. Select the **Help / Apply License** command from the main menu.
3. The Apply License dialog box (Figure 16) appears. Click the **Select** button in the Apply License dialog box to display the Open dialog box (Figure 15).

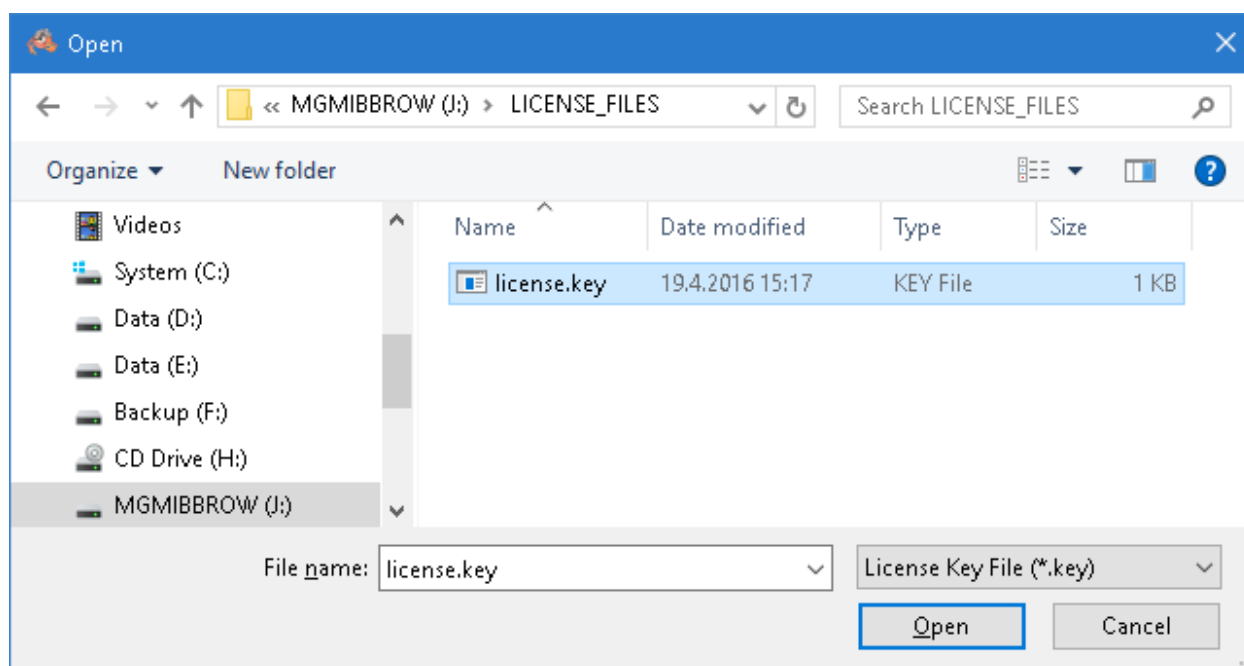


Figure 15: Selecting the license.key file

4. Navigate to the drive and folder containing your `license.key` file for MG-SOFT MIB Browser Professional Edition. Select either the `license.key` file or the Zip archive containing it and click the **Open** button (Figure 15).

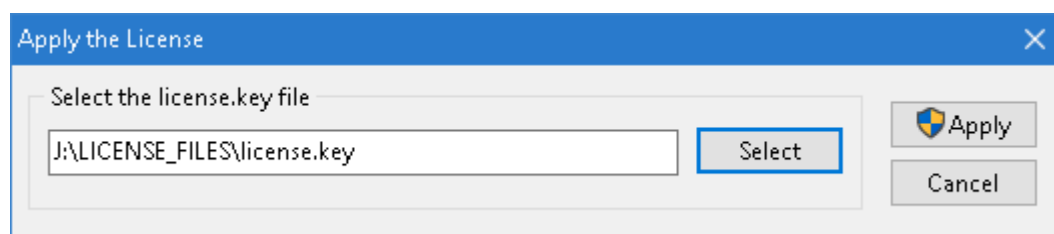


Figure 16: Applying the license.key file

5. Click the **Apply** button in the Apply License dialog box (Figure 16). The software will copy the specified `license.key` file to the proper location in order for MIB Browser to read it and unlock its features accordingly (after a restart).

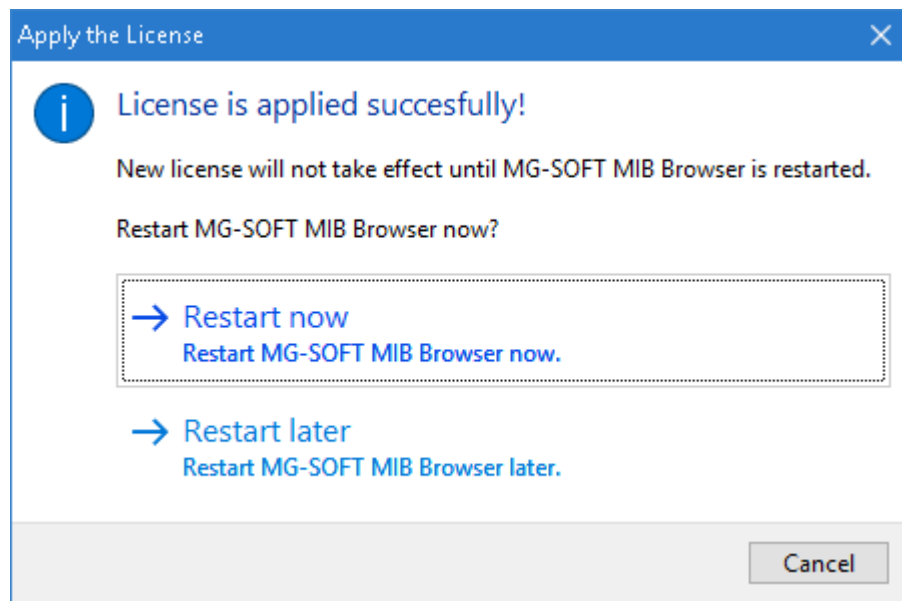


Figure 17: Applying the license.key file - restarting MIB Browser

6. Click the **Restart now** option in the dialog box that informs you about the successfully copied license. After MIB Browser restart, the selected license should be applied and you can start using the software.

Tip: You can check if the license key has been properly applied by verifying if the About MIB Browser dialog box (accessible via the **Help / About** command) displays your license details correctly.

5 CONTACT REMOTE SNMP AGENT AND QUERY ALL ITS OBJECT INSTANCES

To monitor or manage an SNMP device on the network, you have to contact its SNMP agent. Once you have successfully contacted the SNMP agent, you can retrieve values of all object instances implemented in the managed device by using the SNMP Walk operation.

5.1 Contacting Remote SNMP Agent

1. In the main window, make sure the **Query** tab is selected (Figure 18).
2. Into the **Remote SNMP Agent** drop-down list, type the IP or IPv6 address of the SNMP agent that you wish to query. For more details about specifying agent addresses, see the [Using IPv4 or IPv6 Address](#) section.
3. Click the **Contact Remote SNMP Agent** toolbar button or select the **SNMP / Contact** command.
4. MIB Browser contacts the selected SNMP agent and displays its response in the **Query Results** panel (Figure 18).

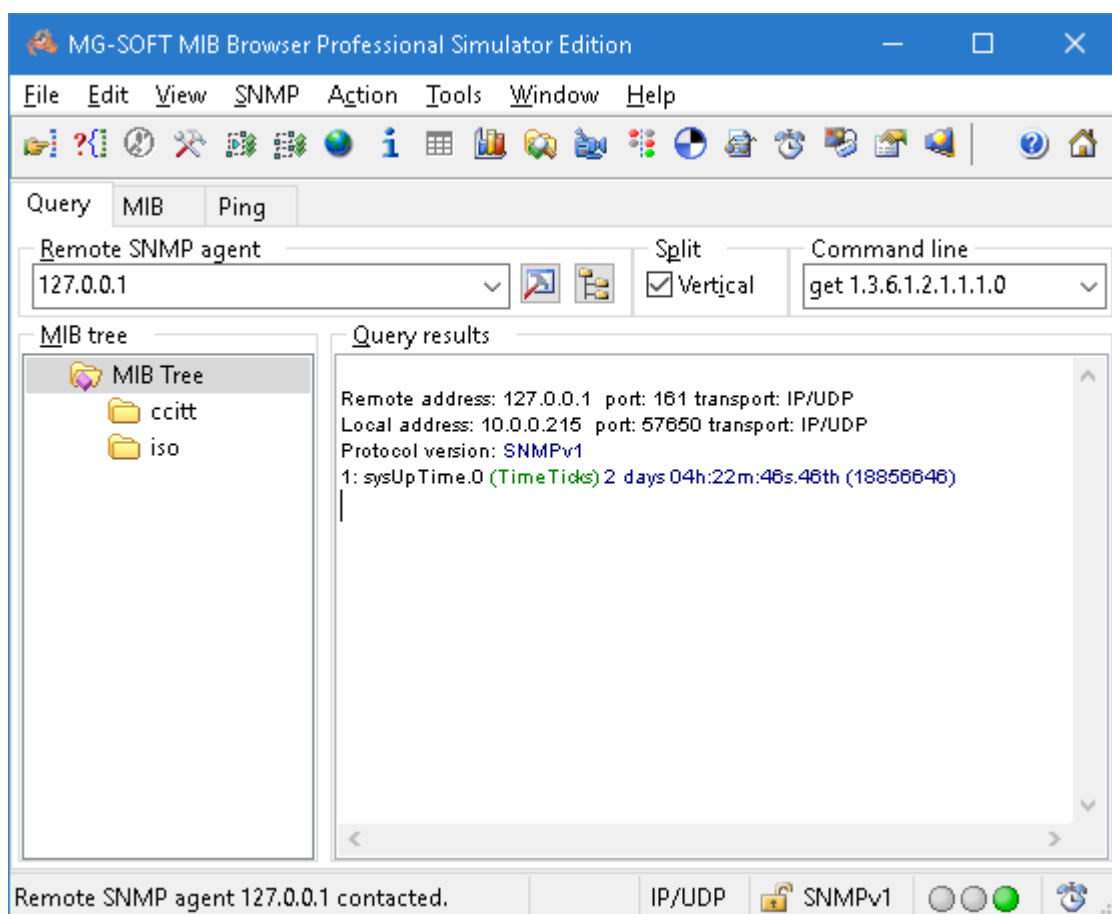
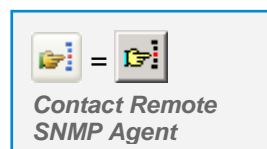


Figure 18: MIB Browser displaying a response from the contacted SNMP agent

5.1.1 Using IPv4 or IPv6 Address

To contact an SNMP agent, you have to know its IP (Internet Protocol) address. Most of the today's Internet uses IPv4 (Internet Protocol Version 4) for communication. But since there is a growing shortage of IPv4 addresses, IPv6 (Internet Protocol Version 6) has been introduced and is expected to gradually replace the IPv4.

To contact and query an SNMP agent on the network, enter its IPv4 address or, if the agent supports it, its IPv6 address into the **Remote SNMP Agent** input line on the MIB Browser desktop (Figure 18). Before entering the IPv6 address, read the [IPv6 Address with Scope ID](#) section.

The logo consists of the text "IPv6" in a bold, sans-serif font, centered within a rectangular frame that has a slight 3D effect.

Note: The Internet Protocol Version 6 (IPv6) is available only in **DOCSIS/DH** and better editions of **MG-SOFT MIB Browser Pro**.

IPv4 Address

The **IPv4** address convention has the following format:

XXX.XXX.XXX.XXX

Example:

192.168.116.172
saso.mg-soft.si

Note: When using the numerical form of the IPv4 address, the address has to be given in decimal notation. Besides, you can also contact an SNMP agent by using its domain name.

IPv6 Address

The **IPv6** address convention has the following format:

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

Example:

fe80:0000:0000:0000:02c1:27ff:fe00:02d9
andrejb.ipv6.mg-soft.si

The address can be simplified by removing the leading zeros:

fe80:0:0:0:2c1:27ff:fe00:2d9

For further simplification, sequences of zeros can be compressed:

fe80::2c1:27ff:fe00:2d9

Note: In order to use the IPv6 as transport protocol for querying SNMP agents, the IPv6 protocol has to be installed on the computer that runs MIB Browser.

Note: When using the numerical form of the IPv6 address, the address has to be given in hex notation. Besides, you can also contact an SNMP agent by using its domain name.

IPv6 Address with Scope ID

When **not** using global IPv6 addresses, you typically need to append the scope ID to the IPv6 address of the SNMP agent when entering it into the MIB Browser's **Remote SNMP Agent** input line (Figure 19).

A scope ID identifies the network interface over which traffic is sent and received. The notation that is used to specify the scope ID with an address is Address%ScopeID.

Example:

```
fe80::24f7:5359:f256:48a%5
andrejb.ipv6.mg-soft.si%5
```

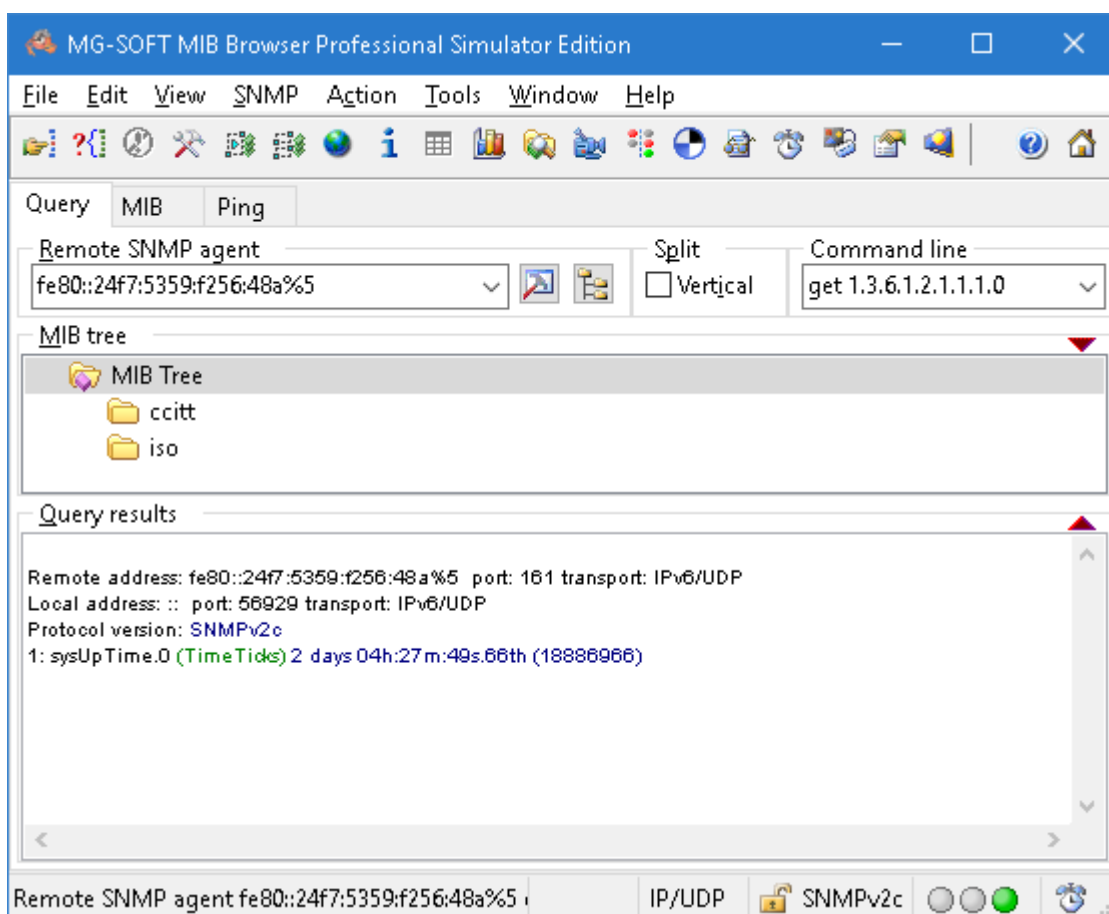


Figure 19: IPv6 address with scope ID in the Remote SNMP Agent input line

Tip: You can use the IPv6 address without scope ID, if you in the MIB Browser Preferences dialog box specify your local IPv6 address (together with the scope ID) as the binding interface for communication over IPv6.

For instruction on how to select a binding interface, see the [Selecting Binding Interface](#) section.

5.1.2 Selecting Binding Interface

MIB Browser allows computers with two or more network interface adapters to manage SNMP agents on different subnets from one computer.

To specify which binding interface should be used for sending and receiving SNMP packets:

1. Open the MIB Browser Preferences dialog box by using the **View / MIB Browser Preferences** command.
2. In the MIB Browser Preferences dialog box choose the **General / Transport** preferences.
3. The SNMP Transport Protocol Preferences panel appears (Figure 20).

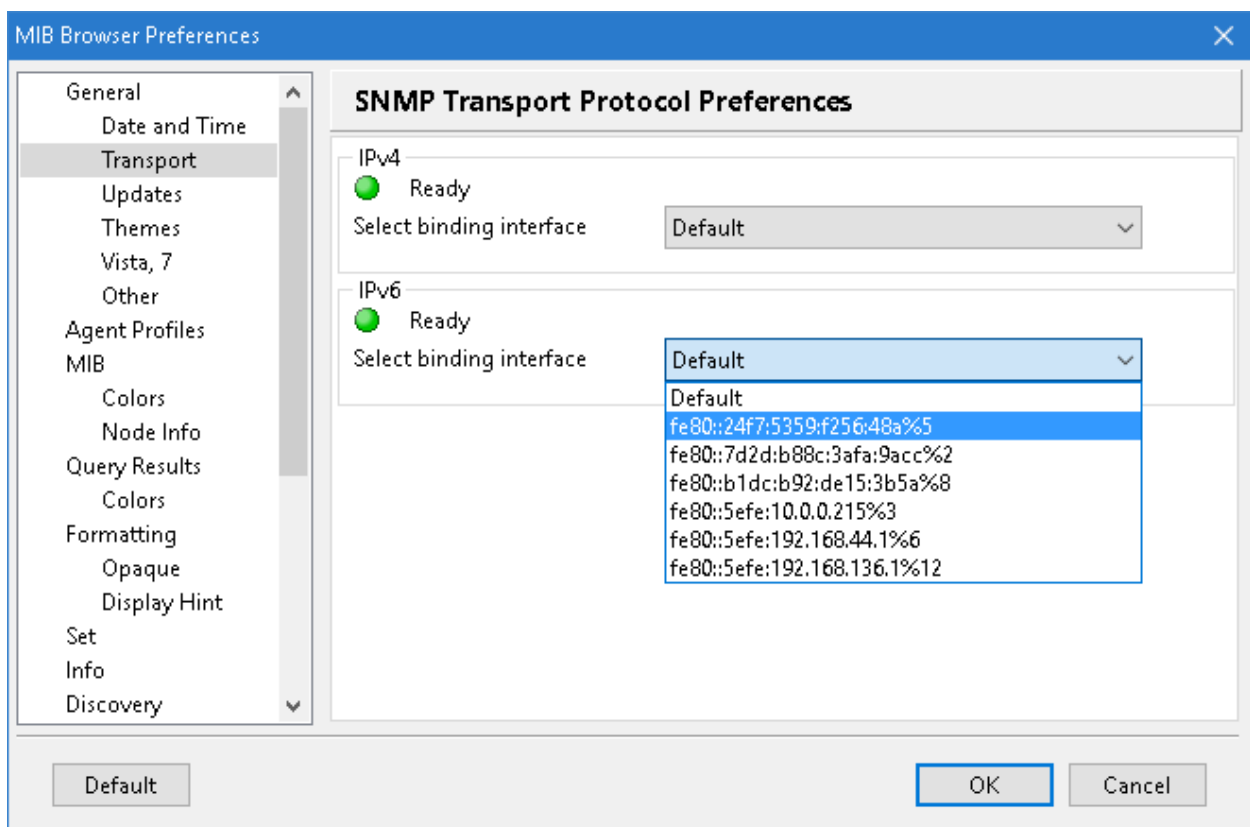


Figure 20: Selecting binding interface in the MIB Browser Preferences dialog box

4. Select the desired binding interface in the corresponding transport protocol frame (IPv4, IPv6).
5. Click the **OK** button and restart MIB Browser for the changes to take effect.

5.2 Selecting Nodes in MIB Tree

In MIB Browser, loaded MIB modules are organized and represented in a MIB tree structure with nodes called MIB nodes. You can see the MIB tree structure in the **MIB tree** panel (Figure 22) in MIB Browser's main window.

To select a node in the MIB tree, proceed as follows:

1. In the MIB tree panel, expand the MIB tree by selecting the **Expand** pop-up command (Figure 21).

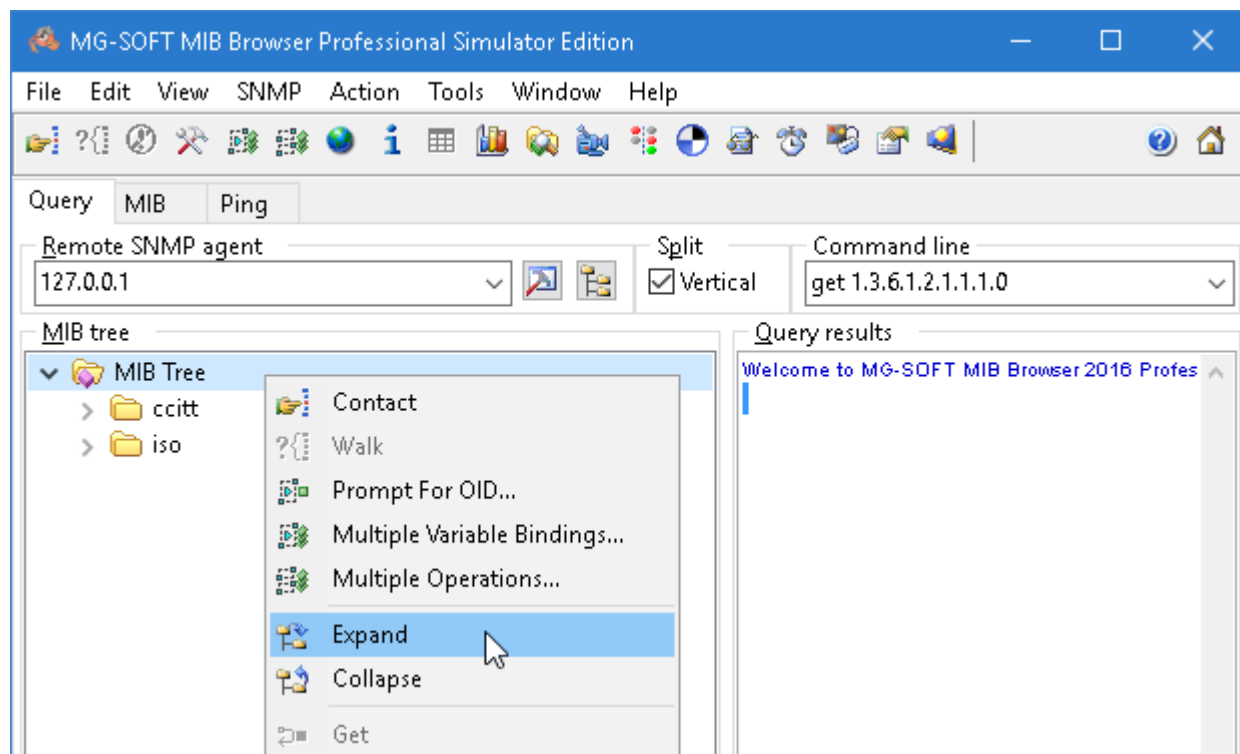


Figure 21: Expanding the MIB tree

No MIB Modules Loaded

Tip: If there are no MIB modules loaded in MIB Browser, switch to the **MIB** tab in the main window and load MIB modules (see the [Manually Loading MIB Modules](#) section).

Tip: MIB Browser will automatically load MIB modules implemented in the contacted SNMP agent and compiled in MIB Compiler, if you perform the SNMP Walk operation from the root node (called MIB Tree). For instructions, see the [Retrieving All Object Instance Values with SNMP Walk Operation](#) section.

2. In the expanded MIB tree (Figure 22), locate and select the node on which you wish to perform an SNMP operation (e.g., Walk, Get, Set, etc.).

Once a MIB tree node is selected, you can perform the majority of SNMP operations on it in two ways:

- ❑ By right-clicking a MIB tree node and selecting the respective command (e.g., **Contact**, **Walk**, **Get**, **Set**, etc.) from the pop-up context menu, or
- ❑ By selecting the command from the main menu (e.g., **SNMP / Contact**, **SNMP / Walk**, **SNMP / Get**, etc.).

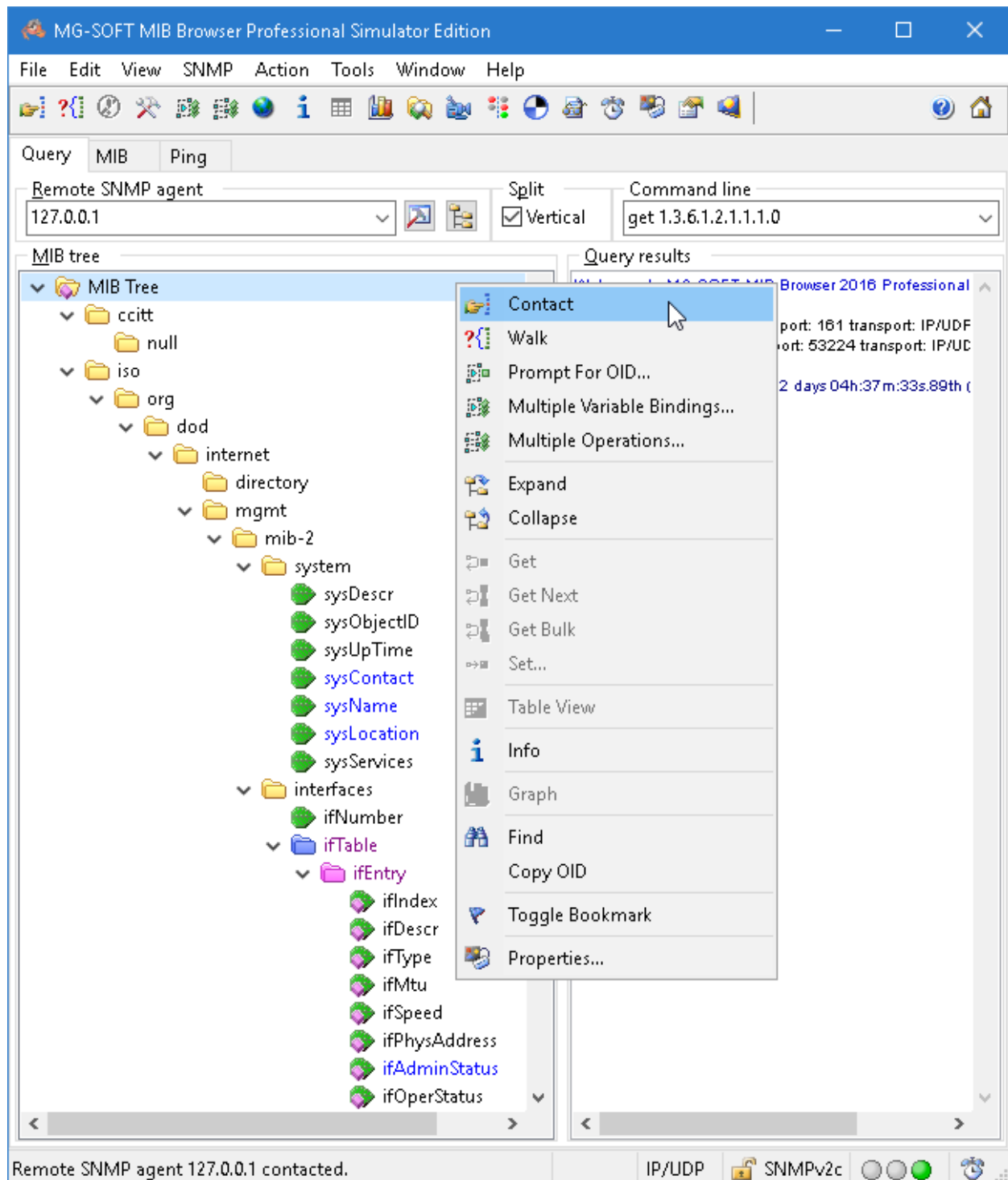

















Figure 22: Expanded pop-up menu command and a displayed MIB tree in the MIB tree panel

5.2.1 Symbols Used for Different Types of MIB Nodes

The following symbols are used to represent different types of MIB tree nodes:

-  Object identifier node
-  Object type scalar node
-  Object type table node
-  Object type row node
-  Object type columnar node
-  Trap type node
-  Notification type node
-  Object identity node
-  Object group node
-  Notification group node
-  Textual convention node
-  Type assignment node
-  Module compliance node
-  Agent capabilities node
-  Module identity node

For more information on different types of nodes (MIB objects), please refer to the SMI specification ([RFC2578](#), [RFC2579](#) and [RFC2580](#)).

5.2.2 Colors Used for Representing Different Access Types of MIB Nodes

By default, the colors of MIB node **names** (e.g., sysUpTime, sysContact, sysLocation, etc.) indicate the node access type as defined in the MIB (e.g., **read-only**, **read-write**, **read-create**, **not-accessible**, etc.). This way, you can tell at a glance which nodes (i.e., corresponding MIB object instances) are writable, creatable, not accessible, etc.

[Figure 23](#) shows the default node name colors indicating different node access levels (defined by the node Access/Max-Access clause values).

Tip: The node access colors can be configured in the program preferences (**View/MIB Browser Preferences/MIB Tree Color Preferences**).

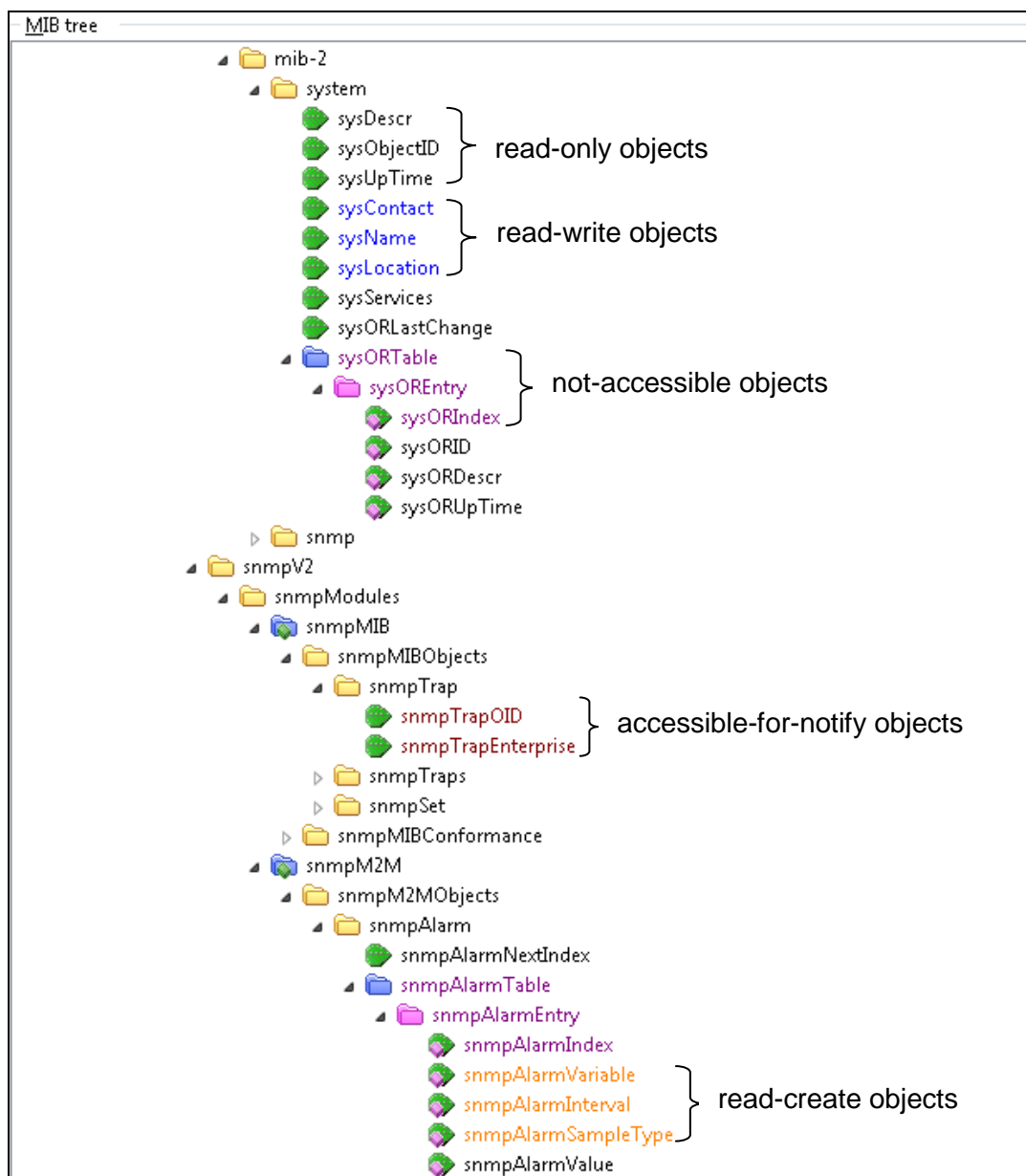


Figure 23: MIB nodes of different access types (default colors)

5.2.3 Finding MIB Tree Nodes by Name or OID

To search for a specific node in the MIB tree (starting from the root node):

1. Right-click the MIB tree root node and select the **Find** pop-up command.
2. The Find Object in MIB Tree dialog box appears (Figure 24).

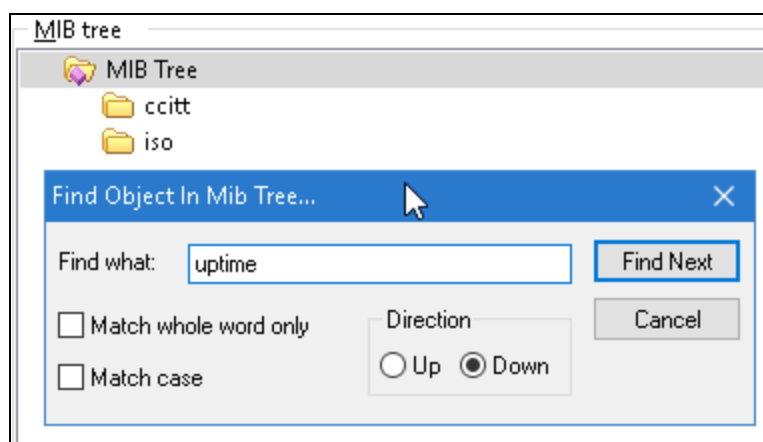


Figure 24: The Find Object in MIB Tree dialog box

3. Into the **Find what** input line, type the name (e.g., sysUpTime) or OID (e.g., 1.3.6.1.2.1.1.3) of the node you are searching for, select the **Down** search direction and click the **Find Next** button.

Select the **Match whole word only** search option to find only those strings that are whole words and not part of a larger word (e.g., ads1 will find ads1 and Ads1, but not ads12).

Select the **Match case** search option to make the search case sensitive. If this option is enabled, the search will find only those strings in which the capitalization matches the one used in the **Find what** input line (e.g., ads1 will find ads1, but not Ads1).

4. The MIB tree is automatically expanded and the found node is selected (provided that the MIB module that defines the node is loaded in MIB Browser).

Tip: Use the **Edit / Find Next** command or press the **F3** button to find the next node, whose name or OID matches the search criteria.

5.3 Retrieving All Object Instance Values with SNMP Walk Operation

You can retrieve all object instances with their current values that a managed device supports by using the SNMP Walk operation.

You can perform the SNMP Walk operation from any node in the MIB tree. When MIB Browser starts the SNMP Walk operation, it first sends an SNMP GetNext request with the OID value of a selected object to the SNMP agent. In response, it gets the OID and the current value of the first instance that in lexicographical order follows the selected object. To identify and query the next object instance implemented in lexicographical order, MIB Browser sends another SNMP GetNext request with the OID it has received in response to the previous SNMP GetNext request. In this way, MIB Browser traverses the MIB tree by issuing successive SNMP GetNext requests to the SNMP agent and retrieves all instance values of the selected object. It stops when the SNMP agent returns an OID value that no longer matches the selected but some other MIB object/subtree.

5.3.1 Performing SNMP Walk Operation

1. Contact an SNMP agent as described in the [Contacting Remote SNMP Agent](#) section.
2. In the MIB tree, click the node from which you wish to start the SNMP Walk operation.

Note that you can select either:

- ❑ The root node of the MIB tree (the first node in the MIB tree called the MIB Tree, [Figure 25](#)). MIB Browser will 'walk' the whole MIB tree and return all values implemented in the queried SNMP agent.
- ❑ A root node of any MIB sub tree (e.g., `system`). MIB Browser will perform the SNMP Walk operation on the whole sub tree (e.g., `system` sub tree).
- ❑ A columnar object (e.g., `ifInOctets`). MIB Browser will repeatedly send SNMP GetNext requests to retrieve all instance values of the selected columnar object.
- ❑ A scalar object (e.g., `sysUpTime`). MIB Browser will query only the selected scalar object and display its instance value.

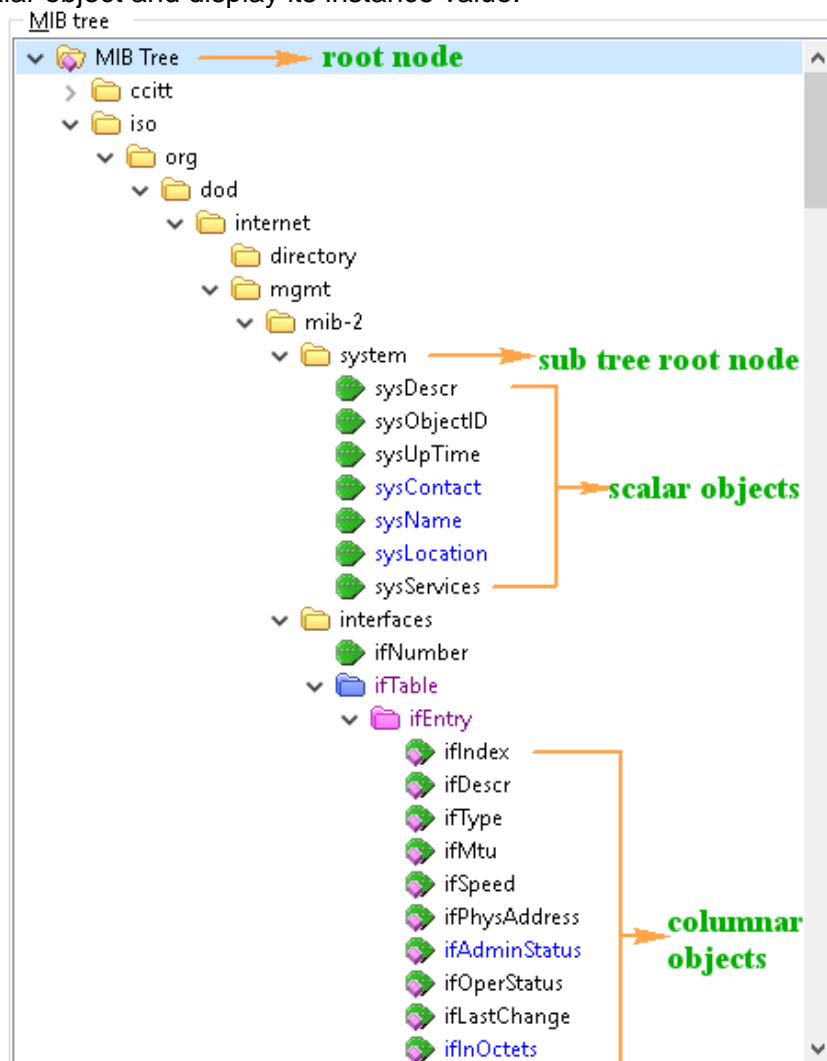
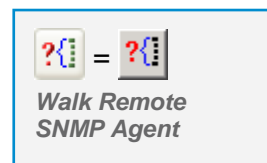


Figure 25: Terminology used for MIB tree objects and nodes

3. From the main menu, select the **SNMP / Walk** command or click the **Walk Remote SNMP Agent** toolbar button.
4. The program queries the desired object instances in the SNMP agent and displays its values in the Query Results panel.



If, while performing the SNMP Walk operation, MIB Browser comes across an OID that is not defined by any of the loaded MIB modules, it prompts you with the Search Compiled MIB Modules To Resolve OID dialog box (Figure 26).

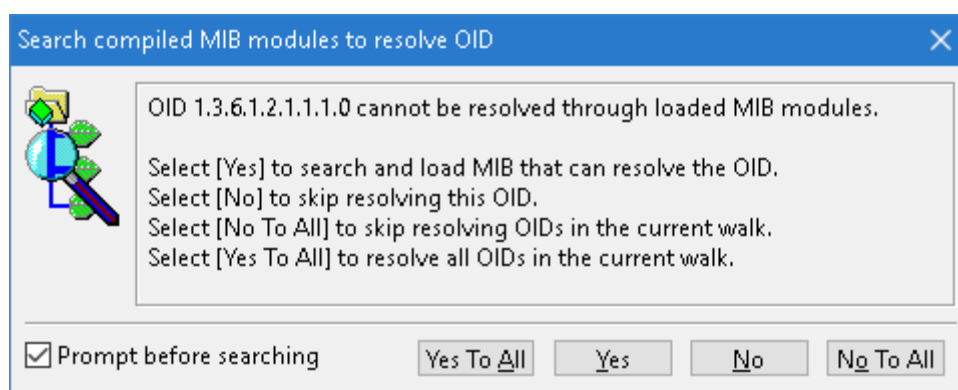


Figure 26: Search Compiled MIB Modules To Resolve OID dialog box

To continue with the SNMP Walk operation, select one of the options:

- ❑ **Yes To All** - MIB Browser will resolve all OIDs in the current walk and load all MIB modules that resolve these OIDs.
- ❑ **Yes** - MIB Browser will search for and load a MIB module that will resolve the current OID.
- ❑ **No** - MIB Browser will skip the resolving of the current OID and continue with the operation.
- ❑ **No To All** - MIB Browser will not load any additional MIB modules, i.e., it will not resolve the current OID, as well as any other OIDs not defined in the already loaded MIB modules that MIB Browser may come across in the current walk.

Tip: If you want MIB Browser to automatically search for compiled MIB modules and resolve OIDs without prompting you, uncheck the **Prompt before searching for MIB modules** checkbox in the MIB Browser Preferences dialog box in the MIB Tree and MIB Modules Preferences panel.

If you want the program to perform the SNMP Walk operation on the whole MIB tree from any selected object, check the **Until No-Such or End-Of-MIB-View** checkbox in the MIB Browser Preferences dialog box.

1. Use the **View / MIB Browser Preferences** command to open the MIB Browser Preferences dialog box. When it opens, select the **Query Results** preferences to display the Query Results Preferences panel.
2. In the Query Results Preferences panel, check the **Until No-Such or End-Of Mib-View** checkbox.

Example:

How to query all object instances in the system sub tree in an SNMP agent by using the SNMP Walk operation?

Contact the SNMP agent by using the **SNMP / Contact** command. In the MIB tree, click the root node of the *system* sub tree. Use the **SNMP / Walk** command or right-click the *system* node and select the **Walk** pop-up command. MIB Browser performs the SNMP Walk operation on the *system* sub tree. The remote SNMP agent returns the values of all *system* sub tree object instances and MIB Browser displays them in the Query Results panel (Figure 27).

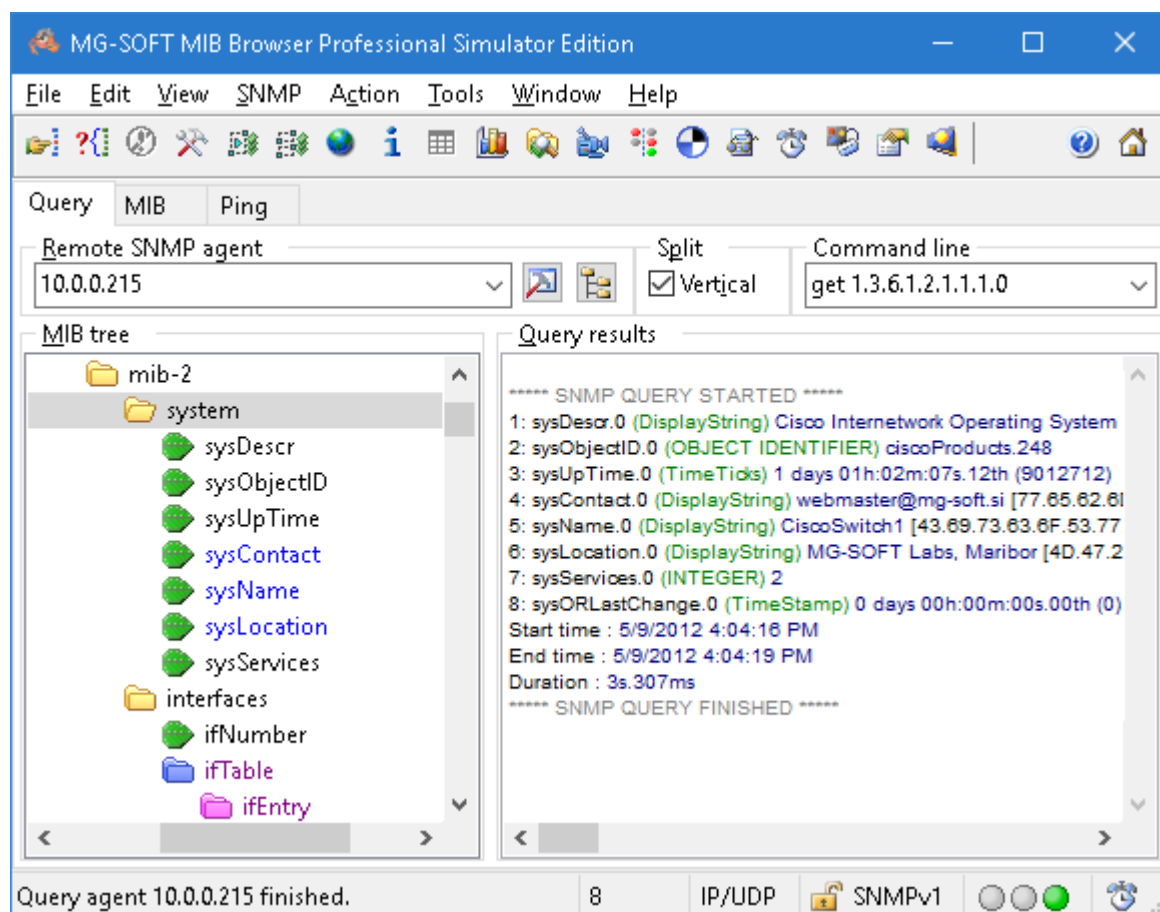


Figure 27: Results of the SNMP Walk operation on the *system* sub tree

SNMP Walk Operation with SNMP GetBulk Requests

MIB Browser can be configured to use SNMP GetBulk requests instead of GetNext requests when traversing an SNMP agent's MIB tree. When using SNMP GetNext requests, MIB Browser receives in response to each request only one object instance with its value. On the other hand, when using SNMP GetBulk requests, MIB Browser can receive in response to each request one or more (e.g., 100) object instances with corresponding values. In this way the use of SNMP GetBulk requests minimizes network interactions and time when retrieving a large amount of management information.

Note: The SNMP GetBulk operation is supported only in the SNMPv2c and SNMPv3 protocol.

To perform SNMP Walk operation with SNMP GetBulk requests:

1. Contact the desired SNMP agent as described in the [Contacting Remote SNMP Agent](#) section.
2. To configure MIB Browser to use the SNMP GetBulk operation, open the SNMP Protocol Preferences dialog box by using the **View / SNMP Protocol Preferences** command.
3. In the opened SNMP Protocol Preferences dialog box, select either the **SNMPv2c** or the **SNMPv3** radio button (the SNMPv1 protocol does not support SNMP GetBulk operation).

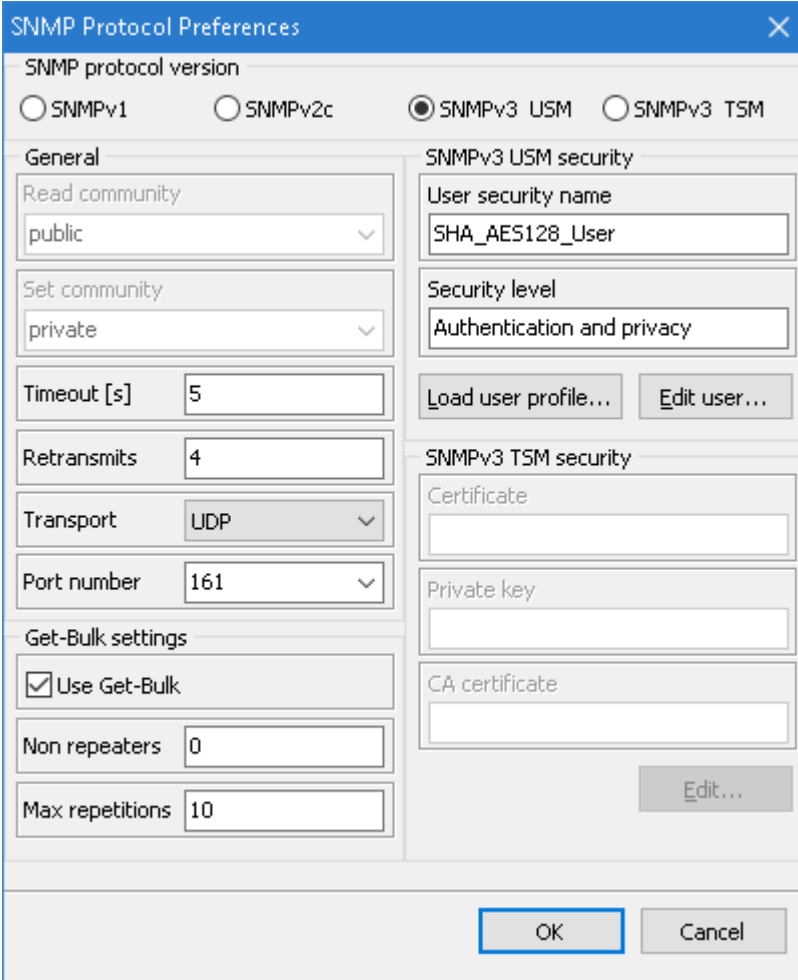
The image shows the 'SNMP Protocol Preferences' dialog box. At the top, under 'SNMP protocol version', there are four radio buttons: 'SNMPv1', 'SNMPv2c', 'SNMPv3 USM' (which is selected), and 'SNMPv3 TSM'. The dialog is divided into two main sections. The left section, titled 'General', contains fields for 'Read community' (set to 'public'), 'Set community' (set to 'private'), 'Timeout [s]' (set to 5), 'Retransmits' (set to 4), 'Transport' (set to 'UDP'), and 'Port number' (set to 161). Below these is the 'Get-Bulk settings' section, which includes a checked 'Use Get-Bulk' checkbox, 'Non repeaters' (set to 0), and 'Max repetitions' (set to 10). The right section, titled 'SNMPv3 USM security', contains a 'User security name' field (set to 'SHA_AES128_User') and a 'Security level' dropdown (set to 'Authentication and privacy'). Below these are buttons for 'Load user profile...' and 'Edit user...'. The bottom section, titled 'SNMPv3 TSM security', contains fields for 'Certificate', 'Private key', and 'CA certificate', with an 'Edit...' button at the bottom right. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

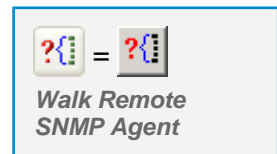
Figure 28: Specifying SNMP GetBulk settings

4. In the **Get-Bulk settings** frame check the **Use Get-Bulk** checkbox ([Figure 28](#)).
5. In the **Non repeaters** input line, set the number of non-repeaters to zero (0), and into the **Max repetitions** input line, enter the desired maximum number of object instances that will be returned in the SNMP GetBulk response.

Note: When you use the SNMP GetBulk operation in the main window, the 'non-repeaters' value has to be set to zero (0). Otherwise the program returns only one instance regardless of the 'max-repetitions' value.

To learn more about the use of SNMP GetBulk operation, see the [SNMP GetBulk usage example](#).

6. Click **OK** to close the SNMP Protocol Preferences dialog box. MIB Browser automatically contacts the SNMP agent and applies the new settings.
7. Select a node in the MIB tree from which you wish to perform the SNMP Walk operation (for more details see the step 2 in the [Performing SNMP Walk Operation](#) section).
8. From the main menu, select the **SNMP / Walk** command or click the **Walk Remote SNMP Agent** toolbar button.
9. MIB Browser traverses the selected part of the MIB tree by issuing successive SNMP GetBulk requests to the SNMP agent. It displays the retrieved object instances with values in the Query Results panel.



5.4 Viewing MIB Node Properties

With MIB Browser you can check properties of MIB nodes as they are defined in MIB definition modules. MIB node properties are displayed in the MIB Node Properties window.

To see the properties of a MIB node:

1. First, specify a MIB node. You can specify a node by clicking it in a MIB tree (displayed in e.g., the main window or in the Select Object Identifier window). Or, you can specify a node by entering its OID value or name into an **OID** input line (available in e.g., the Set dialog box).
2. When you have specified a MIB node, use the **View / MIB Node Properties** command or click the **MIB Node Properties** toolbar button, which is available in different instances in MIB Browser.
3. The MIB Node Properties window opens (Figure 29).

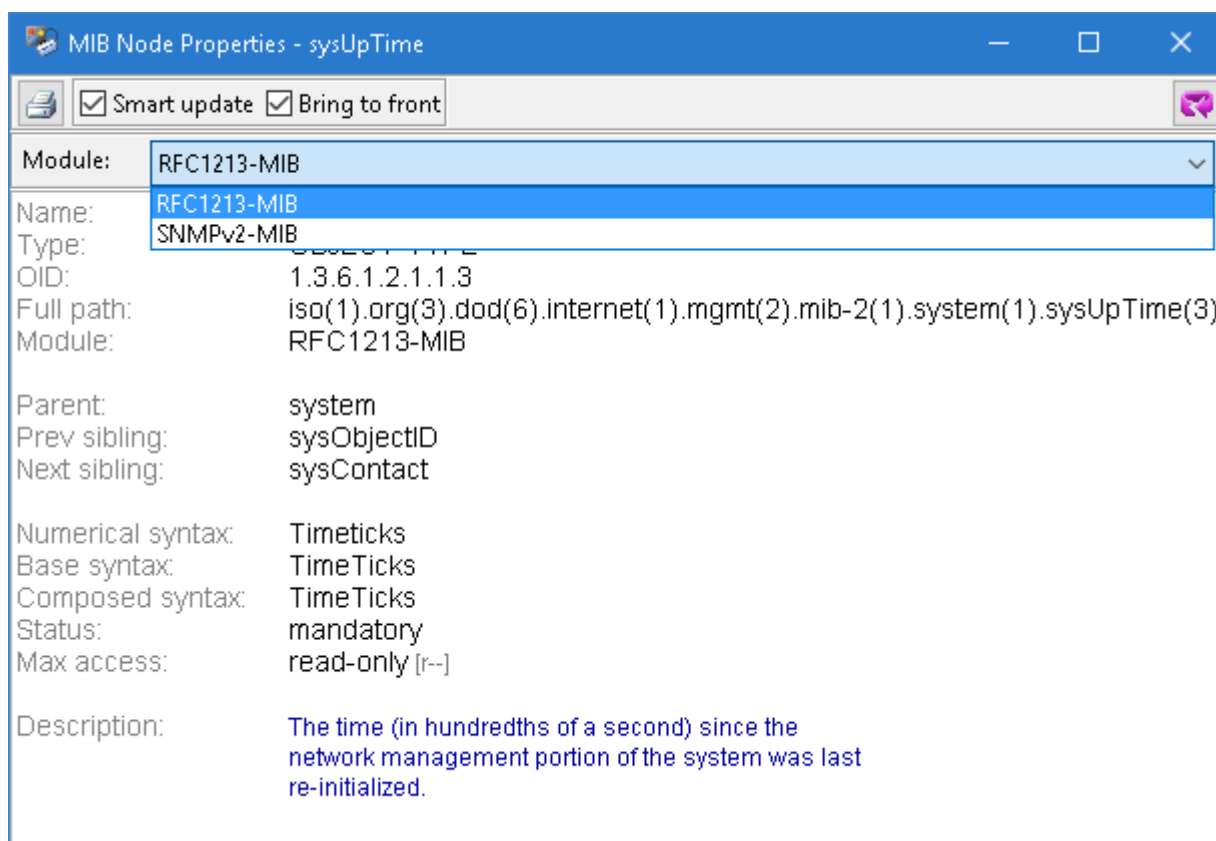
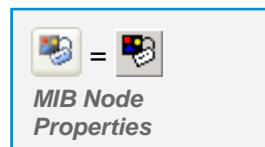


Figure 29: MIB Node Properties window with a displayed drop-down list of MIB modules

4. If you display the **Module** drop-down list, you will see which of the loaded MIB modules define the selected node or either directly or indirectly import this node definition from other MIB modules.

5. The window displays the properties of the selected node as they are specified in the SMIDB file of the MIB module that is currently selected in the **Module** drop-down list.

Note: When more than one MIB module is listed in the **Module** drop-down list, you can select among the listed MIB modules. By selecting another MIB module, the content of the window panel is updated displaying node properties as recorded in the SMIDB file of the newly selected module.

Note: If the name of the MIB module selected in the **Module** drop-down list matches the name of the MIB module displayed in the **Module** line in the window's panel (Figure 29), the selected MIB module defines this node.

6 SPECIFY SNMP PROTOCOL PARAMETERS

In this section, you will learn how to specify SNMP protocol parameters that MIB Browser uses when it communicates with a remote SNMP agent.

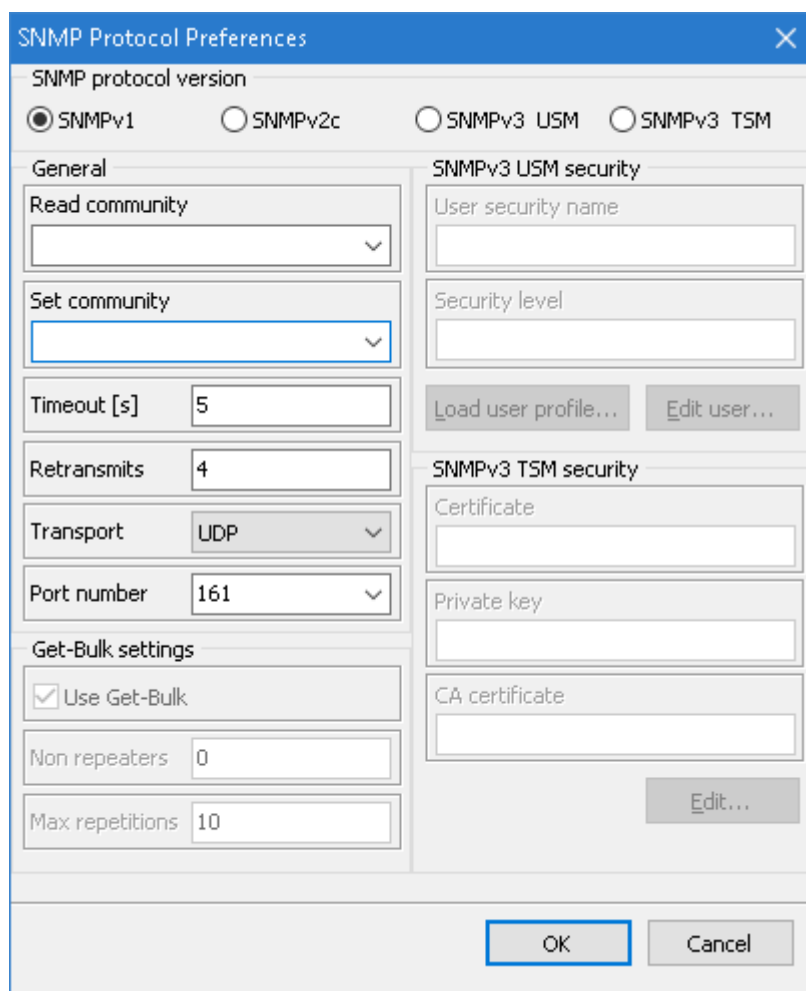
It is important that you specify the parameters correctly, because if they do not match the parameters expected by the SNMP agent, the agent will not respond.

Tip: MIB Browser lets you configure and use SNMP agent profiles to manage different SNMP agents. An SNMP agent profile permanently stores all information required for accessing and managing a particular SNMP agent on the network (including its address and SNMP protocol parameters). For more information on SNMP agent profiles, see the [Configure and Use SNMP Agent Profiles](#) section of this manual.

1. To specify SNMP protocol preferences, select the **View / SNMP Protocol Preferences** command from the main menu or click the **SNMP Protocol Preferences** toolbar button.
2. The SNMP Protocol Preferences dialog box opens (Figure 30).



SNMP Protocol Preferences



The dialog box is titled "SNMP Protocol Preferences". It contains several sections:

- SNMP protocol version:** Radio buttons for ☒ SNMPv1, ☐ SNMPv2c, ☐ SNMPv3 USM, and ☐ SNMPv3 TSM.
- General:**
 - Read community: dropdown menu.
 - Set community: dropdown menu.
 - Timeout [s]: text box with value 5.
 - Retransmits: text box with value 4.
 - Transport: dropdown menu with value UDP.
 - Port number: dropdown menu with value 161.
 - Get-Bulk settings:
 - ☒ Use Get-Bulk.
 - Non repeaters: text box with value 0.
 - Max repetitions: text box with value 10.
- SNMPv3 USM security:**
 - User security name: text box.
 - Security level: text box.
 - Buttons: Load user profile..., Edit user...
- SNMPv3 TSM security:**
 - Certificate: text box.
 - Private key: text box.
 - CA certificate: text box.
 - Button: Edit...

At the bottom are **OK** and **Cancel** buttons.

Note: The SNMP Protocol Preferences dialog box can be opened from almost any MIB Browser window by using the **SNMP Protocol Preferences** (hammer) toolbar button.

Figure 30: SNMP Protocol Preferences dialog box

3. You can choose between using the SNMPv1, SNMPv2c or SNMPv3 protocol version by selecting the appropriate radio button in the SNMP Protocol Preferences dialog box.
4. Depending on the version of SNMP protocol you wish to use, read one of the following sections [Using SNMPv1 Protocol](#), [Using SNMPv2c Protocol](#), [Using SNMPv3 USM](#) or [Using SNMPv3 TSM \(TLS/DTLS\)](#) and learn how to specify the parameters.

6.1 Using SNMPv1 Protocol

To use the SNMPv1 protocol, specify the following parameters in the SNMP Protocol Preferences dialog box:

1. First click the **SNMPv1** radio button in the SNMP Protocol Version frame ([Figure 31](#)).

The image shows the 'SNMP Protocol Preferences' dialog box. At the top, under 'SNMP protocol version', the 'SNMPv1' radio button is selected. The dialog is divided into several sections:

- General:** Contains 'Read community' (set to 'public'), 'Set community' (set to 'private'), 'Timeout [s]' (5), 'Retransmits' (4), 'Transport' (UDP), and 'Port number' (161).
- Get-Bulk settings:** Includes a checked 'Use Get-Bulk' checkbox, 'Non repeaters' (0), and 'Max repetitions' (10).
- SNMPv3 USM security:** Includes 'User security name' and 'Security level' text boxes, and 'Load user profile...' and 'Edit user...' buttons.
- SNMPv3 TSM security:** Includes 'Certificate', 'Private key', and 'CA certificate' text boxes, and an 'Edit...' button.

 At the bottom right are 'OK' and 'Cancel' buttons.

Figure 31: Specifying SNMPv1 protocol preferences

2. In the **Read community** drop-down list in the General frame, specify the Read community string (e.g., public). This parameter is used only with SNMP Get and SNMP GetNext requests.
3. In the **Set community** drop-down list, specify the Set community string (e.g., private). This parameter is used only with SNMP Set requests.

4. Into the **Timeout [s]** input line, enter the timeout value in seconds for pending SNMP requests.

The **Timeout** value defines how many seconds the program waits for the SNMP agent to respond to the request. When this time is over, the program, depending on the value of the **Retransmits** parameter, cancels or repeats the query.

5. When using SNMP over UDP, enter the number of retransmits for pending SNMP requests into the **Retransmits** input line. Note that this input line is disabled when using SNMP over TCP, because the underlying TCP protocol ensures reliable data delivery, automatically taking care of packets retransmission when required.

The **Retransmits** value defines how many times the program repeats the query after the first timeout.

6. In the **Transport** drop-down list, select one of the following:
 - ☐ To use **SNMPv1 over UDP** transport protocol (=standard), select the **UDP** entry,
 - ☐ To use **SNMPv1 over TCP** transport protocol, select the **TCP** entry.
7. In the **Port number** drop-down list, specify the port number to which the remote SNMP agent listens. The default UDP and TCP port number of an SNMP agent is **161**.
8. To save the current settings in the SNMP Protocol Preferences dialog box and the agent address specified in the **Remote SNMP agent** drop-down list in the main window as an SNMP agent profile, check the **Add to agent profiles** checkbox.
9. Click the **OK** button to close the SNMP Protocol Preferences dialog box and apply the changes.

6.2 Using SNMPv2c Protocol

To use the SNMPv2c protocol, specify the following parameters in the SNMP Protocol Preferences dialog box:

1. Click the **SNMPv2c** radio button in the SNMP Protocol Version frame ([Figure 32](#)).

The dialog box is titled "SNMP Protocol Preferences" and contains the following sections:

- SNMP protocol version:** Radio buttons for SNMPv1, **SNMPv2c** (selected), SNMPv3 USM, and SNMPv3 TSM.
- General:**
 - Read community: dropdown menu with "public" selected.
 - Set community: dropdown menu with "private" selected.
 - Timeout [s]: input field with "5".
 - Retransmits: input field with "4".
 - Transport: dropdown menu with "UDP" selected.
 - Port number: dropdown menu with "161" selected.
- Get-Bulk settings:**
 - Use Get-Bulk: checked checkbox.
 - Non repeaters: input field with "0".
 - Max repetitions: input field with "10".
- SNMPv3 USM security:**
 - User security name: empty text field.
 - Security level: empty text field.
 - Buttons: "Load user profile..." and "Edit user..."
- SNMPv3 TSM security:**
 - Certificate: empty text field.
 - Private key: empty text field.
 - CA certificate: empty text field.
 - Button: "Edit..."
- Buttons:** "OK" and "Cancel" at the bottom right.

Figure 32: Specifying SNMPv2c protocol preferences

2. In the **Read community** drop-down list in the General frame, specify the Read community string (e.g., `public`). This parameter is used only with SNMP Get, SNMP GetNext and SNMP GetBulk requests.
3. In the **Set community** drop-down list, specify the Set community string (e.g., `private`). This parameter is used only with SNMP Set requests.
4. Into the **Timeout [s]** input line, enter the **timeout** value for pending SNMP requests.

The **Timeout** value defines how many seconds the program waits for the SNMP agent to respond to the request. When this time is over, the program, depending on the value of the Retransmits parameter, cancels or repeats the query.

5. Into the **Retransmits** input line, enter the number of **retransmits** for pending SNMP requests. Note that this input line is disabled when using SNMP over TCP, because the underlying TCP protocol ensures reliable data delivery, automatically taking care of packets retransmission when required.

The **Retransmits** value defines how many times the program repeats the query after the first timeout.

6. In the **Transport** drop-down list, select one of the following:
 - ☐ To use **SNMPv2c over UDP** transport protocol (=standard), select the **UDP** entry,
 - ☐ To use **SNMPv2c over TCP** transport protocol, select the **TCP** entry.
7. In the **Port number** drop-down list, specify the port number, which the remote SNMP agent listens to (e.g., 161).
8. If you want to use the SNMP GetBulk operation when querying SNMP agents, check the **Use Get-Bulk** checkbox ([Figure 32](#)).
9. Into the **Non repeaters** input line, enter the number of non-repeaters and into the **Max repetitions** input line, the maximum number of returned instances in the SNMP GetBulk packet.

The **Non-repeaters** value is the number of variable bindings, counted from the beginning of the list of variable bindings (e.g., in the Multiple Variable Bindings window), for which **only one** instance is returned in the Response to the SNMP GetBulk packet.

The **Max-repetitions** value is the maximum number of instances that are in lexicographical order returned for each variable binding remaining in the list. 'Variable bindings remaining in the list' are in this case variable bindings that do not fall into the category of Non-repeaters and for which more than one instance is returned (the maximum number of returned instances is defined with the Max-repetitions value).

For illustration see the usage [example](#).

Note: When you use the SNMP GetBulk operation in the main window, the 'non-repeaters' value has to be set to zero (0). Otherwise the program returns only one instance regardless of the 'max-repetitions' value.

10. To save the current settings in the SNMP Protocol Preferences dialog box and the agent address specified in the **Remote SNMP agent** drop-down list in the main window as an SNMP agent profile, check the **Add to agent profiles** checkbox.
11. Click the **OK** button to close the SNMP Protocol Preferences dialog box and apply the changes. If the **Add to agent profiles** checkbox was checked, a new SNMP agent profile, named "New - <agent address>", is created in the [SNMP Agent Profiles window](#).

Example:

How to correctly specify the 'non-repeaters' and 'max-repetitions' parameters and use the SNMP GetBulk operation to return multiple instances of objects?

The SNMP GetBulk operation is an optimization of the SNMP GetNext operation that allows SNMP agents to return large packets in response to GetBulk requests. SNMP GetBulk packets have two fields in request PDU, the **non-repeaters** and the **max-repetitions** fields, which are not found in any other SNMP PDU (Get, GetNext, Set). In MIB Browser, you can specify the number of **non-repeaters** and **max-repetitions** in the SNMP Protocol Preferences dialog box (**View / SNMP Protocol Preferences** command) after checking the **Use Get-Bulk** checkbox ([Figure 32](#)).

SNMP GetBulk operation in MIB Browser's main window:

To perform the SNMP GetBulk operation in the main window, you have to set the 'non-repeaters' value in the SNMP Protocol Preferences dialog box to zero (0). Otherwise the program returns only one object instance with its value because the use of non-repeaters makes sense only with multiple variable binding PDUs. You can set the 'max-repetitions' parameter to any value in order to determine the maximum number of object instances returned in one SNMP GetBulk packet. If you, for example, set it to 8, the program will return eight instances with corresponding values that in lexicographical order follow the instance of the object selected in the MIB tree.

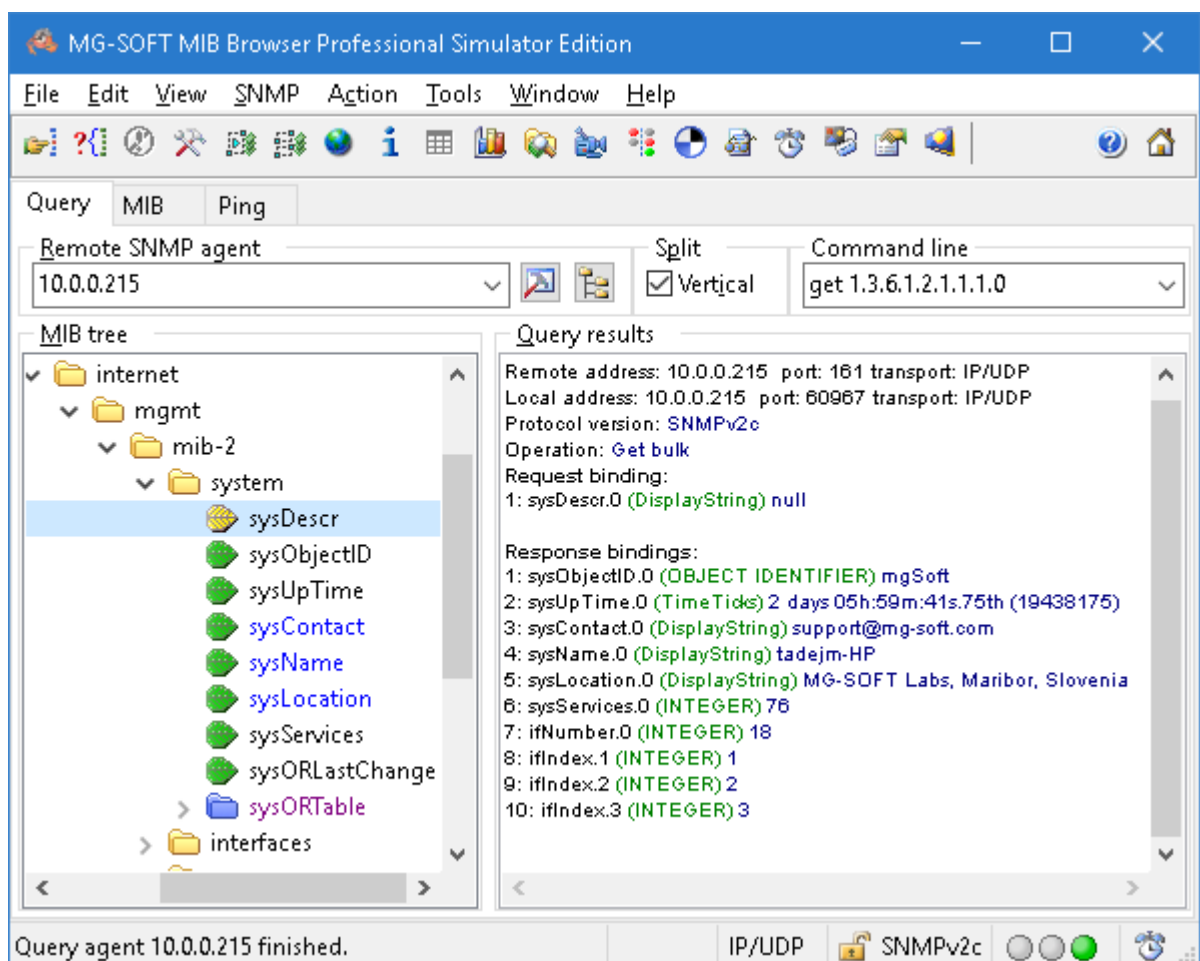


Figure 33: Multiple object instances with corresponding values returned in SNMP GetBulk packet

To perform the SNMP Get Bulk operation in the main window, click a node in the MIB tree (e.g., `sysDescr`) from which you wish to perform the SNMP Walk operation. When you have selected the node, use the **SNMP / Get Bulk** command. MIB Browser will perform the SNMP Walk operation from the selected node and in lexicographical order return the specified number (defined with 'max-repetitions') of object instances with values (Figure 33).

SNMP GetBulk operation in the Multiple Variable Bindings window:

Using the 'non-repeaters' parameter makes sense only with multiple variable binding PDUs. You can create such PDU by making a list of variable bindings in the Multiple Variable Bindings window (opened with the **SNMP / Multiple Variable Bindings** command).

You can make a list of variable bindings in the MVB window by dragging the objects from the MIB tree displayed in the main window (for instructions see the [Making Multiple Variable Bindings List](#) section). For example, you can make a list of three scalar objects (e.g., from the `system` sub tree) and two columnar objects (e.g., from the `ifTable` table), as shown in [Figure 34](#). In the SNMP Protocol Preferences dialog box, set the 'non-repeaters' parameters to the value that corresponds to the number of scalar objects in the list. Set the value of 'max-repetitions' to the maximum number of instances (e.g., 4) that you wish to retrieve in lexicographical order for the remaining two columnar objects.

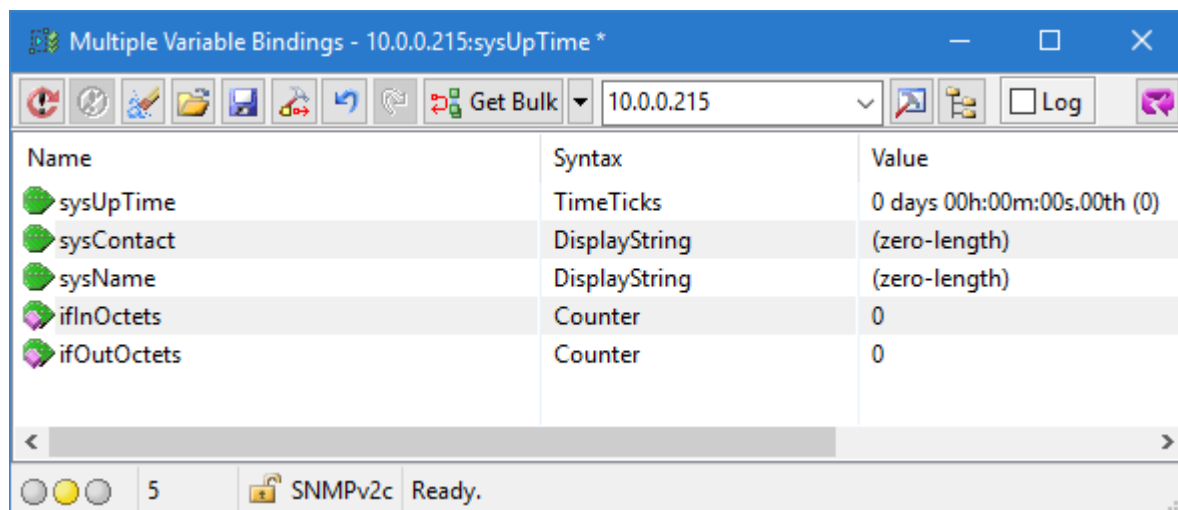


Figure 34: A list of variable bindings in the Multiple Variable Bindings window

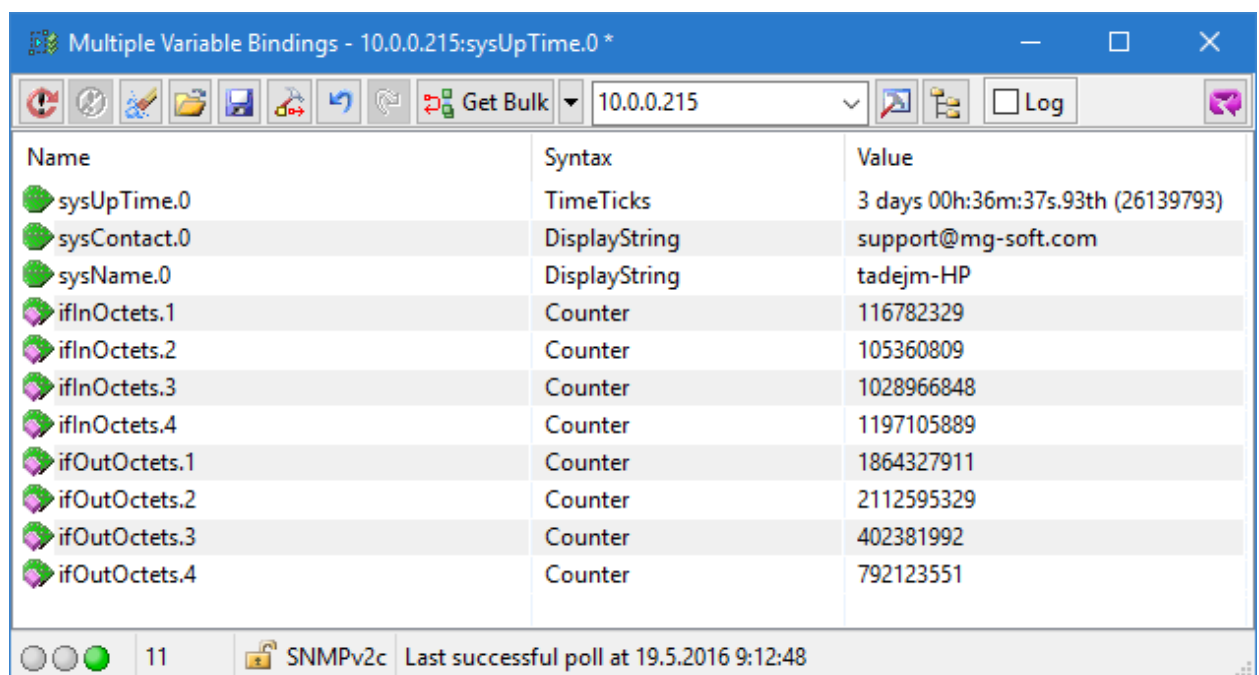
A set of parameters for the SNMP GetBulk operation:

Non-repeaters: 3

Max-repetitions: 4

Number of variable bindings in the list: 5 (3 scalar and 2 columnar objects)

After you have set all parameters, click in the Multiple Variable Bindings window toolbar the arrow next to the programmable button for SNMP operations. Select the **Get Bulk** operation from the list and then click the **Get Bulk** button. MIB Browser sends the SNMP GetBulk request PDU with the list of variable bindings to the SNMP agent. For the first three variable bindings in the list, it retrieves only one object instance with the corresponding value, where as for each of the remaining two variables it returns four object instances with their values ([Figure 35](#)).



Name	Syntax	Value
sysUpTime.0	TimeTicks	3 days 00h:36m:37s.93th (26139793)
sysContact.0	DisplayString	support@mg-soft.com
sysName.0	DisplayString	tadejm-HP
ifInOctets.1	Counter	116782329
ifInOctets.2	Counter	105360809
ifInOctets.3	Counter	1028966848
ifInOctets.4	Counter	1197105889
ifOutOctets.1	Counter	1864327911
ifOutOctets.2	Counter	2112595329
ifOutOctets.3	Counter	402381992
ifOutOctets.4	Counter	792123551

11 SNMPv2c Last successful poll at 19.5.2016 9:12:48

Figure 35: Object instances and their values returned in response to SNMP GetBulk request with multiple variable bindings

6.3 Using SNMPv3 Protocol with User-based Security Model (USM)

To use the SNMPv3 protocol with the standard User-based Security Model (USM), specify the following parameters in the SNMP Protocol Preferences dialog box:

1. Click the **SNMPv3 USM** radio button in the SNMP Protocol version frame (Figure 36).
2. Into the **Timeout [s]** input line, enter the **timeout** value for pending SNMP requests.
3. Into the **Retransmits** input line, enter the number of **retransmits** for pending SNMP requests. Note that this input line is disabled when using SNMP over TCP, because the underlying TCP protocol ensures reliable data delivery, automatically taking care of packets retransmission when required.
4. In the **Transport** drop-down list, select one of the following:
 - ❑ To use **SNMPv3 USM over UDP** transport (=standard), select the **UDP** entry,
 - ❑ To use **SNMPv3 USM over TCP** transport, select the **TCP** entry.
5. In the **Port number** drop-down list, specify the port number (UDP or TCP), which the remote SNMP agent listens to (e.g., 161).
6. Check the **Use Get-Bulk** checkbox and enter the number of **non-repeaters** and the maximum number of returned instances in the SNMP Get Bulk packet (**max-repetitions**).

The image shows the 'SNMP Protocol Preferences' dialog box. At the top, under 'SNMP protocol version', the 'SNMPv3 USM' radio button is selected. The dialog is divided into several sections:

- General:** Contains 'Read community' (set to 'public'), 'Set community' (set to 'private'), 'Timeout [s]' (set to 5), 'Retransmits' (set to 4), 'Transport' (set to 'UDP'), and 'Port number' (set to 161).
- SNMPv3 USM security:** Contains 'User security name' (set to 'SHA_DES_User'), 'Security level' (set to 'Authentication and privacy'), and buttons for 'Load user profile...' and 'Edit user...'.
- SNMPv3 TSM security:** Contains fields for 'Certificate', 'Private key', and 'CA certificate', along with an 'Edit...' button.
- Get-Bulk settings:** Contains a checked 'Use Get-Bulk' checkbox, 'Non repeaters' (set to 0), and 'Max repetitions' (set to 10).

At the bottom right are 'OK' and 'Cancel' buttons.

Figure 36: Specifying SNMPv3 USM protocol preferences

7. The **User security name** and the **Security level** read-only fields in the SNMPv3 Security frame display the user name and security level of the currently selected SNMPv3 USM user profile. The **Edit user** button opens the [SNMPv3 Security Parameters dialog box](#) that lets you edit the current USM user profile.
8. If no SNMPv3 USM user profile is selected, click the **Load user profile** button.
9. The SNMPv3 USM User Profiles window appears ([Figure 37](#)). It displays a list of existing SNMPv3 user profiles configured in MIB Browser and lets you manage them.

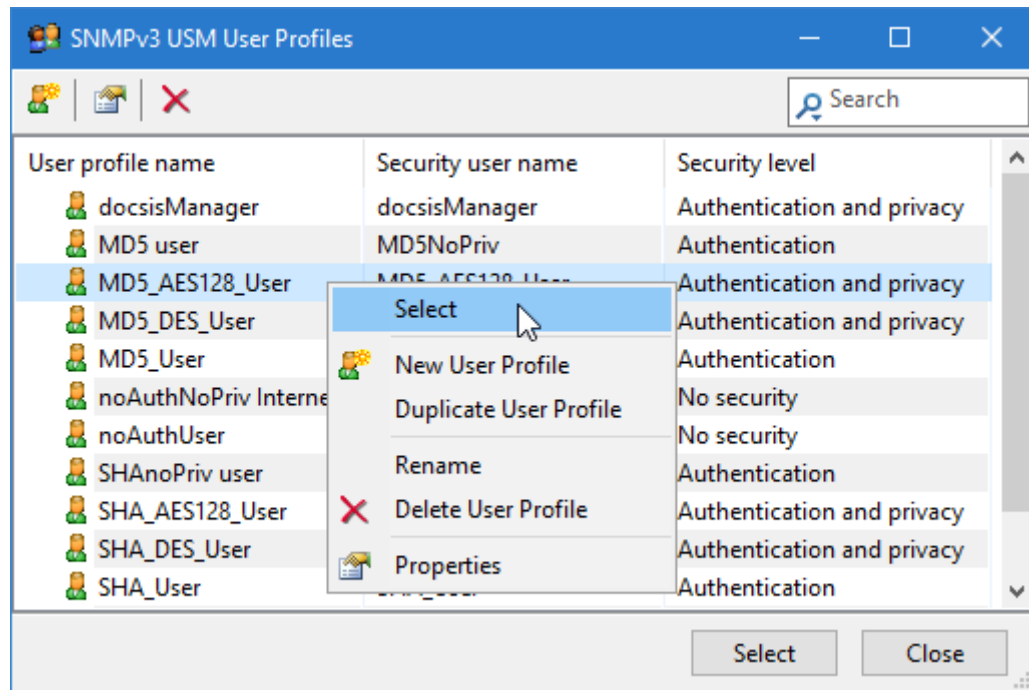


Figure 37: SNMPv3 USM User Profiles window

10. To create a new SNMPv3 USM user profile, proceed as described in the [Creating New SNMPv3 USM User Profile](#) section.
11. To use an existing SNMPv3 USM user profile, select the relevant line in the SNMPv3 USM User Profiles window and click the **Select** button or pop-up command ([Figure 37](#)).
12. The SNMPv3 USM User Profiles window closes and the **User security name** and the **Security level** read-only fields in the SNMP Protocol Preferences dialog box display the user name and security level of the selected SNMPv3 USM user profile ([Figure 36](#)).
13. To save the current settings in the SNMP Protocol Preferences dialog box and the agent address specified in the **Remote SNMP agent** drop-down list in the main window as an SNMP agent profile, check the **Add to agent profiles** checkbox.
14. After you have specified all parameters, click the **OK** button to close the SNMP Protocol Preferences dialog box and apply the changes. If the **Add to agent profiles** checkbox was checked, a new SNMP agent profile, named "New - <agent address>", is created in the [SNMP Agent Profiles window](#).

6.3.1 Creating New SNMPv3 USM User Profile

In this section you will see how to create and configure a new SNMPv3 USM user profile.

1. Open the SNMPv3 USM User Profiles window (Figure 37) by clicking the **Load user profile** button in the SNMP Protocol Preferences dialog box (Figure 36).
2. In the SNMPv3 USM User Profiles window, click the **New User Profile** button or select the **New User Profile** pop-up command.
3. When the SNMPv3 Security Parameters dialog box opens, specify the following parameters.

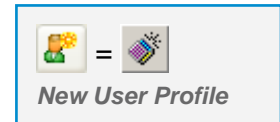

A screenshot of the "SNMPv3 Security Parameters (USM)" dialog box. It has a blue title bar with a close button. The fields are: "User profile name" (Sha512-Aes128 User Profile), "Security user name" (Sha2AesUser), "Context name" (empty), "Context engine ID" (checkbox unchecked, #), "Authentication protocol" (HMAC-SHA2-512), "Privacy protocol" (CFB-AES-128), "Do not localize Authentication and Privacy keys" (checkbox unchecked), "Diffie-Hellman key exchange" (checkbox unchecked), and "Manager Random" (empty). There are "Change Password..." buttons next to the authentication and privacy protocols. At the bottom are "Save to profile...", "OK", and "Cancel" buttons.

Figure 38: Specifying SNMPv3 USM user parameters

4. Into the **User profile name** input line enter a name for the user profile.

Note: The user profile name is only a label name under which you store the SNMPv3 USM user profile and has no effect on the SNMPv3 protocol itself. The User profile name will also appear in the **User profile name** drop-down list in the first column of the SNMPv3 USM User Profiles window .

5. Into the **Security user name** input line, enter a name for the SNMPv3 security user. The Security user name represents the user in a format that is Security Model independent.
6. Into the **Context** input line, enter the SNMPv3 context name.
7. For communicating with an SNMP agent through a proxy, you should check the **Context engine ID** checkbox and specify the SNMPv3 context engine ID. If the checkbox is not checked, the automatically computed Context engine ID is used for that profile.

To overwrite the default Context engine ID, enter a properly formatted binary value by starting the line with the # character and continue with any number of character codes in decimal, octal (prefix 0) or hex (prefix 0x) notation. Here is an example:

Enter any of the following four values into the input line:

```
# 022 064 0357
# 18 52 239
# 0x12 0x34 0xef
# 022 52 0xEF
```

The above four values will all do the same; set the Context engine ID value to 0x1234EF.

8. Select the SNMPv3 USM authentication protocol from the **Authentication protocol** drop-down list. In addition to the standard HMAC-MD5-96 and HMAC-SHA-96 authentication protocols (RFC 3414), MIB Browser supports also the **HMAC-SHA-2** authentication protocols for use with SNMPv3 USM, as specified in [RFC 7860](#). These are HMAC-SHA-2-224, HMAC-SHA-2-256, HMAC-SHA-2-384 and HMAC-SHA-2-512.
9. Click the **Change Password** button next to the **Authentication protocol** drop-down list. This will open the Password For Authentication Protocol dialog box ([Figure 39](#)).

Tip: To see the typing, uncheck the **Hide typing** checkbox.

Figure 39: Password For Authentication/Privacy Protocol dialog box

10. Enter the authentication password into the **Password** input line and then confirm it by re-entering it into the **Password confirmation** input line below.

Tip: For more information about specifying passwords and security keys in MIB Browser, see the [Specifying Password or Security Key](#) section and its subsections.

11. Click the **OK** button. The Password For Authentication Protocol dialog box closes.
12. Select the SNMPv3 USM privacy protocol from the **Privacy Protocol** drop-down list. In addition to the standard CBC-DES (RFC 3414) and CFB-AES-128 (RFC 3826) privacy protocols, MIB Browser supports also the CFB-AES-192, CFB-AES-256 and CBC-3DES privacy protocols, which provide stronger security (encryption).

Note: There is currently no standard for using AES-192, AES-256 and 3DES privacy protocols in SNMPv3 USM. When using these privacy protocols with MD5 and SHA authentication protocols that do not provide long enough output to accommodate the 192- or 256-bit size keys for AES-192 and AES-256 or the 168-bit size key for 3DES, some mechanism needs to be employed to produce localized keys of an adequate size. MG-SOFT MIB Browser uses the key extension

mechanism used by Cisco and some other parties, which is described in the Reeder 3DES Internet draft document (<https://tools.ietf.org/html/draft-reeder-snmpv3-usm-3desede-00>). Note that this mechanism is not employed when using the above privacy protocols with SHA2 authentication protocols that produce the hash output of an adequate size (e.g., SHA2-256, etc.), since no key extension is needed in such case.

13. Click the **Change Password** button next to the **Privacy Protocol** drop-down list.
14. The Password For Privacy Protocol dialog box appears.

Note: The Password For Authentication Protocol dialog box and the Password For Privacy Protocol dialog box have the same appearance.

15. Enter the privacy password into the **Password** input line and then confirm it by re-entering it into the **Password confirmation** input line below. Close the dialog box by clicking the **OK** button.
16. In the SNMPv3 Security Parameters dialog box (Figure 38) you can check the **Do not localize Authentication and Privacy keys** checkbox. In this case MIB Browser will use *non-localized* Authentication and Privacy keys when communicating with remote SNMPv3 agents.

Note: The *Diffie-Hellman key exchange* feature is available only in the **DOCSIS/DH, Developer's**, and **Simulator** editions of MIB Browser. For more information about this feature, check the **Diffie-Hellman Key Exchange for DOCSIS-Based SNMPv3 Agents** section.

17. After you have specified all the parameters, click the **OK** button. The SNMPv3 Security Parameters dialog box closes and a new line representing the newly configured SNMPv3 user profile appears in the SNMPv3 USM User Profiles window (Figure 37).

6.3.2 Specifying Password or Security Key

MIB Browser offers two methods for entering passwords and one method for entering security keys for the SNMPv3 authentication and privacy protocols.

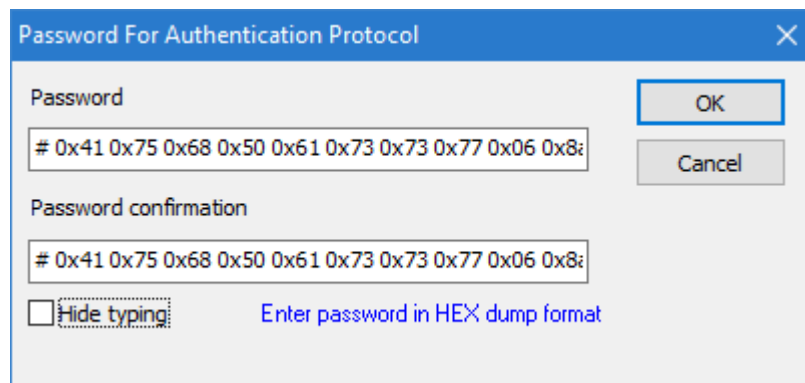
- ❑ If a **Password** is entered, MIB Browser will compute the security key required for the SNMPv3 authentication or privacy protocol from the given password according to the algorithm defined in the *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol* document (RFC 3414).
- ❑ If a **Security key** is entered, MIB Browser does not apply the USM password-to-key algorithm. Instead, if the **Do not localize Authentication or Privacy keys** checkbox on the SNMPv3 Security Parameters dialog box is **not (!)** checked, MIB Browser applies only the key localization algorithm to the entered security key and then uses the localized security key for communicating with the SNMPv3 agent. If that checkbox is checked, MIB Browser uses the security key exactly as it was entered.

Entering the Password in Plain ASCII Text

1. To specify a password, open the Password For Authentication/Privacy Protocol dialog box (Figure 39) from the SNMPv3 Security Parameters dialog box by clicking the **Change Password** button (for Authentication or Privacy protocol).
2. Into the **Password** input line; enter a password, which must be a plain ASCII text (e.g., AuthPassword).
3. The **Enter password in ASCII text** note appears in blue at the bottom of the dialog box (Figure 39). Click the **OK** button.
4. MIB Browser will compute the security key from the given password according to the algorithm defined in the *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol* document (RFC 3414).

Entering the Password in HEX Dump Format

1. In the SNMPv3 Security Parameters dialog box, click the **Change Password** button (for Authentication or Privacy protocol) to open the Password For Authentication/Privacy Protocol dialog box.
2. Into the **Password** input line; enter a hex-dump password. This is achieved by entering the # character at the beginning of the input line and specifying the character codes in hex (each preceded with 0x). This method allows entering passwords that contain non-printable characters. (E.g., for AuthPassword passphrase the input would be: # 0x41 0x75 0x74 0x68 0x50 0x61 0x73 0x73 0x77 0x6f 0x72 0x64).



Tip: To see the typing, uncheck the **Hide typing** checkbox.

Figure 40: Entering password in HEX dump format

3. The **Enter password in HEX dump format** note appears in blue at the bottom of the dialog box (Figure 40). Click the **OK** button.
4. MIB Browser will compute the security key from the given password according to the algorithm defined in the *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol* document (RFC 3414).

Entering the Security Key

1. To enable this feature, first open the MIB Browser Preferences dialog box (**View / MIB Browser Preferences**) and choose the **General / Other** preferences. Then in

the displayed MIB Browser Preferences panel, check the **Enable auth/privacy binary key editing** checkbox. Click the **OK** button.

2. MIB Browser shows the **Edit Key** button in the Password For Authentication/Privacy Protocol dialog box.

Note: If the **Enable auth/privacy binary key editing** checkbox in the MIB Browser Preferences dialog box is not checked, the **Edit Key** button is not shown in the Password For Authentication/Privacy Protocol dialog box.

3. Open the Password For Authentication/Privacy Protocol dialog box (click the **Change Password** button in the SNMPv3 Security Parameters dialog box) and click the **Edit Key** button.
4. The Binary Key For Authentication/Privacy Protocol dialog box appears (Figure 41).

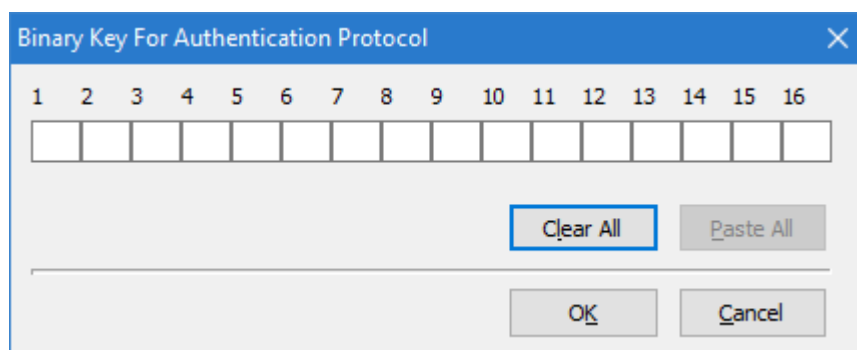


Figure 41: Binary Key For Privacy Protocol dialog box

5. The Binary Key For Authentication/Privacy Protocol dialog box displays a number of input fields, one for each byte (octet) of the security key. The actual number of input fields shown depends on the selected authentication protocol (e.g., 16 for MD5, 20 for SHA, 28 for SHA2-224, etc.).
6. Enter the security key by specifying the octet values in hex in provided input fields.
7. Click the **OK** button to close the Binary Key For Authentication/Privacy Protocol dialog box.
8. The **Entered is binary key** note appears in blue at the bottom of the Password For Authentication/Privacy Protocol dialog box.

Note: If the **Do not localize Authentication or Privacy keys** checkbox in the SNMPv3 Security Parameters dialog box is checked, MIB Browser will not (!) compute the security key from the given input. MIB Browser will communicate with the agent with the security key as it was entered.

If the **Do not localize Authentication or Privacy keys** checkbox in the SNMPv3 Security Parameters dialog box is **not** checked, MIB Browser applies the security key localization algorithm to the entered security key and then uses the localized security key for communication with the SNMPv3 agent.

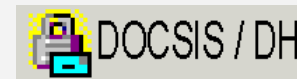
For more details, check the *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol* specification (RFC 3414).

6.3.3 Diffie-Hellman Key Exchange for DOCSIS-Based SNMPv3 Agents

The **DOCSIS/DH**, **Developer's**, and **Simulator Edition** of MG-SOFT MIB Browser support the Diffie-Hellman key exchange mechanism, that lets you successfully contact and manage DOCSIS-based SNMPv3 agents implementing the Diffie-Hellman key exchange method (e.g., cable modems, CMTS, etc.).

To use the Diffie-Hellman method for key exchange between MIB Browser and an SNMP agent:

1. Open the SNMP Protocol Preferences dialog box (**View / SNMP Protocol Preferences** command) and click the **Edit User** button to edit settings of the currently selected SNMPv3 USM user profile. Alternatively, click the **Load user profile** button to open the SNMPv3 USM User Profiles window, select an SNMPv3 USM user profile and use the **Properties** pop-up command to edit the user profile settings. The SNMPv3 Security Parameters dialog box opens (Figure 42).
2. In the displayed SNMPv3 Security Parameters dialog box, specify all security parameters (see the [Creating New SNMPv3 USM User Profile](#) section), except the passwords for authentication and privacy protocols.



Note: This feature is available only in **DOCSIS/DH**, **Developer's**, and **Simulator** editions of **MG-SOFT MIB Browser**.

The dialog box titled "SNMPv3 Security Parameters (USM)" contains the following fields and controls:

- User profile name:** docsisManager profile
- Security user name:** docsisManager
- Context name:** (empty text box)
- Context engine ID:** ☐ #
- Authentication protocol:** HMAC-MD5 (dropdown menu)
- Privacy protocol:** CBC-DES (dropdown menu)
- Change Password...** buttons for both authentication and privacy protocols.
- Do not localize Authentication and Privacy keys:** ☒
- Diffie-Hellman key exchange:** ☒
- Manager Random:** # 0x22 0xE8 0xEF 0xA2 0xA9 0xA9 0x42 0xF1 0x78 0x38 0x
- Buttons:** Save to profile..., OK, Cancel

Figure 42: Diffie-Hellman key exchange settings

3. Check the **Diffie-Hellman key exchange** checkbox to enable the Diffie-Hellman key exchange feature (Figure 42).
4. Into the **Manager Random** input line, enter the manager's random number in hexadecimal (0x prefix) notation starting with #.

Tip: MIB Browser implements the Diffie-Hellman key generator, a utility for generating the manager random and public key pairs that can be used for performing the Diffie-Hellman key

ignition operation. This utility can be accessed by selecting the **Tools / Diffie-Hellman Key Generator** command.

5. Make sure that the ***Do not localize Authentication and Privacy keys*** checkbox is checked.
6. Click the **OK** button to close the SNMPv3 Security Parameters dialog box. MIB Browser and the selected SNMP agent perform the Diffie-Hellman key ignition operation.

Note: If the ***Diffie-Hellman key exchange*** checkbox is checked, the Diffie-Hellman key ignition is performed when you contact an SNMP agent for the first time.

6.4 Using SNMPv3 Protocol with Transport Security Model (TSM)

In addition to the standard User-based Security Model (USM), MG-SOFT MIB Browser supports also the Transport Security Model (TSM) for SNMP, as defined in [RFC 5591](#).

The Transport Security Model enables using new transport models for SNMP that employ lower-layer, secure transports (such as TLS and DTLS) and commonly deployed security infrastructures (e.g., X.509 public key infrastructure). In particular, MIB Browser supports the Transport Layer Security Transport Model (TLSTM) that enables conveying SNMPv3 messages over TLS and DTLS protocols. These are in turn passed over TCP and UDP, respectively. SNMP over TLS and DTLS is commonly referred to as "SNMP over (D)TLS" and specified in [RFC 6353](#). (D)TLS provides authentication, message data integrity, and privacy at the transport layer and is used to establish a secure "tunnel" between two SNMP entities, over which SNMP messages are exchanged.

This section explains how to configure SNMPv3 TSM settings in MIB Browser for using [SNMPv3 over TLS over TCP](#) and [SNMPv3 over DTLS over UDP](#).

This document uses the traditional SNMP network management terms of "manager" and "agent", which correspond to (D)TLS terms of "client" and "server", where client actively opens the connection and sends requests to the server and the server passively listens for incoming connections and responds to the client's requests.

6.4.1 Using SNMPv3 over TLS

To use the **SNMPv3 over TLS over TCP**, specify the following parameters in the SNMP Protocol Preferences dialog box:

1. Click the **SNMPv3 TSM** radio button in the SNMP Protocol Version frame ([Figure 43](#)).
2. Into the **Timeout [s]** input line, enter the [timeout](#) value for pending SNMP requests.
3. From the **Transport** drop-down list, select the **TLS (TCP)** transport protocol to enable SNMP over Transport Layer Security (TLS) over Transmission Control Protocol (TCP).
4. In the **Port number** drop-down list, specify the TCP port number, which the remote SNMP agent listens to for incoming SNMP over TLS requests (e.g., **10161**).
5. To use the SNMP GetBulk operation when querying the SNMP agent, check the **Use Get-Bulk** checkbox ([Figure 43](#)).
6. Into the **Non repeaters** input line, enter the number of non-repeaters and into the **Max repetitions** input line, the maximum number of returned instances in the SNMP GetBulk packet.
7. The **Certificate**, **Private key** and **CA certificate** read-only fields in the **SNMPv3 TSM security** frame display the name of the manager certificate file, manager private key file and the name of the **CA certificate** file of the currently specified SNMPv3 TSM settings (if any).

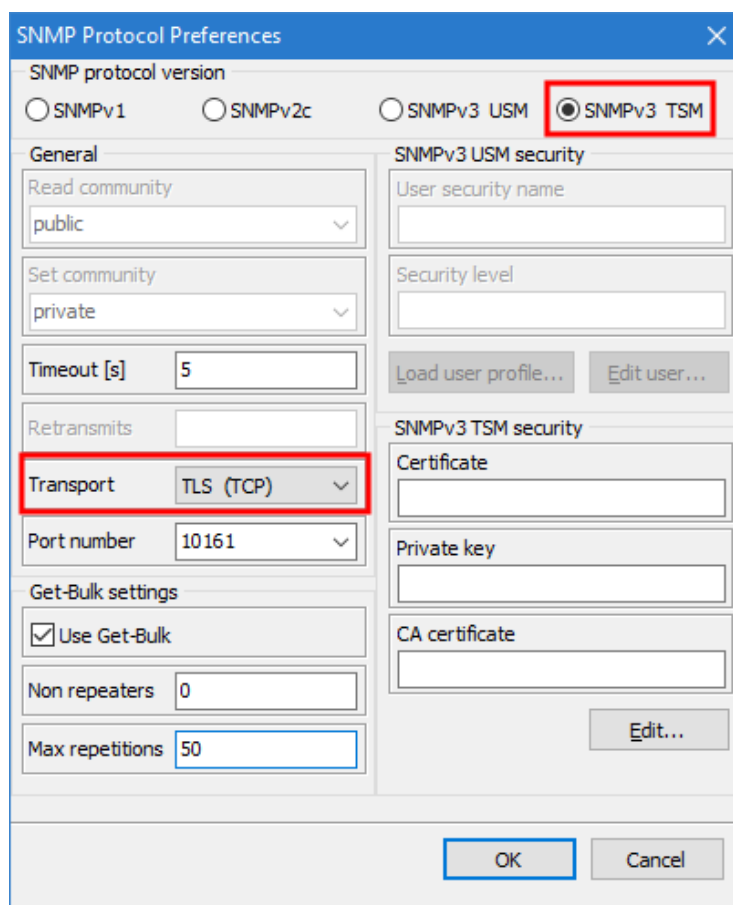


Figure 43: Selecting the SNMPv3 TSM protocol

- Click the **Edit** button below the **SNMPv3 TSM security** frame to open the SNMPv3 Security Parameters (TSM) dialog box (Figure 44).

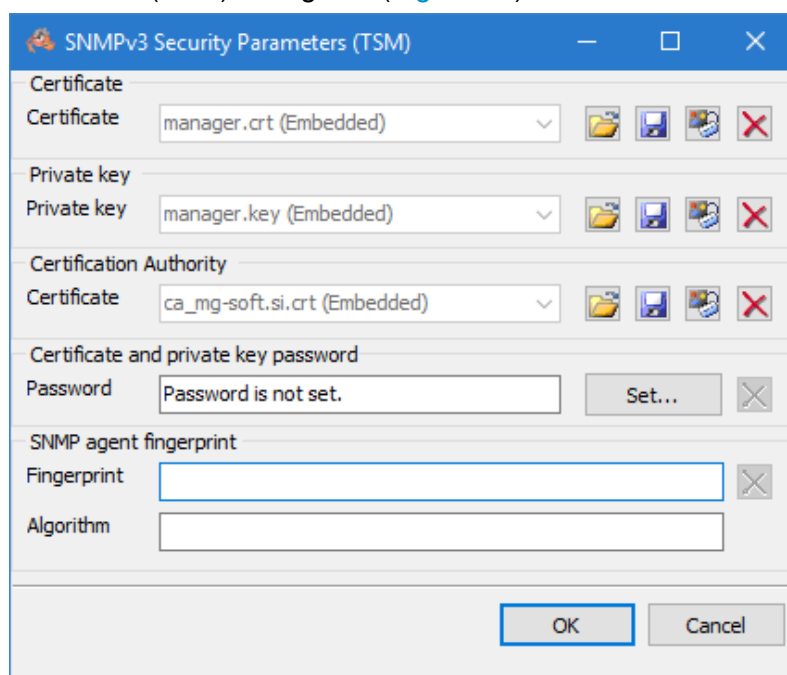



Figure 44: Specifying the SNMPv3 TSM security parameters

9. Click the **Load** button () next to the **Certificate** input line to open the standard Open dialog box and select the X.509 digital certificate file in PEM format, containing the **manager (client) public key** (Figure 45).
10. After selecting the manager certificate file (e.g., .crt or .pem) on disk, click the **Open** button to load the certificate into MIB Browser.

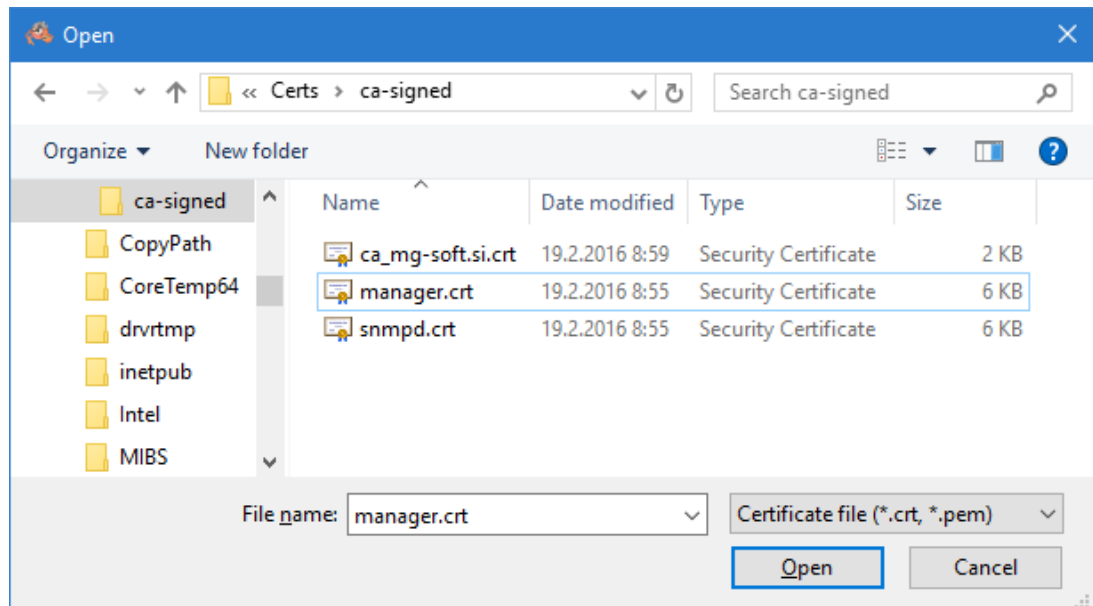





Figure 45: Loading the manager X.509 digital certificate for SNMPv3 over (D)TLS

11. In the **Private key** frame, click the **Load** button () to open the standard Open dialog box and select the file containing the **manager private key** in PEM format (e.g., .key or .pem) from disk.

Tip: Click the Properties button () next to the **Certificate** or **Private key** input line to view full details of the loaded digital certificate or private key, respectively.

12. In the **Certification Authority** frame, click the **Load** button () to open the standard Open dialog box and select the X.509 digital certificate file (in PEM format), containing the **CA authority public key**. This certificate will be used for verifying the agent (server) certificate. If the agent uses a self-signed certificate, leave this input line empty.
13. To enter the password for decrypting the manager private key (if encrypted), click the **Set** button in the **Private key password** frame, and enter the corresponding password twice into the dialog box that appears.
14. The **Fingerprint** and **Algorithm** are two read-only text fields that get automatically populated after establishing a TLS connection with the agent and accepting its certificate (when no CA certificate is provided). Fingerprint is a cryptographic hash of the agent certificate in hex. (unique identification of the certificate) and algorithm is the name of algorithm used for producing the fingerprint (e.g., sha1, md5, sha256, etc.).

15. After you have specified all the parameters, click the **OK** button to close the SNMPv3 Security Parameters (TSM) dialog box. The specified certificate(s) and private key appear read-only in the respective fields in the SNMP Protocol Parameters dialog box (Figure 46).

The image shows the 'SNMP Protocol Preferences' dialog box. At the top, 'SNMP protocol version' has four radio buttons: 'SNMPv1', 'SNMPv2c', 'SNMPv3 USM', and 'SNMPv3 TSM' (which is selected). The dialog is divided into two main sections. The left section, titled 'General', contains fields for 'Read community' (set to 'public'), 'Set community' (set to 'private'), 'Timeout [s]' (set to '5'), 'Retransmits' (empty), 'Transport' (set to 'TLS (TCP)'), 'Port number' (set to '10161'), 'Get-Bulk settings' with a checked 'Use Get-Bulk' checkbox, 'Non repeaters' (set to '0'), and 'Max repetitions' (set to '50'). The right section, titled 'SNMPv3 TSM security', contains fields for 'User security name' (empty), 'Security level' (empty), 'Certificate' (set to 'manager.crt (Embedded)'), 'Private key' (set to 'manager.key (Embedded)'), and 'CA certificate' (set to 'ca_mg-soft.si.crt (Embedded)'). There are buttons for 'Load user profile...', 'Edit user...', and 'Edit...' (next to the CA certificate). At the bottom right are 'OK' and 'Cancel' buttons.

Figure 46: SNMP Protocol Preferences - SNMPv3 TSM settings (SNMPv3 over TLS/TCP)

16. Click the **OK** button to close the SNMP Protocol Parameters dialog box. This will establish an SNMPv3 over TLS/TCP session with the agent and perform the **Contact** operation - retrieve an object instance value from it (Figure 47).

Note 1: If you have not specified the CA certificate for validating the agent certificate, MIB Browser displays a dialog box asking if you wish to accept the agent's certificate (fingerprint) presented during the (D)TLS handshake while establishing a (D)TLS session with a particular SNMP agent (server) for the first time. If you (permanently or temporarily) accept the server certificate, MIB Browser saves the certificate fingerprint (so no prompting occurs in future sessions with the agent), establishes a (D)TLS session and performs the Contact operation. In case you choose the option to reject the certificate (fingerprint), the (D)TLS session is aborted and the Contact operation is not performed.

Note 2: You can view and delete saved fingerprints in the MIB Browser Preferences dialog box (View / MIB Browser Preferences), in the Agent Profiles/Fingerprints view.

The green lock symbol in the status bar (🔒) indicates a secure SNMPv3 over (D)TLS communication.

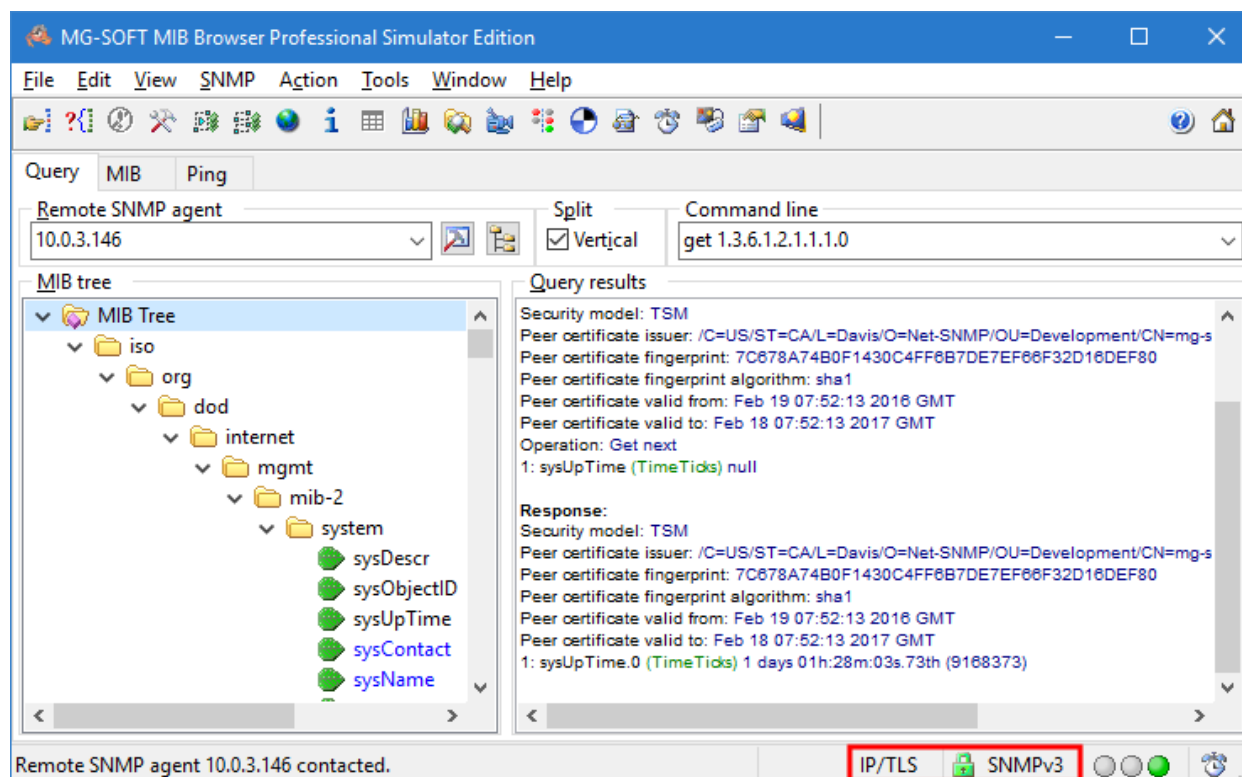


Figure 47: Example of a successful *Contact* operation using *SNMPv3 over TLS/TCP*

- After successfully contacting the agent, you can use the **SNMPv3 over TLS** session to perform any other operation (e.g., Get, GetNext, Set, Walk, etc.) against the agent, as described in other sections of this document.

6.4.2 Using SNMPv3 over DTLS

MG-SOFT MIB Browser supports SNMPv3 over Datagram Transport Layer Security (DTLS) over User Datagram Protocol (UDP).



To use the **SNMPv3 over DTLS over UDP**, specify the following parameters in the SNMP Protocol Preferences dialog box:


- Click the **SNMPv3 TSM** radio button in the SNMP Protocol Version frame (Figure 48).


The image shows the 'SNMP Protocol Preferences' dialog box. At the top, under 'SNMP protocol version', the 'SNMPv3 TSM' radio button is selected and highlighted with a red rectangle. The dialog is divided into two main sections. The left section, titled 'General', contains fields for 'Read community' (set to 'public'), 'Set community' (set to 'private'), 'Timeout [s]' (set to 5), 'Retransmits' (set to 4), 'Transport' (a drop-down menu set to 'DTLS (UDP)' and highlighted with a red rectangle), 'Port number' (set to 10161), 'Use Get-Bulk' (checked), 'Non repeaters' (set to 0), and 'Max repetitions' (set to 50). The right section, titled 'SNMPv3 TSM security', contains fields for 'User security name', 'Security level', 'Certificate' (set to 'manager.crt (Embedded)'), 'Private key' (set to 'manager.key (Embedded)'), and 'CA certificate' (set to 'ca_mg-soft.si.crt (Embedded)'). There are buttons for 'Load user profile...', 'Edit user...', and 'Edit...' in the right section. At the bottom are 'OK' and 'Cancel' buttons.

Figure 48: SNMP Protocol Preferences - SNMPv3 TSM settings (SNMPv3 over DTLS/UDP)

2. Into the **Timeout [s]** input line, enter the **timeout** value for pending SNMP requests.
3. Into the **Retransmits** input line, enter the number of **retransmits** for pending SNMP requests.
4. From the **Transport** drop-down list, select the **DTLS (UDP)** protocol to enable SNMP over Datagram Transport Layer Security (DTLS) over UDP.
5. In the **Port number** drop-down list, specify the UDP port number, which the remote SNMP agent listens to for incoming SNMP over DTLS requests (e.g., **10161**).
6. To use the SNMP GetBulk operation when querying the SNMP agent, check the **Use Get-Bulk** checkbox (Figure 48).
7. Into the **Non repeaters** input line, enter the number of non-repeaters and into the **Max repetitions** input line, the maximum number of returned instances in the SNMP GetBulk packet.
8. The **Certificate**, **Private key** and **CA certificate** read-only fields in the **SNMPv3 TSM Security** frame display the name of the manager certificate file, manager private key file and the name of the **CA certificate** file of the currently specified SNMPv3 TSM settings (if any).

9. Click the **Edit** button below the **SNMPv3 TSM Security** frame to open the SNMPv3 Security Parameters (TSM) dialog box (Figure 44).
10. Click the **Load** button () next to the **Certificate** input line to open the standard Open dialog box and select the X.509 digital certificate file in PEM format, containing the manager (client) public key (Figure 45).
11. After selecting the manager certificate file (e.g., .crt or .pem) on disk, click the **Open** button to load the certificate into MIB Browser.
12. In the **Private key** frame, click the **Load** button () to open the standard Open dialog box and select the file containing the manager **private key** in PEM format (e.g., .key or .pem) from disk.

Tip: Click the **Properties** button () next to the **Certificate** or **Private key** input line to view full details of the loaded digital certificate or private key, respectively.

13. In the **Certification Authority** frame, click the **Load** button () to open the standard Open dialog box and select the X.509 digital certificate file (in PEM format), containing the CA authority public key. This certificate will be used for verifying the server certificate. If the server uses a self-signed certificate, leave this input line empty.
14. To enter the password for decrypting the manager private key (if encrypted), click the **Set** button in the **Private key password** frame, and enter the corresponding password twice into the dialog box that appears.
15. The **Fingerprint** and **Algorithm** are read-only text fields that get automatically populated after establishing a TLS connection with the agent and accepting its certificate (when no CA certificate is provided). Fingerprint is a cryptographic hash of the agent certificate in hexadecimal (unique identification of the certificate) and algorithm is the name of algorithm used for producing the fingerprint (e.g., sha1, md5, sha256, etc.).
16. After you have specified all the parameters, click the **OK** button to close the SNMPv3 Security Parameters (TSM) dialog box. The specified certificate(s) and private key appear read-only in the respective fields in the SNMP Protocol Parameters dialog box (Figure 48).
17. Click the **OK** button to close the SNMP Protocol Parameters dialog box. This will establish a SNMPv3 over DTLS/UDP session with the agent and perform the **Contact** operation - retrieve an object instance value from it (Figure 49).

Note 1: If you have not specified the CA certificate for validating the agent certificate, MIB Browser displays a dialog box asking if you wish to accept the agent's certificate (fingerprint) presented during the (D)TLS handshake while establishing a (D)TLS session with a particular SNMP agent (server) for the first time. If you (permanently or temporarily) accept the server certificate, MIB Browser saves the certificate fingerprint (so no prompting occurs in future sessions with the agent), establishes a (D)TLS session and performs the Contact operation. In case you choose the option to reject the certificate (fingerprint), the (D)TLS session is aborted and the Contact operation is not performed.

Note 2: You can view and delete saved fingerprints in the MIB Browser Preferences dialog box (View / MIB Browser Preferences), in the Agent Profiles/Fingerprints view.

The green lock symbol in the status bar (🔒) indicates a secure SNMPv3 over (D)TLS communication.

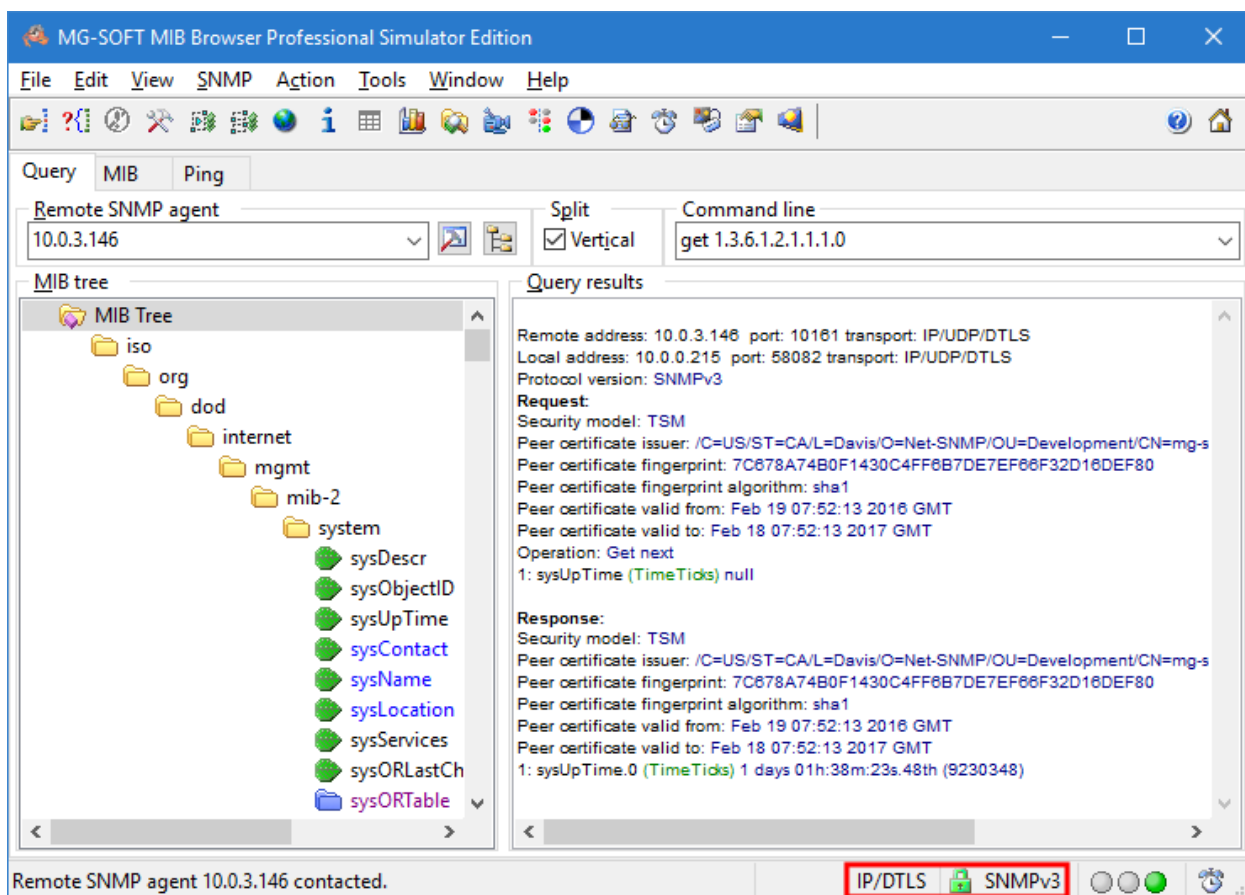


Figure 49: Example of a successful *Contact* operation using *SNMPv3 over DTLS/UDP*

18. After successfully contacting the agent, you can perform any other operation (e.g., Get, GetNext, Set, Walk, etc.) against the agent by using the SNMPv3 over DTLS communication.

7 CONFIGURE AND USE SNMP AGENT PROFILES

In this section, you will learn how to create, configure and use SNMP agent profiles. An SNMP agent profile stores all information required for contacting and managing a particular SNMP agent on the network. Once you configure SNMP agent profiles in MIB Browser, you can contact and query an SNMP agent by simply choosing its profile from the SNMP Agent Profiles window, which is accessible from virtually all other MIB Browser windows that allow retrieving and modifying SNMP variable values. SNMP agent profiles can also be saved to and imported from a file. This way, you can easily transfer the information for accessing SNMP agents from one computer running MIB Browser to another.

By default, the SNMP Agent Profiles window provides also information about the [status of SNMP agents](#) (Up, Down, Error) for which the profiles exist. Namely, when this window is open, MIB Browser polls (in 10 minutes interval) each SNMP agent represented by an agent profile icon (🖨️) and displays its status (e.g.,: 🟢) in the SNMP Agent Profiles window. This way, you can tell at a glance which SNMP agent is currently responding to SNMP queries and which is not.

7.1 Creating New SNMP Agent Profiles

To create and configure a new SNMP agent profile:

1. Select the **View / SNMP Agent Profiles** command or click the **SNMP Agent Profiles** button.
2. The SNMP Agent Profiles window opens ([Figure 50](#)). It contains a hierarchical structure composed of icons representing folders and agent profiles.



Tip: For more information about creating and managing folders, please see the [Organizing SNMP Agent Profiles in Folders](#) section of this manual.

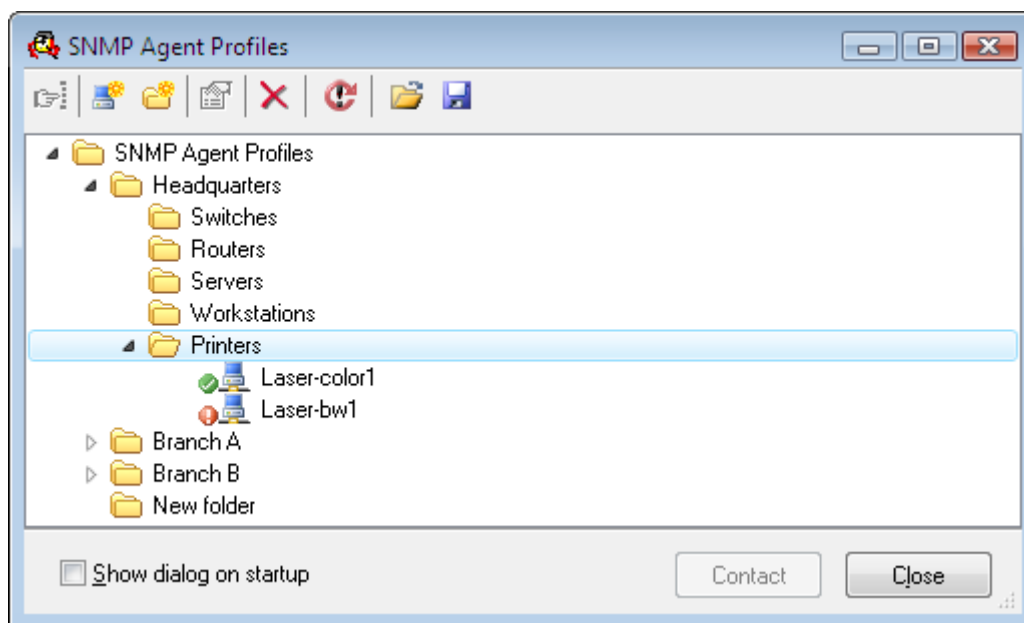


Figure 50: SNMP Agent Profiles window

3. To create a new agent profile in a particular folder, right-click the desired folder icon and choose the **New Agent Profile** pop-up command or click the **New Agent Profile** toolbar button.
4. A new agent profile icon appears under the selected folder icon and you can type in the agent profile name next to the icon (Figure 51).

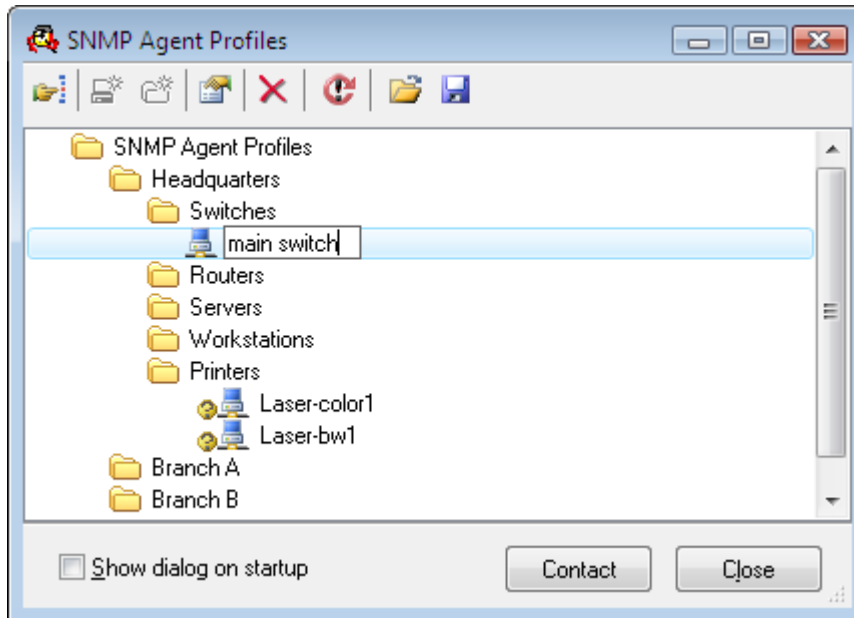


Figure 51: A new SNMP agent profile icon

5. To configure the agent profile properties, select the agent profile icon and choose the **Properties** pop-up command or click the **Properties** toolbar button.

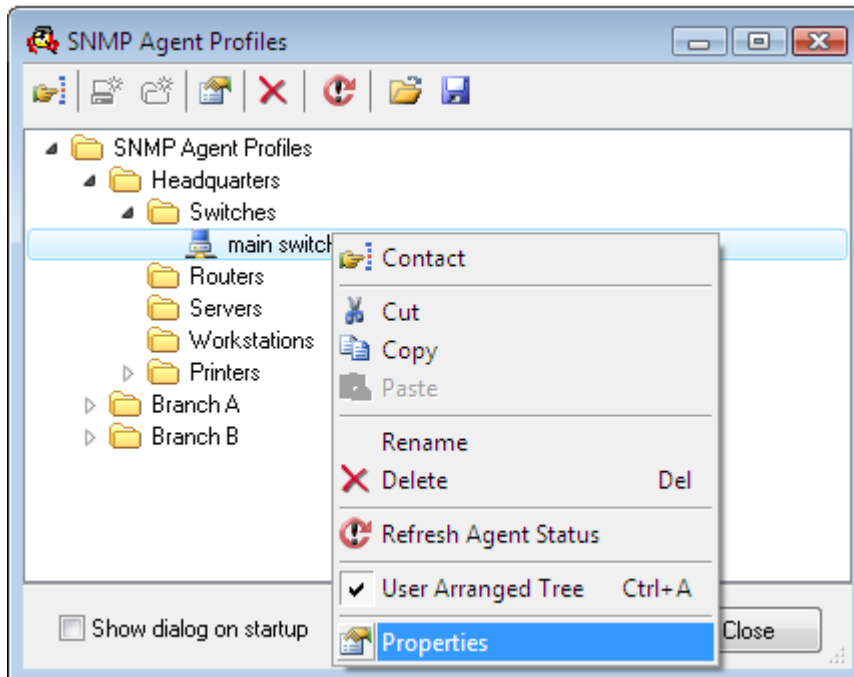


Figure 52: Opening the Agent Profile Properties dialog box

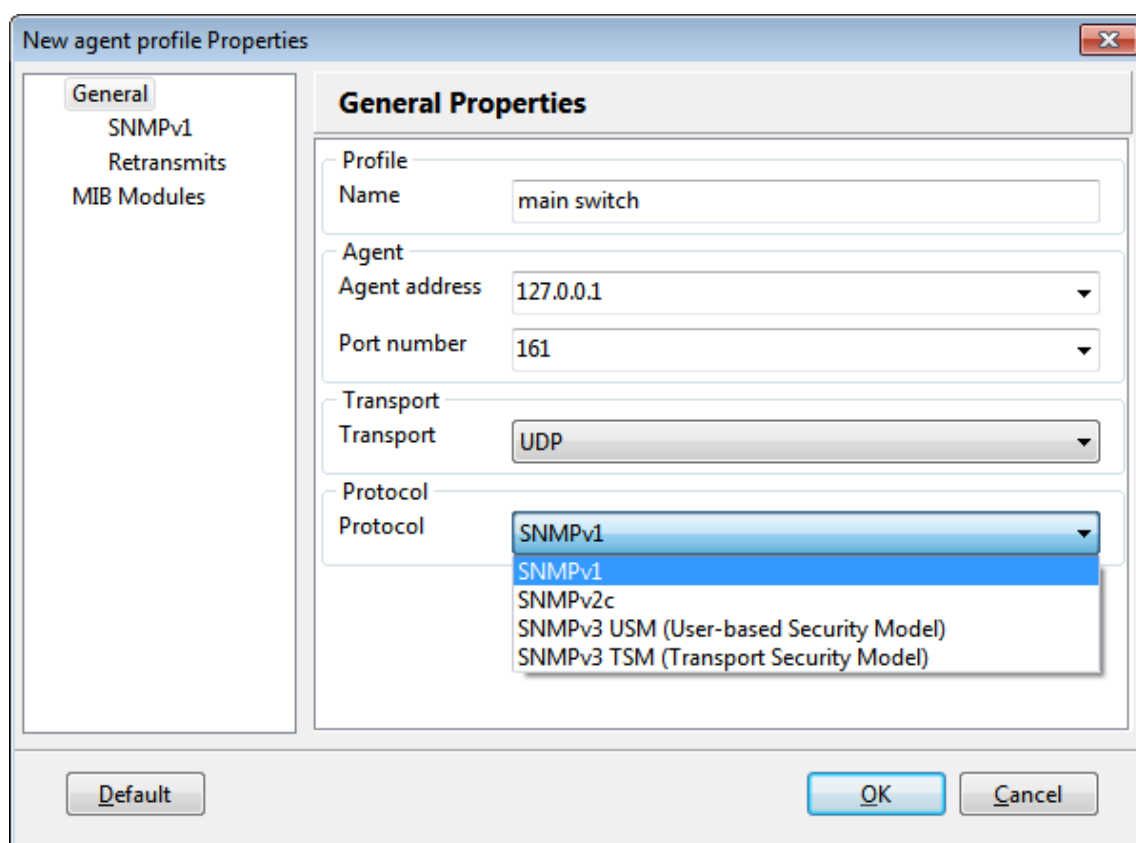


Figure 53: Agent Profile Properties dialog box, General panel

6. The Agent Profile Properties dialog box opens, displaying the **General** panel, where you can configure the basic agent profile properties (Figure 53), like the profile name, agent address and port, transport protocol and SNMP protocol version. Depending on the SNMP protocol version selected, different settings are available in the Agent Profile Properties dialog box. Refer to the respective sections below for using [SNMPv1](#), [SNMPv2c](#), [SNMPv3 USM](#) and [SNMPv3 TSM with \(D\)TLS](#) protocol version.

7.1.1 Using SNMPv1 Protocol

To use the **SNMPv1** protocol, specify the following parameters in the Agent Profile Properties dialog box, **General** panel (Figure 53):

1. Into the **Name** input line, enter the name for the agent profile. This is only a label under which the SNMP agent profile is stored (e.g., a name of the device). This label will be also displayed as the name of the profile in the SNMP Agent Profiles window.
2. In the **Agent Address** drop-down list, specify the [IPv4 or IPv6](#) address of the SNMP agent to be managed.
3. In the **Transport** drop-down list, select one of the following:
 - ❑ To use **SNMP over UDP** transport protocol (=standard), select the **UDP** entry,
 - ❑ To use **SNMP over TCP** transport protocol, select the **TCP** entry.
4. In the **Port Number** drop-down list, specify the port number on which the SNMP agent listens to for incoming SNMP requests (the default port number is **161**).

5. In the **Protocol** drop-down list, select the **SNMPv1** option. The **SNMPv1** entry appears in the navigation tree of the SNMP Agent Profiles window.
6. Click the **SNMPv1** entry in the navigation tree to display the **SNMPv1 Properties** panel (Figure 54).

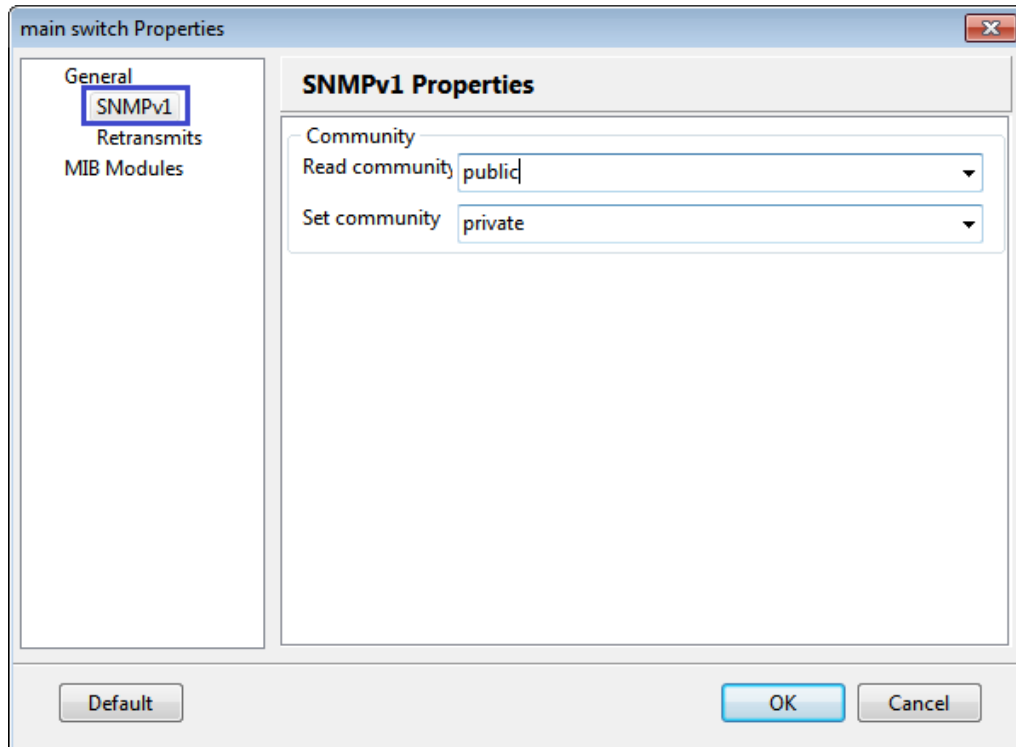


Figure 54: Agent Profile Properties dialog box, SNMPv1 community settings

7. In the **Read community** drop-down list, specify the Read community name (e.g., **public**). This string will be included into all SNMP Get and SNMP GetNext requests sent by MIB Browser to the given SNMP agent.
8. In the **Set community** drop-down list, specify the Set community name (e.g., **private**). This string will be included into all SNMP Set requests sent by MIB Browser to the given SNMP agent.
9. Click the **Retransmits** entry in the navigation tree to display the Timeout and Retransmit Properties panel (Figure 55).

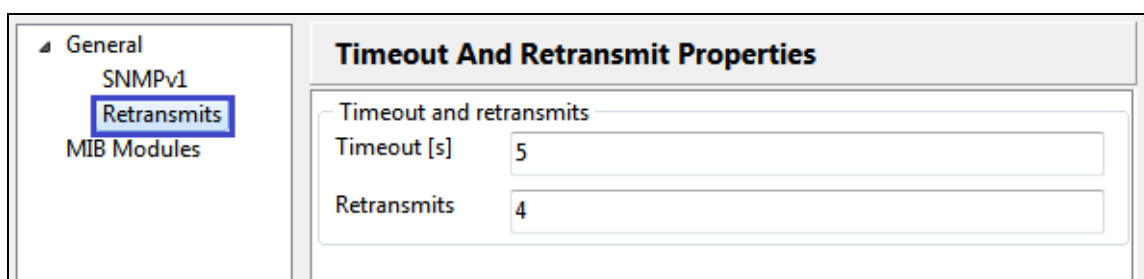


Figure 55: Setting the timeout and retransmit agent profile properties

10. Into the **Timeout [s]** input line, enter the timeout value in seconds for pending SNMP requests.

The **Timeout** value defines how many seconds the program waits for the SNMP agent to respond to the request. When this time is over, the program, depending on the value of the Retransmits parameter, cancels or repeats the query.

11. When using SNMP over UDP, enter the number of retransmits for pending SNMP requests into the **Retransmits** input line. Note that this input line is disabled when using SNMP over TCP, because the underlying TCP protocol ensures reliable data delivery, automatically taking care of packets retransmission when required.

The **Retransmits** value defines how many times the program re-sends the request after the first timeout.

12. To enable automatic loading of specific MIB modules when using the agent profile, refer to the [Automatically Load MIB Modules](#) section.
13. Click the **OK** button to apply all changes and close the Agent Profile Properties dialog box.

7.1.2 Using SNMPv2c Protocol

To use the SNMPv2c protocol, specify the following parameters in the Agent Profile Properties dialog box, **General** panel ([Figure 56](#)):

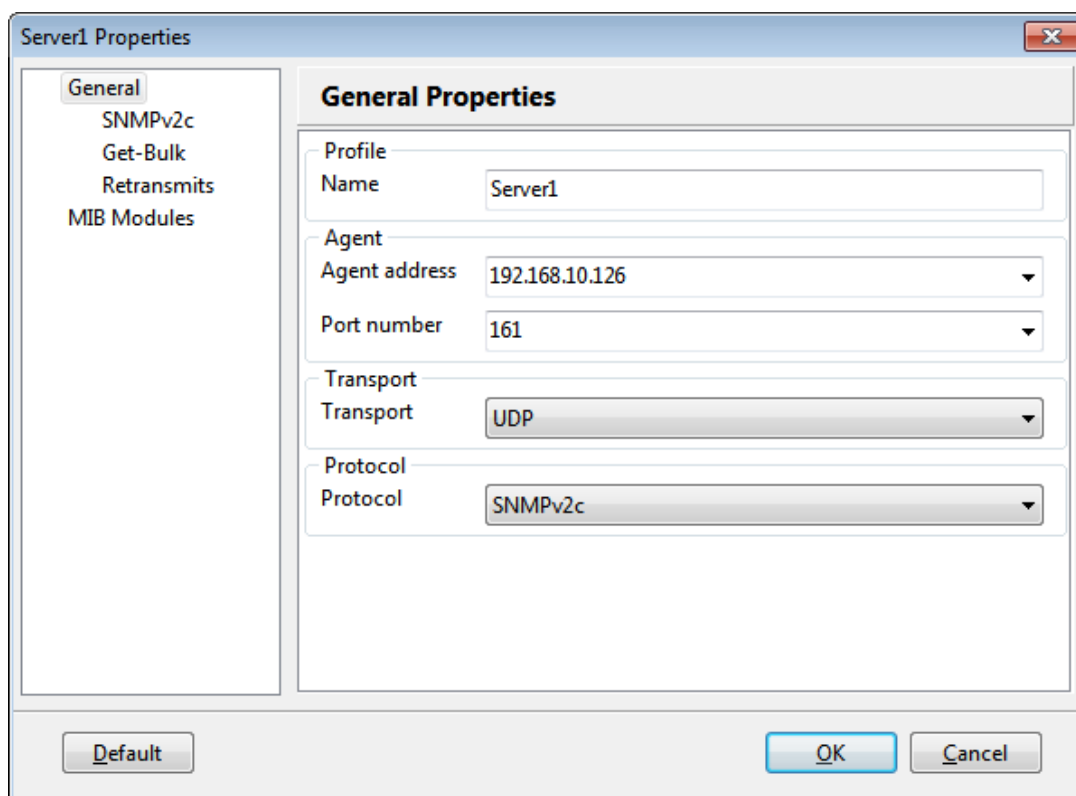


Figure 56: Agent Profile Properties dialog box, SNMPv2c protocol selected

1. Into the **Name** input line, enter the name for the agent profile (e.g., a name of the device). This is only a label under which the SNMP agent profile is stored. This label will be also displayed as the name of the profile in the SNMP Agent Profiles window.
2. In the **Agent Address** drop-down list, specify the **IPv4** or **IPv6** address of the SNMP agent to be managed.
3. In the **Transport** drop-down list, select one of the following:
 - ❑ To use **SNMP over UDP** transport protocol (=standard), select the **UDP** entry,
 - ❑ To use **SNMP over TCP** transport protocol, select the **TCP** entry.
4. In the **Port Number** drop-down list, specify the port number on which the SNMP agent listens to for incoming SNMP requests (the default port number is **161**).
5. In the **Protocol** drop-down list, select the **SNMPv2c** option. The **SNMPv2c** entry appears in the navigation tree of the SNMP Agent Profiles window.
6. Click the **SNMPv2c** entry in the navigation tree to display the SNMPv2c Properties panel (Figure 57).

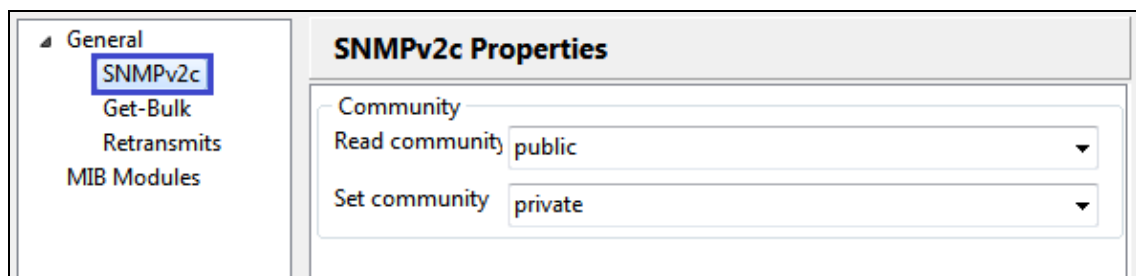


Figure 57: Agent Profile Properties dialog box, SNMPv2c community settings

7. In the **Read community** drop-down list, specify the Read community string (e.g., **public**). This parameter is used with SNMP Get, SNMP GetNext and SNMP GetBulk requests.
8. In the **Set community** drop-down list, specify the Set community string (e.g., **private**). This parameter is used only with SNMP Set requests.
9. Click the **Get-Bulk** entry in the navigation tree to display the Get-Bulk Properties panel (Figure 58).

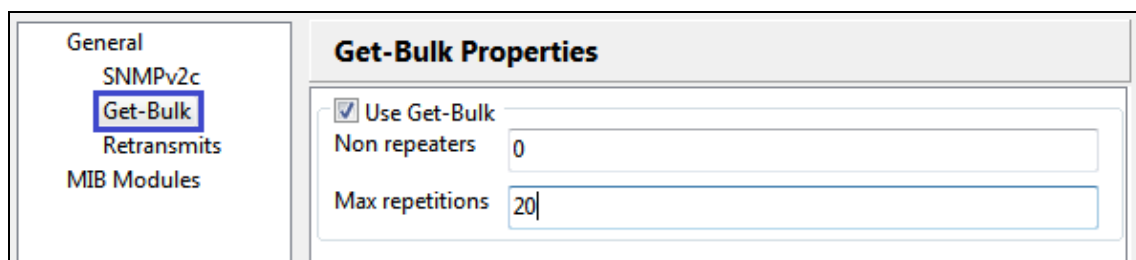


Figure 58: Setting the Get-Bulk agent profile properties

10. To use the SNMP GetBulk operation for querying SNMP agents, check the **Use Get-Bulk** checkbox.
11. Into the **Non repeaters** input line, enter the number of OIDs in the Get-Bulk PDU for which only one instance should be returned and into the **Max repetitions** input line,

the maximum number of object instances for OIDs for which more than one instance should be returned in a Response to the SNMP Get-Bulk request.

The **Non-repeaters** value is the number of variable bindings in the SNMP GetBulk PDU, counted from the beginning of the list of variable bindings, for which **only one** instance is returned.

The **Max-repetitions** value is the maximum number of instances that are in lexicographical order returned for each variable binding remaining in the list. 'Variable bindings remaining in the list' are in this case variable bindings that do not fall into the category of Non-repeaters and for which more than one instance is returned (the maximum number of returned instances is defined with the Max-repetitions value).

For illustration see the usage [example](#).

Note: When you use the SNMP GetBulk operation in the main window, the 'Non-repeaters' value should be set to zero (0). Otherwise, the program will retrieve only one object instance regardless of the 'Max-repetitions' value.

12. Click the **Retransmits** entry in the navigation tree to display the Timeout and Retransmit Properties panel ([Figure 59](#)).

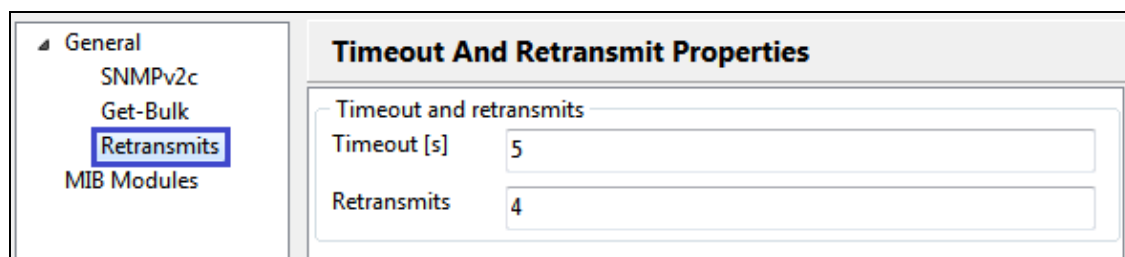


Figure 59: Setting the timeout and retransmits agent profile properties (SNMPv2c)

13. Into the **Timeout [s]** input line, enter the timeout value in seconds for pending SNMP requests.

The **Timeout** value defines how many seconds the program waits for the SNMP agent to respond to the request. When this time is over, the program, depending on the value of the Retransmits parameter, cancels or repeats the query.

14. When using SNMP over UDP, enter the number of retransmits for pending SNMP requests into the **Retransmits** input line. Note that this input line is disabled when using SNMP over TCP, because the underlying TCP protocol ensures reliable data delivery, automatically taking care of packets retransmission when required.

The **Retransmits** value defines how many times the program re-sends the request after the first timeout.

15. To enable automatic loading of specific MIB modules when using the agent profile, refer to the [Automatically Load MIB Modules](#) section.
16. Click the **OK** button to apply all changes and close the Agent Profile Properties dialog box.

7.1.3 Using SNMPv3 Protocol with User-Based Security Model

To use the SNMPv3 protocol with User-Based Security Model (USM), specify the following parameters in the Agent Profile Properties dialog box, General Properties panel:

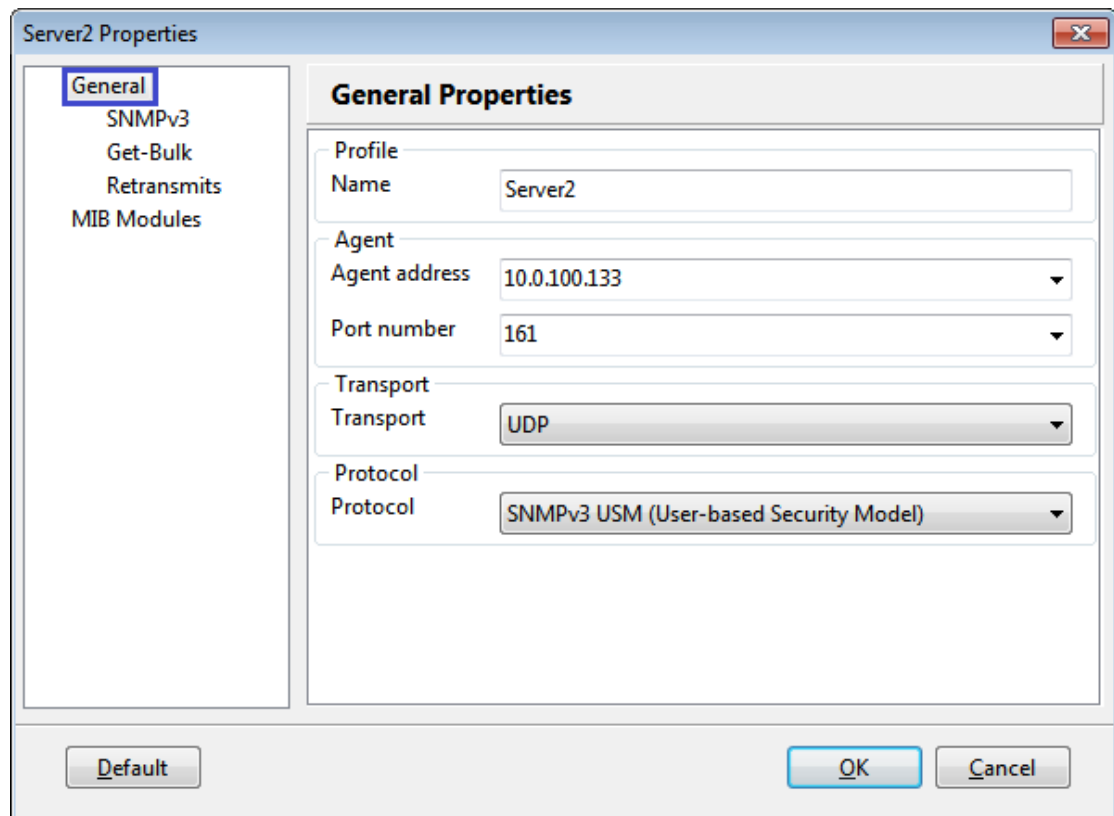


Figure 60: Agent Profile Properties dialog box, SNMPv3 USM protocol selected

1. Into the **Name** input line, enter the name for the agent profile (e.g., a name of the device). This is only a label under which the SNMP agent profile is stored. This label will be also displayed as the name of the profile in the SNMP Agent Profiles window.
2. In the **Agent Address** drop-down list, specify the **IPv4** or **IPv6** address of the SNMP agent to be managed.
3. In the **Port Number** drop-down list, specify the port number on which the SNMP agent listens to for incoming SNMP requests (the default port number is **161**).
4. In the **Transport** drop-down list, select one of the following:
 - ☐ To use **SNMP over UDP** transport protocol (=standard), select the **UDP** entry,
 - ☐ To use **SNMP over TCP** transport protocol, select the **TCP** entry.
5. In the **Protocol** drop-down list, select the **SNMPv3 USM (User-based Security Model)** option. The **SNMPv3** entry appears in the navigation tree of the SNMP Agent Profiles window.

- Click the **SNMPv3** entry in the navigation tree to display the SNMPv3 Properties panel, which lets you choose an existing or create a new SNMPv3 USM user profile to be used for managing the given SNMP agent (Figure 61).

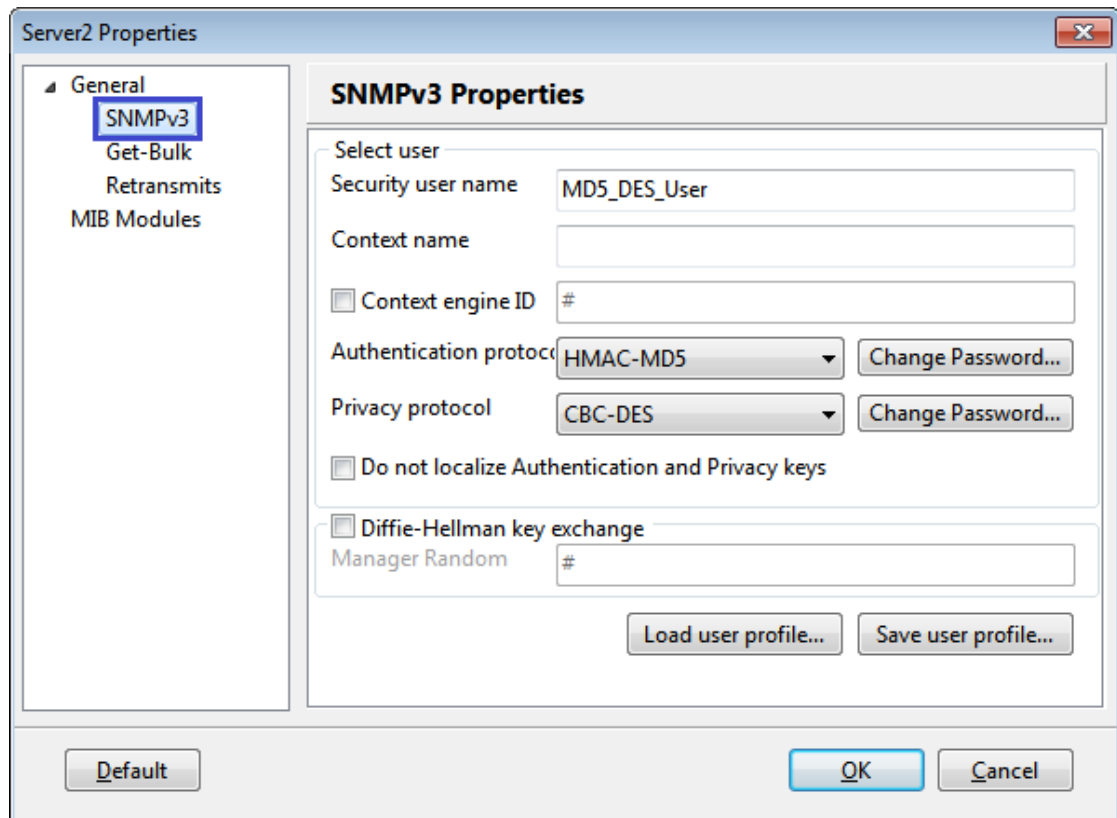


Figure 61: Agent Profile Properties dialog box, SNMPv3 properties

To Load and Use an Existing SNMPv3 USM User Profile

- Click the **Load User Profile** button in the SNMPv3 Properties panel of the Agent Profile Properties dialog box.
- The SNMPv3 USM User Profiles window appears (Figure 62). It displays a list of all existing SNMPv3 user profiles configured in MIB Browser.
- Select the line that represents the SNMPv3 USM user profile you want to use in the SNMPv3 USM User Profiles window and use the **Select** button or pop-up command (Figure 62).
- The SNMPv3 USM User Profiles window closes and the SNMPv3 panel of the Agent Profile Properties dialog box displays the SNMPv3 security parameters of the selected SNMPv3 USM user profile (Figure 61).

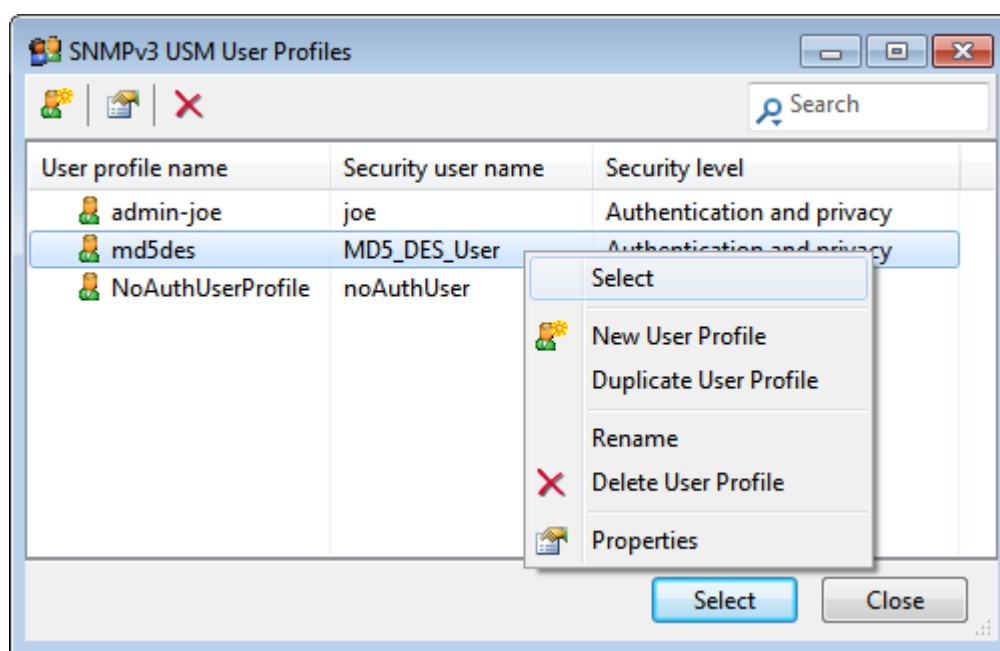


Figure 62: SNMPv3 USM User Profiles window

- For instructions on configuring the 'Get-Bulk' and the 'Timeout and Retransmit' and 'Load MIB Modules' settings in the Agent Profile Properties dialog box, refer to the corresponding sections ([GetBulk](#), [Retransmits](#), [Automatically Load MIB Modules](#)).
- Click the **OK** button to apply the changes and close the Agent Profile Properties dialog box.

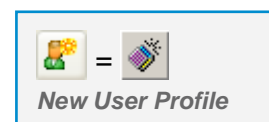
To Create and Use a New SNMPv3 USM User Profile

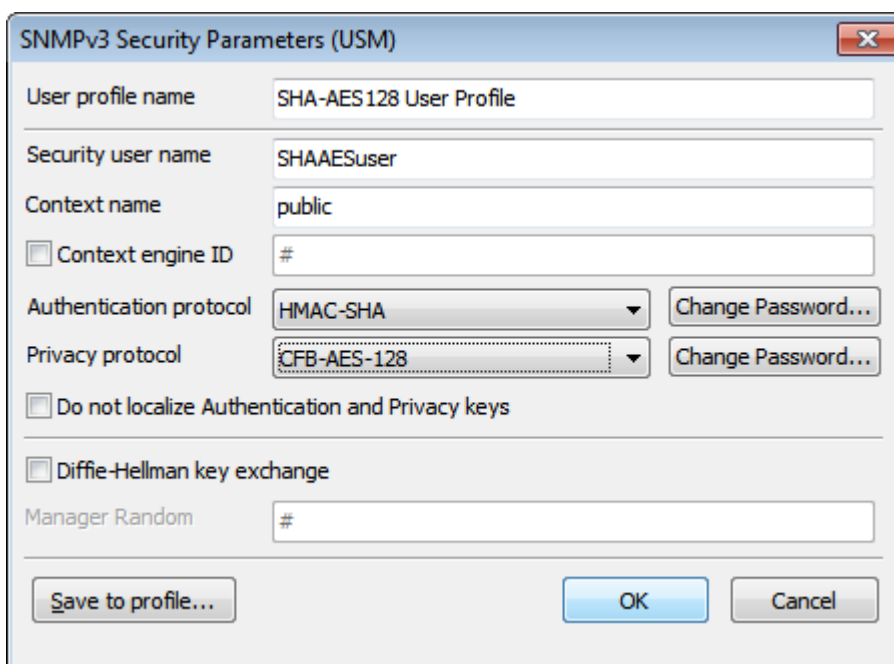
To create and use a new SNMPv3 USM user profile, you can either:

- Enter the SNMPv3 USM user security parameters directly into the SNMPv3 Properties panel of the Agent Profile Properties dialog box and save the configuration as a new SNMPv3 USM user profile using the **Save user profile** button, or
- Open the SNMPv3 USM User Profiles window, create a new SNMPv3 USM user profile and select it.

This section describes the second option, as follows:

- Open the SNMPv3 USM User Profiles window ([Figure 62](#)) by clicking the **Load user profile** button in the Agent Profile Properties dialog box (SNMPv3 Properties panel) ([Figure 61](#)).
- In the SNMPv3 USM User Profiles window, click the **New User Profile** button or select the **New User Profile** pop-up command.
- When the SNMPv3 Security Parameters (USM) dialog box opens ([Figure 63](#)), specify the following parameters:





The dialog box titled "SNMPv3 Security Parameters (USM)" contains the following fields and controls:

- User profile name:** Text input field containing "SHA-AES128 User Profile".
- Security user name:** Text input field containing "SHAESuser".
- Context name:** Text input field containing "public".
- Context engine ID:** A checkbox labeled "Context engine ID" is unchecked. The adjacent text input field contains "#".
- Authentication protocol:** A dropdown menu showing "HMAC-SHA". To its right is a "Change Password..." button.
- Privacy protocol:** A dropdown menu showing "CFB-AES-128". To its right is a "Change Password..." button.
- Do not localize Authentication and Privacy keys:** An unchecked checkbox.
- Diffie-Hellman key exchange:** An unchecked checkbox.
- Manager Random:** A text input field containing "#".
- Buttons:** "Save to profile...", "OK", and "Cancel" are located at the bottom.

Figure 63: Specifying parameters for SNMPv3 security users

4. Into the **User profile name** input line, enter a name for the user profile.

Note: The User profile name is only a label name under which you store the SNMPv3 USM user profile and has no effect on the SNMPv3 protocol itself. The User profile name will also appear in the **User profile name** drop-down list in the first column of the SNMPv3 USM User Profiles window.

5. Into the **Security user name** input line, enter a name for the SNMPv3 security user. The Security user name represents the user in a format that is security model independent.
6. Into the **Context name** input line, enter the SNMPv3 Context name.
7. For communicating with an SNMP agent through a proxy, you should check the **Context engine ID** checkbox and specify the SNMPv3 Context engine ID. If the checkbox is not checked, the automatically computed Context engine ID is used for that profile.

To overwrite the default Context engine ID, enter a properly formatted binary value by starting the line with the # character and continue with any number of character codes in decimal, octal (prefix 0) or hex (prefix 0x) notation. Here is an example:

Enter any of the following four values into the input line:

```
# 022 064 0357
# 18 52 239
# 0x12 0x34 0xef
# 022 52 0xEF
```

The above four values will all do the same; set the Context engine ID value to 0x1234EF.

8. Select the SNMPv3 USM authentication protocol from the **Authentication protocol** drop-down list. In addition to the standard HMAC-MD5-96 and HMAC-SHA-96 authentication protocols (RFC 3414), MIB Browser supports also the **HMAC-SHA-2** authentication protocols for use with SNMPv3 USM, as specified in [RFC 7860](#). These are HMAC-SHA-2-224, HMAC-SHA-2-256, HMAC-SHA-2-384 and HMAC-SHA-2-512.
9. Click the **Change Password** button next to the **Authentication protocol** drop-down list. This will open the Password For Authentication Protocol dialog box ([Figure 64](#)).

Tip: To see the typing, uncheck the **Hide typing** checkbox.

Figure 64: Password For Authentication/Privacy Protocol dialog box

10. Enter the password into the first **Password** input line and then confirm it by re-entering it into the **Password confirmation** input line below.

Tip: For more information about specifying passwords and security keys in MIB Browser, see the [Specifying Password or Security Key](#) section and its subsections.

11. Click the **OK** button. The Password For Authentication Protocol dialog box closes.
12. Select the SNMPv3 USM privacy protocol from the **Privacy Protocol** drop-down list. In addition to the standard CBC-DES (RFC 3414) and CFB-AES-128 (RFC 3826) privacy protocols, MIB Browser supports also the CFB-AES-192, CFB-AES-256 and CBC-3DES privacy protocols, which provide stronger security (encryption).

Note: There is currently no standard for using AES-192, AES-256 and 3DES privacy protocols in SNMPv3 USM. When using these privacy protocols with MD5 and SHA authentication protocols that do not provide long enough output to accommodate the 192- or 256-bit size keys for AES-192 and AES-256 or the 168-bit size key for 3DES, some mechanism needs to be employed to produce long enough localized keys. MG-SOFT MIB Browser uses the key extension mechanism used by Cisco and some other parties, which is described in the Reeder 3DES Internet draft document (<https://tools.ietf.org/html/draft-reeder-snmpv3-usm-3desede-00>). Note that this mechanism is not employed when using the above privacy protocols with SHA2 authentication protocols that produce the hash output of an adequate size (e.g., SHA2-256, etc.), since no key extension is needed in such case.

13. Click the **Change Password** button next to the **Privacy Protocol** drop-down list.
14. The Password For Privacy Protocol dialog box appears.

Note: The Password For Authentication Protocol dialog box and the Password For Privacy Protocol dialog box have the same appearance.

15. Enter the privacy password into the **Password** input line and then confirm it by re-entering it into the **Password confirmation** input line below. Close the dialog box by clicking the **OK** button.
16. In the SNMPv3 Security Parameters (USM) dialog box (Figure 63) you can check the **Do not localize Authentication and Privacy keys** checkbox. In this case MIB Browser will use *non-localized* Authentication and Privacy keys when communicating with remote SNMPv3 agents.

Note: The *Diffie-Hellman key exchange* feature is available only in the **DOCSIS/DH**, **Developer's**, and **Simulator** editions of MIB Browser. For more information about this feature, check the **Diffie-Hellman Key Exchange for DOCSIS-Based SNMPv3 Agents** section.

17. After you have specified all the parameters, click the **OK** button. The SNMPv3 Security Parameters (USM) dialog box closes and a new line representing the newly configured SNMPv3 user profile appears in the SNMPv3 USM User Profiles window (Figure 62).
18. Select the new SNMPv3 USM user profile in the SNMPv3 USM User Profiles window and click the **Select** button or pop-up command (Figure 62).
19. The SNMPv3 USM User Profiles window closes and the SNMPv3 Properties panel of the Agent Profile Properties dialog box displays the SNMPv3 security parameters of the selected SNMPv3 USM user profile (Figure 65).

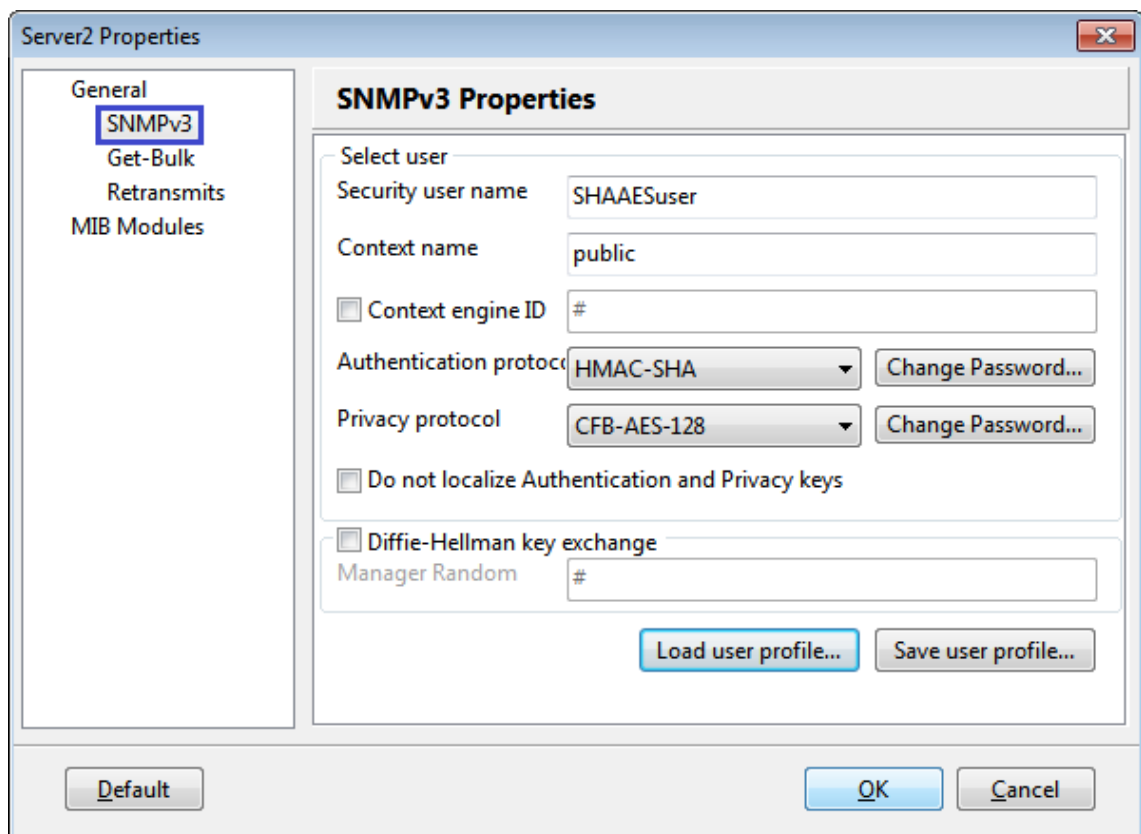


Figure 65: Agent Profile Properties dialog box, SNMPv3 properties (new USM user selected)

20. For instructions on configuring the 'Get-Bulk' and the 'Timeout and Retransmit' and 'Load MIB Modules' settings in the Agent Profile Properties dialog box, refer to the

corresponding sections ([GetBulk](#), [Retransmits](#), [Automatically Load MIB Modules](#)). This section describes only settings that are specific to SNMPv3 USM protocol.

21. Click the **OK** button to apply the changes and close the Agent Profile Properties dialog box.

7.1.4 Using SNMPv3 Protocol with Transport Security Model (TLS/DTLS)

To use the SNMPv3 protocol with Transport Security Model (TSM) using (D)TLS transport, specify the following parameters in the Agent Profile Properties dialog box, General Properties panel:

Figure 66: Agent Profile Properties dialog box, SNMPv3 TSM/DTLS protocol selected

1. Into the **Name** input line, enter the name for the agent profile (e.g., a name of the device). This is only a label under which the SNMP agent profile is stored. This label will be also displayed as the name of the profile in the SNMP Agent Profiles window.
2. In the **Agent Address** drop-down list, specify the [IPv4](#) or [IPv6](#) address of the SNMP agent to be managed.
3. In the **Port Number** drop-down list, specify the port number on which the SNMP agent listens to for incoming SNMP requests (the default port number for SNMP over (D)TLS is [10161](#)).
4. In the **Protocol** drop-down list, select the **SNMPv3 TSM (Transport Security Model)** option.

5. In the **Transport** drop-down list, select one of the following transports:
 - ❑ To use **SNMP over DTLS over UDP**, select the **DTLS (UDP)** entry,
 - ❑ To use **SNMP over TLS over TCP**, select the **TLS (TCP)** entry.
6. Click the **TLS/DTLS** entry in the navigation tree to display the TLS/DTLS Properties panel, which lets you specify X.509 certificate(s) and private key for SNMPv3 over (D)TLS communication to be used for managing the given SNMP agent (Figure 67).

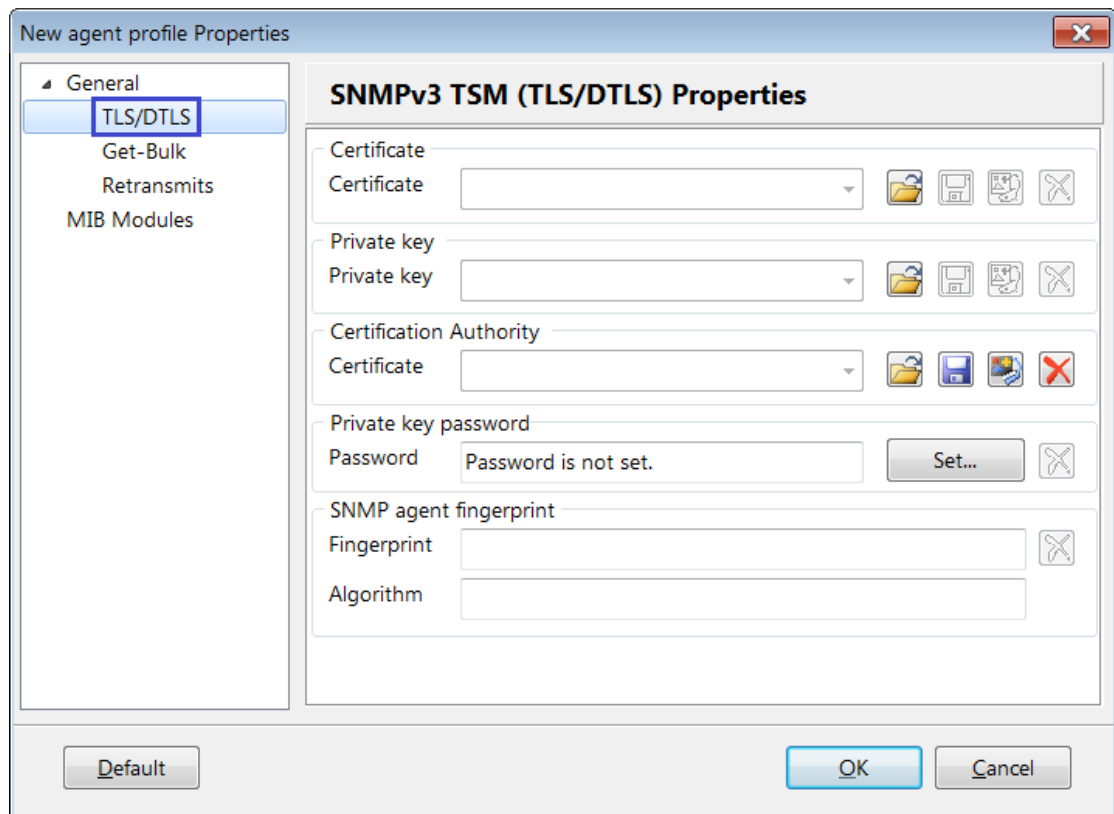


Figure 67: Agent Profile Properties dialog box, SNMPv3 TSM (TLS/DTLS) properties - empty

7. In the **Certificate** frame, click the **Load** button (📁) to open the standard Open dialog box and select the X.509 digital certificate file in PEM format, containing the **manager (client) public key** (Figure 45).

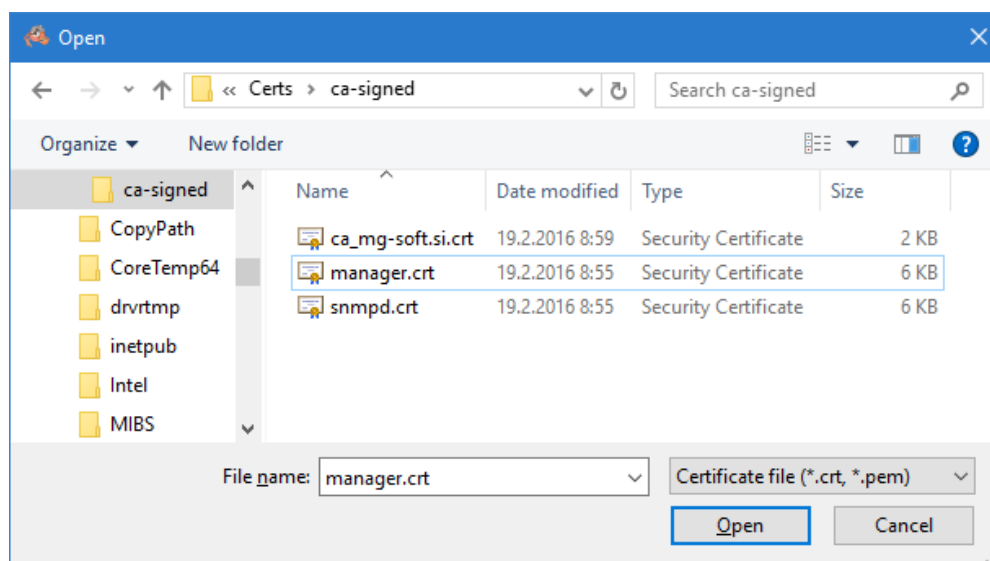


Figure 68: Loading an X.509 digital certificate for SNMPv3 over (D)TLS

8. After selecting the manager certificate file (e.g., .crt or .pem) on disk, click the **Open** button to load the certificate into MIB Browser.
9. In the **Private key** frame, click the **Load** button (📁) to open the standard Open dialog box and select the file containing the **manager private key** in PEM format (e.g., .key or .pem) from disk.

Tip: Click the Properties button (🔍) next to the **Certificate** or **Private key** input line to view full details of the loaded digital certificate or private key, respectively.

10. In the **Certification Authority** frame, click the **Load** button (📁) to open the standard Open dialog box and select the X.509 digital certificate file (in PEM format), containing the **CA authority public key**. This certificate will be used for verifying the server certificate. If the server uses a self-signed certificate, leave this input line empty.
11. To enter the password for decrypting the manager private key (if encrypted), click the **Set** button in the **Private key password** frame, and enter the corresponding password twice into the dialog box that appears.
12. The **Fingerprint** and **Algorithm** are two read-only text fields that get automatically populated after establishing a TLS connection with the agent and accepting its certificate (when no CA certificate is provided). Fingerprint is a cryptographic hash of the agent certificate in hex. (unique identification of the certificate) and algorithm is the name of algorithm used for producing the fingerprint (e.g., sha1, md5, sha256, etc.).

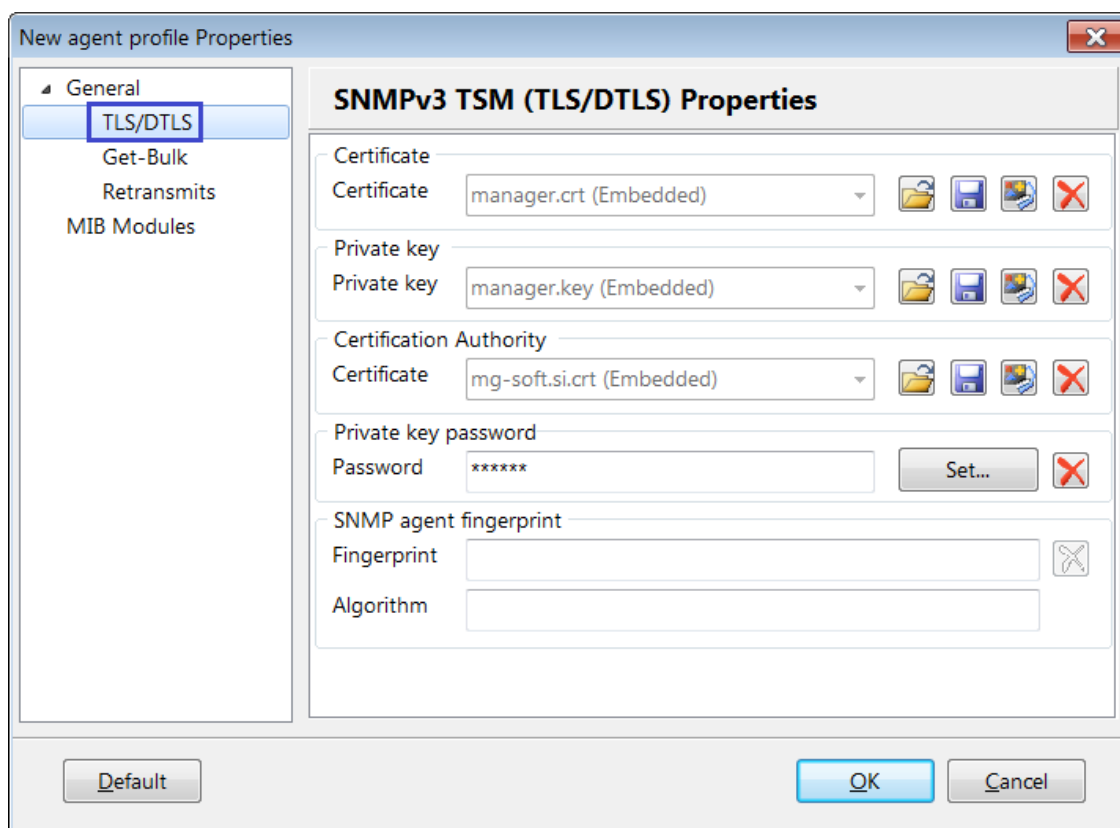


Figure 69: Agent Profile Properties dialog box, SNMPv3 TSM (TLS/DTLS) properties - specified

13. For instructions on configuring the remaining settings in the Agent Profile Properties dialog box, refer to the corresponding sections ([GetBulk](#), [Retransmits](#), [Automatically Load MIB Modules](#)). This section describes only settings that are specific to SNMPv3 TSM (TLS/DTLS) protocol.
14. Click the **OK** button to close the Agent Profile Properties dialog box.

7.1.5 Automatically Load MIB Modules

To enable and configure automatic loading of specific MIB modules when using the given agent profile, proceed as follows.

1. Click the **MIB Modules** entry in the navigation tree of the Agent Profile Properties dialog box to display the Load MIB Modules Properties panel ([Figure 70](#)).

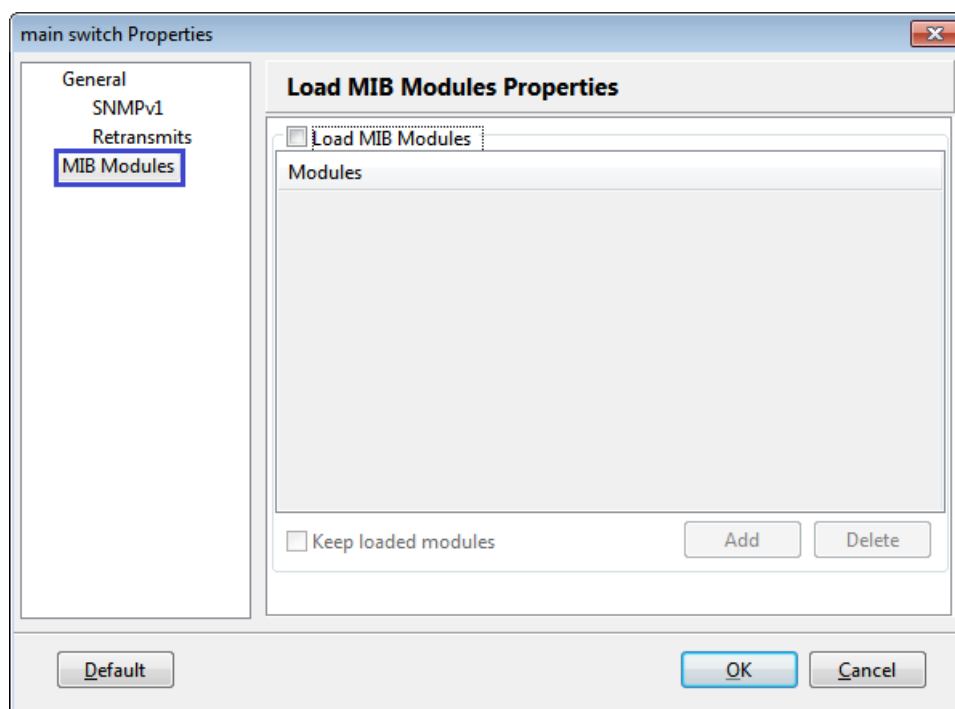


Figure 70: Agent Profile Properties dialog box, Load MIB Modules properties - empty

2. Check the **Load MIB Modules** checkbox at the top of the Load MIB Modules Properties panel to enable loading MIB modules listed in the Modules panel below.
3. Click the **Add** button below the Modules panel to open the **Select MIB Modules** window (Figure 71).

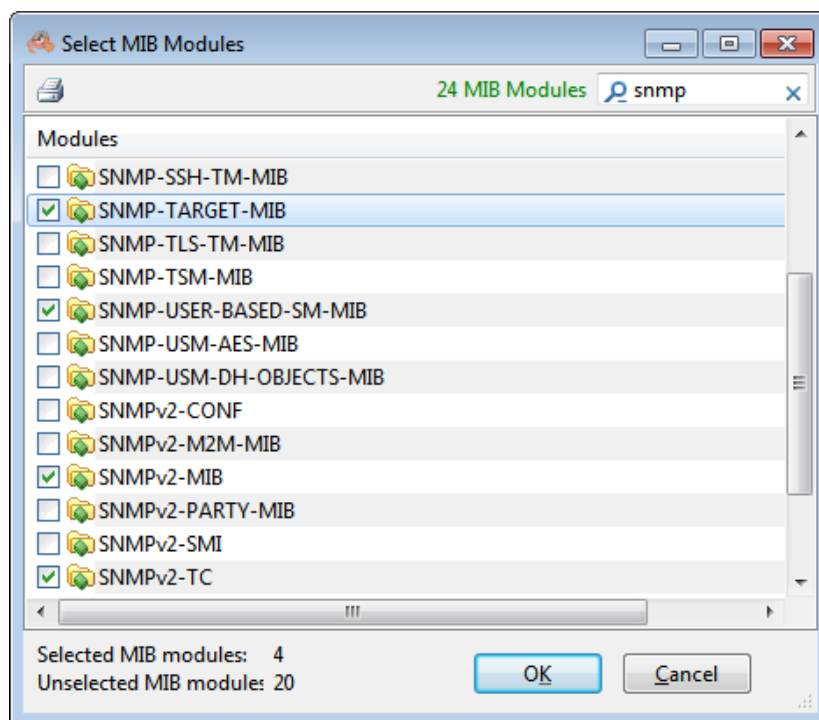


Figure 71: Selecting MIB modules to be loaded with the agent profile

4. The **Select MIB Modules** window lists the names of all registered MIB modules and lets you select the desired modules to be loaded together with the agent profile.
5. Check the checkboxes in front of the modules you wish to load when managing the given SNMP agent. Use the **Live search** tool in the upper-right corner of the window to display only those modules that match the search phrase, e.g., `snmp` (Figure 71).
6. After selecting the desired modules, click the **OK** button to close the Select MIB Modules window. The selected MIB modules appear in the Agent Profile Properties dialog box, in the Modules list (Figure 72).
7. To enable loading the specified modules without first unloading all modules (i.e., adding the specified modules to the already loaded modules - if any), check the **Keep loaded modules** checkbox below the Modules list.
8. To add additional modules to the Modules list, repeat steps 3 to 6 above. To remove modules from the list, select them in the Modules list and click the **Delete** button.

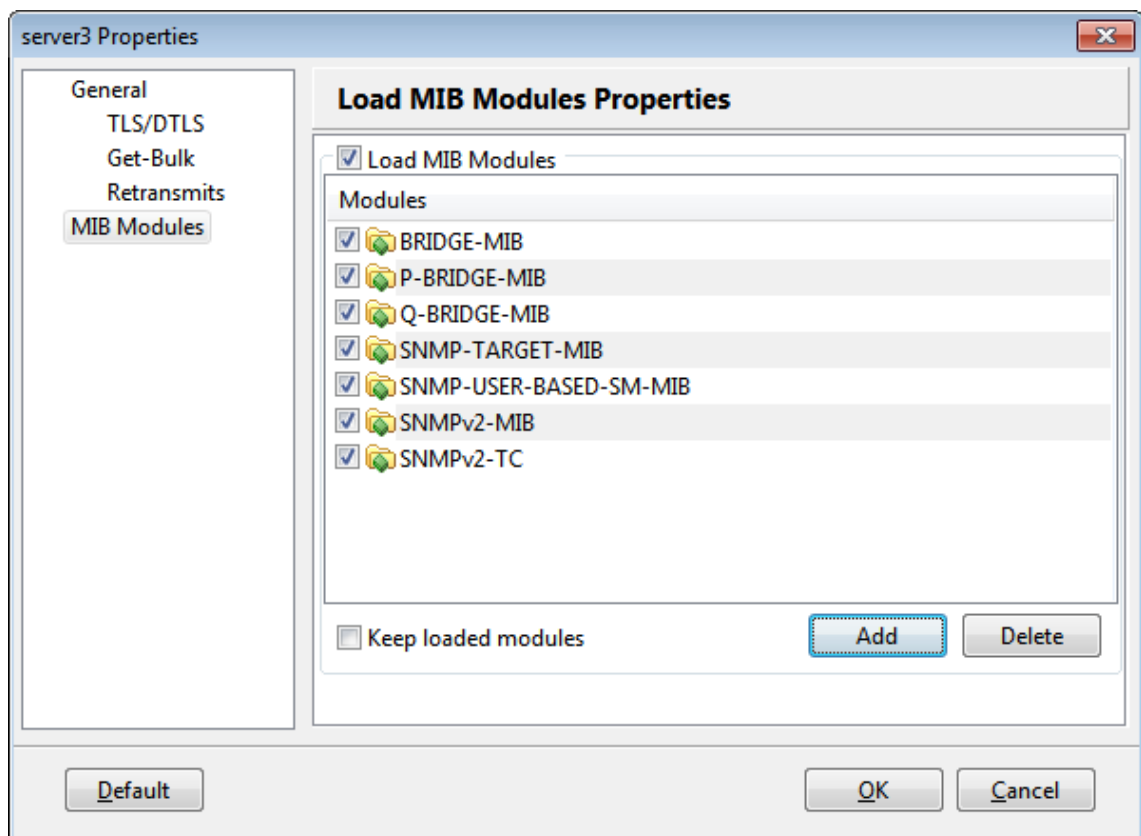


Figure 72: Agent Profile Properties dialog box, Load MIB Modules properties - modules specified

9. Click the **OK** button to close the Agent Profile Properties dialog box.

7.2 Using SNMP Agent Profiles to Manage SNMP Agents

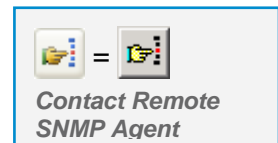
Once you create and configure a SNMP agent profile in MIB Browser, you can simply select that profile to query or manage the corresponding SNMP agent in any MIB Browser window.

To select an SNMP agent profile and contact the SNMP agent in the main window:

1. Select the **View / SNMP Agent Profiles** command or click the **SNMP Agent Profiles** button to open the SNMP Agent Profiles window (Figure 73).
2. Expand the hierarchical tree structure and select the SNMP agent profile that contains parameters for contacting and managing the SNMP agent you want to manage.
3. Use the **Contact** pop-up command or click the **Contact** button to close the SNMP Agent Profiles window and contact the SNMP agent.



SNMP Agent Profiles



Contact Remote SNMP Agent

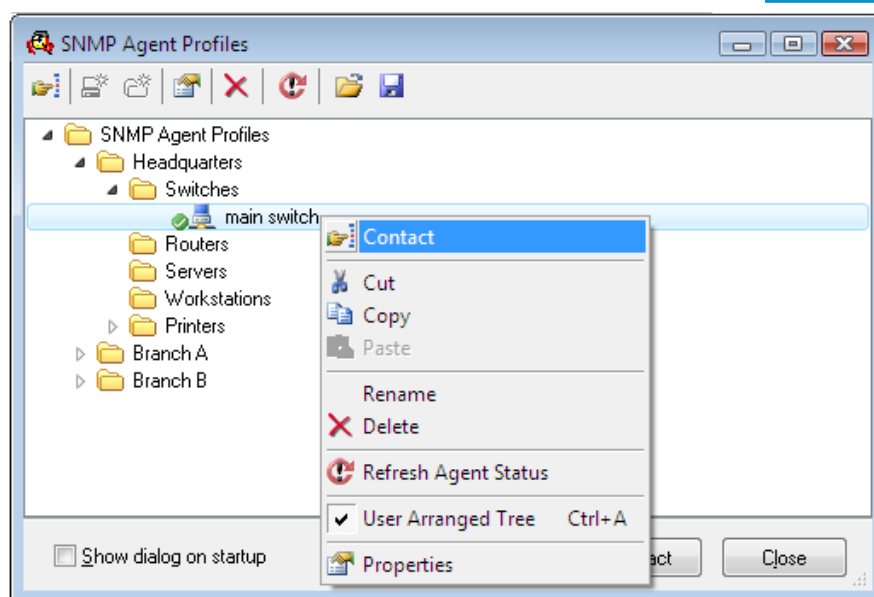


Figure 73: SNMP Agent Profiles window

4. MIB Browser contacts the SNMP agent using the agent address and SNMP access parameters specified in the selected agent profile and displays the agent response in the **Query Results** panel (Figure 18).

Note: The agent address and SNMP access parameters (SNMP version, community name or SNMPv3 user profile, port, timeout and retries, etc.) are automatically copied from the selected agent profile into the **Remote SNMP agent** drop-down list and into the **SNMP Protocol Preferences dialog box**, respectively. If configured in the agent profile, the specified MIB modules are also loaded in the MIB tab of the main window.

- Once the SNMP agent has been successfully contacted, you can use any other SNMP operation (e.g., Get, GetNext, Walk, Set, etc.) to retrieve or modify the values of object instances implemented in that SNMP agent.

7.3 Organizing SNMP Agent Profiles in Folders

The SNMP Agent Profiles window lets you group SNMP agent profiles into folders. Each folder can contain any number of agent profiles and (sub)folders. This mechanism allows you to organize agent profiles in hierarchical tree structures and group related profiles.

- Select the **View / SNMP Agent Profiles** command or click the **SNMP Agent Profiles** button.
- The SNMP Agent Profiles window opens (Figure 74). It contains a hierarchical tree structure composed of icons representing folders and SNMP agent profiles.

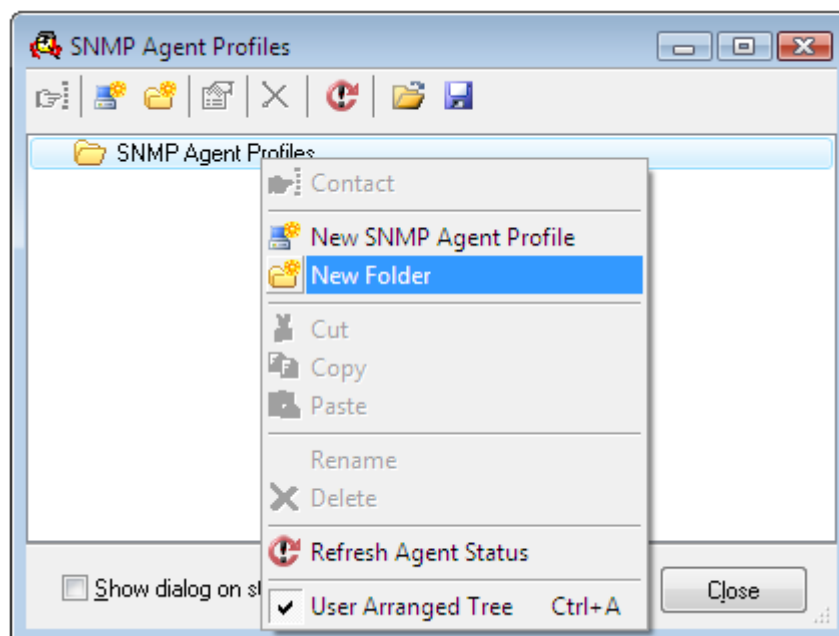
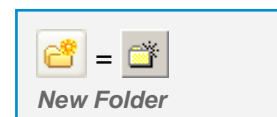


Figure 74: Creating a new folder in the SNMP Agent Profiles window

To create a new folder

- Select the folder under which you want to create a new folder and select the **New Folder** pop-up command or click the **New Folder** toolbar button (Figure 74).
- A new folder with the default name appears below the selected folder in the SNMP Agent Profiles window (Figure 75). Repeat this procedure to create additional folders in the SNMP Agent Profiles window.



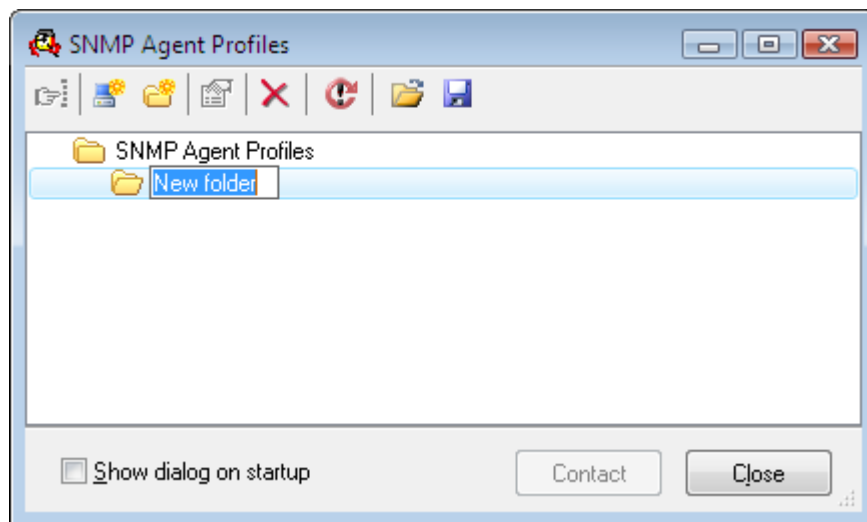


Figure 75: A new folder created in the SNMP Agent Profiles window

To create a new SNMP agent profile

1. Select the folder in which you want to create a new SNMP agent profile and choose the **New SNMP Agent Profile** pop-up command or click the **New SNMP Agent Profile** toolbar button.
2. A new agent profile icon with the default name appears below the selected folder in the SNMP Agent Profiles window (Figure 76).

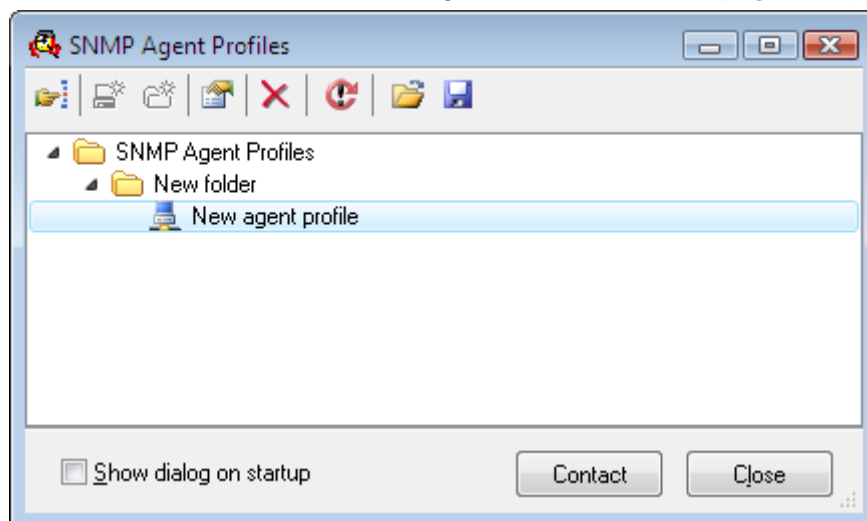
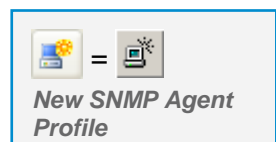


Figure 76: A new SNMP agent profile added to the SNMP Agent Profiles window

Tip: For more information on configuring SNMP Agent Profiles, see the [Creating New SNMP Agent Profile](#) section of this manual.

To create SNMP agent profiles for discovered SNMP agents

MIB Browser lets you discover remote SNMP agents in a specified IP address range and then create SNMP agent profiles for all discovered SNMP agents with a single command.

To create SNMP agent profiles for discovered SNMP agents:

1. First, run the discovery operation to get a list of discovered SNMP agents, as described in the [Discovering Remote SNMP Agents](#) section of this manual.
2. Once the Remote SNMP Agent Discovery window displays a list of discovered SNMP agents, select the agents for which you want to create SNMP agent profiles and use the **Add To Agent Profiles** pop-up command ([Figure 77](#)).

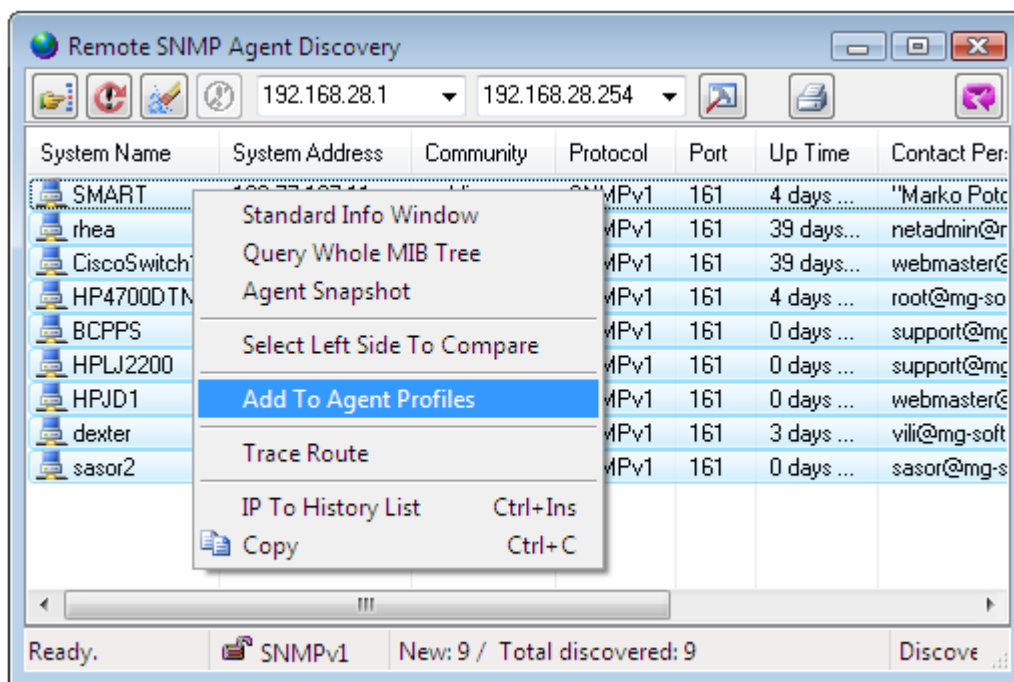


Figure 77: Creating SNMP agent profiles for discovered SNMP agents

3. MIB Browser creates SNMP agent profiles for all selected SNMP agents. The properties of created agent profiles (address, SNMP version, community name or SNMPv3 USM user profile, port) match the properties displayed in the Remote SNMP Agent Discovery window. Icons representing discovered SNMP agents are placed into the 'Discovery' folder, which is created automatically in the SNMP Agent Profiles window ([Figure 78](#)).

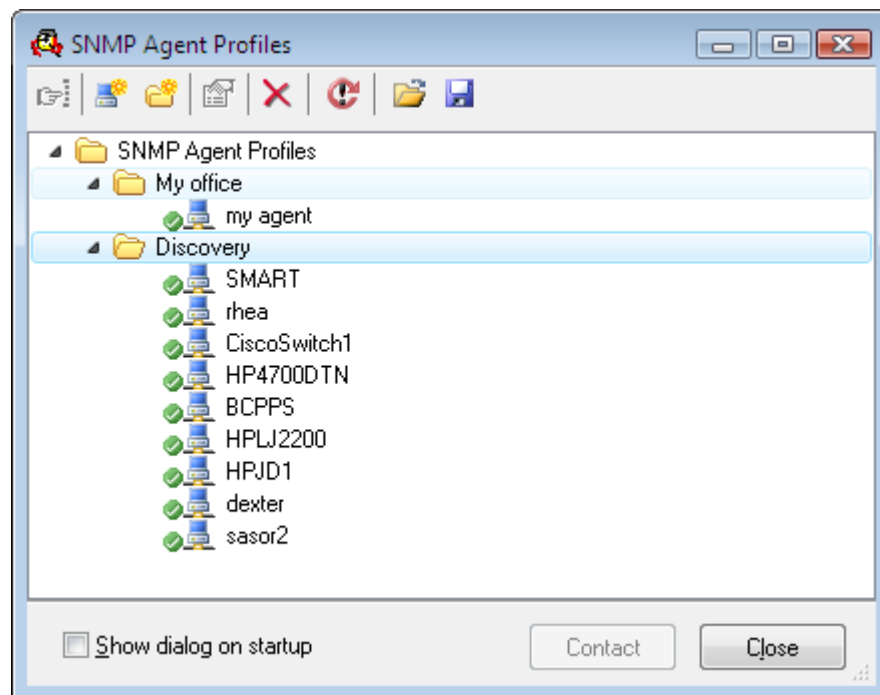


Figure 78: SNMP agent profiles created for discovered SNMP agents

To move a folder

1. Select the folder you want to move and use the drag&drop technique to move the folder (and all items it contains) to a new position in the SNMP Agent Profiles window.
2. If the folder contains any subordinated items, they are moved together with the folder.

To move a SNMP agent profile to another folder

1. Select the agent profile you want to move and use the drag&drop technique to move it to another folder in the SNMP Agent Profiles window.



To rename a folder or an SNMP agent profile

1. Select the item you want to rename and choose the **Rename** pop-up command.
2. Type the new name for the item and press the **Enter** key to apply the change.

To delete a folder or an SNMP agent profile





1. Select the item you want to delete and choose the **Delete** pop-up command.
2. Click the **OK** button in the dialog box that appears to confirm the removal.
3. The selected item and all subordinated items (if any) are permanently deleted.

7.4 Viewing Current Status of SNMP Agents

By default, the SNMP Agent Profiles window provides information about the current status of SNMP agents (Up, Down, Error) for which the agent profiles exist. When the SNMP Agent Profiles window is open, MIB Browser polls (in 10 minutes interval) each SNMP agent represented by an agent profile icon () and indicates its status by means of the status symbols (e.g.,: ) . This way, you can tell at a glance which SNMP agent is currently responding to SNMP queries and which is not.

The following symbols are used in combination with the SNMP agent profile icons to reflect the status of SNMP agents:

Symbol: Agent Status:

-  Up (agent is responding)
-  Down (agent is not responding)
-  Error (agent is responding with SNMPv3 Report messages)*
-  Unknown (query is in progress)

* - Indicates a probable error in [SNMPv3 user security](#) configuration.

To manually refresh the agent status indication:

1. Select the desired agent profile icon in the SNMP Agent Profiles window and choose the **Refresh Agent Status** pop-up command or toolbar button.
2. MIB Browser queries the selected agent by using the address and SNMP access parameters specified in the selected agent profile and updates its status symbol according to the results of the query (current agent responsiveness).

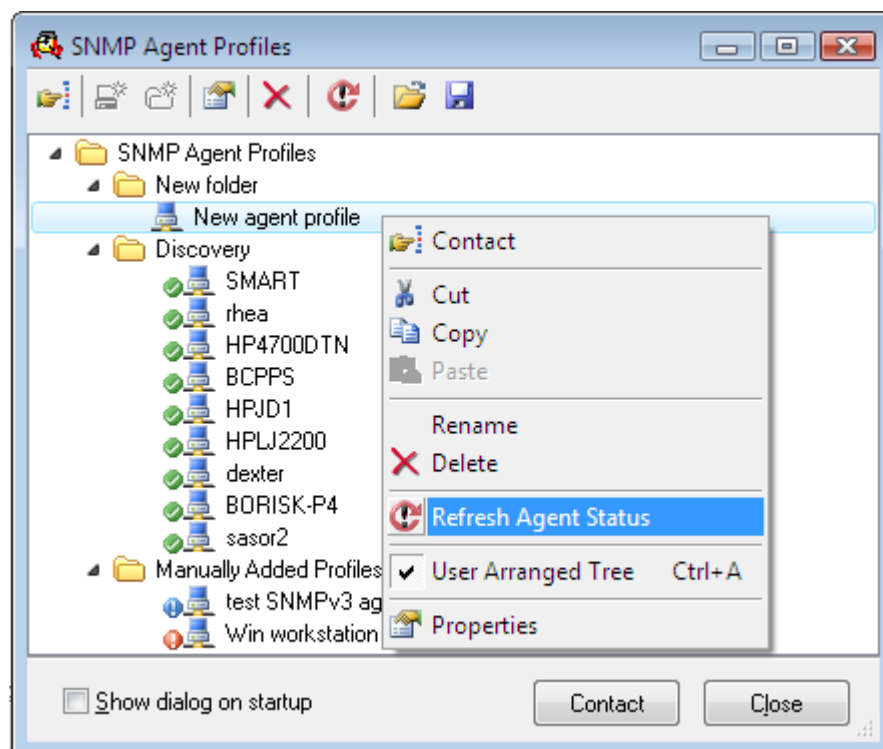


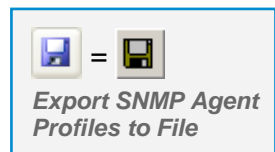
Figure 79: Manually refreshing the SNMP agent status

7.5 Exporting and Importing SNMP Agent Profiles

MIB Browser lets you export and import the entire SNMP agent profiles configuration to/from a file. Such a file can be used for backup purposes or for transferring the SNMP agent profiles configuration to other copies of MIB Browser.

To export the existing SNMP agent profiles to a file:

1. Select the **View / SNMP Agent Profiles** command or click the **SNMP Agent Profiles** button to open the SNMP Agent Profiles window (Figure 73).
2. Click the **Export Agent Profiles to File** button.
3. Specify the file name and destination path in the standard Save As dialog box that appears and click the **Save** button to save the entire SNMP agent profiles configuration (including folders) to an XML file with the .apfx filename extension.



To import SNMP agent profiles from a file:

1. Select the **View / SNMP Agent Profiles** command or click the **SNMP Agent Profiles** button to open the SNMP Agent Profiles window (Figure 73).
2. Click the **Import Agent Profiles from File** button, select the agent profiles file (.apfx or .apf) in the standard Open dialog box that appears and click the **Open** button.
3. MIB Browser imports the SNMP agent profiles configuration from the selected file and displays it under the newly created "Imported" folder in the SNMP Agent Profiles window.

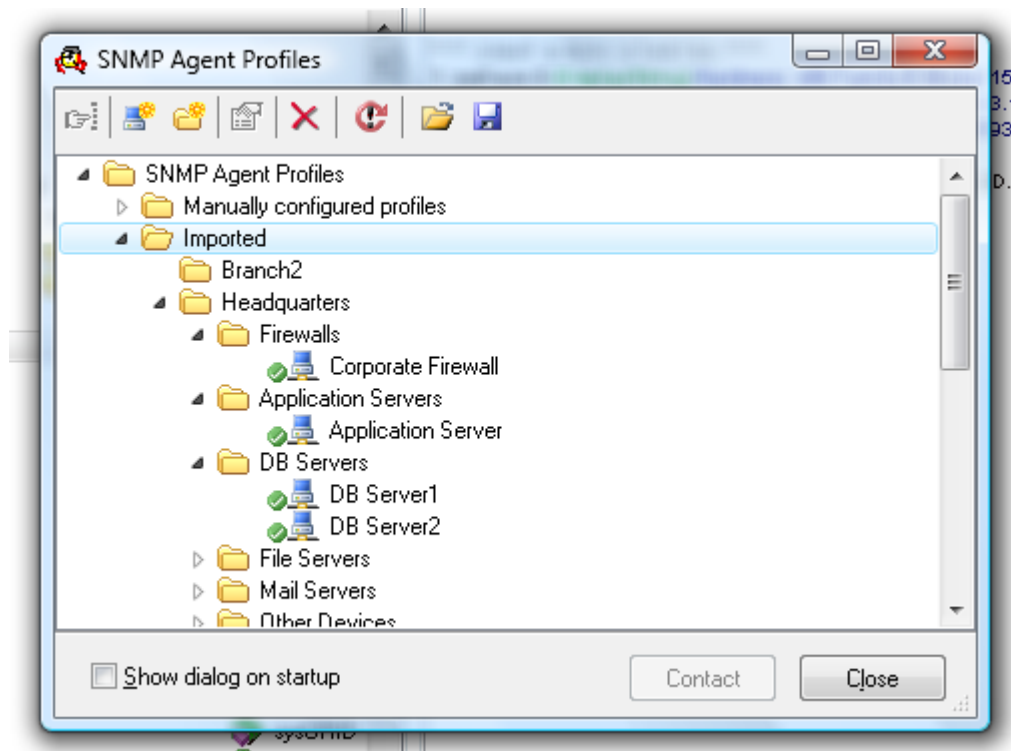


Figure 80: Imported SNMP agent profiles configuration

8 LOAD MIB MODULES IN MIB BROWSER

The loading of MIB files into MG-SOFT MIB Browser is an important step that will provide you with an overview of the MIB objects defined in the module, allow you to view the description and properties of MIB objects and let you manage devices that implement the given MIB module(s) in an effective and user-friendly manner (where OIDs are resolved to names, retrieved values are formatted according to MIB definitions, etc.)

While the standard MIB files come pre-packed, MIB files supplied by vendors of SNMP manageable devices first have to be compiled into the SMIDB binary format that can be loaded and utilized by MG-SOFT applications.

There are two ways to compile MIB files and load them in MIB Browser:

- ❑ Using the **Import MIB** feature, which lets you select MIB files on disk and automatically compile and load them into MIB Browser. This is the easiest way of loading third-party MIB modules into MIB Browser and requires no or minimal user intervention.
- ❑ Using the bundled MG-SOFT MIB Compiler GUI application to compile the MIB definition files and save them to SMIDB format and then load compiled MIB files in MIB Browser application.

This section describes both options stated above.

8.1 Importing MIB Files Directly into MIB Browser

MG-SOFT MIB Browser offers a convenient **Import MIB** feature that lets you select vendor-specific MIB definition files on disk and load them into MIB Browser. During the import process MIB definition files are scanned for dependencies and compiled behind the scenes using the command line version of MG-SOFT MIB Compiler. Compiled MIB modules are automatically saved and loaded in MIB Browser.

To import one or more MIB files into MIB Browser, proceed as follows:

1. Select the **MIB / Import MIB** command to open the **Import MIB(s)** dialog box (Figure 81).

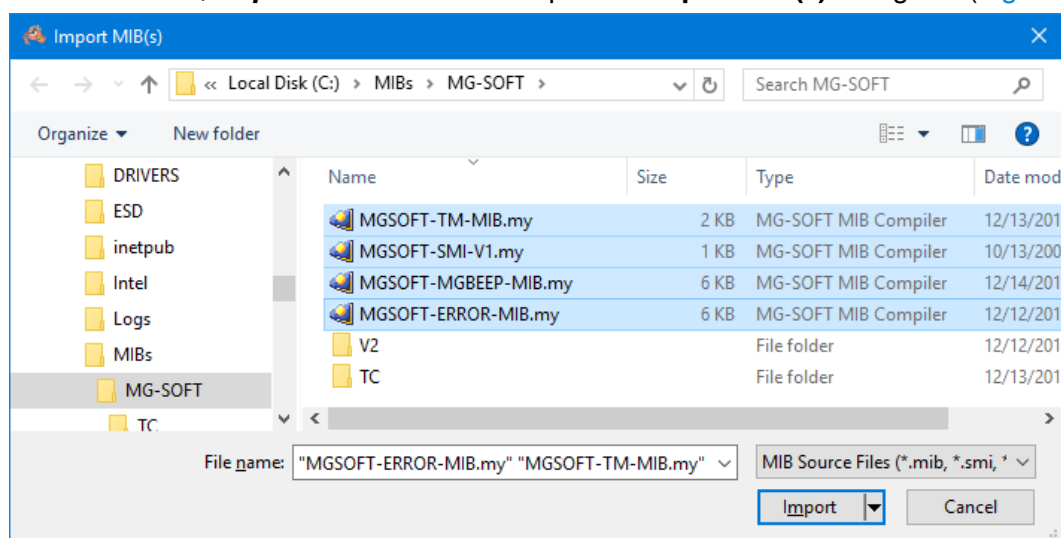


Figure 81: Selecting MIB files for import

2. In the **Import MIB(s)** dialog box, browse to the folder/path containing the MIB definition files you wish to import. Select the desired MIB file(s) and click the **Import** button.

Tip 1: By default, the **Import MIB(s)** dialog box will display files with the common MIB file extensions (.mib, .smi, .my, .mi2, .sm2). If your MIB definition files have a different extension (e.g., .txt, etc.), select the **All Files (*.*)** file mask in the drop down list in the bottom-right section of the **Import MIB(s)** dialog box to enable displaying files with any extension.

Tip 2: You can select more than one MIB definition file in the **Import MIB(s)** dialog box by holding down the **SHIFT** key (for adjacent selections) or the **CTRL** key (for non-adjacent selections) while clicking the MIB files on disk.

Tip 3: It is recommended to keep all MIB files that you wish to import in the same folder.

3. The **Import MIB Module(s)** window appears and displays the current activity being performed and the progress bar of the import operation (Figure 82). Click the **Show details** button in the Import MIB Module(s) window to view more details about the import process in the Details panel (i.e., a list of MIB files, their current import status and corresponding log). The import operation involves several phases. First, all selected MIB files are pre-scanned for module definitions.

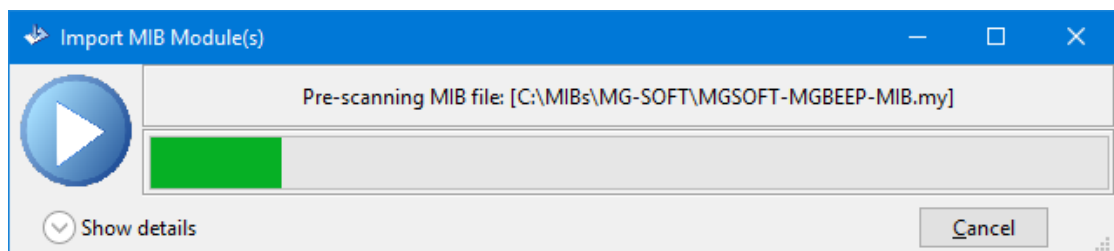


Figure 82: The Import MIB Module(s) window - pre-scanning MIB file(s)

4. Then, the first MIB file is scanned by using the command line version of MG-SOFT MIB Compiler. The scan operation checks if all MIB modules that are imported by the given MIB module are available (this is done recursively). If any required MIB module is missing (i.e., is not registered), MIB Browser displays the **Imported MIB Not Found** dialog box (Figure 83) with the following options:
 - ❑ **Scan** - choose this option to scan a specific folder for the missing MIB definition file(s). This operation will also register all found MIB definition files.
 - ❑ **Select** - choose this option to manually select the missing file(s) on disk.
 - ❑ **Skip** - choose this option to skip the missing file - the MIB module that imports the missing MIB module will fail to compile.
 - ❑ **Log** - choose this option to view the import log and cancel the entire import operation.

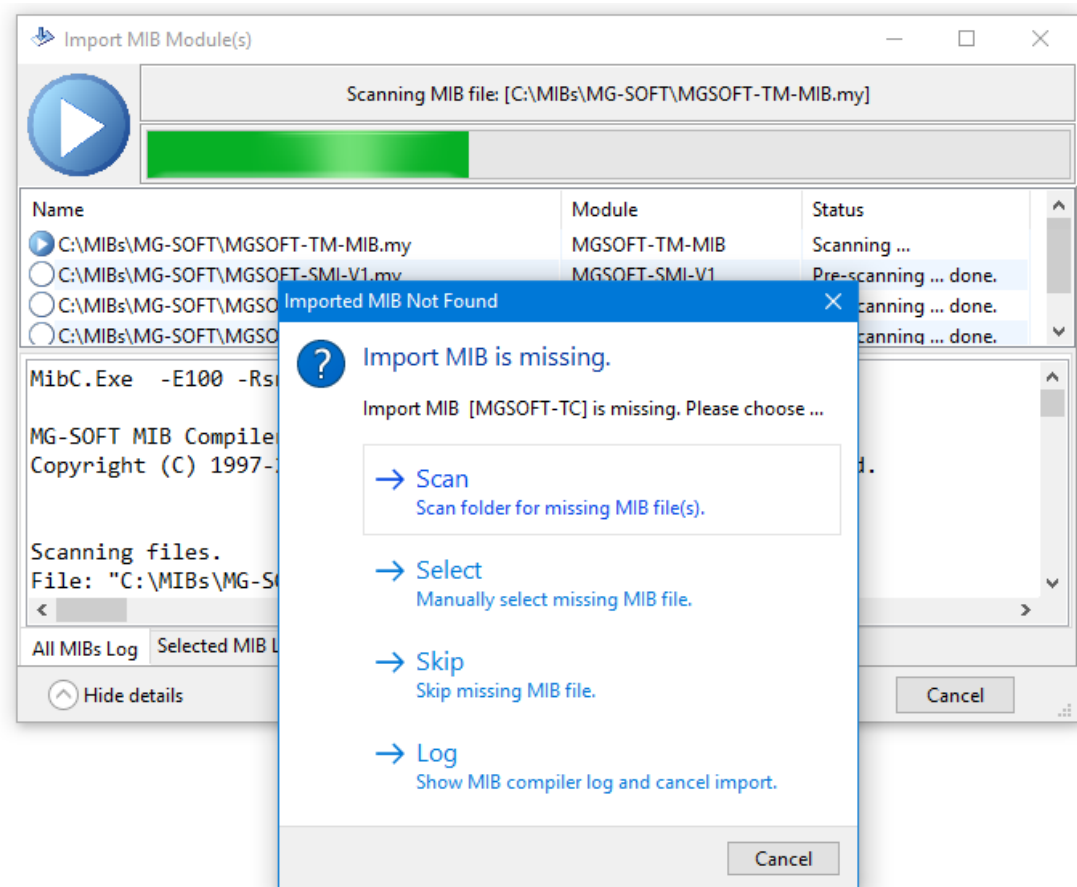


Figure 83: The Imported MIB Not Found dialog box lets you resolve missing imports issues

5. When all imports are satisfied, the MIB definition file is compiled. If compilation finishes successfully, the compiled MIB module is automatically saved to SMIDB format and registered for use with MG-SOFT applications. Both, MIB definition source file and compiled file (SMIDB), are copied to the local import location.
6. The scan and compile operations are performed on all MIB modules to be imported. You can observe the progress of individual MIB files being scanned and compiled in the Details panel of the Import MIB Module(s) window (click the **Show details** button to display the Details panel).
7. If an error occurs while compiling a MIB file (e.g., a syntax error is detected in the MIB definition file), MIB Browser displays the **Error Compiling MIB** dialog box (Figure 84) with the following options:
 - ❑ **Skip** - choose this option to skip compiling the erroneous MIB module.
 - ❑ **Run MIB Compiler GUI** - choose this option to start the bundled MG-SOFT MIB Compiler GUI application in order to debug the problem in it. Note that this action will cancel the entire import operation. You can perform the import operation later, after solving the compilation issue (e.g., fix broken MIB definition) in MG-SOFT MIB Compiler.

Tip: For instructions on examining errors and resolving compilation problems in MIB Compiler, please refer to the bundled **MIB Compiler User Manual** in PDF format; section **"Resolve Compilation Problems"**. MIB Compiler User Manual is also accessible online: http://www.mg-soft.si/files/MIB_Compiler.pdf

- ❑ **Show Log** - displays the import log and cancels the entire import operation.
- ❑ **Close** - closes this dialog box and cancels the entire import operation.

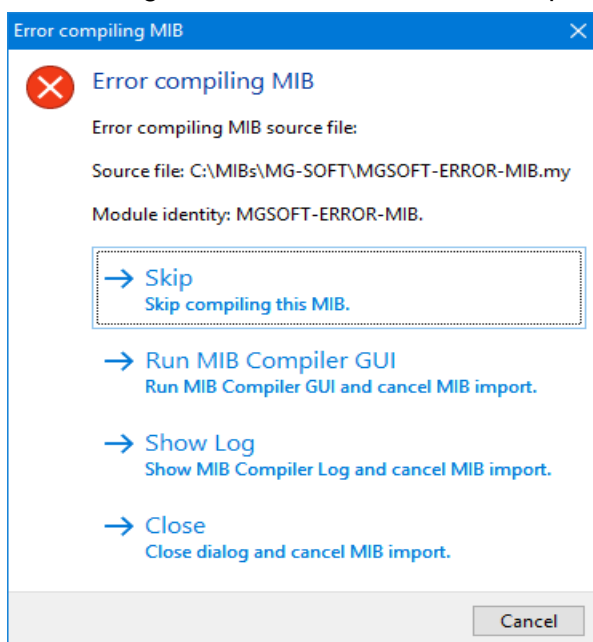


Figure 84: The Error Compiling MIB dialog box appears in case a compilation error occurs

8. When the import operation completes, the Import MIB Module(s) window displays the **Done.** message and the import result: the number of successfully imported MIB modules and the number of MIB modules that failed to import - if any. If the Details panel is open, you can view the list of processed MIB files and their import status (upper section) and the corresponding import log (lower section), as shown in [Figure 85](#).

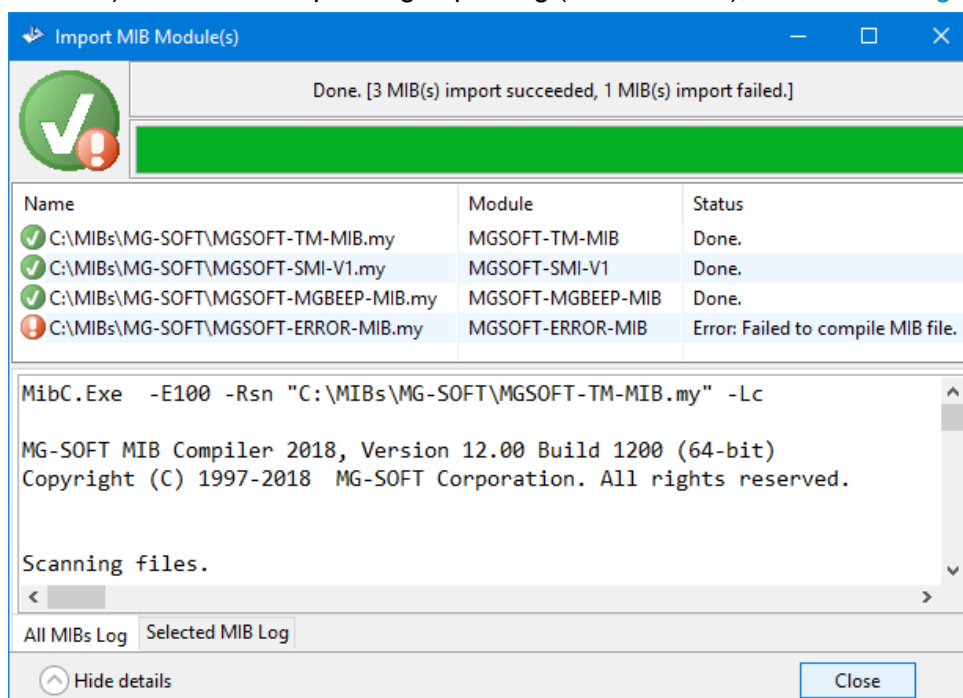


Figure 85: Viewing the final results of a MIB import operation

9. Click the **Close** button to close the Import MIB Module(s) window and automatically load the successfully imported MIB module(s) in MIB Browser.
10. In the MIB Tree panel of the main window, expand the MIB tree to view the structure of imported MIB module(s) (Figure 86). You can [view the properties of MIB tree nodes](#) and invoke SNMP operations on them, such as [SNMP Get](#), [GetNext](#), [Walk](#), [Set](#), etc. Please refer to the corresponding sections of this document for instructions on how to perform desired actions.

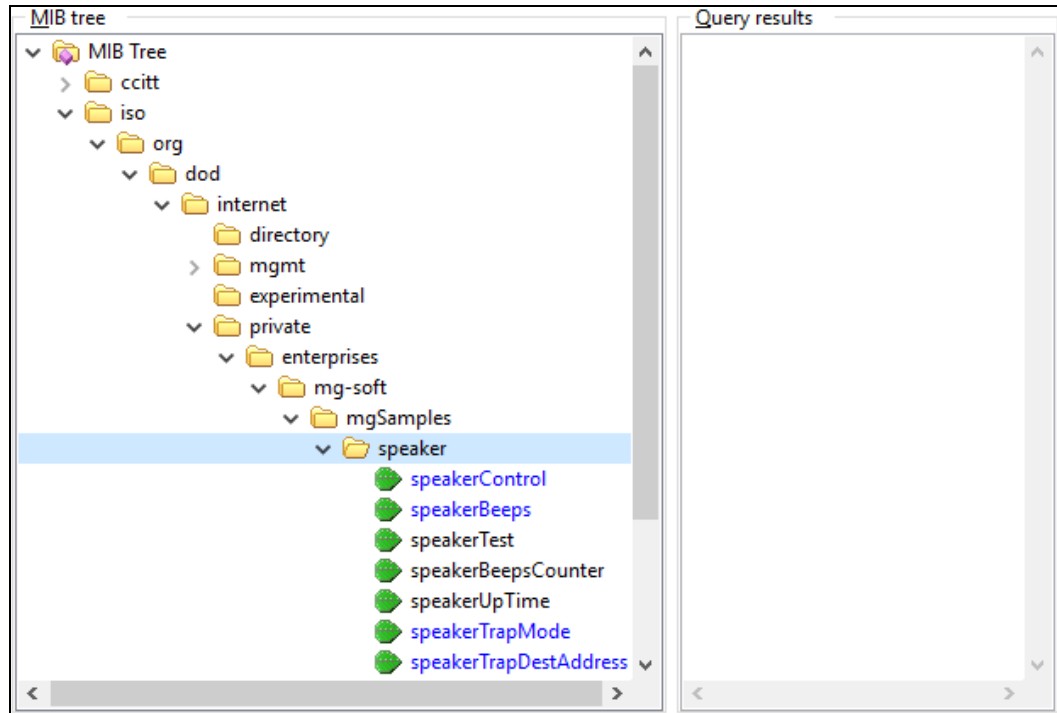


Figure 86: Viewing the structure and nodes of the imported MIB modules

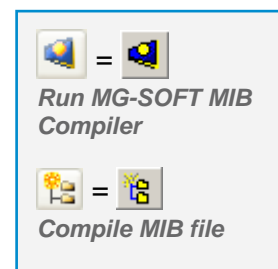
8.2 Compiling MIB Files in MG-SOFT MIB Compiler

This section describes how to compile a MIB file in the enclosed MG-SOFT MIB Compiler application. MIB Compiler is a program that converts MIB module definition files into binary SMIDB format, which can then be loaded and utilized by MIB Browser.

Tip: To automatically compile MIB files and load them into MIB Browser, use the **Import MIB** operation in MIB Browser, as described in the [Importing MIB Files Directly into MIB Browser](#) section.

To launch MG-SOFT MIB Compiler from MIB Browser, click the **Run MG-SOFT MIB Compiler** toolbar button in the main window or use the **Action / Run MIB Compiler** command. The MIB Compiler desktop appears (Figure 87).

1. To compile a MIB definition (source) file, select the **File / Compile** command in the MIB Compiler main menu, or click



- the **Compile MIB file** toolbar button. The standard Open dialog box appears.
2. Select the MIB file that you wish to compile and click the **Open** button. The Open dialog box closes.
 3. MIB Compiler compiles the selected file. The compiled MIB file (MIB module) is displayed in the Compiled MIB Modules dialog box (Figure 87).
 4. To save the compiled MIB module, select its name from the list of compiled MIB modules and click the **Save** button.
 5. The Save As dialog box appears. Specify the file name and saving destination and save it to the SMIDB file format by clicking the **Save** button.

Tip: For detailed instructions on compiling MIB files, please refer to the MIB Compiler User Manual, especially sections that describe how to efficiently compile a group of MIB files using the **Batch Compile** command.

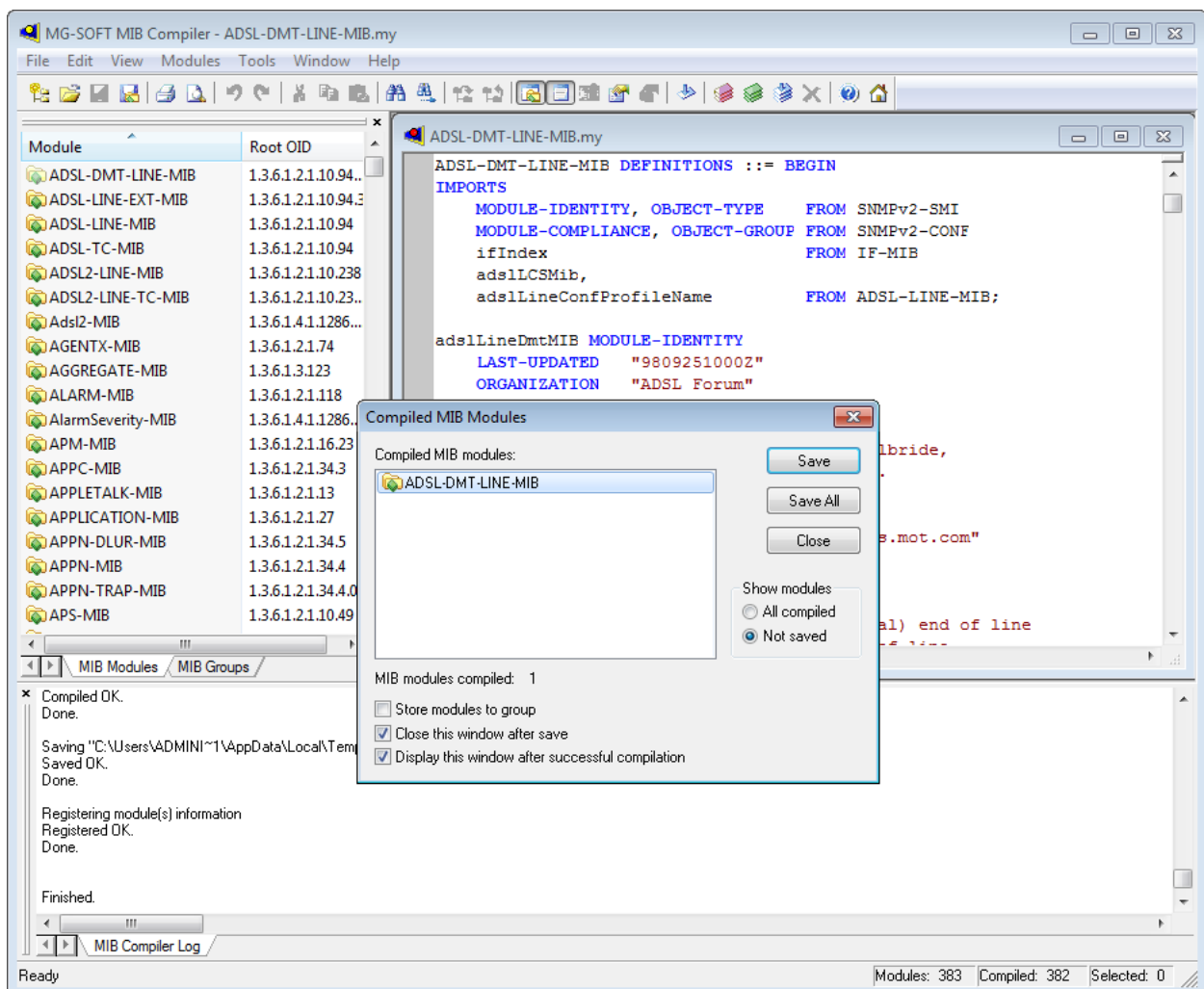


Figure 87: Compiling MIB files with MG-SOFT MIB Compiler

8.3 Manually Loading MIB Modules in MIB Browser

Once a MIB file is compiled, you can load it in MIB Browser. To load a MIB module:

1. In MIB Browser's main window, switch to the **MIB** tab.
2. In the lower window panel, switch to the **MIB Modules** tab.
3. Click the **Refresh Contents of the MIB Module Lists** button located in the middle section of the MIB tab.
4. In the lower window panel (MIB Modules tab), select the desired MIB module from the list by clicking its name (Figure 88).

Tip: To select more than one MIB module, hold down the **Ctrl** key on the keyboard and click the desired MIB file names.

5. To quickly find MIB modules by their names, use the **Live search** tool, as described in the [next section](#).
6. To load the selected MIB module, simply double-click it, or use the **Load Selected MIB Modules** button located in the central section of the MIB tab or the **Load** pop-up command (Figure 88).
7. MIB Browser loads the selected MIB module and displays it in the list of loaded MIB modules in the upper panel.

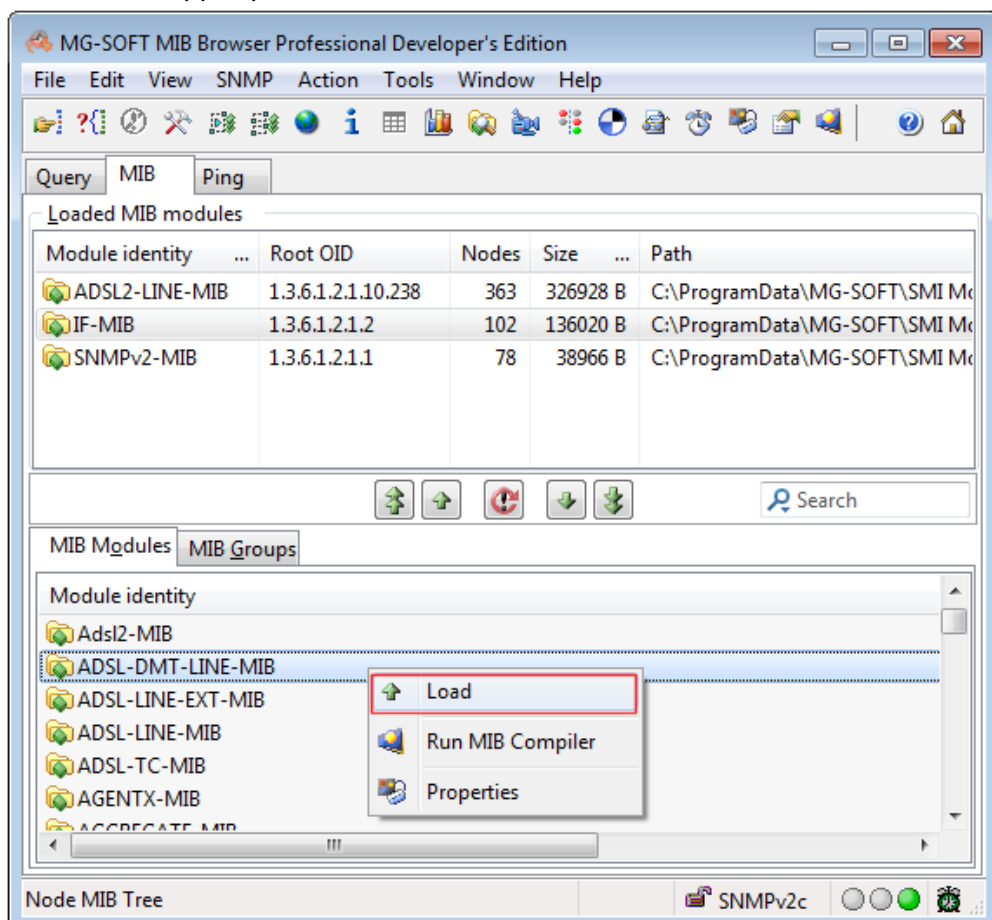
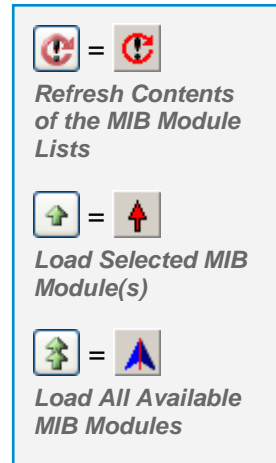
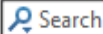



Figure 88: Loading MIB modules

8.4 Searching for MIB Modules

The **MIB** tab of the main window contains the convenient **Live search** tool . The Live search tool lets you perform incremental text search to quickly find and display only those MIB modules that match the search criteria, i.e., contain the entered text in any of the selected columns. Search can be performed within three categories of items: loaded MIB modules, not loaded MIB modules and MIB groups.

To quickly find one or more MIB modules by the name:

1. In MIB Browser's main window, switch to the **MIB** tab.
2. In the **Live search** tool located in the middle-right section of the MIB tab, click the search symbol (.
3. The **Search Options** drop-down menu is displayed ([Figure 89](#)).

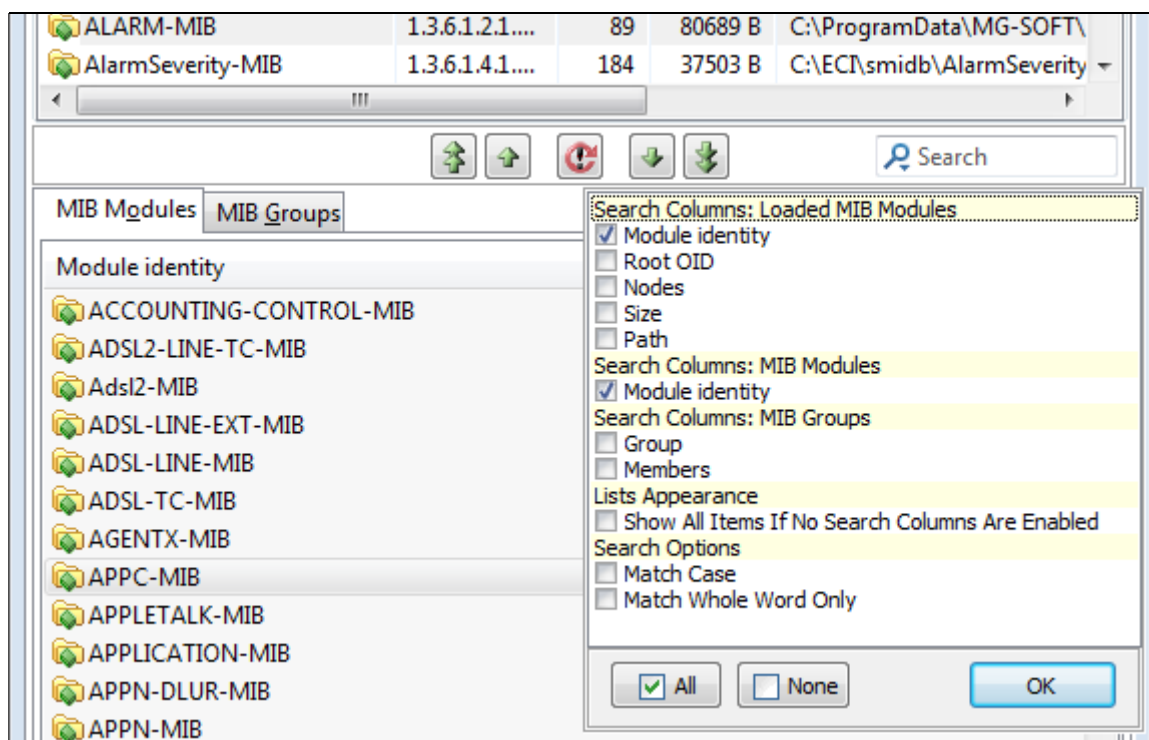


Figure 89: Setting the Live search options in the MIB tab of the main window

4. In the Search Options drop-down menu, select the desired search options by checking the checkboxes in front of them. First, select the columns you wish to search in. For example, to search by MIB module name (identity) in the group of loaded and not-loaded MIB modules, select the **Module identity** column in both categories ([Figure 89](#)). Click the **OK** button at the bottom of the Search Options drop-down menu to close it and apply the changes.

Select the **Match case** search option to make the search case sensitive. If this option is enabled, the search will find only those strings in which the capitalization matches the one used in the search query (e.g., ADSL will find ADSL, but not Adsl).

Select the **Match whole word only** search option to find only those strings that are whole words and not part of a larger word (e.g., `ads1` will find `ads1` and `ads1-line`, but not `ads12`).

- Click inside the Live search box and start typing the search query. The Live search tool automatically performs incremental search as you type the characters into the search box and progressively updates the list of narrowed results in the upper and lower window panels (if search is enabled in both panels).

For example, to find all MIB modules that **contain** the word `NOTIFICATION` in their names, start typing the word “notification” into the Live search tool and stop when you are satisfied with the results (e.g., `notif`). The upper and lower window panels will display all MIB modules that contain the entered text anywhere in the name (Figure 90).

- The search results (total number of matches) is displayed in front of the Live search tool. Place your mouse pointer over the search results to display a tooltip (Figure 90). with more detailed search results (number of matches in each category).

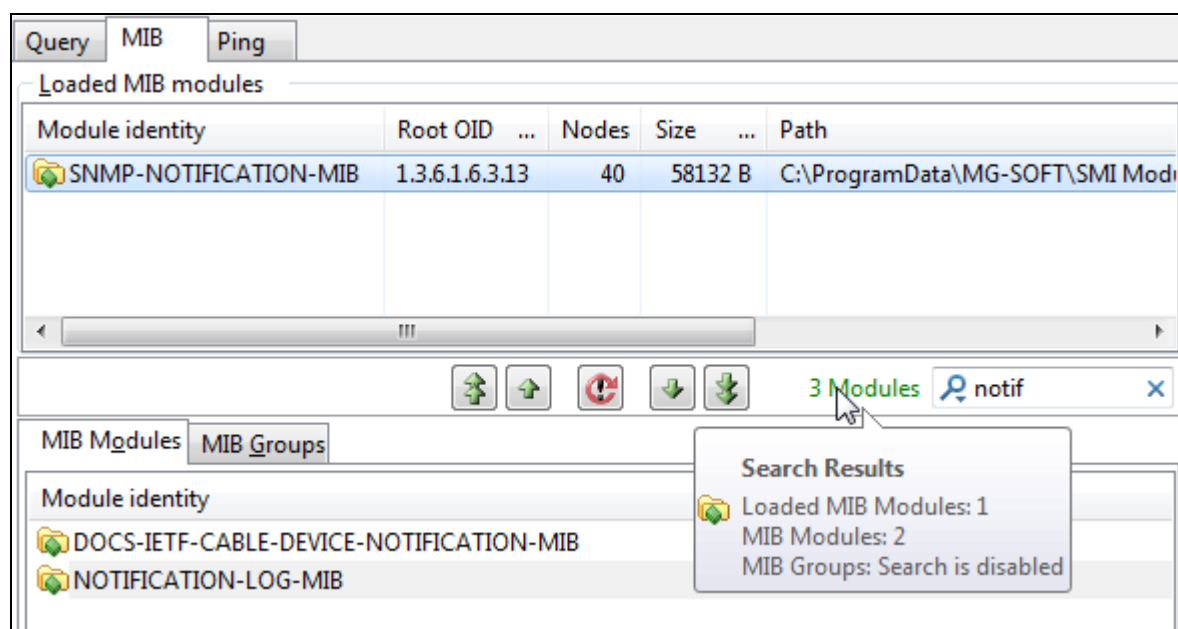


Figure 90: Viewing the search results in the MIB tab of the main window

- To load the found MIB modules, select them in the lower window panel and click the **Load Selected MIB Modules** button located in the central section of the MIB tab or select the **Load** pop-up command (Figure 88).
- To unload the found MIB modules, select them in the upper window panel and click the **Unload Selected MIB Modules** button located in the central section of the MIB tab or select the **Unload** pop-up command.
- To cancel the search, click the **Cancel Current Search** symbol (✕) in the Live search box or delete the text from it.

8.5 Saving MIB Modules to MIB Group

For more effective MIB module management, you can save two or more MIB modules to a MIB group and later load all MIB modules from that group with a single click of a button.

1. In MIB Browser's main window, switch to the **MIB** tab.
2. In the lower panel (MIB Modules tab), select any number of MIB modules that you wish to save to a MIB group. Load them into MIB Browser by using the **Load** pop-up command.
3. When loading is completed, the list of loaded MIB modules appears in the Loaded MIB Modules frame (upper panel).
4. Right-click inside the Loaded MIB Modules frame and select the **Save MIB Group** pop-up command.
5. The Enter New Group Name dialog box appears (Figure 91).
6. Specify the name for the new group and click the **OK** button.
7. The new MIB group with a list of MIB modules appears in the MIB Groups view.

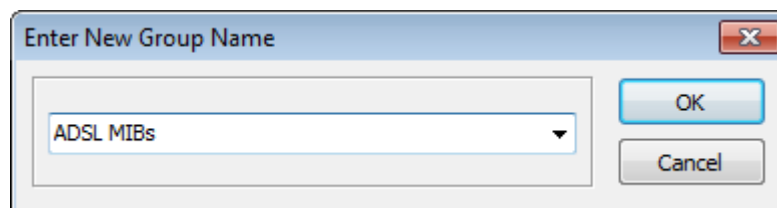


Figure 91: Enter New Group Name dialog box

8.5.1 Loading MIB Group

To load the saved group of MIB modules into MIB Browser:

1. In MIB Browser's main window, switch to the **MIB** tab.
2. In the **MIB Groups** tab view, right-click the MIB group that you wish to load and select the **Load** pop-up command (Figure 92).
3. MIB Browser loads all MIB modules saved in the selected MIB group.

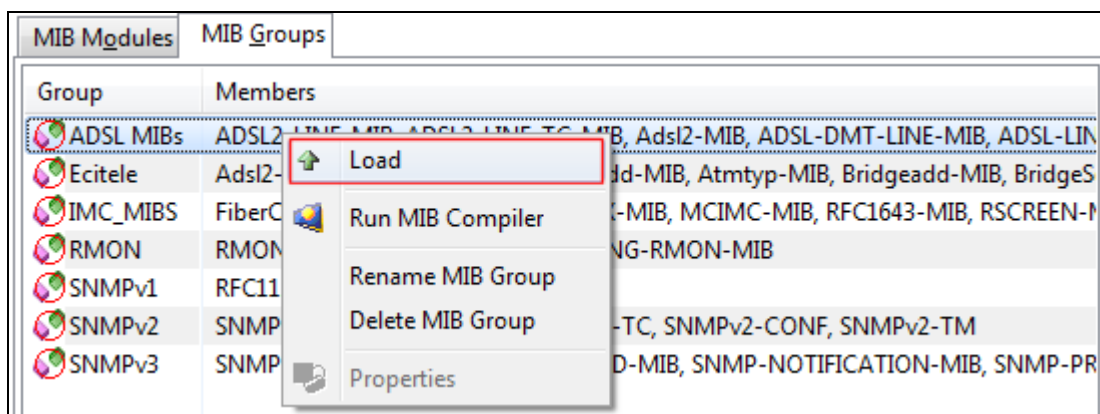


Figure 92: MIB Groups view pop-up menu

8.5.2 Renaming MIB Group

You can change the name of any group in the MIB Groups view.

1. In the main window, switch to the **MIB** tab.
2. Right-click the MIB group that you wish to rename and select the **Rename MIB Group** pop-up command.
3. Enter the new name of the MIB group into the label.

8.5.3 Deleting MIB Group

1. In the main window, switch to the **MIB** tab.
2. Right-click the MIB group that you wish to delete and select the **Delete MIB Group** pop-up command. Confirm the deletion by clicking the **Yes** button.

8.6 Checking MIB Module Properties

With MIB Browser you can check the properties of compiled MIB modules. MIB module properties are displayed in the Module Database Properties window.

To see the properties of a MIB module:

1. Switch to the **MIB** tab in the main window.
2. In the upper or lower panel of the MIB tab, select a MIB module by right-clicking it.
3. In the displayed pop-up menu, click the **Properties** command ([Figure 93](#)).

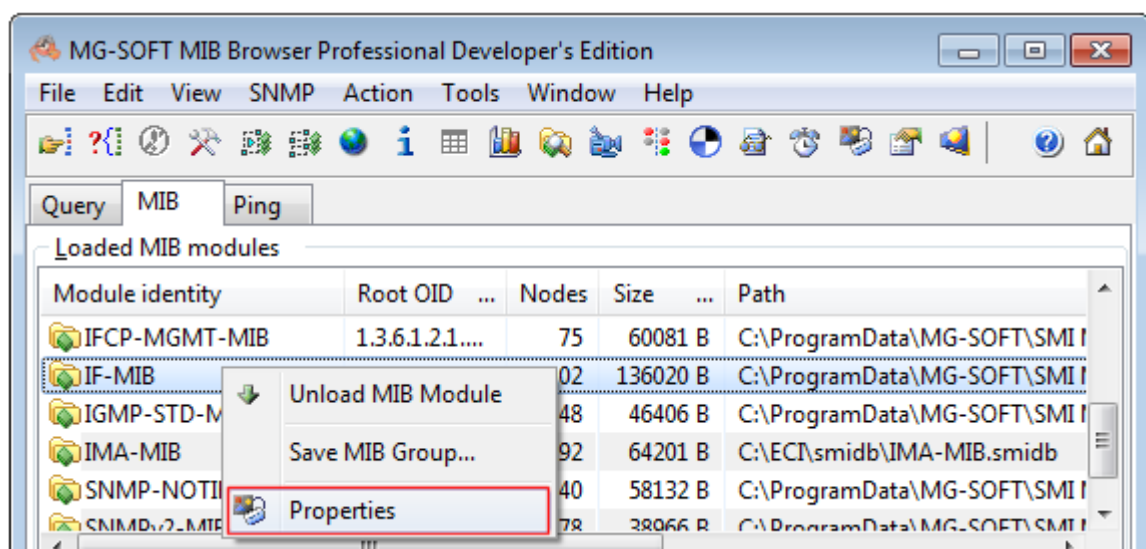


Figure 93: MIB tab with loaded MIB modules and a displayed pop-up menu

4. The Module Database Properties window opens ([Figure 94](#)).

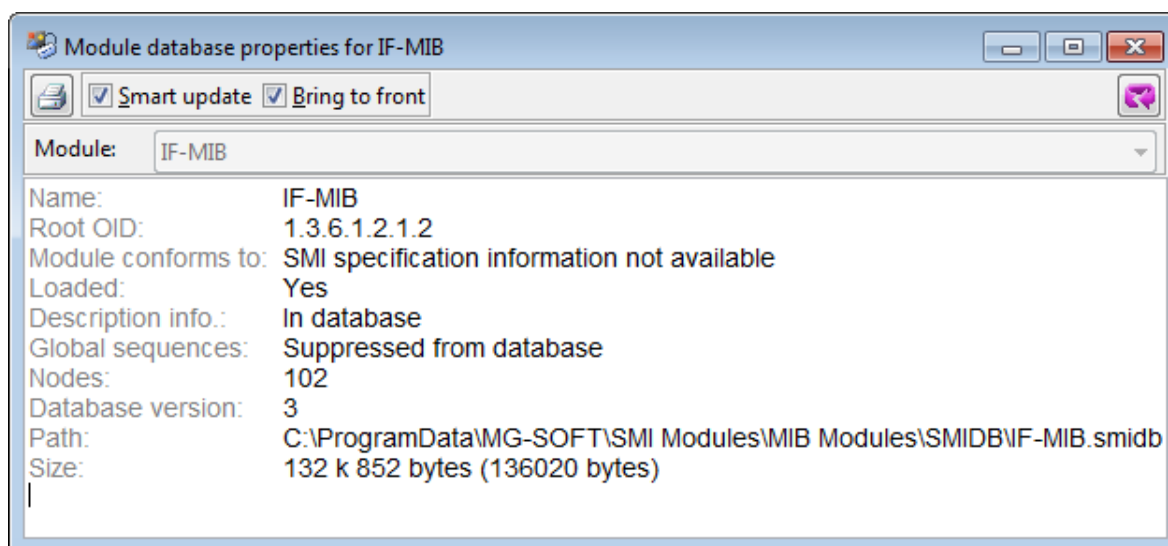


Figure 94: Module Database Properties window

5. The Module Database Properties window shows properties of the selected MIB module (e.g., IF-MIB).

Note: The *Module* drop-down list is disabled showing the name of the currently selected MIB module.

Tip: The Module Database Properties window can be used also for viewing properties of MIB modules that are listed in the Scan Agent For Implemented MIB Modules window. See the [Scan SNMP Agent for Implemented MIB Modules](#) section.

9 QUERY OBJECT INSTANCES BY USING SNMP GET REQUESTS

With MIB Browser, you can send SNMP Get requests to remote SNMP agents and in this way retrieve values of managed information from any SNMP manageable device on the network. SNMP Get requests are used when OID values of the queried object instances are already known.

In this section, you will learn how to use the SNMP Get operation to retrieve information from arbitrary SNMP devices on the network.

9.1 SNMP Get Requests for Scalar Objects

1. In the main window, switch to the **Query** tab.
2. Into the **Remote SNMP Agent** drop-down list, specify the IP address of the remote SNMP agent that you wish to manage.
3. If necessary, adjust SNMP access parameters in the SNMP Protocol Preferences dialog box (see the [Specify SNMP Protocol Parameters](#) section).
4. Contact the remote SNMP agent by using the **SNMP / Contact** command.
5. In the MIB tree, select the scalar object (🟢) that you wish to query.

Tip: If the desired scalar object is not present in the MIB tree, [load the MIB module](#) that defines it (e.g., to be able to select a scalar object from the MIB-II “system” subtree, load the SNMPv2-MIB or the RFC1213-MIB module).

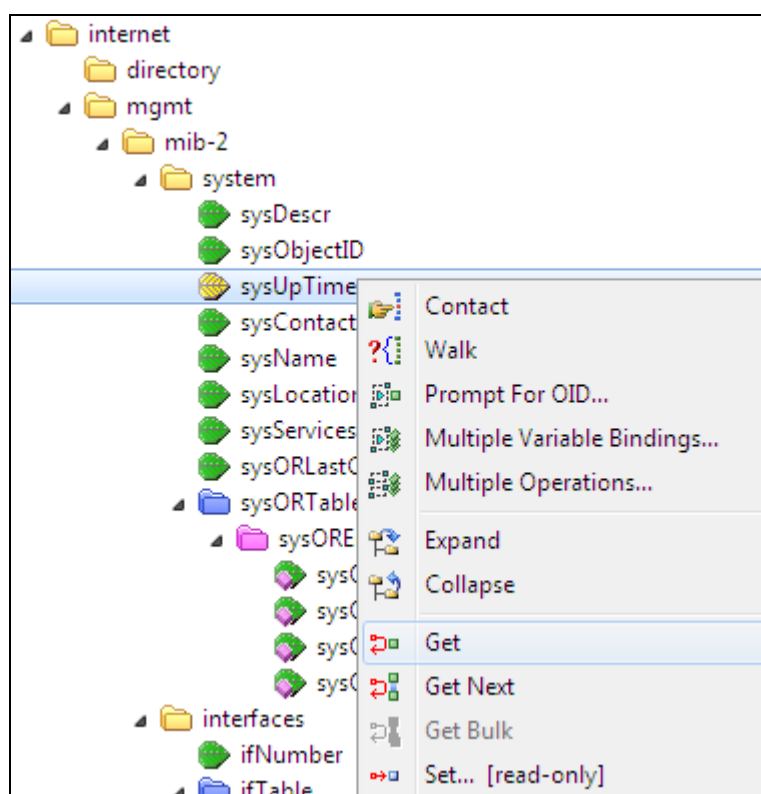


Figure 95: Selecting the SNMP Get command on a scalar object in the MIB tree

6. Select the **SNMP / Get** command from the main menu or right-click the scalar object and choose the **Get** command from the pop-up (context) menu (Figure 95).
7. MIB Browser sends an SNMP Get request with the selected object to the SNMP agent.
8. In response it receives the value of the queried object instance and displays it in the Query Results panel (Figure 96).

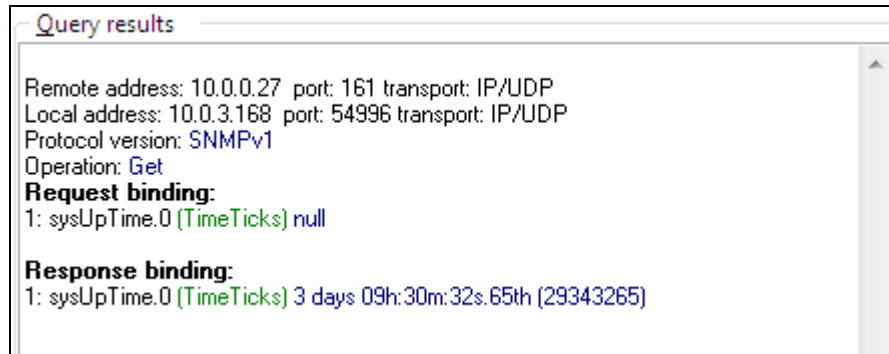


Figure 96: Viewing the SNMP Get operation request and response in the Query results panel

Note: If the selected object is not implemented in the queried SNMP agent, MIB Browser prints an error code, which it receives from the queried SNMP agent.

9.2 SNMP Get Requests for Columnar Objects

If the selected node in the MIB tree is not a scalar but a columnar object, the procedure is different. In this case you have to specify the instance of the selected columnar object (e.g., `ifDescr` object) that the program should query (e.g., `ifDescr.9`).

1. To contact an SNMP agent, repeat steps 1-4 described in the [SNMP Get Requests for Scalar Objects](#) section.
2. After you have contacted the agent, expand the MIB tree and select the columnar object (🌿) that you wish to query (Figure 97).

Tip: If the desired columnar object is not present in the MIB tree, [load the MIB module](#) that defines it (e.g., to be able to select a columnar object from the MIB-II "ifTable", load the IF-MIB or the RFC1213-MIB module).

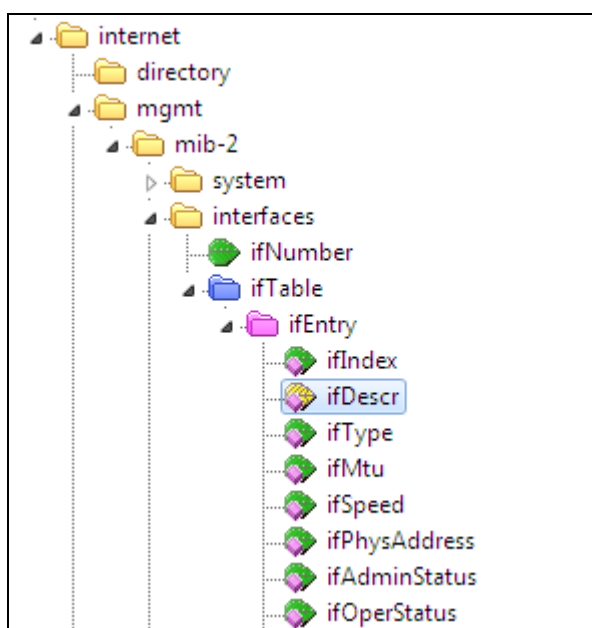


Figure 97: Selecting a columnar object in the MIB tree

3. Select the **SNMP / Get** command from the main menu or the **Get** command from the pop-up menu. In both cases the sub menu of the **Get** command appears (Figure 98).

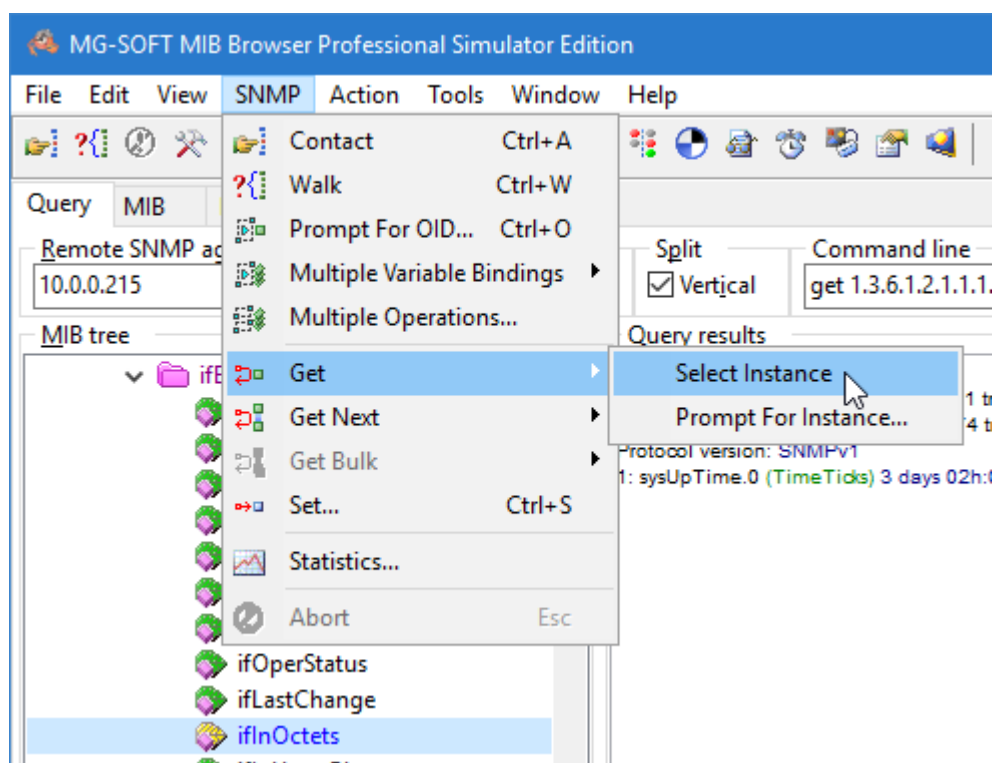


Figure 98: SNMP Get command and its sub menu

4. When the selected MIB tree node is a columnar object, you have to specify its instance. To specify the instance, in the sub menu of the **Get** command choose between:

- ❑ **Select Instance** - If you select this command, MIB Browser will search for all available instances of the selected object and display them in the Select Table Instance(s) window (Figure 99). You should pick one instance from the list and double-click it, or click the **Use Selected Instances** toolbar button.

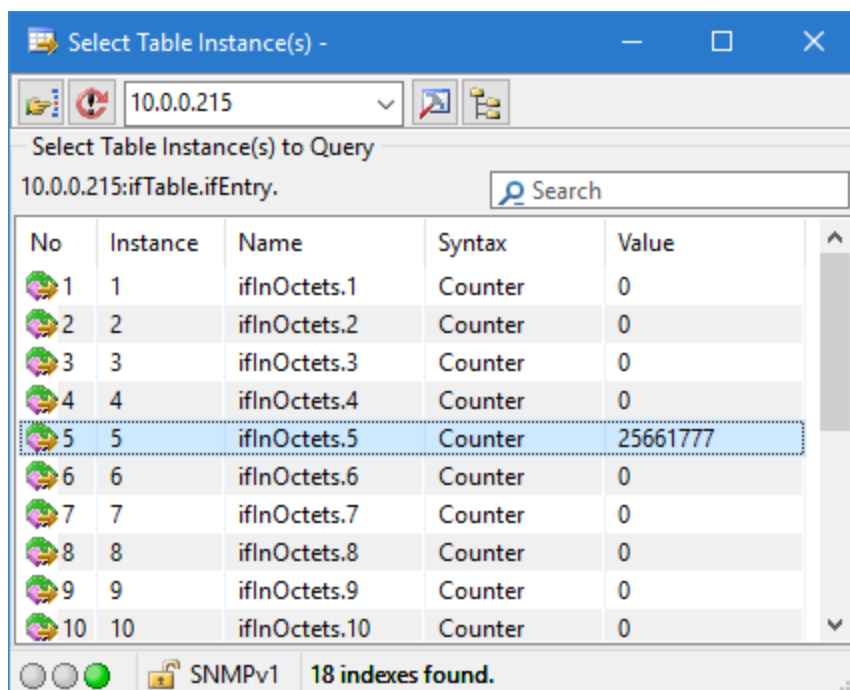
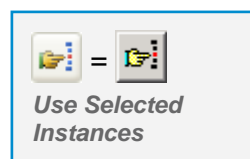


Figure 99: Selecting a columnar object instance in the Select Table Instance(s) window

- ❑ **Prompt For Instance** - If you select this command, MIB Browser will open the Instance To Query dialog box (Figure 100). You should specify the desired instance and click the **OK** button.

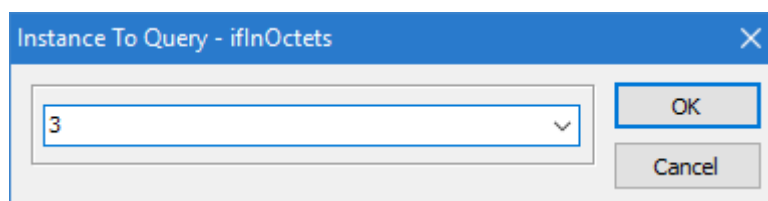


Figure 100: Specifying a columnar object instance in the Instance To Query dialog box

5. MIB Browser queries the specified instance of the selected columnar object with the SNMP Get request and displays its value in the Query Results panel.

Example:

How to use the SNMP Get operation to check the number of octets received on a selected interface by a particular SNMP agent?

First, contact the SNMP agent by using the **SNMP / Contact** command. In the displayed MIB tree, click the `ifInOctets` columnar node in the SNMP table called `ifTable`. Use the **SNMP / Get / Select Instance** command. The Select Table Instance dialog box appears (Figure 99) and displays a list of indexes of available instances. Choose the index (e.g., number 3) specifying the interface that you wish to query and double-click it. The Select Table Instance dialog box closes. MIB Browser queries the selected object instance (`ifInOctets.3`) with the SNMP Get request and displays its value (the total number of octets received on the selected interface) in the Query Results panel (Figure 101).

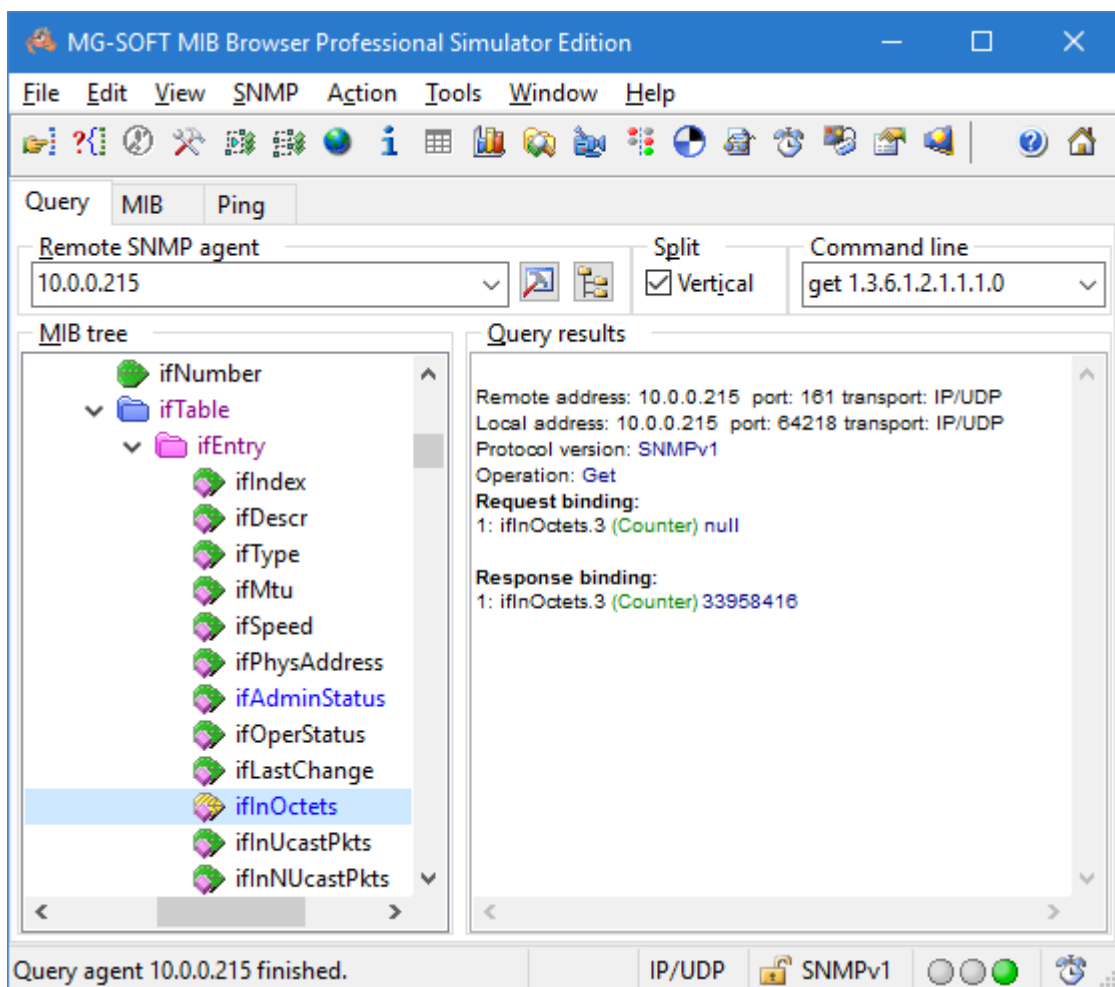


Figure 101: Number of octets received on the selected device displayed in the Query Results panel

10 QUERY OBJECT INSTANCES BY USING SNMP GETNEXT REQUESTS

By using the SNMP GetNext request you can query an object instance in an SNMP agent that in lexicographical order follows the instance of the object that you have selected in the MIB tree.

10.1 SNMP GetNext Request for Scalar Objects

1. In the main window, switch to the **Query** tab.
2. Into the **Remote SNMP Agent** drop-down list, specify the IP address of the remote SNMP agent that you wish to manage.
3. If necessary, adjust SNMP access parameters in the SNMP Protocol Preferences dialog box (see the [Specify SNMP Protocol Parameters](#) section).
4. Contact the remote SNMP agent by using the **SNMP / Contact** command.
5. Expand the MIB tree and select one scalar object (e.g., `sysUpTime`, [Figure 102](#)). Note that by using the SNMP GetNext operation, you will not receive in response the value of the selected object instance (e.g., `sysUpTime`) but of the object instance that in lexicographical order follows the selected one (e.g., `sysContact`).

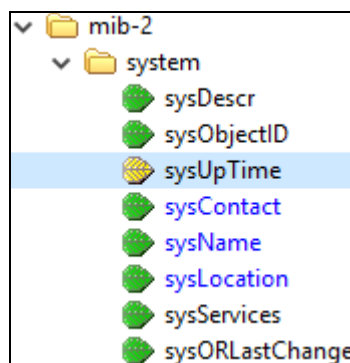


Figure 102: Selecting a scalar object

6. Select the **SNMP / Get Next** command from the main menu or right-click the scalar object and choose the **GetNext** command from the pop-up menu.
7. The value of the object instance that in lexicographical order follows the instance of the selected object is displayed in the Query Results panel.

10.2 SNMP GetNext Request for Columnar Objects

If the selected node in the MIB tree is a columnar object (e.g., `ifInOctets`), you have to specify, which of its instances the program should query (e.g., `ifInOctets.9`). Note that when you query an instance of a columnar object with the SNMP GetNext request, the agent does not return the value of the selected instance (e.g., `ifInOctets.9`) but of the next instance (e.g., `ifInOctets.10`) that is implemented in the table.

1. To contact an SNMP agent, repeat steps 1-4 described in the [SNMP GetNext Request for Scalar Objects](#) section.
2. After you have contacted the agent, expand the MIB tree and click the columnar object that you wish to query.
3. Use the **SNMP / Get Next** command from the main menu or right-click the columnar object and choose the **GetNext** command from the pop-up menu. A sub menu of the **GetNext** command appears ([Figure 103](#)).

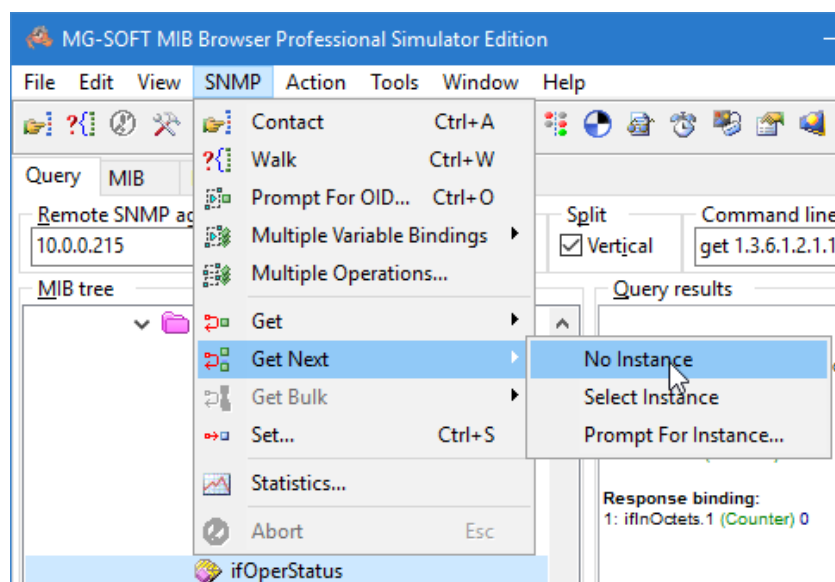


Figure 103: SNMP GetNext command and its sub menu

4. When the selected MIB tree node is a columnar object, you have to specify its instance. To specify the instance, in the sub menu of the **GetNext** command choose between:
 - ❑ **No Instance** - MIB Browser queries the first instance of the selected columnar object.
 - ❑ **Select Instance** - MIB Browser displays a list of all available instances for the selected columnar object in the Select Table Instance(s) window ([Figure 99](#)). Select the desired instance by double-clicking it.
 - ❑ **Prompt for Instance** - MIB Browser opens the Instance To Query dialog box ([Figure 100](#)). Specify the desired instance and click the **OK** button.
5. MIB Browser sends an SNMP GetNext request with the specified object instance and in response returns the value of the next instance. It displays the results in the Query Results panel.

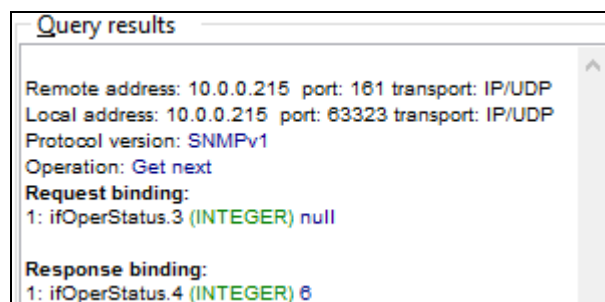


Figure 104: SNMP GetNext request and response

Example:

What is the difference between SNMP Get and SNMP GetNext operations if you perform them on the same node (e.g., on the `sysName` node to retrieve the administratively assigned name of a managed device)?

The difference between SNMP Get and SNMP GetNext operation is in the response you receive from the SNMP agent.

Through this example you will see that SNMP Get operation returns the value of the instance of the object that has been selected in the MIB tree and whose OID has been sent in request to the SNMP agent. Meanwhile, SNMP GetNext operation does not return the instance value of the selected object, whose OID is sent in request, but of the object that in lexicographical order follows the selected object.

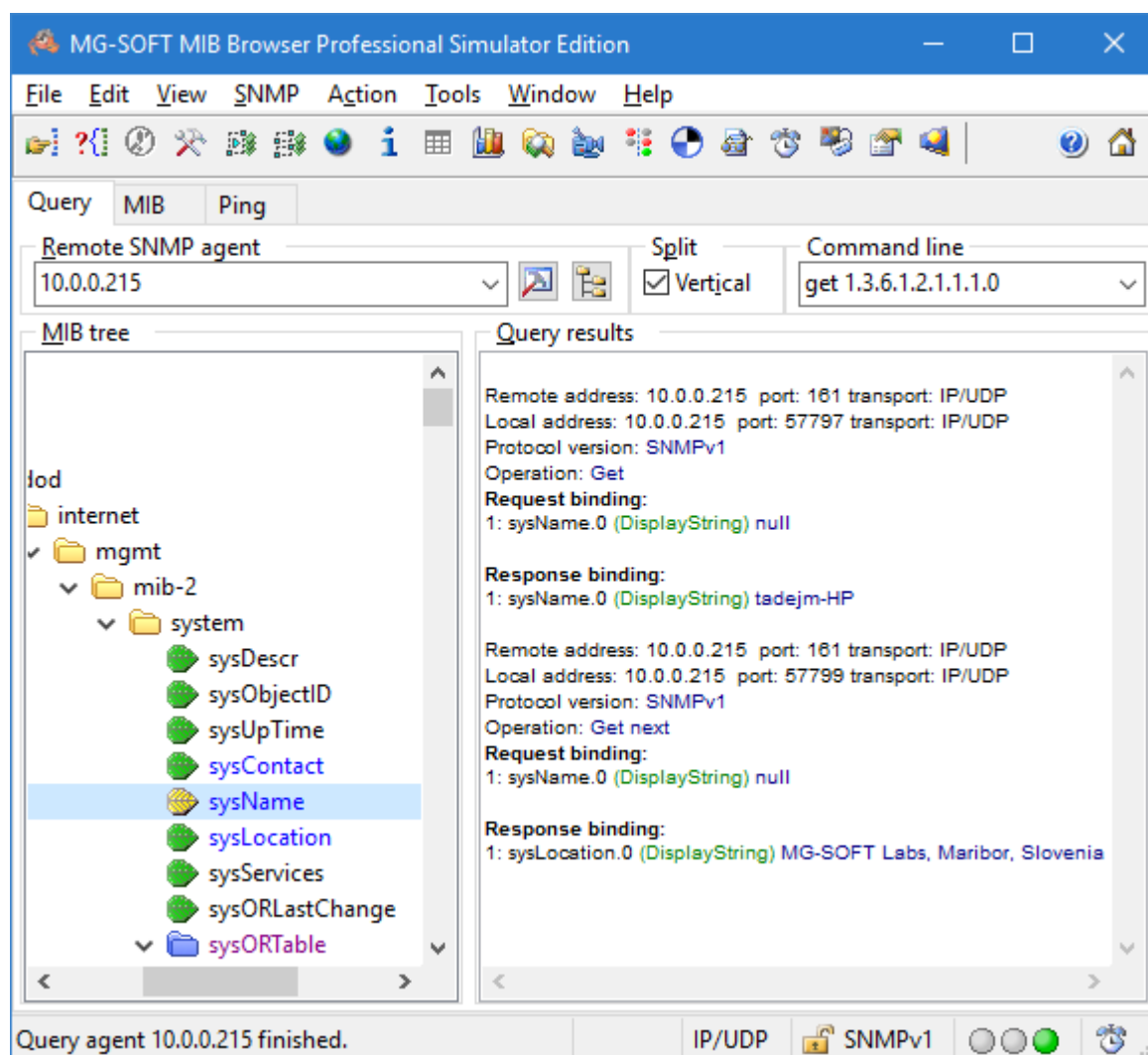


Figure 105: SNMP Get and SNMP GetNext operation on the `sysName` node

To retrieve the value of the `sysName` object with the SNMP Get operation, first contact the SNMP agent by using the **SNMP / Contact** command. Then click the `sysName` node in the MIB tree and use the **SNMP / Get** command. MIB Browser sends the SNMP Get request for the selected object (`sysName.0`) to the SNMP agent. In response it gets the

value of the instance of the selected object (`sysName.0`) and displays it in the Query Results panel (Figure 105). In this case, the returned value is an administratively assigned name of the managed device (e.g., `CiscoSwitch1`).

To see the difference between SNMP Get and SNMP GetNext operation, click the `sysName` node again and this time use the **SNMP / GetNext** command. MIB Browser sends the SNMP GetNext request for the selected object (`sysName.0`) to the SNMP agent. The agent does not return the instance value of the selected object but of the next object (`sysLocation.0`) in lexicographical order implemented in the device. The results are displayed in the Query Results panel (e.g., `MG-SOFT Labs, Maribor`, Figure 105).

11 QUERY OBJECT INSTANCES BY USING COMMAND LINE INTERFACE

MIB Browser main window incorporates the convenient **Command line** interface for performing SNMP querying operations. It lets you easily retrieve the desired information from any SNMP device by entering the SNMP operation type and the requested OID (e.g., "get sysUpTime.0" or "get 1.3.6.1.2.1.1.3.0") into the Command line input line. Any type of querying operation (Get, GetNext, GetBulk, Walk) can be used on any OID implemented in remote SNMP agents, without the need to have the MIB module(s) that define the respective OIDs. Of course, having these MIB modules loaded in MIB Browser is an advantage, as it enables resolving OIDs to human-readable names, and lets you perform the commands on the currently selected node (OID) in the MIB tree.

Supported command line commands and parameters:

Long	Short	Parameters	Description
contact	c		Contact remote SNMP agent
walk	w		Walk
get	g	[object1]...[objectN]	Get
getnext	n, gn	[object1]...[objectN]	GetNext
getbulk	b, gb	[object1]...[objectN]	GetBulk
clear	cl		Clear Query Results window
help	h, ?		Print this help

Parameters in angle brackets [] are optional. If omitted, the OID of the currently selected object in the MIB tree is used as a parameter.

11.1 Using SNMP Get Command

One can use the SNMP **get** command by either explicitly or implicitly specifying the OID to be retrieved. The first method involves typing/pasting the object instance to be retrieved as a parameter into the command line, while the second method requires selecting the desired object in the MIB tree and then entering only the get (or getnext or getbulk) command to the command line. The advantage of the former method is that it allows querying arbitrary OIDs, even if you do not have the MIB modules that define these OIDs.

Using Get Command without Using the MIB Tree

1. In the main window, switch to the **Query** tab.
2. Into the **Remote SNMP Agent** drop-down list, specify the IP address of the remote SNMP agent that you wish to manage.
3. If necessary, adjust SNMP access parameters in the SNMP Protocol Preferences dialog box (see the [Specify SNMP Protocol Parameters](#) section).

4. Into the **Command line** drop-down list, enter the **get** command and the **OID** of the object instance you wish to query and press the **Enter** key, e.g.:

```
get 1.3.6.1.2.1.1.6.0
```

or, if the MIB module that defines the requested OID is loaded in MIB Browser:

```
get sysLocation.0
```

Note: To successfully retrieve the value of an object instance by using the SNMP **Get** operation, you need to specify the exact instance of the object to be queried (e.g., append **.0** instance to the OID/name of the scalar object or whatever instance of the columnar object you want to retrieve, e.g., **.1**, **.2**, ...).

Tip: You can also use the short version of the command, e.g.:

```
g 1.3.6.1.2.1.1.6.0
```

or (if the MIB module that defines the requested OID is loaded in MIB Browser):

```
g sysLocation.0
```

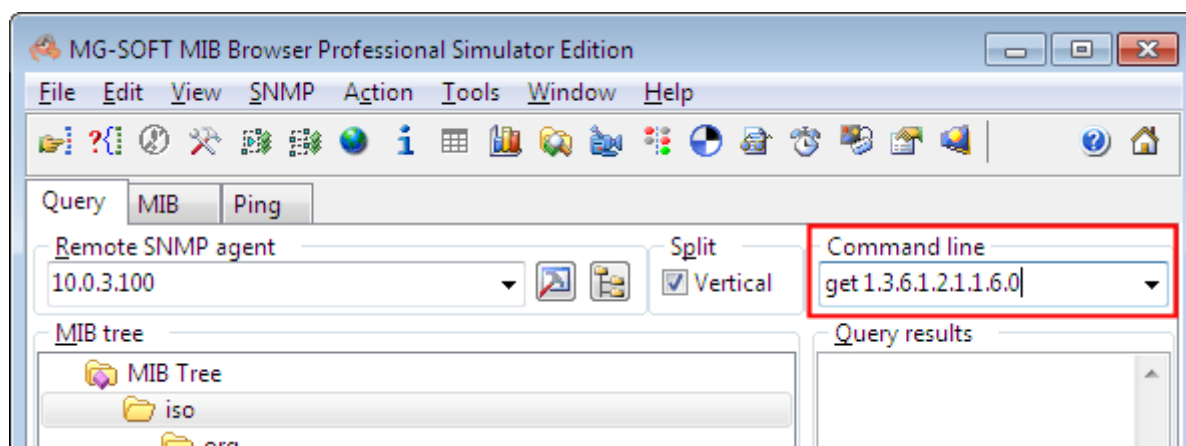


Figure 106: Entering a get command into the Command line drop-down list

5. MIB Browser queries the specified object instance by means of the SNMP Get request and displays the results in the Query results window panel.

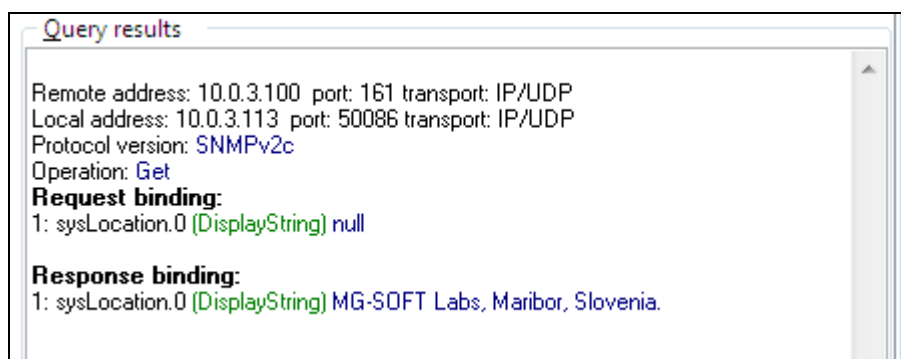


Figure 107: Viewing results of a get command into the Query results window panel

Using Get Command on Objects Selected in the MIB Tree

1. In the main window, switch to the **Query** tab.
2. Into the **Remote SNMP Agent** drop-down list, specify the IP address of the remote SNMP agent that you wish to manage.
3. If necessary, adjust SNMP access parameters in the SNMP Protocol Preferences dialog box (see the [Specify SNMP Protocol Parameters](#) section).
4. In the MIB tree, select the leaf object, that you wish to query (e.g., sysLocation).

Tip: If the desired object is not present in the MIB tree, [load the MIB module](#) that defines it (e.g., to be able to select a scalar object from the MIB-II “system” subtree, load the SNMPv2-MIB or the RFC1213-MIB module).

Note: If you select a scalar object (🟢) in the MIB tree, MIB Browser automatically appends the instance (.0) to the OID of the scalar object when the Get operation is performed. If you select a columnar object (🟡) in the MIB tree, MIB Browser will prompt you with the Select Table Instance dialog box to select the instance of the columnar object to be retrieved.

5. Into the **Command line** drop-down list, enter the **get** command and press the **Enter** key.

Tip: You can also use the short version of the command, e.g.:

g

6. MIB Browser queries the selected object instance by means of the SNMP Get request and displays the results in the Query results window panel.

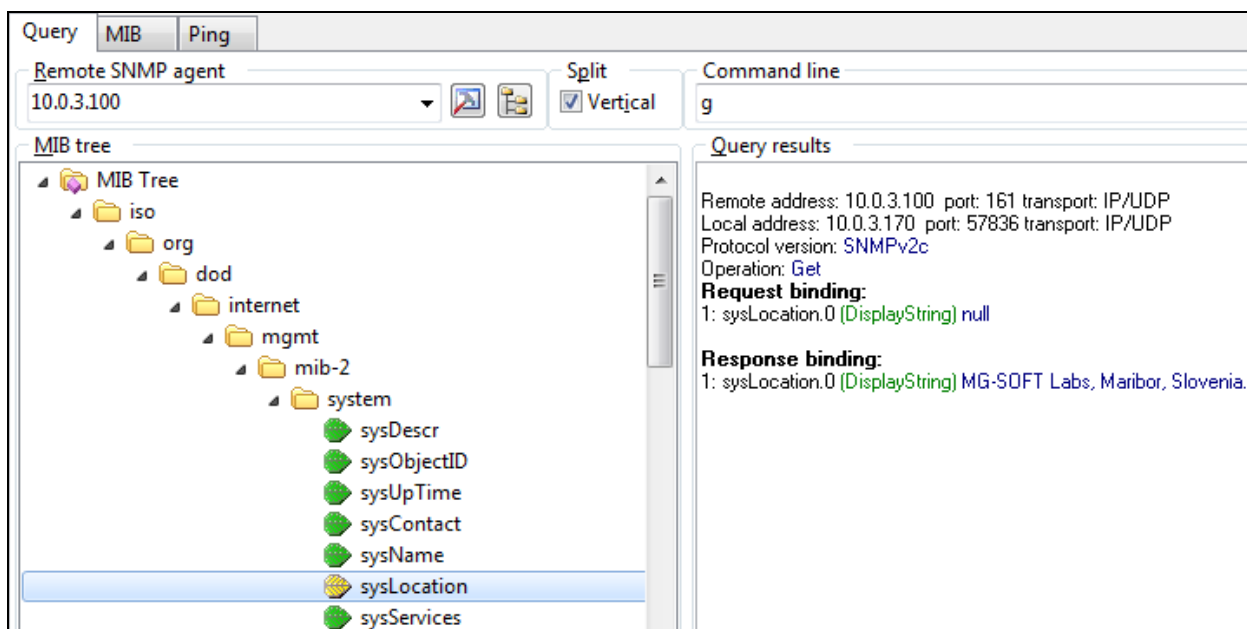


Figure 108: Using the get command while object is selected in the MIB tree

11.2 Using SNMP GetNext Command

This section describes how to use the **getnext** command by specifying the OID to be included into the SNMP GetNext message as a command line parameter. Alternatively, one can perform the GetNext operation also by selecting an object (node) in the MIB tree and then entering only the getnext command into the command line, as described for the [get command](#).

1. In the main window, switch to the **Query** tab.
2. Into the **Remote SNMP Agent** drop-down list, specify the IP address of the remote SNMP agent that you wish to manage.
3. If necessary, adjust SNMP access parameters in the SNMP Protocol Preferences dialog box (see the [Specify SNMP Protocol Parameters](#) section).
4. Into the **Command line** drop-down list, enter the **getnext** command and the **OID** to be include into the GetNext message and press the **Enter** key, e.g.:

```
getnext 1.3.6.1.2.1.1.4
```

or, if the MIB module that defines the requested OID is loaded in MIB Browser:

```
getnext sysContact
```

Note: Note that the SNMP **GetNext** operation retrieves the first OID that in lexicographical order follows the specified OID. For example, to retrieve the value of the `sysLocation.0` object instance, enter the name or OID of the object (`1.3.6.1.2.1.1.4` or `sysContact`) **without the instance identifier (.0)** into the Command line.

Note that one can specify any OID as a parameter of the GetNext command, for example, `getnext 1.3` and `getnext org` are both valid GetNext commands.

Tip: You can also use a shorter version of the command, e.g.:

```
gn 1.3.6.1.2.1.1.4
```

or

```
n sysContact
```

5. MIB Browser sends an SNMP GetNext request containing the specified OID to the remote SNMP agent and displays the results in the Query results window panel:

```
Remote address: 10.0.3.100 port: 161 transport: IP/UDP
Local address: 10.0.3.163 port: 59525 transport: IP/UDP
Protocol version: SNMPv2c
Operation: GetNext
Request binding:
1: sysContact (DisplayString) null
```

```
Response binding:
1: sysContact.0 (DisplayString) admin@mg-soft.com
```

11.3 Using Walk Command

This section describes how to use the **walk** command in the command line interface.

1. In the main window, switch to the **Query** tab.
2. Into the **Remote SNMP Agent** drop-down list, specify the IP address of the remote SNMP agent that you wish to manage.
3. If necessary, adjust SNMP access parameters in the SNMP Protocol Preferences dialog box (see the [Specify SNMP Protocol Parameters](#) section).
4. In the MIB tree, select the object, which the Walk operation should start from (e.g., internet)

Tip: If the desired object is not present in the MIB tree, [load the MIB module](#) that defines it (e.g., to be able to select the “internet” node, load the SNMPv2-MIB or the RFC1213-MIB module).

5. Into the **Command line** drop-down list, enter the **walk** command and press the **Enter** key.

Tip: You can also use the short version of the command, e.g.:

w

6. MIB Browser performs the Walk operation from the selected object and displays the retrieved object instances and their values in the Query results window panel.

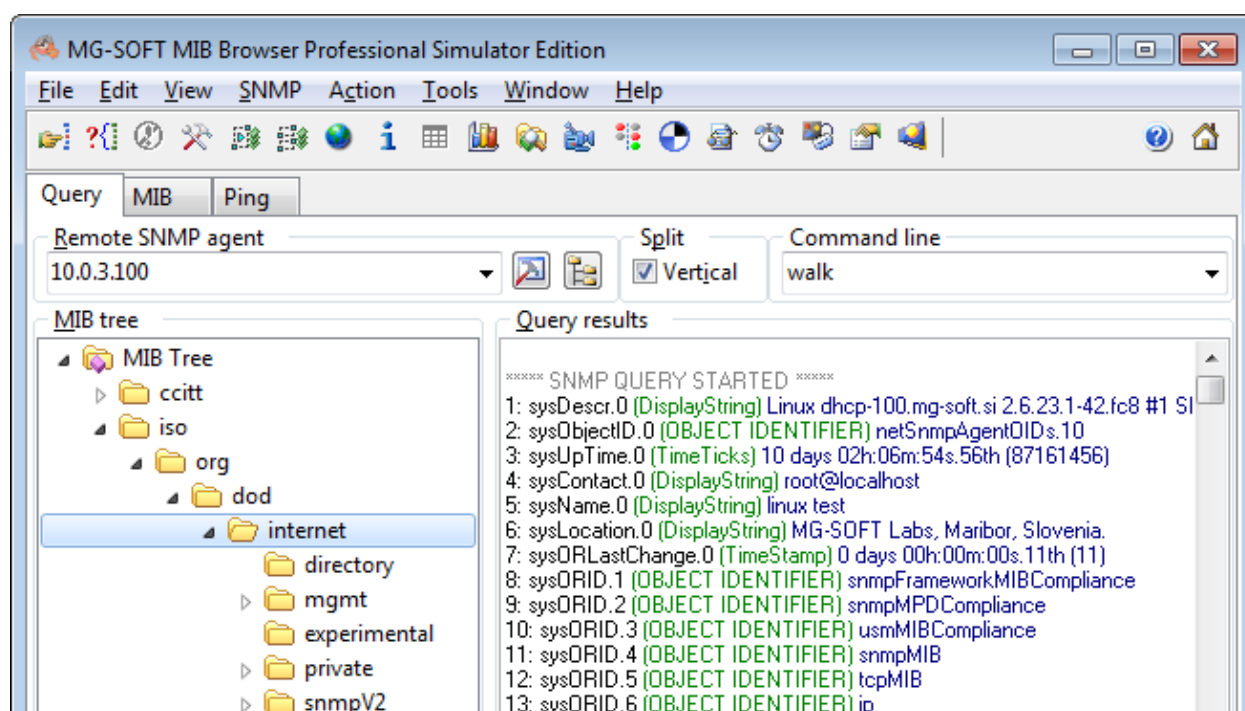


Figure 109: Running the Walk command on the selected subtree

11.4 Retrieving Multiple Object Instances with One Request

The command line interface lets you retrieve more than one object instance with a single SNMP request, as described in this section.

11.4.1 Using Get Command with Multiple Variable Bindings

*Example: How to query 3 object instances (sysUpTime.0 ifInOctets.1 ifInOctets.2) with one **get** command:*

1. Enter the following command into the **Command line** drop-down list and press the **Enter** key:

```
get 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.2.2.1.10.1 1.3.6.1.2.1.2.2.1.10.2
```

or, if the MIB modules that define the requested OIDs are loaded in MIB Browser:

```
get sysUpTime.0 ifInOctets.1 ifInOctets.2
```

2. MIB Browser will send an SNMP Get request containing multiple (i.e., 3) variable bindings in the variable bindings list and display the retrieved values in the Query results window panel:

```
Remote address: 10.0.3.100 port: 161 transport: IP/UDP
Local address: 10.0.3.170 port: 57256 transport: IP/UDP
Protocol version: SNMPv2c
Operation: Get
```

Request bindings:

```
1: sysUpTime.0 (TimeTicks) null
2: ifInOctets.1 (Counter) null
3: ifInOctets.2 (Counter) null
```

Response bindings:

```
1: sysUpTime.0 (TimeTicks) 8 days 22h:27m:43s.00th (77206300)
2: ifInOctets.1 (Counter) 3581578
3: ifInOctets.2 (Counter) 695377014
```

11.4.2 Using GetNext Command with Multiple Variable Bindings

*Example: How to query 3 object instances (sysUpTime.0 ifInOctets.1 ifInOctets.2) with one **getnext** command:*

1. Enter the following command into the **Command line** drop-down list and press the **Enter** key:

```
getnext 1.3.6.1.2.1.1.3 1.3.6.1.2.1.2.2.1.10 1.3.6.1.2.1.2.2.1.10.1
```

or, if the MIB modules that define the above OIDs are loaded in MIB Browser:

```
getnext sysUpTime ifInOctets ifInOctets.1
```

- MIB Browser will send an SNMP GetNext request containing multiple (i.e., 3) variable bindings in the variable bindings list and display the retrieved values, i.e., that values of object instances that in lexicographical order follow the requested objects or object instances:

```
Remote address: 10.0.3.100  port: 161 transport: IP/UDP
Local address: 10.0.3.170  port: 57256 transport: IP/UDP
Protocol version: SNMPv2c
Operation: GetNext
```

Request bindings:

```
1: sysUpTime (TimeTicks) null
2: ifInOctets (Counter) null
3: ifInOctets.1 (Counter) null
```

Response bindings:

```
1: sysUpTime.0 (TimeTicks) 8 days 22h:27m:43s.00th (77206300)
2: ifInOctets.1 (Counter) 3581578
3: ifInOctets.2 (Counter) 695377014
```

11.4.3 Using GetBulk Command with Multiple Variable Bindings

*Example How to use the **getbulk** command to retrieve a scalar object instance (sysUpTime.0) and 3 instances of two columnar objects (ifInOctets.x, ifOutOctets.x):*

- Select the **View / SNMP Protocol Preferences** command to open the SNMP Protocol Preferences dialog box and configure the following.
 - In the **SNMP protocol version** frame, select the **SNMPv2c** radio button (note that the GetBulk operation is not available in SNMPv1).

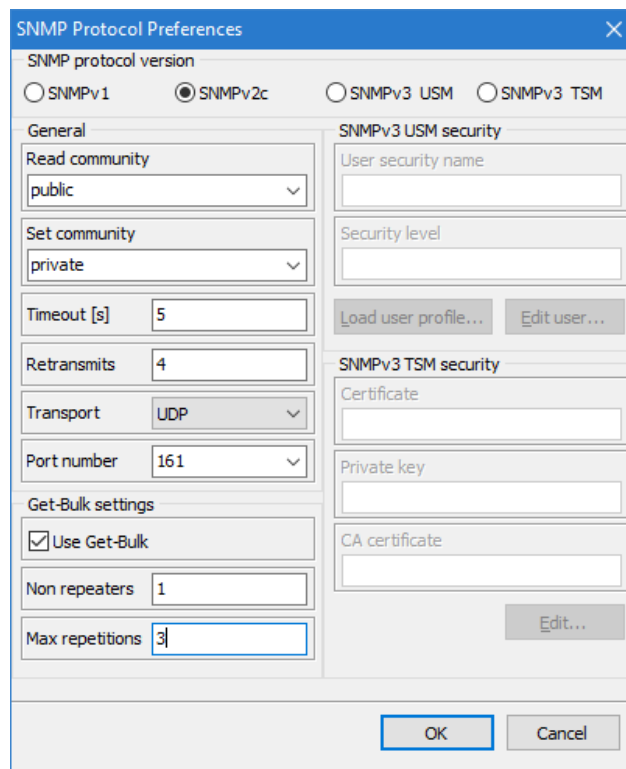


Figure 110: Specifying the SNMP GetBulk parameters for a specific purpose

- ❑ In the **Get-Bulk settings** frame check the **Use Get-Bulk** checkbox ([Figure 28](#)).
 - ❑ In the **Non repeaters** input line, set the number of non-repeaters to 1, and into the **Max repetitions** input line, enter number 3. For a detailed description of the GetBulk **non-repeaters** and **max-repetitions** parameters, refer to [this section](#).
 - ❑ Click the **OK** button to close the SNMP Protocol Preferences dialog box and apply the changes.
2. Enter the following command into the **Command line** drop-down list and press the **Enter** key:

```
getbulk sysUpTime ifInOctets ifOutOctets
```

or, if the MIB modules that define the above OIDs are loaded in MIB Browser:

```
getbulk 1.3.6.1.2.1.1.3 1.3.6.1.2.1.2.2.1.10 1.3.6.1.2.1.2.2.1.16
```

3. MIB Browser will send an SNMPv2c GetBulk request containing multiple (i.e., 3) variable bindings in the variable bindings list and display the retrieved values, i.e., one instance of the first (scalar) object and 3 instances of the remaining two (columnar) objects:

```
Remote address: 10.0.3.100 port: 161 transport: IP/UDP
Local address: 10.0.3.170 port: 57256 transport: IP/UDP
Protocol version: SNMPv2c
Operation: GetBulk
```

Request bindings:

```
1: sysUpTime (TimeTicks) null
2: ifInOctets (Counter) null
3: ifOutOctets (Counter) null
```

Response bindings:

```
1: sysUpTime.0 (TimeTicks) 9 days 01h:19m:52s.75th (78239275)
2: ifInOctets.1 (Counter) 3581578
3: ifOutOctets.1 (Counter) 34523454
4: ifInOctets.2 (Counter) 695377014
5: ifOutOctets.2 (Counter) 268775435
6: ifInOctets.3 (Counter) 198765433
7: ifOutOctets.3 (Counter) 98765438
```

12 STEP-BY-STEP SNMP WALK OPERATION

Step-by-Step SNMP Walk operation can be used to retrieve the OID and the current value of any object instance implemented in a managed device. It can serve as an alternative to the SNMP Walk operation. When using the SNMP Walk operation, the program automatically queries the whole group of object instances by issuing SNMP GetNext requests without stopping. On the other hand, the Step-by-Step SNMP Walk operation allows you a more controlled query because it lets you traverse the MIB tree manually by sending SNMP GetNext requests to object instances one by one. Each SNMP GetNext request uses the OID returned in response to the previous GetNext request.

12.1 Performing Step-by-Step SNMP Walk Operation

1. To perform the Step-by-Step SNMP Walk operation, click the **SNMP / Prompt For OID** command in the main window.
2. The Prompt For OID dialog box opens (Figure 111).
3. In the **Remote SNMP agent** input line, specify the IP address of the remote SNMP agent that you wish to query.

Note: If necessary, adjust the SNMP access parameters in the SNMP Protocol Preferences dialog box, which opens by clicking the **SNMP Protocol Preferences** toolbar button. For more information, see the **Specify SNMP Protocol Parameters** section.

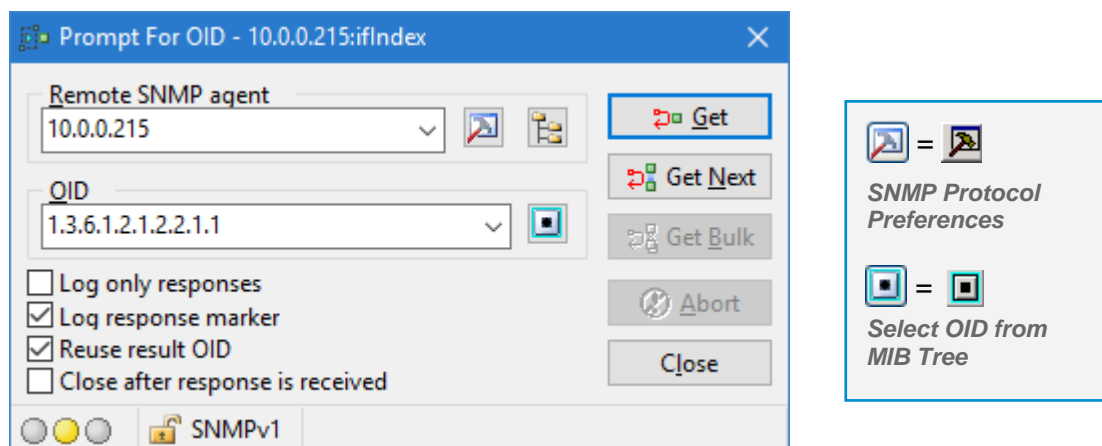


Figure 111: Prompt For OID dialog box

4. In the **OID** drop-down list, specify the OID value of the object instance from which you wish to start the Step-by-Step SNMP Walk operation.

Tip: You can also select the OID from the MIB tree by clicking the **Select OID from MIB Tree** toolbar button. The Select Object Identifier window appears (Figure 112). Expand the MIB tree and select an OID by double-clicking the appropriate node.

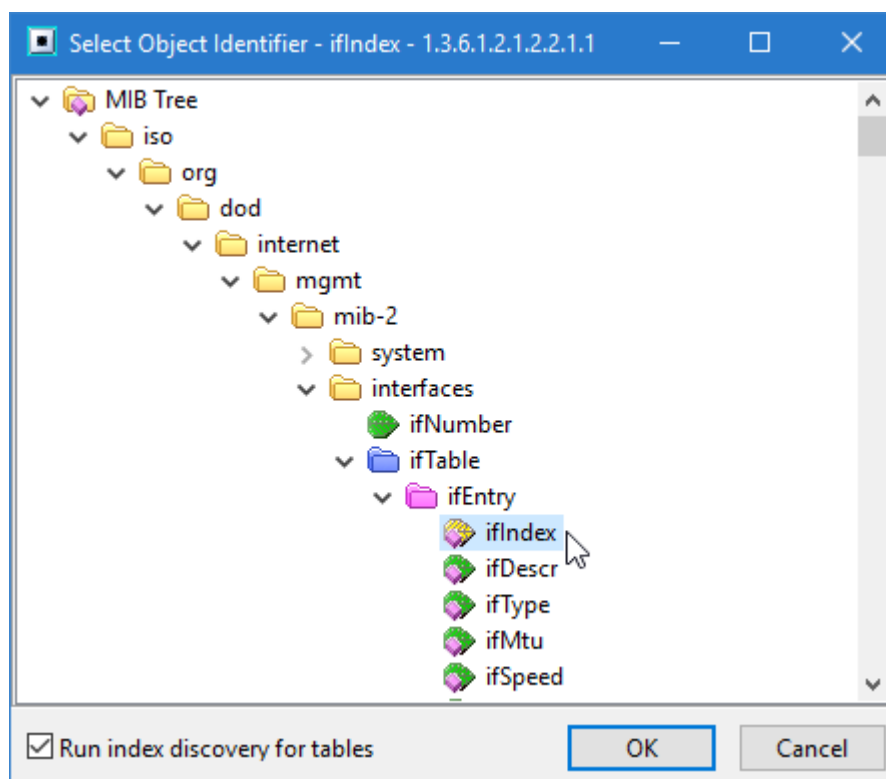


Figure 112: Specifying the OID of an object by selecting it in the MIB tree

5. In the Prompt For OID dialog box, check the **Reuse result OID** checkbox. This means that after every query with the SNMP GetNext request, the value in the **OID** drop-down list is updated with the OID received in response.
6. Make sure that the **Close after response is received** checkbox is unchecked so that you will be able to continue with the operation after the response is received.
7. Click the **Get Next** button in the Prompt For OID dialog box.

Note: If you use the **SNMP Get Bulk** request, the number of responses defined in the **Max repetitions** input line (in SNMP Protocol Preferences dialog box / Get-Bulk Settings frame) is returned. If the **Reuse result OID** checkbox is checked, the last OID returned in the GetBulk packet is used for the next query.

8. MIB Browser sends an SNMP GetNext request to the agent and displays its response in the Query Results panel. In the Prompt For OID dialog box, it updates the value in the **OID** input line with the last OID received in response.
9. To continue with the procedure keep clicking the **Get Next** button and query as many object instances, as you like.

Tip: If you want the program to display only the responses from the remote SNMP agent, check the **Log only responses** checkbox.

Check the **Log response marker** checkbox if you want the program to display separators between the steps.

Example:

How to query (one by one) all object instances of the ifTable by using the Step-by-Step SNMP Walk operation?

In the MIB tree, click the ifTable table node. Use the **SNMP / Prompt For OID** command to open the Prompt For OID dialog box. If necessary, enter the IP address of the agent and make sure that the **Reuse result OID** checkbox is checked and the **Close after response is received** checkbox is not checked. Click the **GetNext** button. MIB Browser sends the SNMP GetNext request to the SNMP agent. In response it receives the OID, syntax and the corresponding value (e.g., ifIndex.1(INTEGER)1) of the first instance implemented in the ifTable and displays it in the Query Results panel. To continue with the query, repeatedly click the **GetNext** button. MIB Browser will each time send an SNMP GetNext request to the agent and update the value of the **OID** drop-down list with the OID received in response (Figure 113). In this way you will query all object instances of the ifTable.

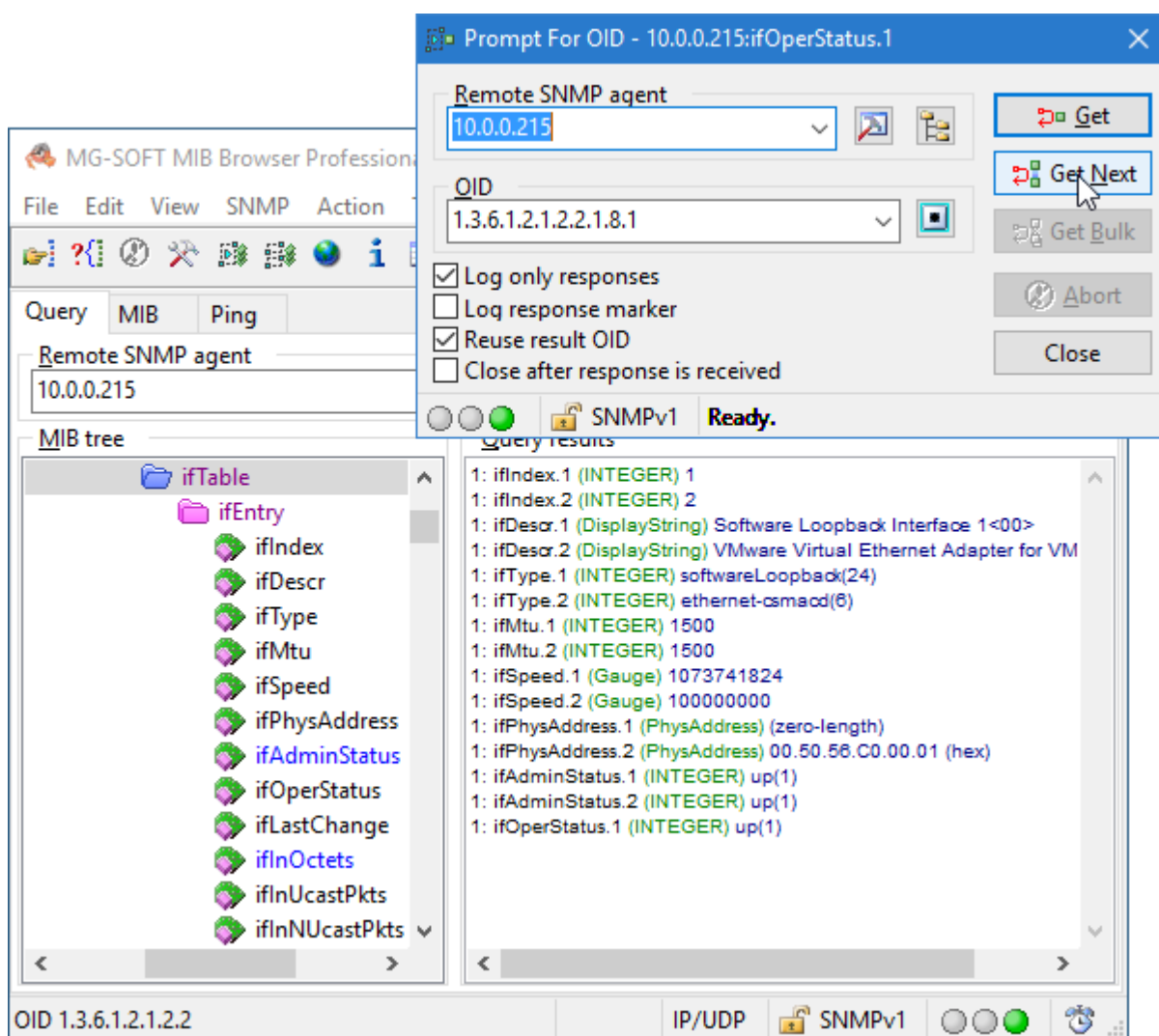


Figure 113: Step-by-Step SNMP Walk operation on the ifTable

13 MODIFY VALUES OF OBJECT INSTANCES IN REMOTE SNMP AGENTS

By using the SNMP Set operation, you can configure and control network devices by modifying the object instance values in their SNMP agents. In this section, you will learn how to change a value of an object instance in a remote SNMP agent.

13.1 Modifying Values of Object Instances by Using the SNMP Set Operation

1. In the main window, switch to the **Query** tab.
2. Into the **Remote SNMP Agent** drop-down list, type or select the IP address of the SNMP agent that you wish to manage.
3. If necessary, adjust the SNMP access parameters (especially the **Set community** string) in the SNMP Protocol Preferences dialog box, which opens by selecting the **View / SNMP Protocol Preferences** command. See also the [Specify SNMP Protocol Parameters](#) section.

Note: Make sure to specify the correct **Set community** string in the SNMP Protocol Preferences dialog box. Only if this parameter is correctly specified, the SNMP Set operation will succeed.

4. Contact the remote SNMP agent by using the **SNMP / Contact** command or the **Contact Remote SNMP Agent** toolbar button.
5. In the displayed MIB tree in the MIB tree panel, click the object of which instance value you wish to modify with the SNMP Set operation. Only instances of **leaf** objects with **read-write**, **read-create** and **write-only** access type can be set by means of the SNMP Set operation. You can quickly determine which leaf objects are writable (read-write, write-only) or creatable (read-create) by looking at the colors of their names in the MIB tree, as explained in the [Colors Used for Representing Different Access Types of MIB Nodes](#).

Note: For SNMP Set requests with more than one OID binding in PDU, you should use the Multiple Variable Bindings window. See the instructions in the [SNMP Set Requests with Multiple Variable Bindings](#) section.

6. Right-click a writable object and select the **Set** command from the context menu ([Figure 114](#)). Alternatively, select the object and choose the **Tools / Set Window** command. If the selected MIB tree node is a columnar object, the Select Table Instance window ([Figure 99](#)) appears, where you need to specify the instance of the object and double-click it.

Tip: To modify values of columnar object instances, you can use the Table View window and edit values directly in the table view. See the [Modifying Values of Table Object Instances Directly in Table View](#) section.

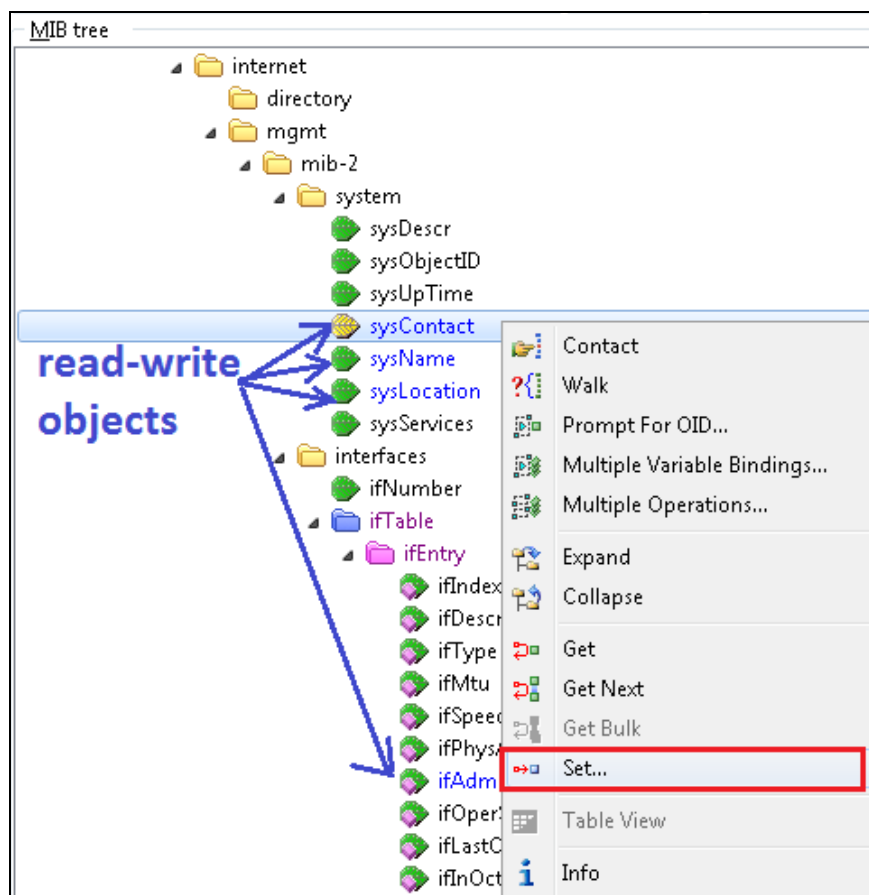


Figure 114: Selecting the Set command from the context menu (notice writable object names in blue)

7. The Set dialog box appears (Figure 115).

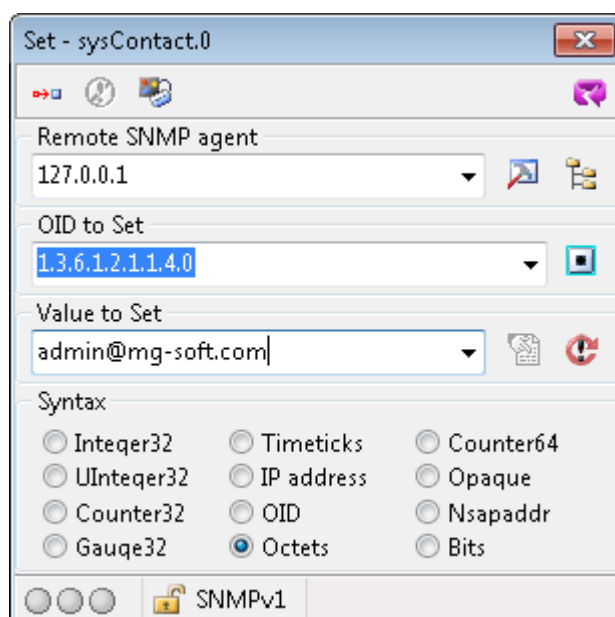


Figure 115: Set dialog box

MIB Node Properties

Click the **MIB Node Properties** toolbar button to open the MIB Node Properties window and check the Max access property. If you want to perform the SNMP Set operation on the selected object, the object has to have either the read-write, write-only or read-create access.

8. Into the **Value to Set** drop-down list, enter the value that you want to set.

If the MIB file specifies pre-defined values for the currently selected object, you can select them in the Select Value dialog box (Figure 116). In order to do this, click the **Select from Value List** toolbar button next to the **Value to Set** drop-down list. The Select Value dialog box appears. Select one value and click the **OK** button.

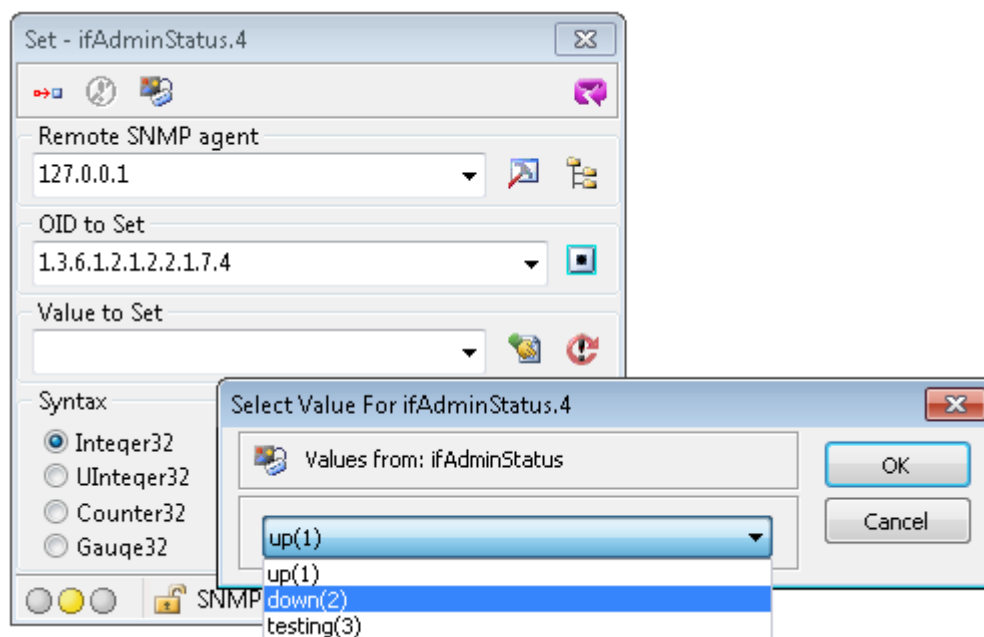
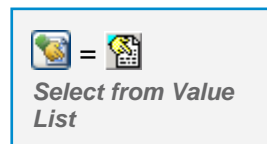


Figure 116: Selecting a pre-defined value (integer-enumeration) to be set

9. After you have defined the new value, select its syntax in the **Syntax** frame.
10. When all parameters in the Set dialog box are specified, click the **Set Value in Remote SNMP Agent** toolbar button.
11. MIB Browser performs the SNMP Set operation and displays the results of the operation in the Query Results panel in the main window.



13.1.1 Specifying Value to Be Set if the SNMP Syntax is BITS

Sometimes, the SNMP syntax of an object instance is **BITS**; which means that the value of such an object instance is represented as a construct of bits.

To specify and set the value of an object instance with the syntax in **BITS**, you can use the Select Bits Value dialog box and make a construct of bits from the pre-defined values.

1. In the Set dialog box (Figure 115) first specify the OID of the instance of the object with syntax in **BITS** (if necessary, see the [Modifying Values of Object Instances by Using the SNMP Set Operation](#) section).
2. To specify the value to be set, open the Select Bits Value dialog box by clicking the **Select From Value List** toolbar button.

- The Select Bits Value dialog box opens and displays a list of pre-defined values for the selected object instance (Figure 117).

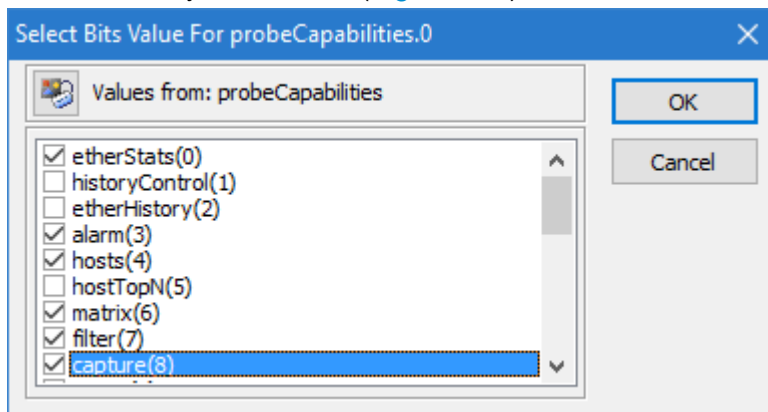
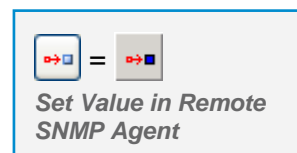


Figure 117: Select Bits Value dialog box

- Select the desired values by checking the corresponding checkboxes. Click the **OK** button.
- MIB Browser maps the new construct of bits into the hexadecimal notation and displays it in the **Value to Set** input line in the Set dialog box.
- In the **Syntax** frame select the **Bits** syntax.
- To set the new value, click the **Set Value in Remote SNMP Agent** toolbar button.



Example:

How to use the SNMP Set request to change the administratively assigned name of the managed device (sysName)?

To contact the SNMP agent, use the **SNMP / Contact** command. In the MIB tree, click the `sysName` node and use the **Tools / Set Window** command to open the Set dialog box. In the **Value to Set** drop-down list, enter the new name for the managed device (e.g., `mymachine`, Figure 118) and click the **Set Value in Remote SNMP Agent** toolbar button. The SNMP agent sets the new value to the `sysName.0` object instance and MIB Browser prints the newly assigned name in the Query Results panel.

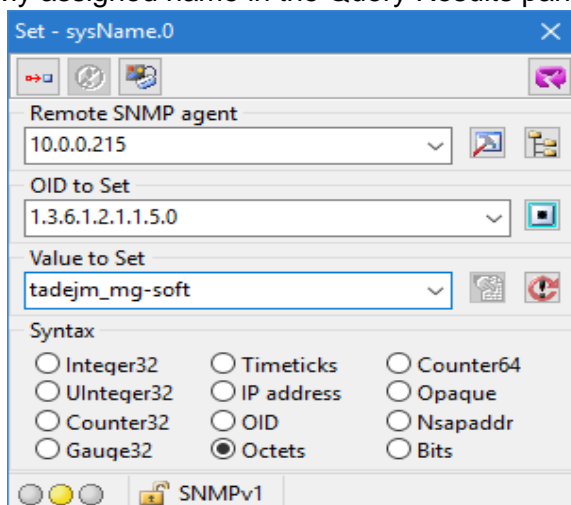




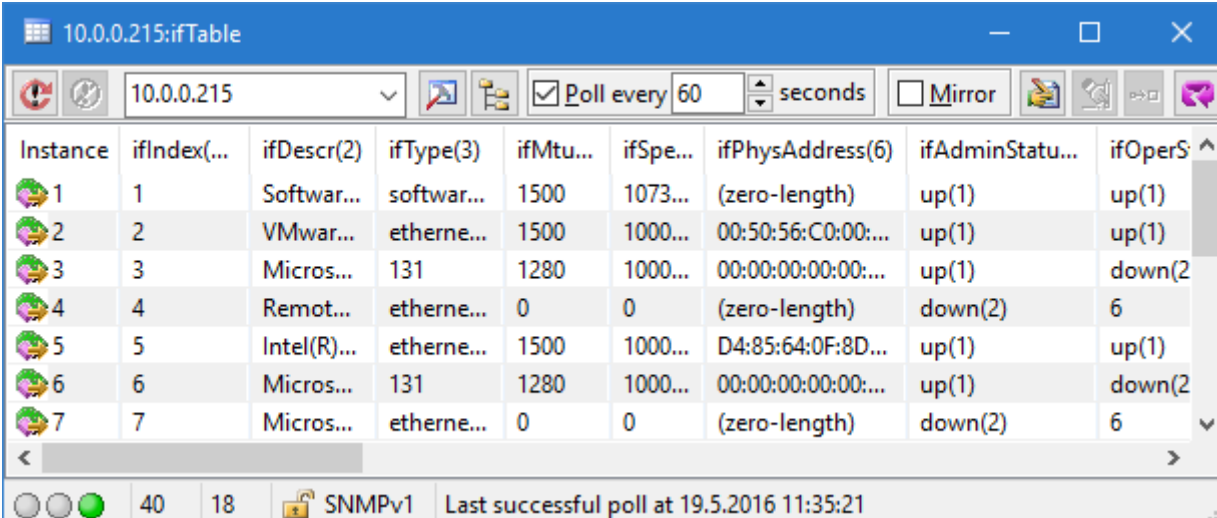
Figure 118: Specifying a new value to be set in the SNMP agent

13.2 Modifying Values of Table Object Instances Directly in Table View

If you wish to modify values of columnar objects in SNMP tables, you can use the Table View window. The Table View window allows direct editing of values of table object instances as well as adding of new rows to displayed SNMP tables.

To modify values of table object instances in an SNMP table:

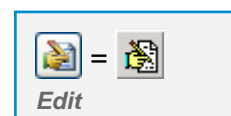
1. In MIB Browser's main window first contact an SNMP agent and expand its MIB tree (as described in the first steps of the [Modifying Values of Object Instances by Using the SNMP Set Operation](#) section).
2. In the MIB tree, select a  table node (e.g., ifTable), or a  row node (e.g., ifEntry) of the SNMP table that you wish to edit.
3. Open the Table View window by selecting the **Tools / Table View** command.
4. The Table View window opens and MIB Browser displays the selected SNMP table (e.g., ifTable) in a tabular form ([Figure 119](#)).



Instance	ifIndex(...)	ifDescr(2)	ifType(3)	ifMtu...	ifSpe...	ifPhysAddress(6)	ifAdminStatu...	ifOperS
1	1	Softwar...	softwar...	1500	1073...	(zero-length)	up(1)	up(1)
2	2	VMwar...	etherne...	1500	1000...	00:50:56:C0:00:...	up(1)	up(1)
3	3	Micros...	131	1280	1000...	00:00:00:00:00:...	up(1)	down(2)
4	4	Remot...	etherne...	0	0	(zero-length)	down(2)	6
5	5	Intel(R)...	etherne...	1500	1000...	D4:85:64:0F:8D...	up(1)	up(1)
6	6	Micros...	131	1280	1000...	00:00:00:00:00:...	up(1)	down(2)
7	7	Micros...	etherne...	0	0	(zero-length)	down(2)	6

Figure 119: An SNMP table (e.g., ifTable) displayed in a tabular form in the Table View window

5. To see which table object instances can be modified, and to enable editing of table instances, click the **Edit** button in the Table View window toolbar.
6. Instance values of table objects that can be modified (e.g., ifAdminStatus) are colored ([Figure 120](#)).



Note: While editing is being used, all other features of the Table View window are disabled.

Instance	ifIndex(...)	ifDescr(2)	ifType(3)	ifMtu...	ifSpe...	ifPhysAddress(6)	ifAdminStatu...	ifOperS
1	1	Softwar...	softwar...	1500	1073...	(zero-length)	up(1)	up(1)
2	2	VMwar...	etherne...	1500	1000...	00:50:56:C0:00:...	up(1)	up(1)
3	3	Micros...	131	1280	1000...	00:00:00:00:00:...	up(1)	down(2)
4	4	Remot...	etherne...	0	0	(zero-length)	down(2)	6
5	5	Intel(R)...	etherne...	1500	1000...	D4:85:64:0F:8D...	up(1)	up(1)
6	6	Micros...	131	1280	1000...	00:00:00:00:00:...	up(1)	down(2)
7	7	Micros...	etherne...	0	0	(zero-length)	down(2)	6

Figure 120: Colored instance values of a writable table object (i.e., ifAdminStatus)

Tip: By default instance values that can be modified are colored blue. You can change color settings in the MIB Browser Preferences dialog box (**View / MIB Browser Preferences**) in the Edit Table View Window Preferences panel, which displays by selecting the **Table View / Edit** preferences in the MIB Browser Preferences dialog box. In the **Colors** frame you can change also other color settings related to table editing.

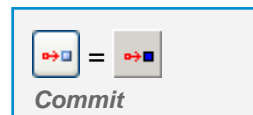
- To edit any instance value of the colored column (or row, if the table is mirrored), click the instance value and an input line will appear (Figure 121).
- Into the input line, enter the value that you wish to set and then click the **Enter** key on the keyboard.
If the input line has the **Select From Value List** toolbar button attached, you can select the value from the list of pre-defined values.

Select from Value List

Instance	ifIndex(...)	ifDescr(2)	ifType(3)	ifMtu...	ifSpe...	ifPhysAddress(6)	ifAdminStatu...	ifOperS
1	1	Softwar...	softwar...	1500	1073...	(zero-length)	up(1)	up(1)
2	2	VMwar...	etherne...	1500	1000...	00:50:56:C0:00:...	up(1)	up(1)
3	3	Micros...	131	1280	1000...	00:00:00:00:00:...	up(1)	down(2)
4	4	Remot...	etherne...	0	0	(zero-length)	down(2)	6
5	5	Intel(R)...	etherne...	1500	1000...	D4:85:64:0F:8D...	up(1)	up(1)
6	6	Micros...	131	1280	1000...	00:00:00:00:00:...	up(1)	down(2)
7	7	Micros...	etherne...	0	0	(zero-length)	down(2)	6

Figure 121: Selecting the value to be set from the list of pre-defined values

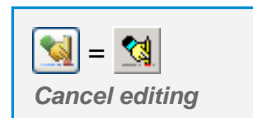
9. When you have specified new values, click the **Commit** toolbar button to set them.



10. MIB Browser sets new values in the remote SNMP agent.

Note: If MIB Browser fails to set any of the modified values, it highlights them with red (by default) background.

11. You can cancel editing at any time, by clicking the **Cancel editing** toolbar button. When editing is canceled, other functions of the Table View window (e.g., polling) are enabled again.



13.3 SNMP Set Requests with Multiple Variable Bindings

In this section, you will learn how to use the Multiple Variable Bindings window to set multiple object instances with a single SNMP Set request.

To perform the SNMP Set operation with multiple variable bindings, you first need to make a list of variable bindings in the Multiple Variable Bindings window, as described in the following sub-section.

13.3.1 Making Multiple Variable Bindings List

Inserting a Scalar Object

To insert a scalar object from the MIB tree into the Multiple Variable Bindings window:

1. In the main window (Query tab), expand the MIB tree.
2. In the MIB tree, click a scalar object (e.g. `sysContact`) that you wish to insert into the Multiple Variable Bindings window.

Note: If you wish to insert a columnar object, see the [Inserting a Columnar Object](#) section.

3. Use the **SNMP / Multiple Variable Bindings** command in the main window. The Multiple Variable Bindings window appears and the selected object is inserted in the window panel ([Figure 122](#)).

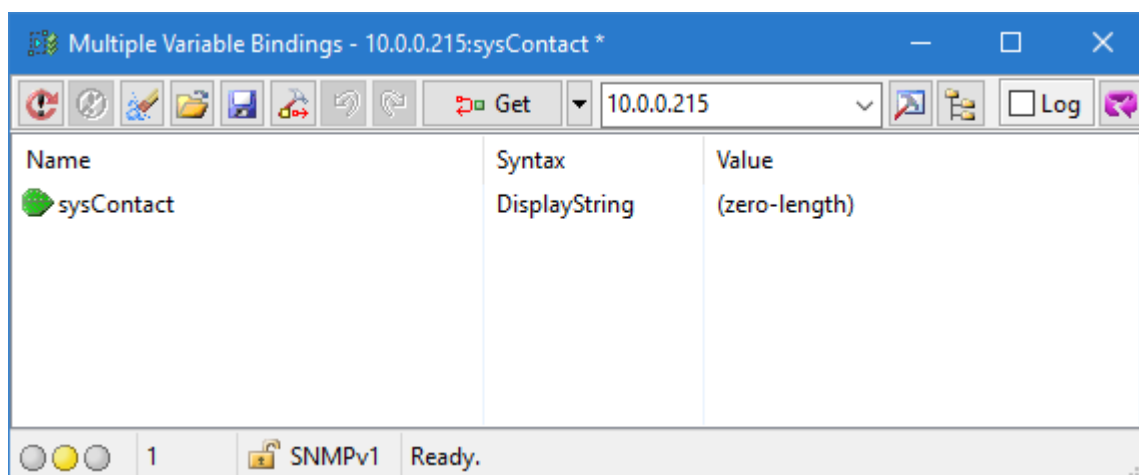


Figure 122: Multiple Variable Bindings window with the selected object

4. To specify the instance of the inserted object, right-click its name in the Multiple Variable Bindings window and use the **Edit** pop-up menu command.
5. The Select dialog box appears ([Figure 123](#)).

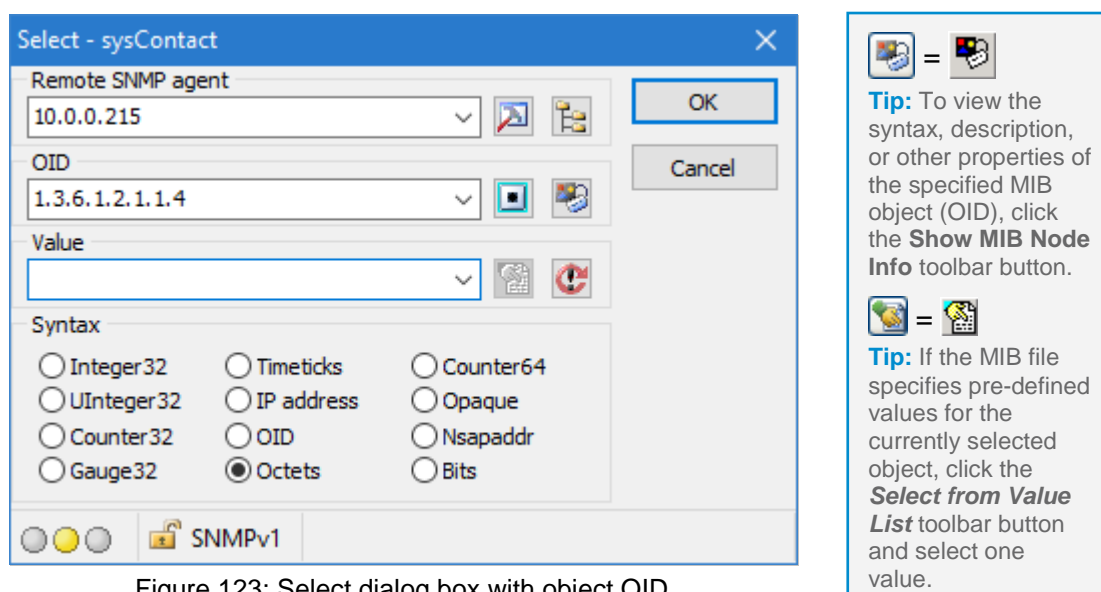
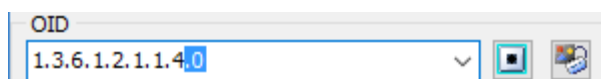


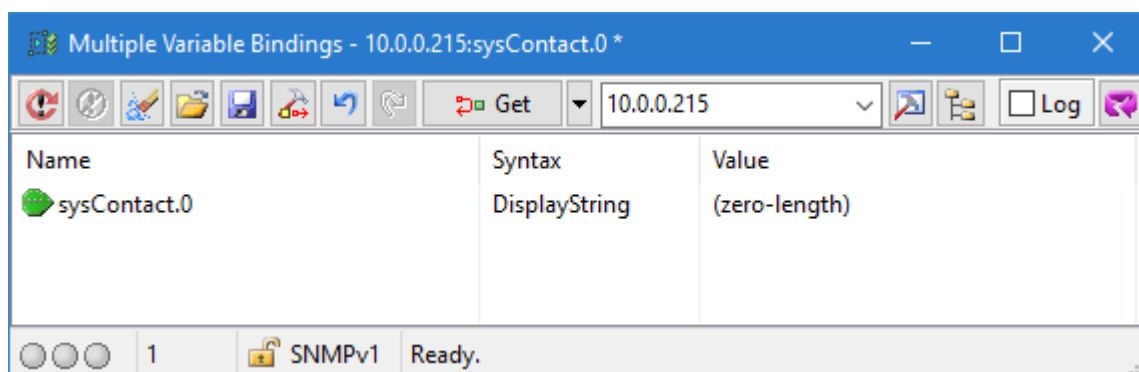
Figure 123: Select dialog box with object OID

- If the selected object is a scalar object, add a **.0** (dot-zero) suffix to the OID value in the **OID** drop-down list (Figure 124).

Figure 124: Specifying the instance of a scalar object in the *OID* input line

Note: The instance of the object must be specified; otherwise the SNMP Set operation will fail.

- Enter (or select from the **Value** drop-down list) the value that should be set to the specified object instance. Choose the appropriate syntax in the **Syntax** frame.
- Click the **OK** button to close the Select dialog box.
- MIB Browser inserts the newly specified object instance name (e.g., `sysContact.0`), syntax and value into the Multiple Variable Bindings window (Figure 125).

Figure 125: A scalar object (`sysContact`) with a specified instance (`sysContact.0`), syntax and value

- To add more bindings to the list, see the [Adding More Objects](#) section.

Inserting a Columnar Object

If you want to insert a columnar node, you have to specify the instance of which value you wish to modify.

1. In the MIB tree in the main window, click a columnar node (e.g., `ifAdminStatus`) or entry node (e.g., `ifEntry`).
2. Use the **SNMP / Multiple Variable Bindings / Select Instance** command.
3. In the opened Select Table Instance window, select the desired instance by double-clicking the appropriate index (e.g., 2, [Figure 126](#)).

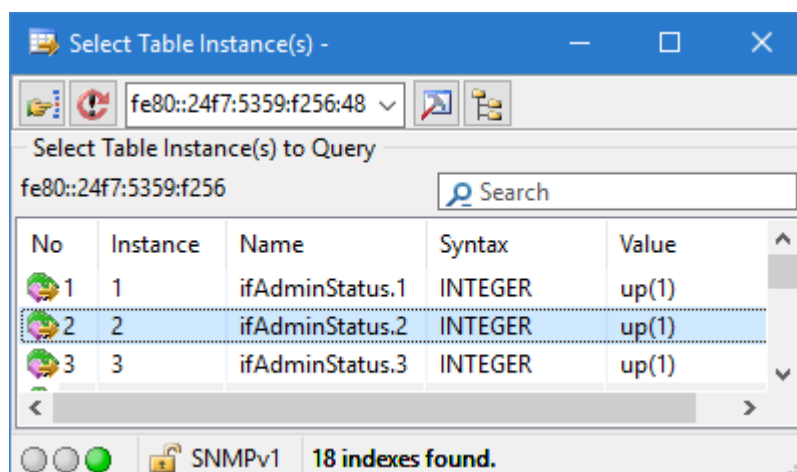


Figure 126: Selecting a columnar object instance

Note: The instance of the object must be specified; otherwise the SNMP Set operation will fail.

4. The selected object instance appears in the Multiple Variable Bindings window ([Figure 127](#)). The instance of the object is indicated with a suffix added to the object name (e.g., `ifAdminStatus.2`).

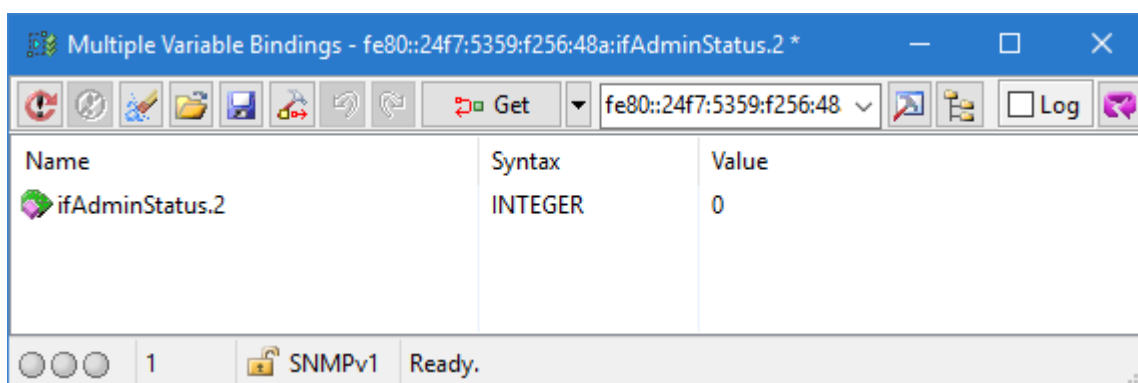


Figure 127: A columnar object (`ifAdminStatus`) with a specified instance (`ifAdminStatus.2`), syntax and value

5. To add more bindings to the list, see the [Adding More Objects](#) section.

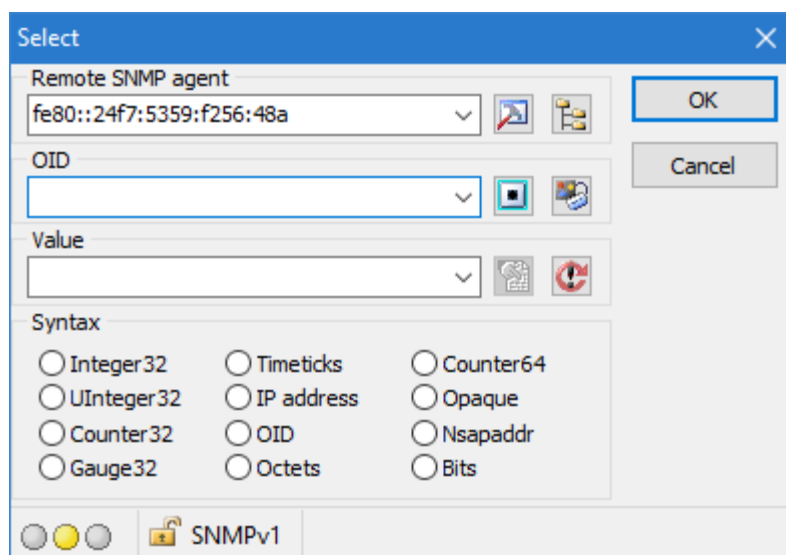
Tip: The simplest way of adding an object to the list of variable bindings:

Drag an object from the MIB tree in the main window and drop it in the Multiple Variable Bindings window panel. Note that you have to specify the instance of the dropped object. You can do that in the Select dialog box, which opens by clicking the **Edit** pop-up menu command (or simply by double-click the object). In the opened Select dialog box (Figure 123), specify the instance of the object, the value that you want to set and its syntax.

Adding More Objects

You can insert any number of objects into an opened Multiple Variable Bindings window:

1. Right-click in the Multiple Variable Bindings window panel and use the **New** pop-up menu command. The Select dialog box appears (Figure 128).



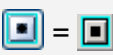

 = 
Select OID from
MIB Tree

Figure 128: Select dialog box

2. In the **OID** input line, specify the OID of the object instance or select it from the MIB tree in the Select Table Instance window, which opens by clicking the **Select OID from MIB Tree** toolbar button.

Note: In case of a scalar object, make sure that the OID suffix is .0. In case of a columnar object, select the instance in the Select Table Instance window or add the instance index to the OID of the object.

3. In the **Value** drop-down list, specify the value that should be set and choose the appropriate syntax in the **Syntax** frame.
4. Click the **OK** button. The dialog box closes and the selected object instance with its new value is inserted into the variable bindings list.

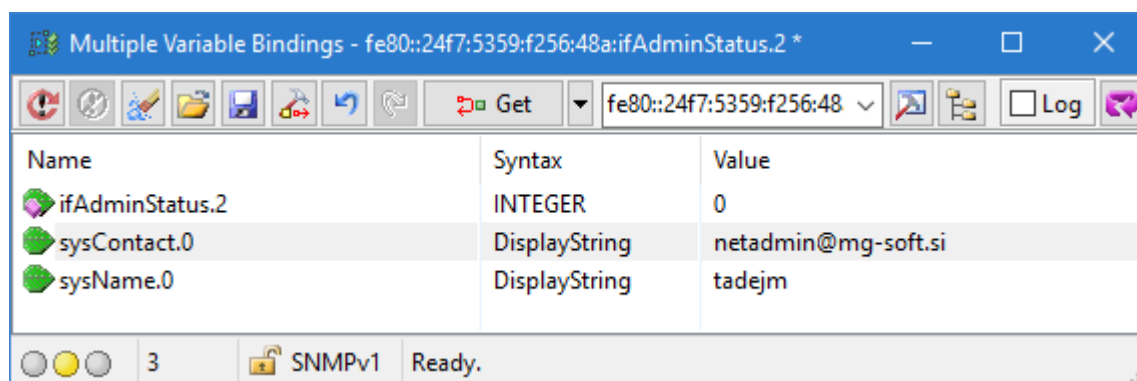


Figure 129: A list of multiple variable bindings

As shown in Figure 129, the suffix added to the OID value or name of an object can be:

- .0 (Indicating a scalar object instance)
- .1, .2, .3, etc. (Indicating a columnar object instance).

5. To add more variable bindings to the list, repeat the procedure from step 1, or use the drag and drop technique described in this [Tip](#).

Inserting a Group of Objects

To insert a group of objects from the main window MIB tree:

1. If necessary, repeat steps 1 to 4 in the [Modifying Values of Object Instances by Using the SNMP Set Operation](#) section.
2. In the MIB tree, click a sub tree root node (e.g., `system` or `ifEntry`) of the objects that you wish to insert into the variable bindings list.
3. Use the **SNMP / Multiple Variable Bindings** command. In case of a table, click the **Select Instance** sub menu command and select the instance in the Insert Table Instance window.
4. The Multiple Variable Bindings window opens. MIB Browser inserts the selected group of objects into the Multiple Variable Bindings window panel.
5. Right-click the object instance name on which you wish to perform the SNMP Set operation and select the **Edit** pop-up command (or double-click the object). The Select dialog box appears ([Figure 123](#)).
6. If the selected object is a scalar object, add a **.0** (dot-zero) suffix to the OID value in the **OID** drop-down list.
7. In the **Value** drop-down list, specify the value that should be set and choose the appropriate syntax in the **Syntax** frame.
8. Click the **OK** button. The Select dialog box closes and the selected object instance is inserted into the multiple variable bindings list with the new value.
9. Repeat steps 5 to 8 for every object instance of which value you wish to set.

13.3.2 Performing SNMP Set Operation with Multiple Variable Bindings

When you have created a list of variable bindings in the Multiple Variable Binding window, you can perform the SNMP Set operation with one SNMP Set request.

To perform the SNMP Set operation, do the following:

1. Click the **Down Arrow** button next to the Get/Get Next/Get Bulk/Set/Trap/Inform programmable toolbar button, select the **Set** operation type (Figure 130) and click the Set toolbar button.

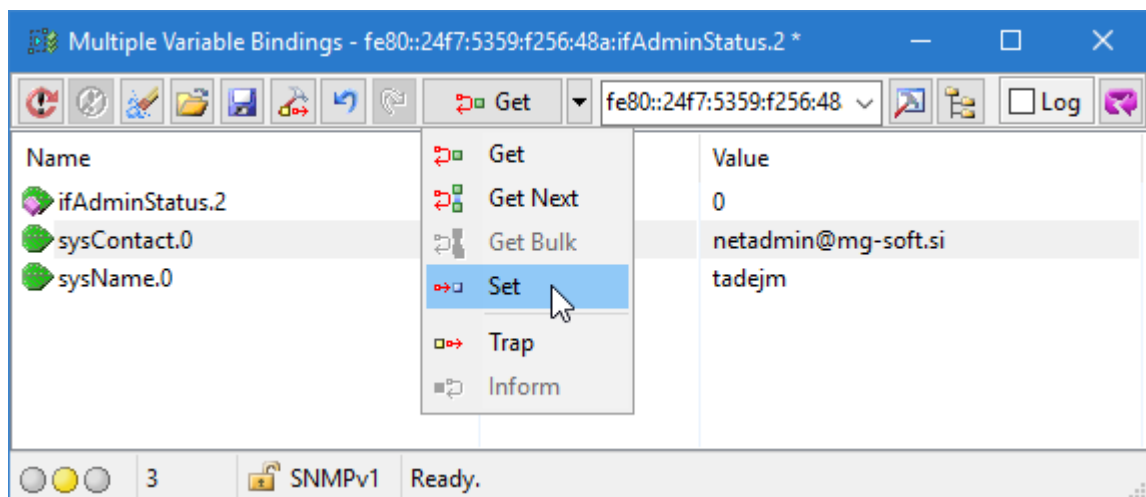


Figure 130: Selecting the operation type

2. MIB Browser sends the packet with all variable bindings to the remote SNMP agent. When it receives the response, it displays the updated values in the Multiple Variable Bindings window panel.

Note: If any of the bindings are colored red, the SNMP Set operation has failed. Go through the procedure described in the [Making Multiple Variable Bindings List](#) again. If this does not solve the problem, check the [Resolving Problems When Performing SNMP Set Operation](#) section.

Example:

How to change the name and location of the managed SNMP agent with one SNMP Set request?

This is possible by using the Multiple Variable Bindings window. In the MIB tree, click the `sysName` node and use the **SNMP / Multiple Variable Bindings** command. The Multiple Variable Bindings window opens with the inserted `sysName` object. Right-click the object name and select the **Edit** pop-up command to open the Select dialog box (Figure 123). Add a `.0` suffix to the OID in the **OID** drop-down list. In the **Value** drop-down list, enter the new name for the agent (e.g., `tinak.mg-soft.si`) and specify the syntax. Click the **OK** button and the new value displays in the Multiple Variable Bindings window.

To set a new location of the agent, click the `sysLocation` node in the main window, hold the mouse button and drag the selected object into the Multiple Variable Bindings window. Now, right-click the object name and select the **Edit** pop-up command to open the Select dialog box. Add the `.0` suffix to the OID and enter the new location into the **Value** drop-down list (e.g., MG-SOFT Corporation, Slovenia). Select the syntax and click the **OK** button. The new value will be displayed in the Multiple Variable Bindings window. Finally, you can send the SNMP Set request. Click the **Down Arrow** button next to the Get/Get Next/Get Bulk/Set/Trap/Inform programmable button, select the **Set** operation type and click the **Set** toolbar button. The SNMP Set operation is performed and the newly specified agent name and location of the agent are displayed in the Multiple Variable Bindings window panel (Figure 131).

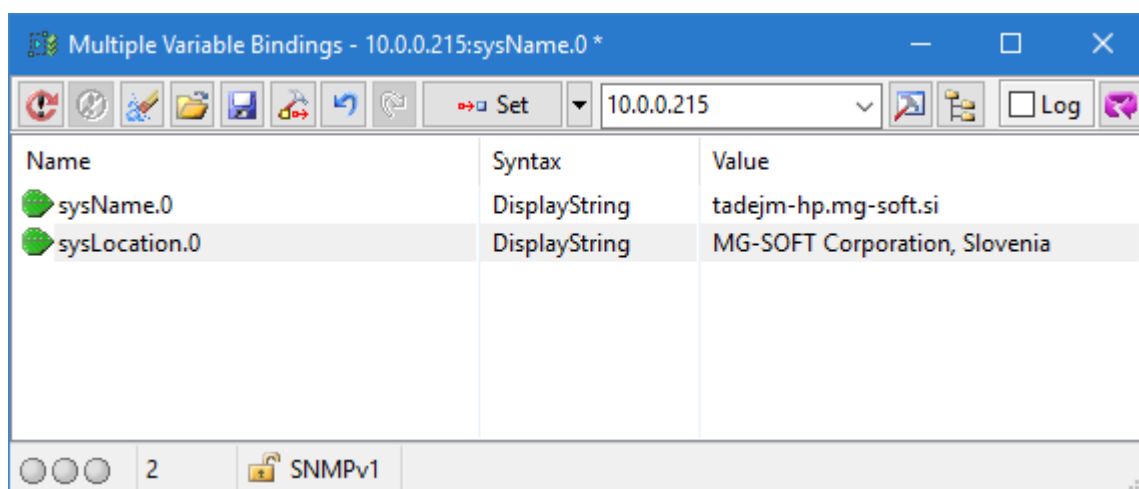


Figure 131: Setting values of object instances with one SNMP set request

13.4 Resolving Problems When Performing SNMP Set Operation

Sometimes MIB Browser cannot successfully perform the SNMP Set operation, the operation is timed out or an error message is returned from the SNMP agent. To resolve the problem, check if the following parameters are specified correctly and change them if necessary:

1. Check the community name in the SNMP Protocol Preferences dialog box ([Figure 31](#)). You can modify values in an SNMP agent only if the name of the community is correct.
2. In the MIB Node Properties window (**View / MIB Node Properties** command, [Figure 29](#)), check if objects of which values you want to modify have the right access. The access has to be `WRITE`, this means either `read-write`, `write-only` or `read-create`. Note that objects with the `read-only` access cannot be modified.
3. Make sure that you are using the correct OID. The instance of an object has to be specified with a `.0` suffix for scalar objects and a relevant suffix for columnar objects.
4. Check if the value to be set and its syntax are defined correctly.
5. If you are using the Multiple Variable Bindings window for the SNMP Set operation, make sure that all variable bindings in the list have `WRITE` access, correctly specified instances, and correctly defined values that will be set (see the [SNMP Set Requests with Multiple Variable Bindings](#) section). If the list of variable bindings contains at least one variable binding that does not fulfill these requirements, the operation will fail.

Tip: You can check the contents of SNMP messages exchanged between MIB Browser and the SNMP agent during the SNMP Set operation in the Generic SNMP Trace window. For more information see the [Tracing Exchanged SNMP Messages](#) section.

14 DISCOVER REMOTE SNMP AGENTS

In this section, you will learn how to discover active SNMP agents on the network by using the Remote SNMP Agent Discovery window.

14.1 Discovering Remote SNMP Agents

1. To discover active SNMP agents on the network, use the **Tools / Discovery Window** command or the **Discover Remote SNMP Agents** toolbar button in the main window.
2. The Remote SNMP Agent Discovery window opens (Figure 132).

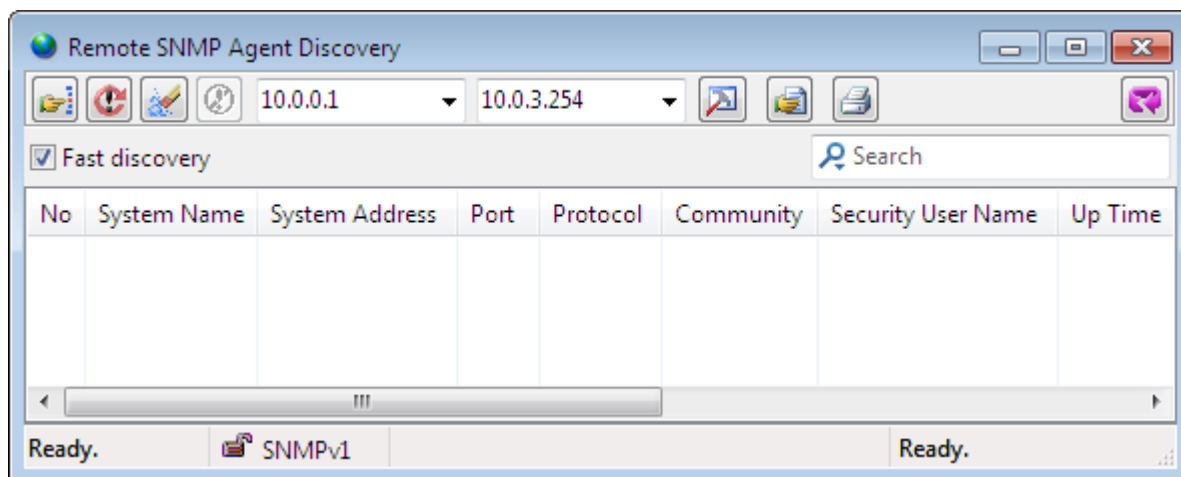
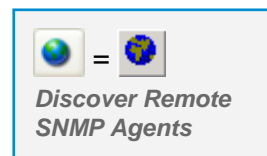


Figure 132: Remote SNMP Agent Discovery window

3. Specify the range of IP addresses within which you want to discover SNMP agents by entering appropriate IP addresses into the **First Address to Discover** input line and the **Last Address to Discover** input line.
4. Adjust SNMP access parameters by clicking the **SNMP Protocol Preferences** toolbar button (🔧). In the [SNMP Protocol Preferences dialog box](#) specify the SNMP access parameters supported by the SNMP agents in your network. It is important to select the correct **SNMP protocol version**, specify the correct **Read community** name (if using SNMPv1 or SNMPv2c) or specify the matching **USM user profile** or **TSM security settings** (if using SNMPv3). If necessary, adjust the **Timeout** and **Retransmits** parameters and specify the **Port** number on which remote agents listen to SNMP requests. Note that MIB Browser will successfully discover only those SNMP agents, whose SNMP access parameters match the ones specified in the SNMP Protocol Preferences dialog box.
5. Check the **Fast discovery** checkbox below the toolbar to speed up the discovery operation by overriding the **Timeout** and **Retransmits** parameters configured in the SNMP Protocol Preferences dialog box and setting these to 10 seconds and zero retransmits, respectively.

6. To start the discovery, click the **Start Remote SNMP Agents Discovery** toolbar button.
7. MIB Browser performs the discovery and displays a list of discovered SNMP agents with their system names, addresses and additional system information mainly obtained by retrieving the agent's MIB-II system group of objects (Figure 133).

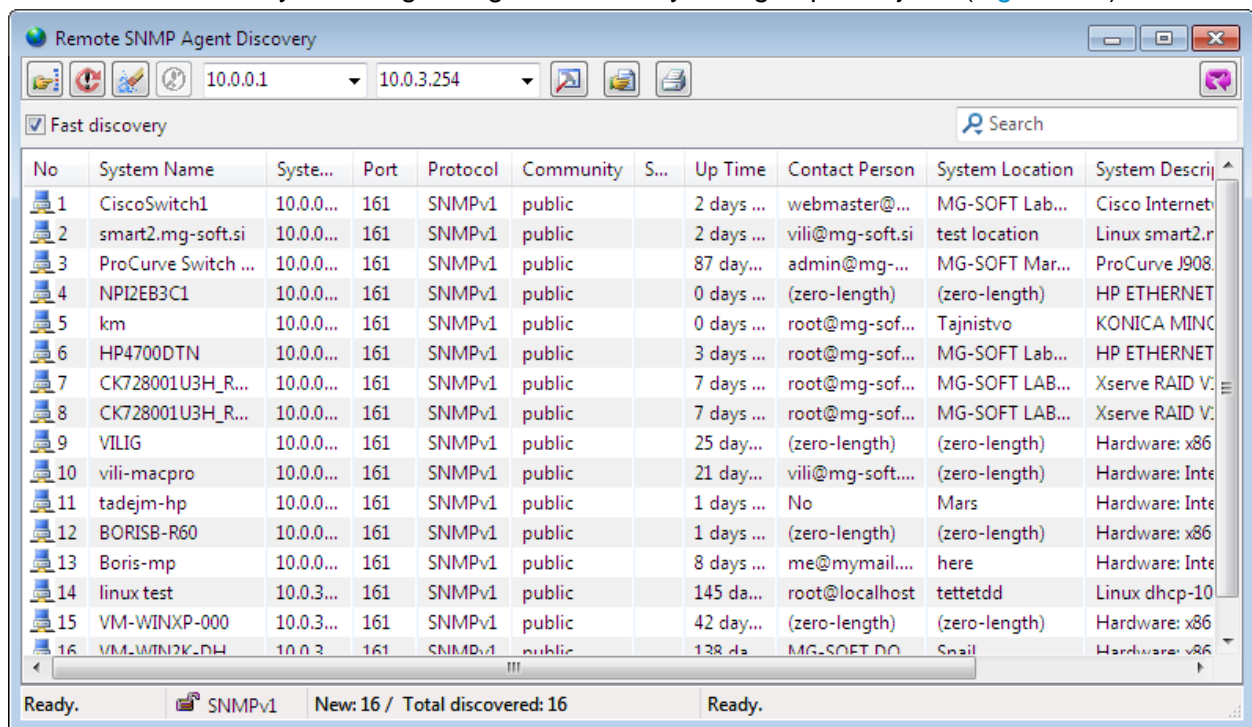
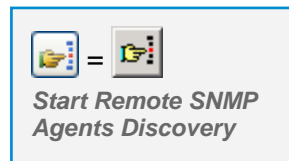







Figure 133: A list of discovered SNMP agents

8. To search for particular discovered SNMP agents, use the **Live search** tool  in the Remote SNMP Agent Discovery window, as follows:
 - ❑ Click the search symbol () in the Live search tool to display the **Search Options** drop-down menu and select the columns you want to search in.
 - ❑ Click the **OK** button to close the Search Options drop-down menu.
 - ❑ Click inside the Live search box and type in the query. The Live search tool automatically performs the search as you type the characters into the search box and displays only those SNMP agents that **contain** the entered text in any of the enabled search columns.
 - ❑ To cancel the search, click the **Cancel Current Search** symbol () in the Live search box or delete the text from it.
9. To print the contents of the Remote SNMP Agent Discovery window, click the **Print** toolbar button () and select the desired printer and printing options in the standard Print dialog box.

10. To view the discovery log, click the **Log** toolbar button (). The Discovery Log window appears, displaying the details of the discovery operation (Figure 135). You can print the log by clicking the **Print** toolbar button or search and filter its content by using the **Live search** tool.

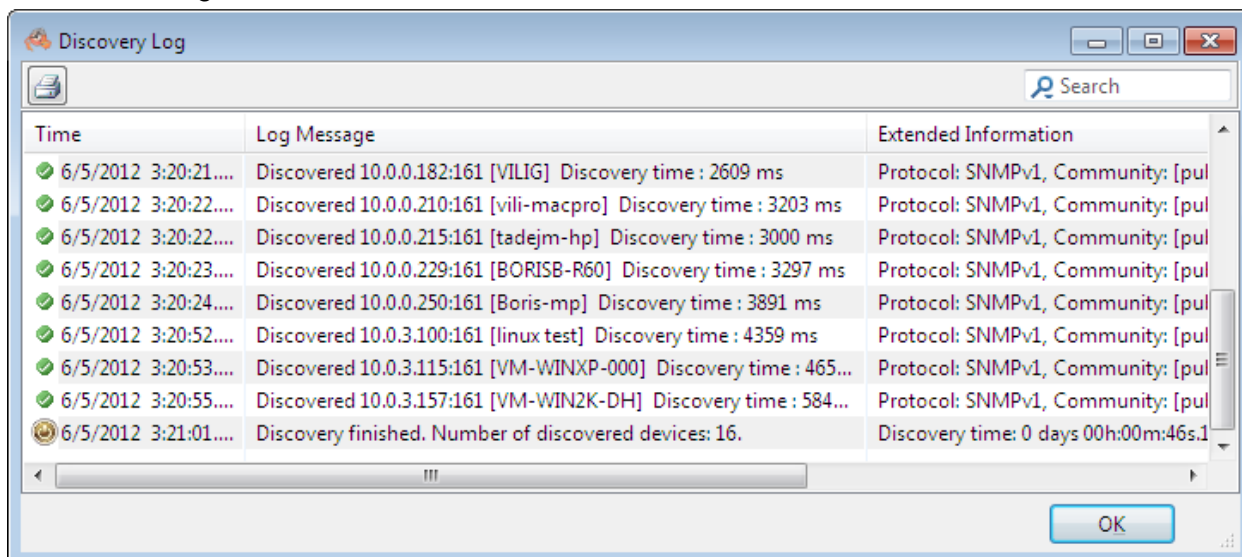


Figure 134: Viewing the discovery log file

14.1.1 Repeating Discovery Operation on Different IP Range

In the currently displayed Remote SNMP Agent Discovery window, enter a new IP discovery range and click the **Refresh** toolbar button. The program clears the list of old and displays the list of newly discovered SNMP agents with their properties.



If you click the **Start Remote SNMP Agents Discovery** toolbar button, MIB Browser adds newly discovered agents to the existing list.



If you click the **Refresh** toolbar button, MIB Browser clears the list before starting a new discovery operation.

14.1.2 Repeating Discovery Operation with Different SNMP Access Parameters

To repeat the discovery operation with different SNMP access parameters, do the following:

1. In the currently displayed Remote SNMP Agent Discovery window, click the **SNMP Protocol Preferences** toolbar button.
2. The SNMP Protocol Preferences dialog box appears. Specify new access parameters and click the **OK** button.
3. In the Remote SNMP Agent Discovery window, click the **Refresh** toolbar button. The program clears the list and then discovers and displays SNMP agents that respond to newly specified SNMP access parameters. Alternatively, click the **Start Remote SNMP**

Agents Discovery toolbar button and MIB Browser will add the newly discovered SNMP agents to the existing ones in the Remote SNMP Agent Discovery window.

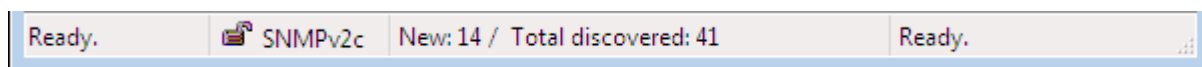


Figure 135: Remote SNMP Agent Discovery window status bar

Note: The status bar of the Remote SNMP Agent Discovery window displays the number of new discovered SNMP agents and the total number of SNMP agents displayed in the window (Figure 135).

14.2 Obtaining More Information About Discovered SNMP Agents

To get more information about the discovered SNMP agents listed in the Remote SNMP Agent Discovery window:

1. Select one or more lines representing SNMP agents in the list and choose the **Standard Info Window** or the **Query Whole MIB Tree** pop-up command.
2. MIB Browser opens one **Info window** for every selected SNMP agent (Figure 136) and queries the agent(s) to retrieve and display more information about the agent(s).

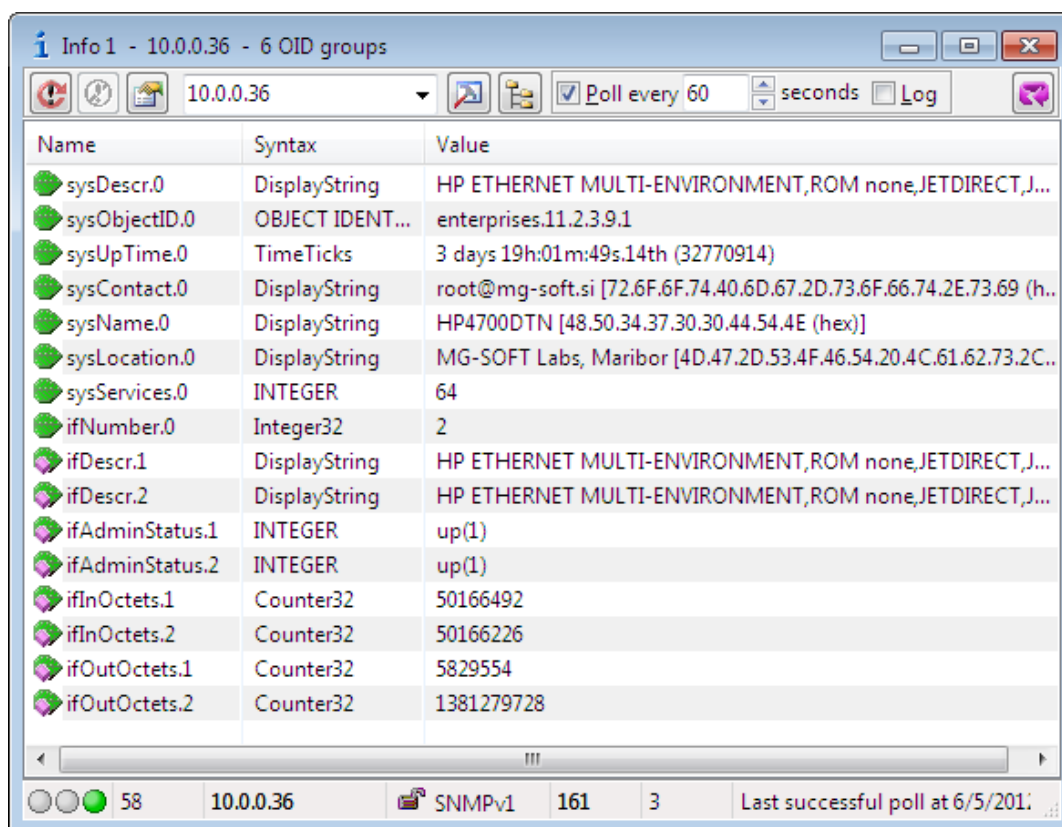



Figure 136: Info window displaying more information about a discovered SNMP agent

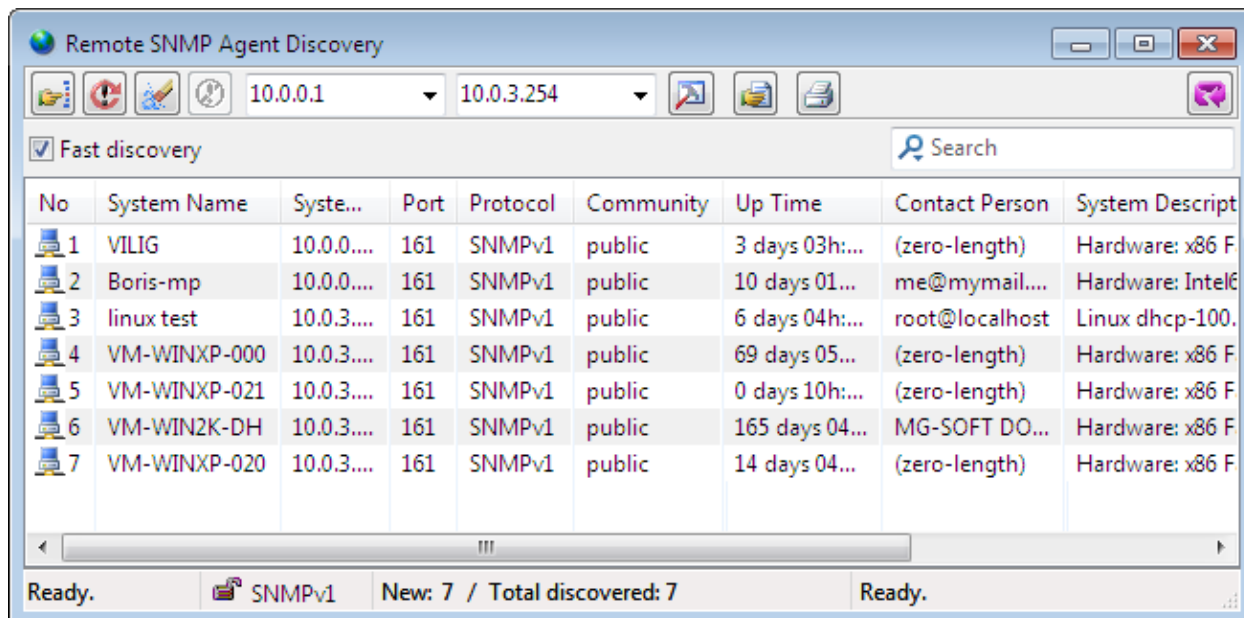
You can quickly create SNMP agent profiles for discovered SNMP agents, as described in the [To create SNMP agent profiles for discovered SNMP agents](#) section.

14.3 Example: How to Discover Only SNMP Agents Implementing a Specific OID

How to discover only those SNMP agents on a particular IP range that implement the HOST-RESOURCES-MIB module (i.e., `hrSystemUptime.0` OID) and support the SNMPv1 protocol version?

First, configure MIB Browser to discover only those SNMP agents that implement (return a value of) a specific object instance. To do this, select the **View / MIB Browser Preferences** command to open the MIB Browser Preferences dialog box and switch to the Discovery view in it. In the Discovery Window Preferences panel, check the **Discover only agents implementing selected OID** checkbox and into the accompanying **OID** input line enter the `hrSystemUptime.0` object instance (`1.3.6.1.2.1.25.1.1.0`). Alternatively, click the **Select OID from MIB tree** button () next to the **OID** input line and select the desired node (and its OID) from the MIB tree. In the **Operation** drop-down list, select the **Get Request**. This way, MIB Browser will use the SNMP Get operation to query the specified object instance while performing the discovery operation.

Open the Remote SNMP Agent Discovery window by using the **Tools / Discovery Window** command. Specify the IP range, on which you wish to discover the SNMP agents. To open the SNMP Protocol Preferences dialog box, click the **SNMP Protocol Preferences** toolbar button. In the SNMP Protocol Version frame, select the **SNMPv1** radio button and click the **OK** button. Click the **Start Remote SNMP Agents Discovery** toolbar button in the Remote SNMP Agent Discovery window and MIB Browser will display a list of SNMP agents that implement the specified OID and support the SNMPv1 protocol version (Figure 137).



The screenshot shows the 'Remote SNMP Agent Discovery' window. At the top, there are IP range dropdowns set to '10.0.0.1' and '10.0.3.254'. Below these is a 'Fast discovery' checkbox which is checked. A search bar is also present. The main area contains a table with 9 columns: No, System Name, System IP, Port, Protocol, Community, Up Time, Contact Person, and System Description. There are 7 rows of data. At the bottom, a status bar shows 'Ready.', 'SNMPv1' selected, and 'New: 7 / Total discovered: 7'.

No	System Name	Syste...	Port	Protocol	Community	Up Time	Contact Person	System Descript
1	VILIG	10.0.0....	161	SNMPv1	public	3 days 03h:...	(zero-length)	Hardware: x86 F
2	Boris-mp	10.0.0....	161	SNMPv1	public	10 days 01...	me@mymail...	Hardware: IntelE
3	linux test	10.0.3....	161	SNMPv1	public	6 days 04h:...	root@localhost	Linux dhcp-100.
4	VM-WINXP-000	10.0.3....	161	SNMPv1	public	69 days 05...	(zero-length)	Hardware: x86 F
5	VM-WINXP-021	10.0.3....	161	SNMPv1	public	0 days 10h:...	(zero-length)	Hardware: x86 F
6	VM-WIN2K-DH	10.0.3....	161	SNMPv1	public	165 days 04...	MG-SOFT DO...	Hardware: x86 F
7	VM-WINXP-020	10.0.3....	161	SNMPv1	public	14 days 04...	(zero-length)	Hardware: x86 F

Figure 137: A list of discovered SNMP agents that implement a specific OID

15 MONITOR SNMP AGENTS IN INFO WINDOWS

In this section, you will learn how to use the Info windows to continuously monitor arbitrary sets of object instance values in one or more SNMP agents and optionally save the retrieved values to CSV files for post-processing in external applications.

15.1 Monitoring SNMP Agent in Info Window

1. In the main window, switch to the **Query** tab.
2. In the **Remote SNMP Agent** drop-down list, specify the IP address of the SNMP agent that you wish to monitor.
3. If necessary, adjust the SNMP access parameters in the SNMP Protocol Preferences dialog box (**View / SNMP Protocol Preferences**).
4. Expand the MIB tree and click a node or a group of nodes (e.g., `system` node) that you wish to query in the Info window.
5. In the main menu, select the **Tools / Info Window** command.
6. MIB Browser opens the Info window. It displays a list of selected object instances, with their names, syntaxes and current values (Figure 138), and repeatedly queries them.

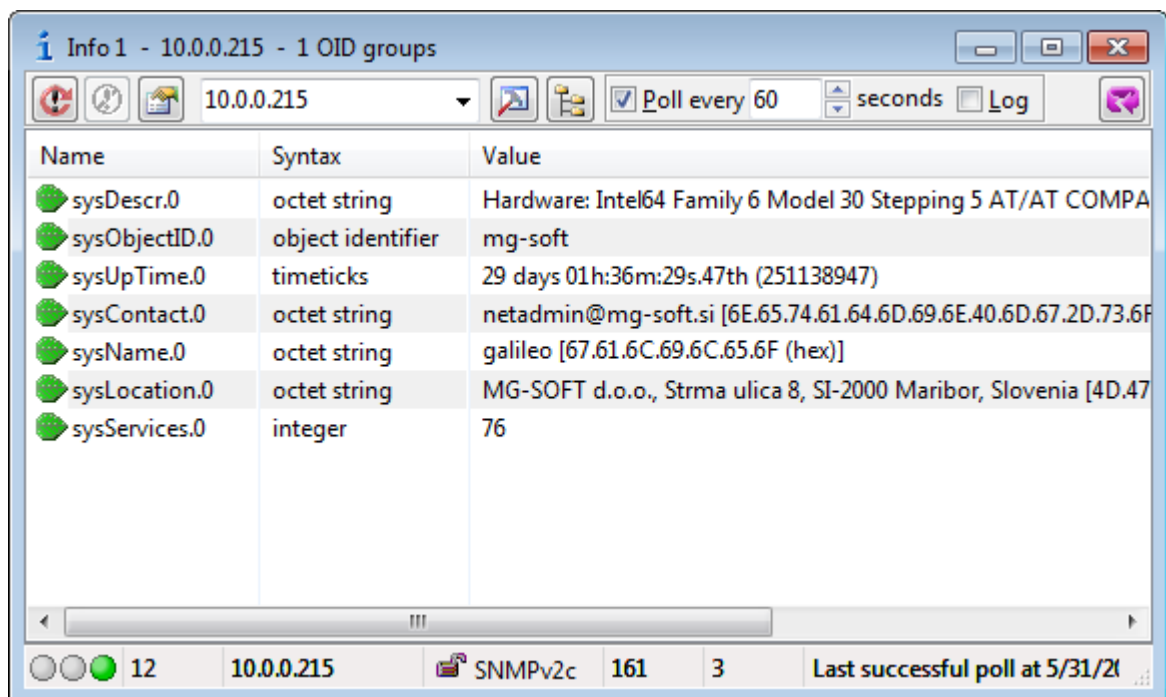


Figure 138: Info window with a list of repeatedly queried object instances

Note: If you select the root node of the MIB tree (called `MIB Tree`) in the main window and open an Info window, MIB Browser will display a list of all object instances implemented in the managed device.

15.1.1 Editing the List of Object Instances Monitored in Info Window

You can edit the list of object instances that are monitored in Info window by removing or adding OID values to the list. You can also change the type of the operation MIB Browser uses when it queries the selected OID values.

To change the set of object instances that are monitored in the Info window, click the **Info Window Properties** toolbar button. The Info Window Properties dialog box appears (Figure 139). It contains a list of all OID values of object instances that are currently monitored in the Info window together with the Query Operation Type information for each instance.

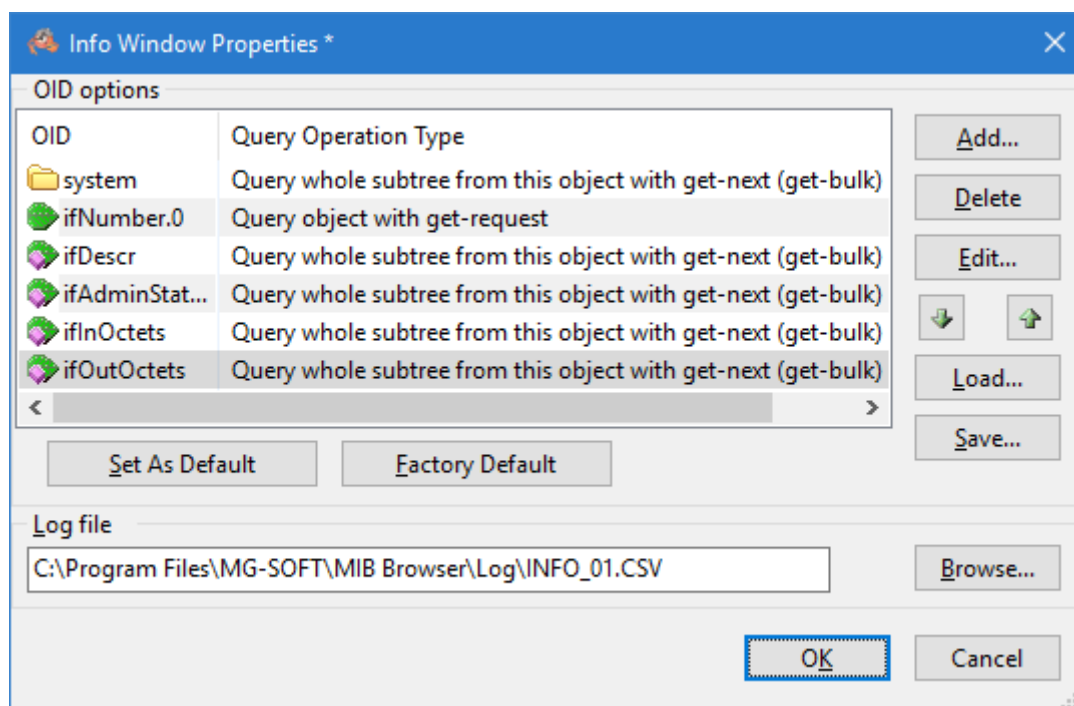
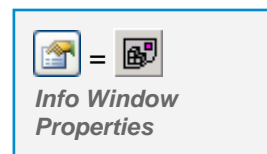
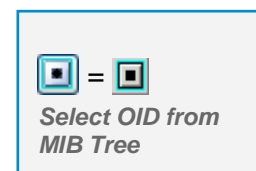


Figure 139: Info Window Properties dialog box

Adding Object Instances to Be Monitored

To add object instances that shall be monitored in the Info window:

1. In the Info Window Properties dialog box click the **Add** button.
2. The Select OID To Query dialog box appears (Figure 140).
3. In the **Start OID** drop-down list, specify the OID value of the object instance or a group of object instances that you wish to add. You can also click the **Select OID from MIB Tree** toolbar button and select the OID in the MIB tree.
4. In the Query Operation Mode frame, choose one of the following query operation types for the selected object instance:



- ❑ **Query object with get-request** - to query the specified object instance with the SNMP Get request, which retrieves the value of the same object instance of which OID was sent in request.
- ❑ **Query whole tree from start object with get-next or get-bulk** - to query all object instances in the MIB tree with the SNMP GetNext or GetBulk request from the object specified in the Start OID drop-down list.
- ❑ **Query whole subtree from start object with get-next or get-bulk** - to query all object instances of the selected sub tree with the SNMP GetNext or GetBulk request from the object specified in the Start OID drop-down list.

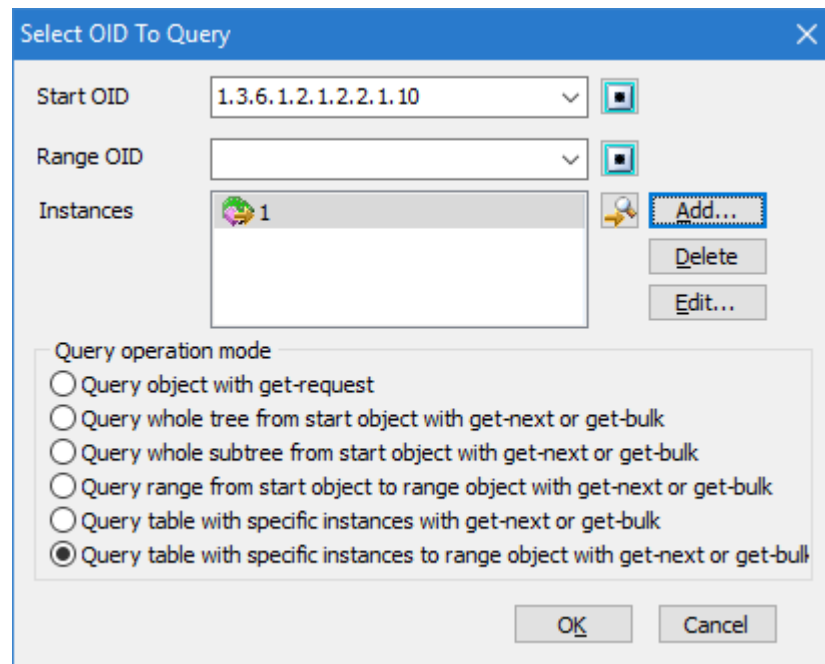


Figure 140: Select OID To Query dialog box

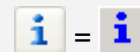
- ❑ **Query range from start object to range object with get-next or get-bulk** - to query all object instances in the MIB tree from the object specified in the Start OID drop-down list to the object specified in the Range OID drop-down list with the GetNext or GetBulk request.
 - ❑ **Query table with specific instances with get-next or get-bulk** - to query only the specified instances of a table with the GetNext or GetBulk request.
 - ❑ **Query table with specific instances to range object with get-next or get-bulk** - to query the specified instances of the table from the object specified in the Start OID drop-down list to the object specified in the Range OID drop-down list with the GetNext or GetBulk request.
5. Click the **OK** button. The Select OID To Query dialog box closes and the new OID values with the query operation type information are added to the list of currently used ones.

Removing Object Instances to Be Monitored

1. From the list of currently used OID values displayed in the Info Window Properties dialog box (Figure 139), select the OID or a group of OIDs that you wish to remove.
2. Click the **Delete** button. The items are removed.

Editing Object Instances to Be Monitored

1. In the Info Window Properties dialog box (Figure 139), click the OID that you wish to edit.
2. Click the **Edit** button. The Select OID To Query dialog box appears (Figure 140).
3. Specify a new OID in the **Start OID** drop-down list or change the query operation mode in the Query Operation Mode frame.
4. Click the **OK** button to close the Select OID To Query dialog box.



Remote SNMP Agent Info toolbar button opens the Info window with the default set of OID parameters.

Tip: Click the **Set As Default** button, to save the newly specified set of OIDs as the default OID set. After that when you open an Info window by using the **Remote SNMP Agent Info** toolbar button in the main window, the default set of OIDs will be used in this window.

5. Click the **OK** button to close the Info Window Properties dialog box.
6. The new set of OID values specifying the object instances is inserted into the Info window panel (Figure 141).

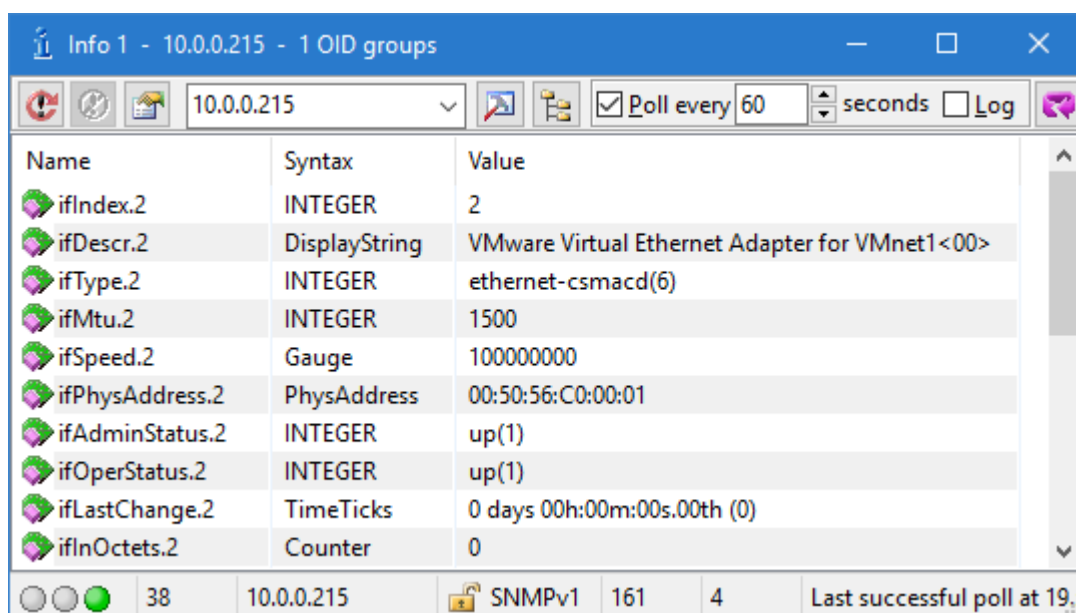
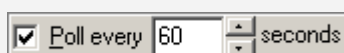


Figure 141: Info window with a new set of OIDs

If the **Poll every X seconds** checkbox is checked, the program continuously monitors the object instances specified in the Info window. You can change the polling interval by entering the new value into the **Poll every X seconds** input line.



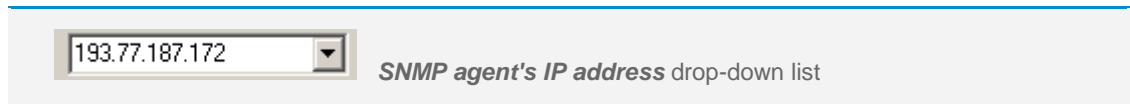
Poll every X seconds checkbox and input line

15.1.2 Monitoring Another SNMP Agent

You can change the SNMP agent currently monitored in the Info window or simply open another Info window to monitor a different SNMP agent in it, as described in section [15.2](#).

To change the SNMP agent in the current Info window:

1. In the Info window drop-down list with SNMP agent IP addresses, specify the IP address of the new SNMP agent.



2. Click the **Refresh** toolbar button to start monitoring the new SNMP agent.

15.1.3 Logging the Queried Object Instance Values

In the Info window, you can log the results of the monitoring to a file in CSV (comma separated values) format. You can then import the values into a database or a spreadsheet application (like Excel), for further processing.

Specifying CSV File

1. Right-click in the Info window panel and select the **Properties** pop-up command. The Info Window Properties dialog box appears ([Figure 139](#)).
2. In the Log File frame, enter the full path of the CSV log file for the Info window or use the **Browse** button to point at it.
3. Click the **OK** button to close the Info Window Properties dialog box and check the **Log** checkbox in the Info window.

15.2 Monitoring More SNMP Agents

MIB Browser can open up to 60 Info windows, which means that you can simultaneously monitor many SNMP agents.

To monitor more SNMP agents:

1. In the main window, switch to the **Query** tab.
2. Into the **Remote SNMP Agent** drop-down list, type or select the IP address of the SNMP agent that you wish to monitor.
3. If necessary, adjust the SNMP access parameters in the SNMP Protocol Preferences dialog box, which opens by selecting the **View / SNMP Protocol Preferences** command.
4. In the MIB tree, click the OID or a group of OIDs that you wish to query in the Info window.

5. In the main window, select the **Tools / Info Window** command. MIB Browser opens the Info window displaying a list of selected OIDs with their syntaxes and values.
6. Repeat the procedure to open as many Info windows as you like.

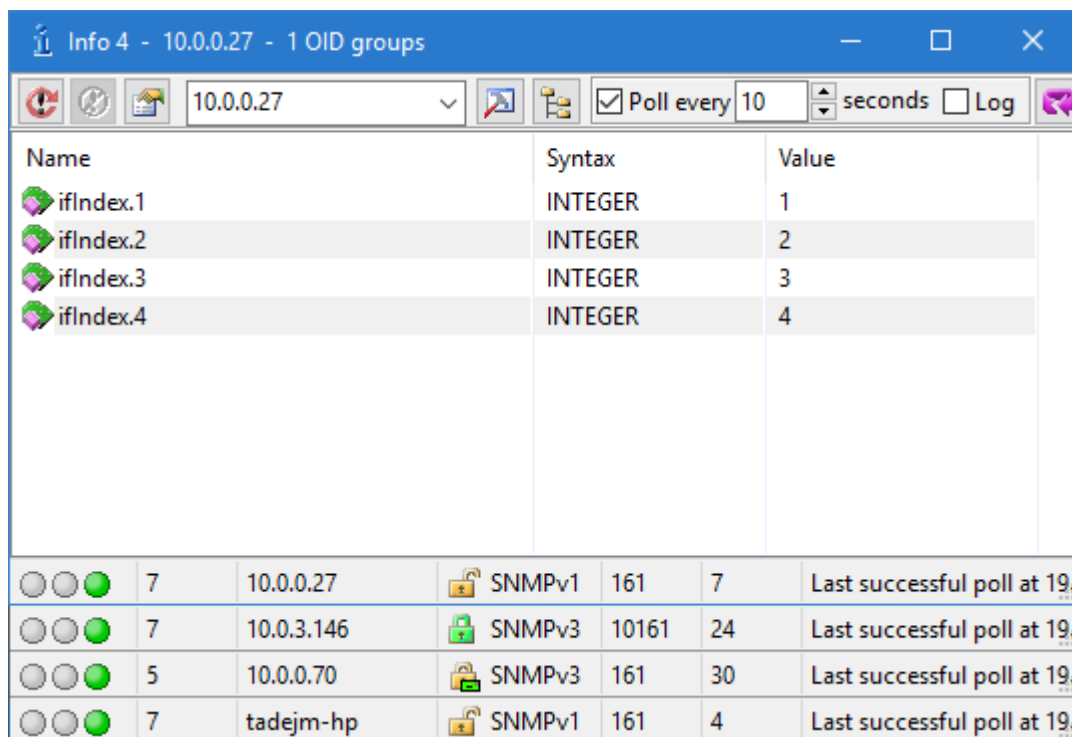


Figure 142: All opened Info windows arranged in ascending order

Tip: You can arrange the opened Info windows in ascending or descending order (Figure 142) by using the Window | Arrange 1 .. Max or Arrange Max .. 1 command in the main window.

16 SCAN SNMP AGENT FOR IMPLEMENTED MIB MODULES

In this section, you will learn how to use the Scan Agent For Implemented MIB Modules window to check which MIB modules are implemented in a particular SNMP agent.

MIB Browser can scan an SNMP agent by performing the SNMP Walk operation on the agent's MIB tree. It retrieves and checks all OIDs implemented in the scanned SNMP agent and searches for MIB modules that resolve these OIDs. Note that MIB Browser detects and displays only compiled and registered MIB modules.

16.1 Searching for Implemented MIB Modules

To check which MIB modules are implemented in a particular SNMP agent:

1. Open the Scan Agent For Implemented MIB Modules window, by selecting the **Tools / Scan Agent For MIBs** command in the main window.
2. The Scan Agent For Implemented MIB Modules window opens (Figure 143).

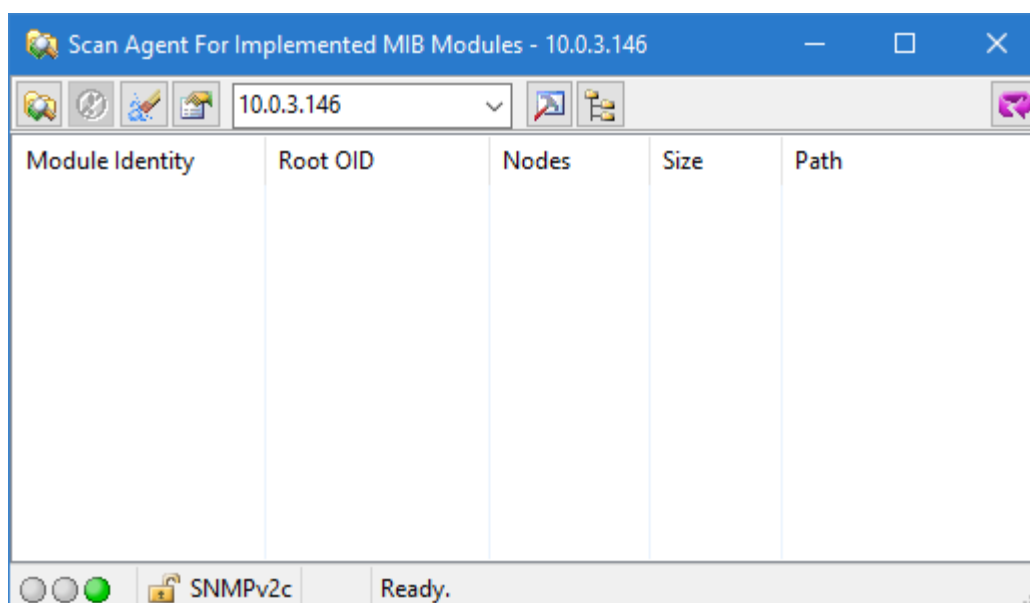
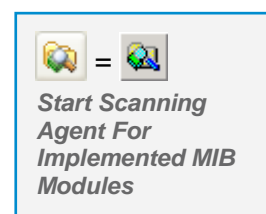


Figure 143: Scan Agent For Implemented MIB Modules window

3. Into the agent's IP address drop-down list, specify the IP address of the SNMP agent that you wish to scan.
4. Additionally, you may change the SNMP protocol parameters in the SNMP Protocol Preferences dialog box (click the **SNMP Protocol Preferences** toolbar button).
5. To start the scanning operation, click the **Start Scanning Agent For Implemented MIB Modules** toolbar button.
6. MIB Browser scans the selected SNMP agent, and in the window's panel, displays a list of all compiled MIB modules (Figure 144) that are implemented in the scanned SNMP agent.



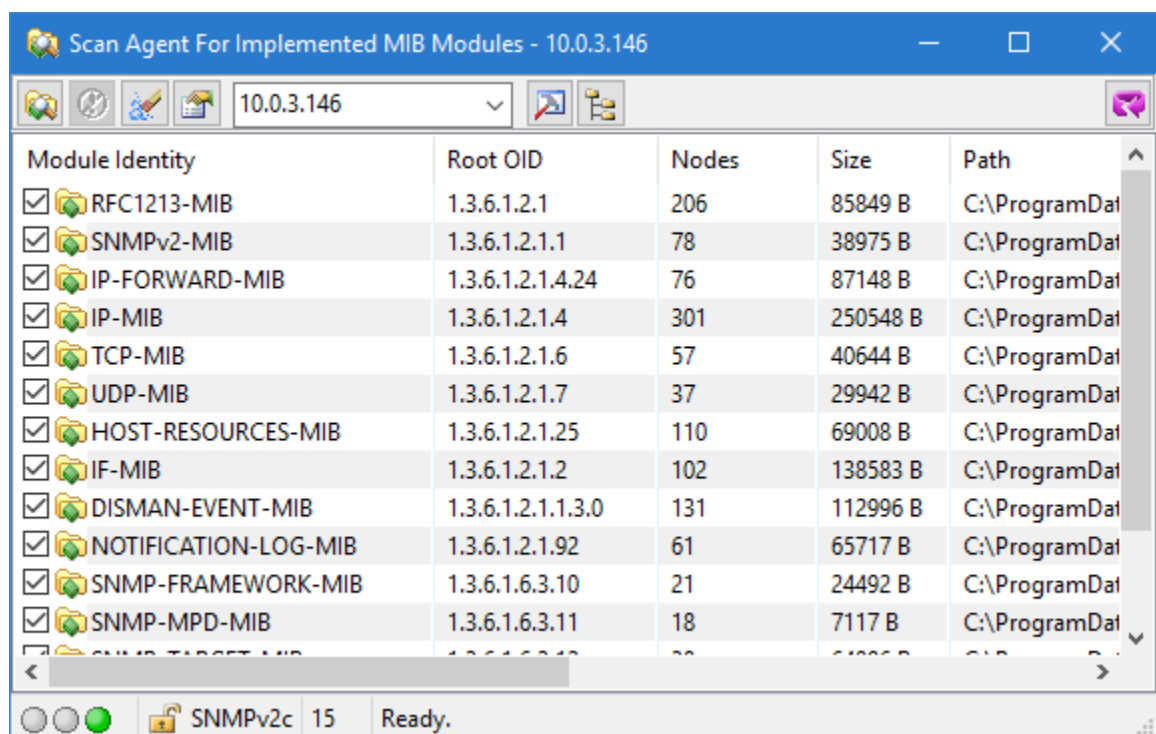


Figure 144: Scan Agent For Implemented MIB Modules window with a list of MIB modules implemented in the scanned SNMP agent

Note: By default, MIB Browser scans for all MIB modules that resolve the OID values retrieved from the scanned SNMP agent. If you want MIB Browser to display only the first MIB module that resolves a particular OID, open the Scan Agent For Implemented MIB Modules Preferences dialog box (Figure 145, **Preferences** toolbar button) and uncheck the **Scan for all MIB modules that resolve OID** checkbox.

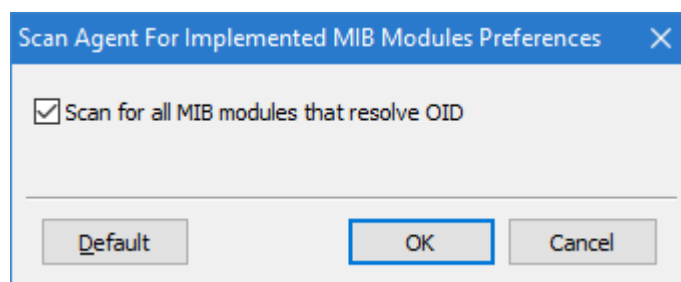
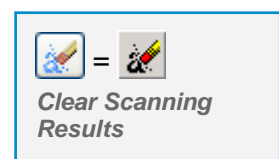
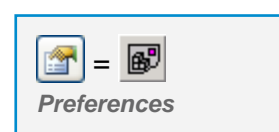


Figure 145: Scan Agent For Implemented MIB Modules Preferences dialog box

To scan another SNMP agent:

1. First clear the window's panel by clicking the **Clear Scanning Results** toolbar button.
2. Specify the IP address of the SNMP agent that you wish to scan and click the **Start Scanning Agent For Implemented MIB Modules** toolbar button.



3. MIB Browser displays a list of MIB modules implemented in the newly specified SNMP agent.

Tip: If you wish to save the scanning results to a file, right-click in the window panel and copy the results to the clipboard. After that, paste the scanning results in any `.txt` application (e.g., Notepad).

Example:

How to check which (registered) MIB modules are implemented in a particular SNMP agent?

You can check which of the compiled MIB modules are implemented in a particular SNMP agent by using the Scan Agent For Implemented MIB Modules window. To open the Scan Agent For Implemented MIB Modules window, select the **Tools / Scan Agent For MIBs** command. When the window opens, specify into the drop-down list the IP address (e.g., 193.77.187.172) of the SNMP agent that you wish to scan. If necessary, change the parameters in the SNMP Protocol Preferences dialog box, which opens by clicking the 'Hammer' toolbar button. To scan the SNMP agent, click the **Start Scanning Agent For Implemented MIB Modules** toolbar button in the Scan Agent For MIB Modules window. MIB Browser scans the selected SNMP agent by performing the SNMP Walk operation on its MIB tree. It searches all compiled and registered MIB modules to determine which of them resolve the retrieved OIDs and displays such MIB modules in the Scan Agent For Implemented MIB Modules window.

16.2 Loading MIB Modules Implemented in SNMP Agent

From the Scan Agent For Implemented MIB Modules window, you can load into MIB Browser any of the discovered MIB modules.

1. Scan an SNMP agent for its implemented MIB modules as described in the [Searching for Implemented MIB Modules](#) section.
2. In the Scan Agent For Implemented MIB Modules window, check the checkboxes in front of the names of MIB modules that you wish to load.
3. After you have specified which MIB modules you wish to load, right-click in the window panel and use the **Load Checked Modules** pop-up command ([Figure 146](#)).
4. MIB Browser loads the selected MIB modules into MIB Browser.
5. You can see the list of all MIB modules that are currently loaded in MIB Browser in the main window (MIB tab / Loaded MIB modules frame).

Note: By using the **Save MIB Group** pop-up command, you can save any number of MIB modules implemented in an SNMP agent to a MIB group. You can check the list of all MIB groups in the main window (MIB tab / MIB Groups tab).

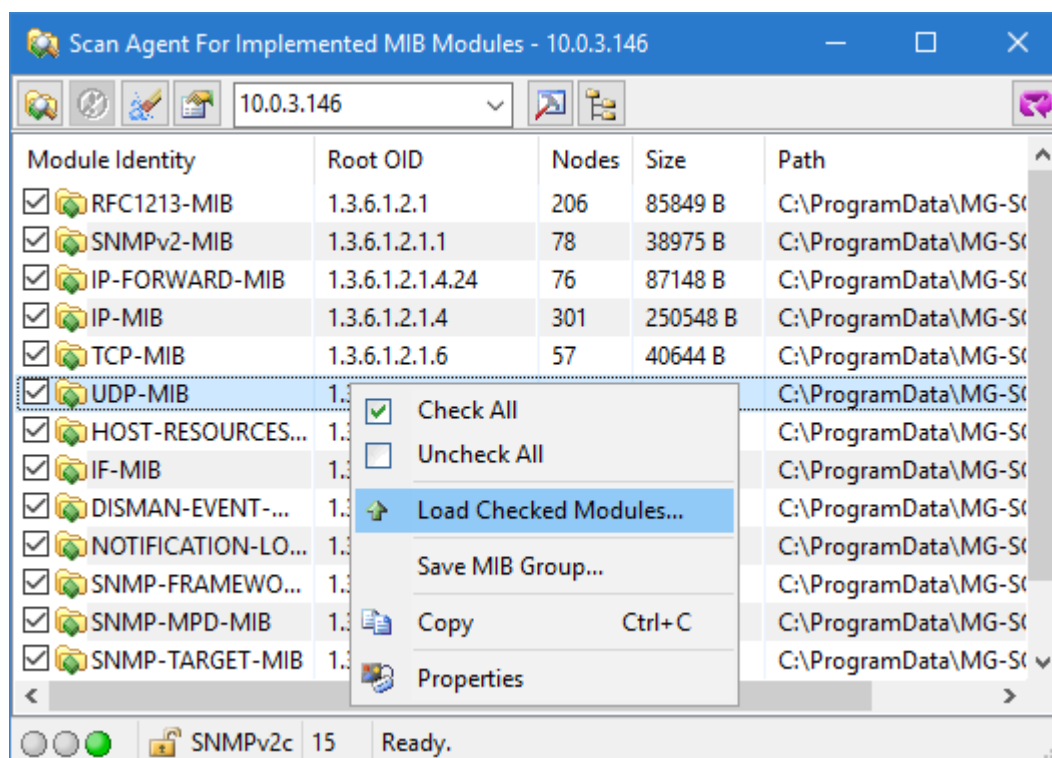


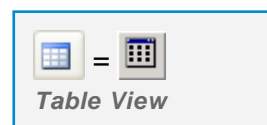
Figure 146: Loading MIB modules from the Scan Agent For Implemented MIB Modules window

17 VIEW, POLL AND MODIFY SNMP TABLES

In this section, you will learn how to use the Table View window to view and poll an SNMP table in a tabular form. You will also learn how to easily modify table instance values directly in the table view as well as how to add new rows to the table.

17.1 Viewing and Polling SNMP Tables in Tabular Form

1. Switch to the **Query** tab in the main window.
2. Into the **Remote SNMP Agent** drop-down list, type or select the IP address of the SNMP agent that you wish to manage.
3. If necessary, adjust the SNMP access parameters in the SNMP Protocol Preferences dialog box, which opens by selecting the **View / SNMP Protocol Preferences** command.
4. Contact the remote SNMP agent by using the **SNMP / Contact** command.
5. Expand the MIB tree and click a table node (e.g., `ifTable`) or a table entry node (e.g., `ifEntry`).
6. Select the **Tools / Table View** command or click the **Table View** toolbar button.
7. MIB Browser opens the Table View window and displays the selected table in a tabular form (Figure 147).



Instance	ifIndex...	ifDesc...	ifType...	ifMtu...	ifSpeed...	ifPhysAddress...	ifAdminStatus...	ifOperSta
1	1	Softw...	softw...	1500	107374...	(zero-length)	up(1)	up(1)
2	2	VMwa...	ether...	1500	100000...	00:50:56:C0:00...	up(1)	up(1)
3	3	Micro...	131	1280	100000	00:00:00:00:00...	up(1)	down(2)
4	4	Remo...	ether...	0	0	(zero-length)	down(2)	6
5	5	Intel(...	ether...	1500	100000...	D4:85:64:0F:8...	up(1)	up(1)
6	6	Micro...	131	1280	100000	00:00:00:00:00...	up(1)	down(2)
7	7	Micro...	ether...	0	0	(zero-length)	down(2)	6
8	8	VMwa...	ether...	1500	100000...	00:50:56:C0:00...	up(1)	up(1)

Figure 147: Table View window

8. If you check the **Poll every X seconds** checkbox in the window toolbar, you can continuously poll the displayed SNMP table and get its recent values every X seconds.

Tip: You can configure MIB Browser to retrieve table values row-by-row when polling an SNMP table. To enable this function, open the MIB Browser Preferences dialog box (**View / MIB Browser Preferences** command) and in the Table View Window Preferences panel, check the **Poll one row at a time** checkbox. Note that when using this query algorithm, you should not be using the SNMP GetBulk operation (adjustable in the SNMP Protocol Preferences dialog box).

You can mirror the contents of the Table View window (Figure 148) by checking the **Mirror** checkbox.

Object	1	2	3	4	5	6	7	8	9	10
ifIndex(1, IDX)	1	2	3	4	5	6	7	8	9	10
ifDescr(2)	Soft...	VMw...	Micr...	Rem...	Intel...	Micr...	Micr...	VMw...	ZyD...	M...
ifType(3)	soft...	ether...	131	ether...	ether...	131	ether...	ether...	71	etl
ifMtu(4)	1500	1500	1280	0	1500	1280	0	1500	0	0
ifSpeed(5)	1073...	1000...	100000	0	1000...	100000	0	1000...	0	0
ifPhysAddress(6)	(zero...	00:50...	00:00...	(zero...	D4:8...	00:00...	(zero...	00:50...	(zero...	(ze
ifAdminStatus(7)	up(1)	up(1)	up(1)	dow...	up(1)	up(1)	dow...	up(1)	dow...	dc
ifOperStatus(8)	up(1)	up(1)	dow...	6	up(1)	dow...	6	up(1)	6	6

Figure 148: Mirrored contents of the Table View window

Red Circle With Exclamation Mark

A MIB object icon with exclamation mark (!) in a red circle appears if at least one columnar object of the displayed table is not implemented in the monitored SNMP agent. Such an icon designates that MIB Browser cannot retrieve the value of the columnar object instance for this row. It also appears in case a timeout occurs while retrieving this row.

17.1.1 Adjusting Tabular Column Widths

You can use the Table View window pop-up menu to adjust the tabular column widths:

- ☐ To their default values (**Adjust as Default**).
- ☐ According to the header width or the widest cell (**Adjust Header and Cell Width**).
- ☐ According to the header width (**Adjust Header Width**).
- ☐ According to the widest cell value (**Adjust Cell Width**).

Tip: If a table OID base syntax is OCTET STRING, the OID value in the Table View window is displayed together with HEX dump in the brackets. If you find this disturbing, then open the MIB Browser Preferences dialog box by using the **View / MIB Browser Properties** command, switch to the Query Results Preferences panel and uncheck the **Extend value information** checkbox.

17.1.2 Copying Displayed SNMP Table

To copy the contents of an SNMP table displayed in the Table View window to the clipboard, do the following:

1. Right-click in the Table View window panel and use the **Copy** pop-up command.
2. MIB Browser copies the contents of the displayed SNMP table and saves it to the clipboard.
3. Open some other application (e.g., Notepad, Word, etc.) and paste the saved SNMP table.

17.2 Modifying Table Object Instance Values

MIB Browser allows you to easily modify and set values of writable table object instances directly in the Table View window (Figure 149). To see the instructions on how to do that, check the [Modifying Values of Table Object Instances Directly in Table View](#) section.

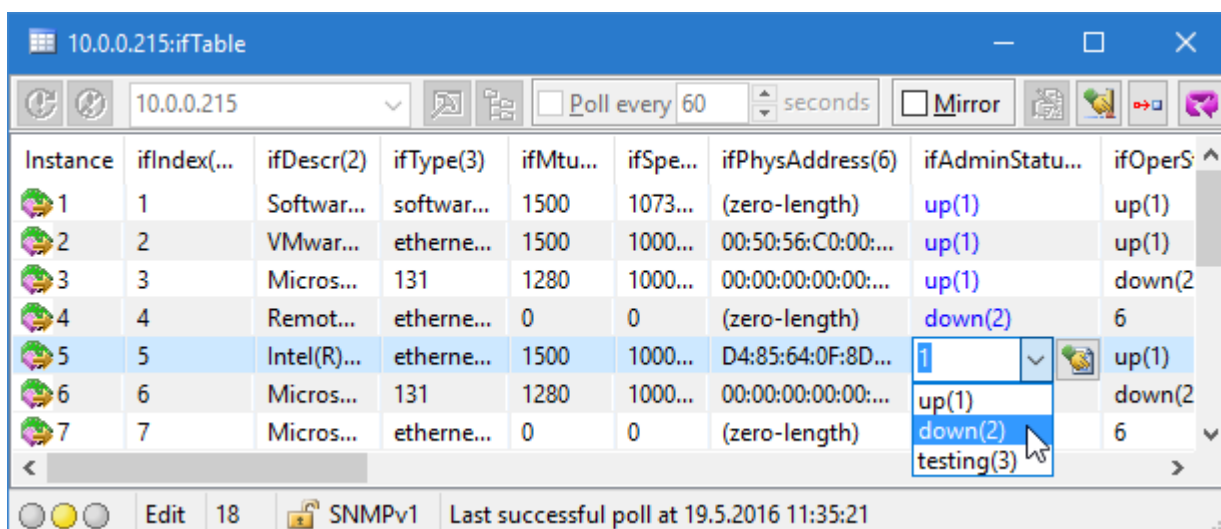


Figure 149: Editing values of table object instances directly in the table view

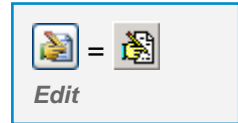
17.3 Adding Row to SNMP Table

The Table View window also allows you to add new rows to a displayed SNMP table. To add a new row to an SNMP table:

1. In the main window MIB tree, click a table node, or entry node, of the SNMP table to which you wish to add a row.

Note: Before adding a row to an SNMP table, make sure that the table supports the add row functionality.

2. Open the Table View window by selecting the **Tools / Table View** command. When the Table View window opens, MIB Browser displays the selected SNMP table in a tabular form (Figure 147).
3. To enable table editing, click the **Edit** button in the Table View window toolbar.
4. Instance values with **read-write** or **read-create** access are colored (blue by default).



Tip: You can specify the color of creatable and writable table object instances in the MIB Browser Preferences dialog box (Edit Table View Window Preferences panel / Colors frame).

5. To add a new row, display the Table View window pop-up menu and use the **Add Row** command.
6. The Add New Table Instance dialog box opens (Figure 150). Specify the instance and index of the new row and click the **OK** button.

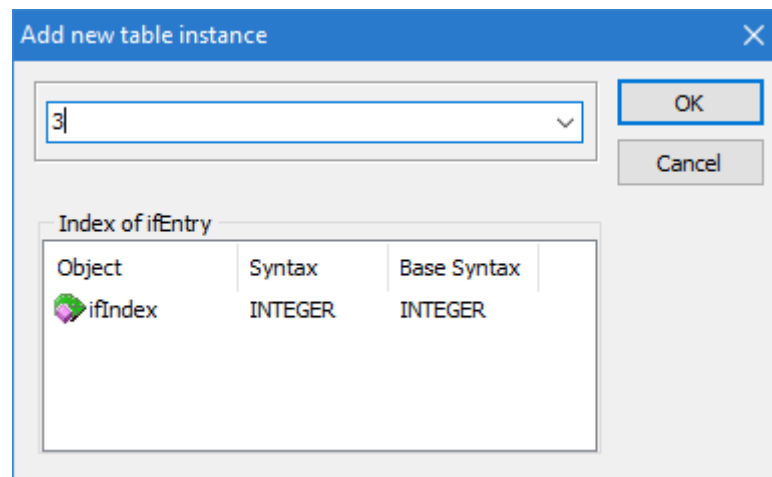
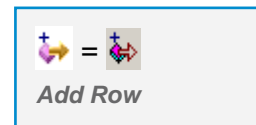


Figure 150: Add New Table Instance dialog box

7. The new row is added to the SNMP table displayed in the Table View window.
8. In the new row, you can edit any table object instance value that can be modified. For instructions see the [Modifying Values of Table Object Instances Directly in Table View](#) section
9. To create the added row in the contacted SNMP agent, click the **Commit** toolbar button.



18 GRAPHIC REPRESENTATION OF OBJECT INSTANCE VALUES

This section describes how to use the Performance Graph window to monitor the values of numerical MIB object instances in form of a graph (line chart).

You can open the Performance Graph window and start graphing the desired SNMP variables (values of MIB object instances) in several ways:

The easiest way to start graphing a SNMP variable is to select a scalar or columnar object of a numeric type in the MIB tree and choose the **Graph** pop-up command on it, as described in the following section.



You can also open a new Performance Graph window from the **Tools** menu and then add variables to it by clicking the **New Graph** button and specifying the variable properties in the dialog box that appears or by using the **drag&drop** technique to add numerical objects (leaf nodes) from the MIB tree in the main window to the Performance Graph window, as explained in the section [18.2](#).

Several Performance Graph windows can be open at the same time and each can monitor one or more variables from one or more SNMP agents.

18.1 Start Graphing Operation Directly from MIB Tree

1. After successfully [contacting the SNMP agent](#), expand the MIB tree in the MIB Browser main window and select a numeric scalar object (e.g., `tcpInErrs`) or columnar object (e.g., `ifInOctets`), whose instance(s) you wish to monitor in a graph (line chart).

Note: Valid objects are those that have a numeric base syntax (e.g., Integer, Counter, Gauge, Timeticks,...). You can view the syntax of any MIB object in the [MIB Node Properties](#) window.

2. If you have selected a scalar object () , right-click it and choose the **Graph** command from the pop-up menu. Proceed in step 6 below.
3. If you have selected a columnar object () , right-click it and choose the **Graph / Select Instance** command from the pop-up menu.
4. The Select Table Instance(s) window appears, displaying all existing instances of the selected columnar object (including the syntax and current value of each object instance).

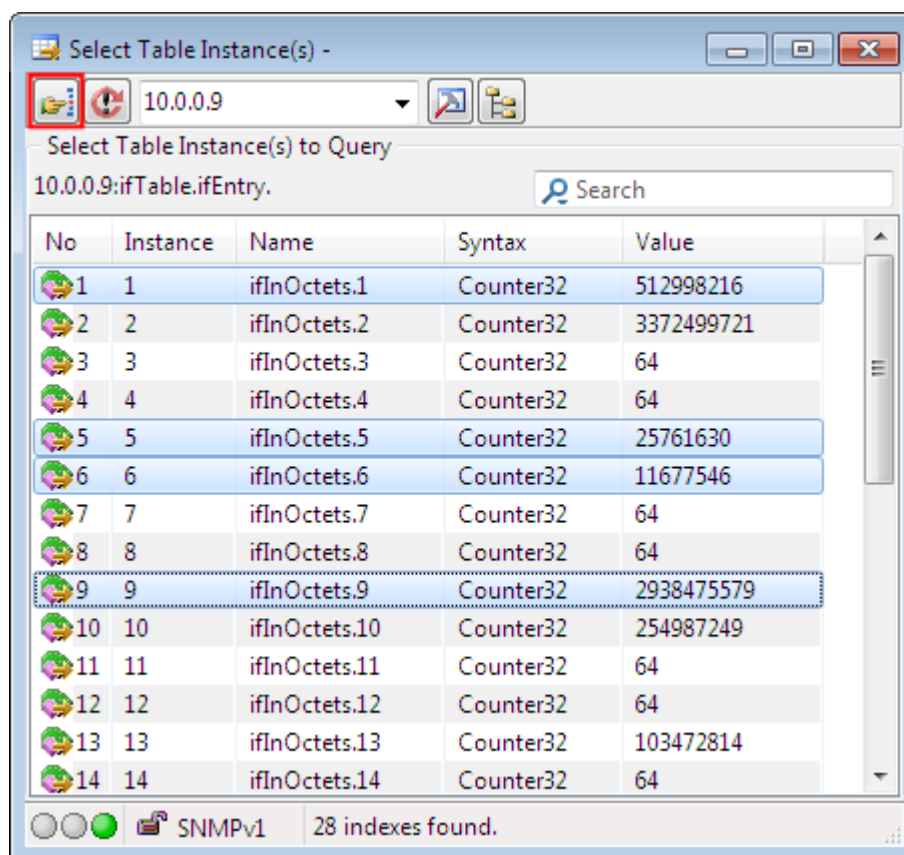


Figure 151: Selecting the instances of a columnar object to be plotted in the same graph

5. Select one or more instance that you wish to graph (use SHIFT+Click to select adjacent rows or CTRL+Click to select non-adjacent rows) and click the **Use Selected Instances** button in the Select Table Instance(s) window.
6. The Graph Line Type dialog box appears, prompting you to select the value to be plotted. Select one of the following:
 - ☐ **Value** - Absolute value of the object instance as retrieved from the SNMP agent.
 - ☐ **Delta** - Difference in the object instance value of the current and previous query.
 - ☐ **Delta/Sec** - Difference in the object instance value of the current and previous query divided by the length of the polling interval.
7. The selected object instance(s) are added as variables to the **Legend** (lower) panel of the Performance Graph window. MIB Browser starts polling the specified SNMP agent and plotting the retrieved values as graph lines in the Performance Graph window (Figure 152).

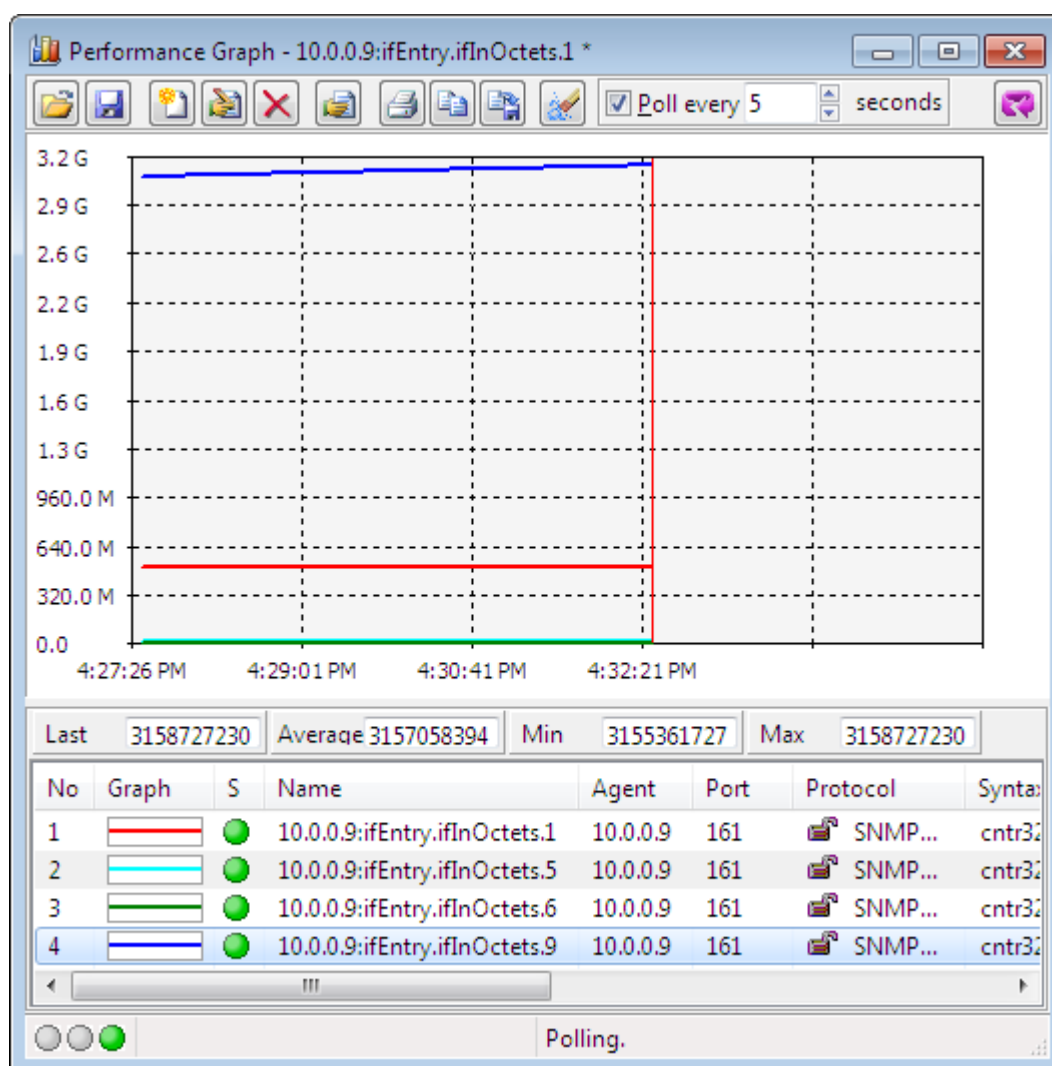


Figure 152: Monitoring values of 4 SNMP variables in the Performance Graph window

18.1.1 Changing the Polling Interval

You can change the polling interval in the Performance Graph window by modifying the **X** parameter in the **Poll every X seconds** input line in the toolbar of the Performance Graph window.

18.1.2 Pausing and Resuming the Graphing Operation

If you wish to pause the graphing operation, uncheck the **Poll every X seconds** checkbox in the Performance Graph window. The program stops polling the specified SNMP agent(s) and plotting the graph line(s). Check this checkbox again to resume the graphing operation.

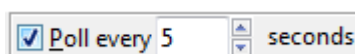


Figure 153: Start/pause the graphing operation and specify the polling interval

18.2 Start Graphing Operation in Conventional Way

This section explains how to open a Performance Graph window from the **Tools** menu and add variables to it by clicking the **New Graph** button and specifying the variable properties in the dialog box that appears and by using the **drag&drop** technique to add numerical objects (leaf nodes) from the MIB tree in the main window to the Performance Graph window.

1. In the main window, select the **Tools / Performance Graph** command or click the **Graph** toolbar button.
2. A new, empty Performance Graph window appears (Figure 154).

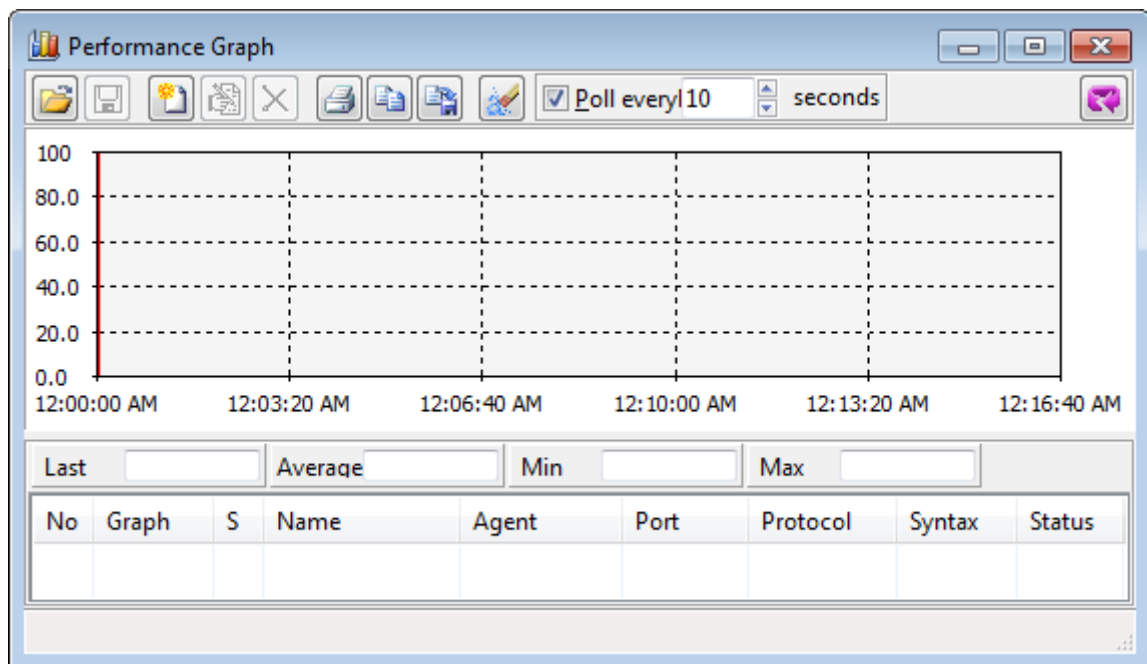
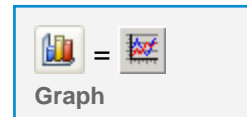


Figure 154: Empty Performance Graph window

When the Performance Graph window is displayed, you can either load already defined graph parameters from a previously **saved** MIB Browser Graph (XML) file or specify new parameters in the Graph Properties dialog box.

18.2.1 Loading Graph Parameters From File

1. Click the **Load Graph From File** toolbar button in the Performance Graph window.
2. The Open dialog box appears.
3. Select an *.mbgx or *.mbg file that you want to load and click the **Open** button. See also the
4. [Appendix: MIB Browser File Formats](#).
5. The program starts plotting a graph in the Performance Graph window (Figure 156).



18.2.2 Adding a Variable to Performance Graph Window

To add a new variable to the Performance Graph window, click the **New graph** toolbar button or select the **New Graph** pop-up command. This will open the Graph Properties dialog box (Figure 155).

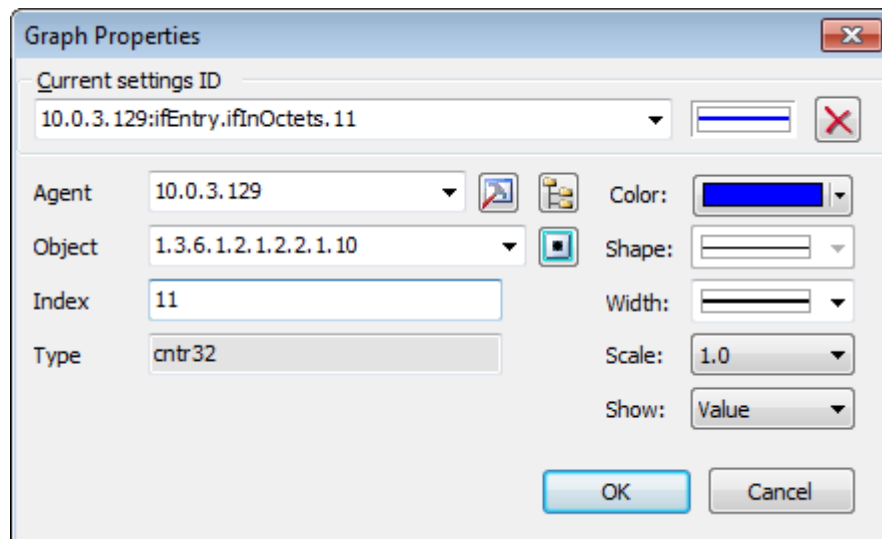


Figure 155: Graph Properties dialog box

Specifying Variable Properties

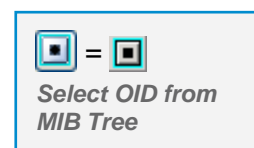
To specify variable properties in the Graph Properties dialog box, you can select one of the existing set of parameters from the **Current settings ID** drop-down list or you can specify the parameters manually, following the guidelines below:

1. To define or change a remote SNMP agent, enter the agent's IP address or select it from the **Agent** drop-down list.

Tip: If you wish to adjust SNMP access parameters, click the **SNMP Protocol References** toolbar button and define them in the SNMP Protocol Preferences dialog box.

2. Into the **Object** input line, enter the OID of the object that you wish to monitor. The object must have a numerical base syntax (e.g., Integer, Counter, Gauge, etc.). You need to specify the instance of the object by entering it into the **Index** input line (Figure 155). For scalar objects the instance is zero (0). For columnar objects you can specify the instance by selecting it from the Select Table Instance(s) window.

The desired object can also be selected from the MIB tree in the Select Object Identifier window, which displays after clicking the **Select OID from MIB Tree** toolbar button. If you select a columnar object, the **Select Table Instance(s)** window appears, where you can select the desired instance by double-clicking it in the window.



3. On the right side of the Graph Properties dialog box, select the color, shape and width of the graph line and adjust the scale, if necessary.

4. From the **Show** drop-down list, select among:
 - ☐ **Value** - The graph shows the actual value retrieved from the SNMP agent.
 - ☐ **Delta/Interval** - The graph shows the difference between the currently and the previously polled value.
 - ☐ **Delta/Sec** - The graph shows the difference between the currently and the previously polled value divided by the length of the polling interval.
5. Click the **OK** button to close the Graph Properties dialog box. The program starts plotting a graph line (Figure 156).

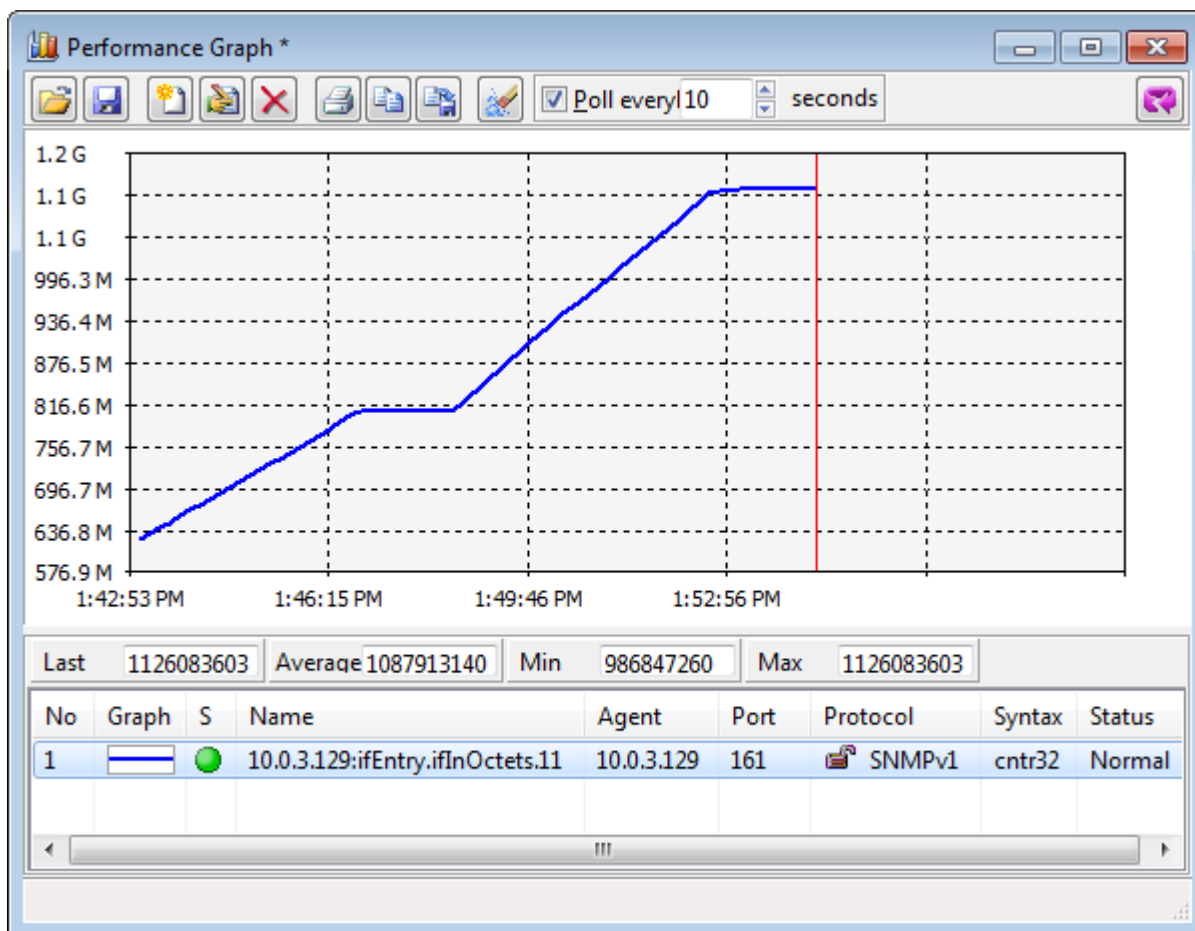


Figure 156: Retrieved values of an object instance presented in a graph chart

Note: In the Performance Graph window, the Legend panel below the Graph panel contains a list of currently displayed graph lines with their properties. Above the graph list, you can see the last, average, minimum and maximum value of the currently selected graph line.

Tip: The window toolbar, legend and status line can be either shown or hidden by using the **View Toolbar**, **View Legend** and **View Status Line** toggle commands in the Performance Graph window pop-up menu. In the pop-up menu, you can also select between the **Fix Y Axis Lower Margin to 0** or the **Fix the Y Axis Lower Margin to the -10% range**, which is normally used when the monitored OID values are very low.

18.3 Adding Additional Variables to Graph

In the Performance Graph window, you can simultaneously monitor different variables from different SNMP agents.

To add more variables (object instances) to the Performance Graph window, you can either:

- ❑ Click the **New Graph** toolbar button (📊) in the Performance Graph window and specify the variable parameters in the Graph Properties dialog box that appears (see the [Adding a](#) section), or
- ❑ Drag&drop numerical objects (leaf nodes) from the MIB tree in the main window to the Performance Graph window ([Figure 157](#)).

18.3.1 Adding Variables by Using Drag&Drop Technique

1. After successfully [contacting the SNMP agent](#), expand the MIB tree and select a numeric scalar object (e.g., `tcpInErrors`) or columnar object (e.g., `ifInOctets`), whose instance(s) you wish to monitor in a graph (line chart).

Note: Valid objects are those that have a numeric base syntax (e.g., Integer, Counter, Gauge, Timeticks,..)

2. Drag&drop the selected object (leaf node) from the MIB tree in the main window to the Performance Graph window ([Figure 157](#)).

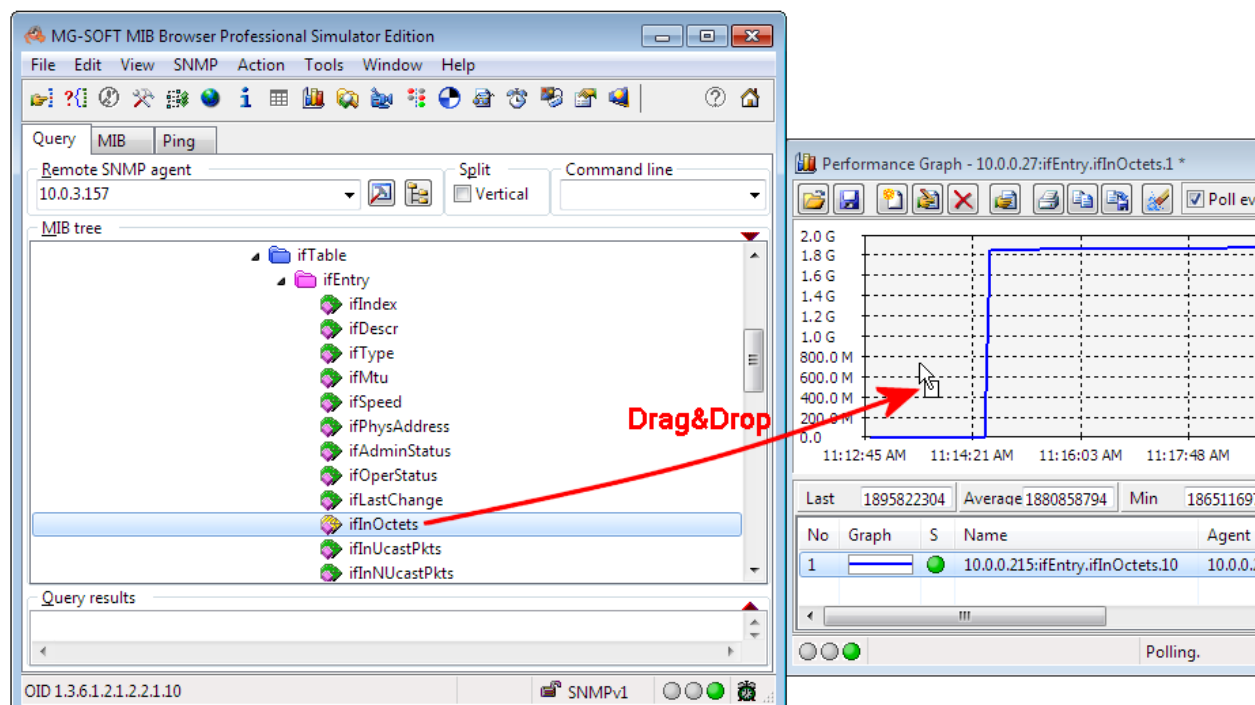


Figure 157: Using Drag&Drop technique to add a new variable to the Performance Graph window

- ❑ If you have used the drag&drop technique to add a scalar object, its only instance (.0) is automatically selected and the variable is added to the Performance Graph window (which starts plotting its value).
 - ❑ If you have used the drag&drop technique to add a columnar object, the **Select Table Instance(s)** window appears, displaying all existing instances of the selected columnar object (including the syntax and current value of each object instance). Select one or more instance that you wish to graph and click the **Use Selected Instances** button in the Select Table Instance(s) window ([Figure 151](#)).
3. The selected object instance(s) are added as new variables to the Legend (lower) panel of the Performance Graph window. MIB Browser starts polling the specified SNMP agent and plotting the retrieved values of new variables as graph lines in the Performance Graph window - upper panel ([Figure 158](#)).

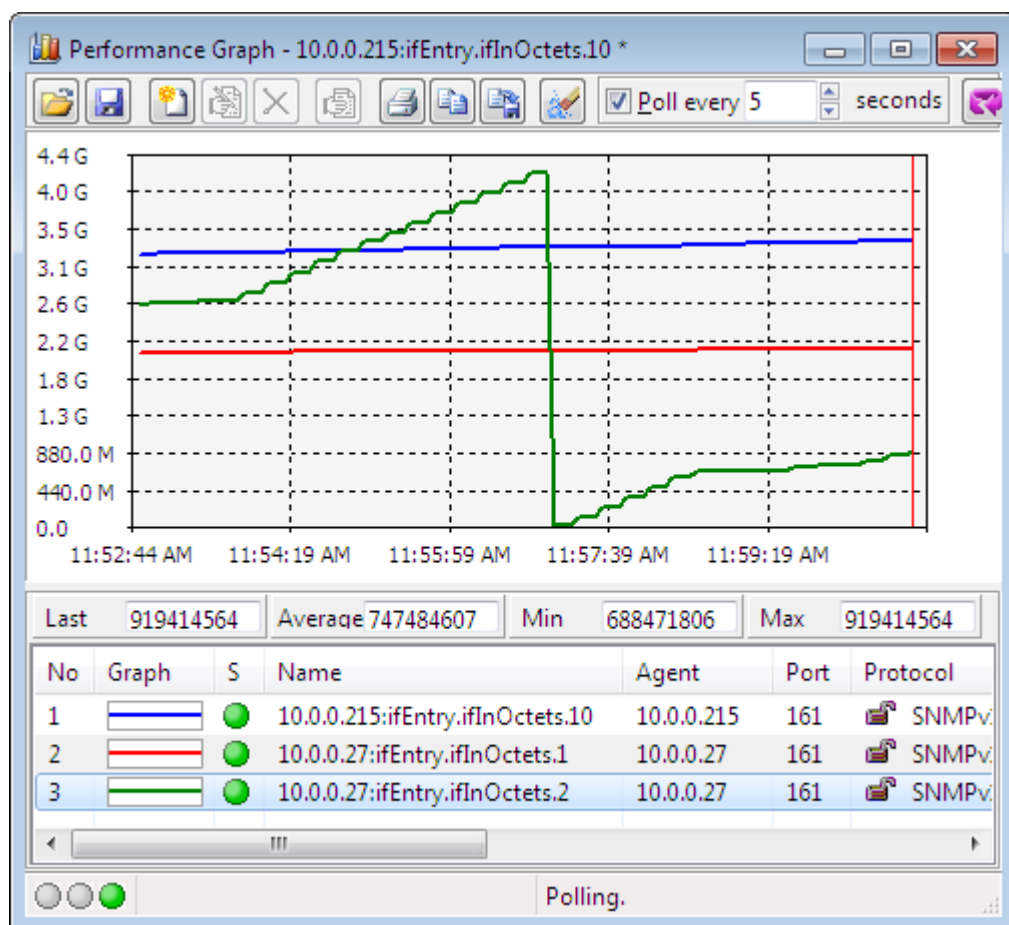


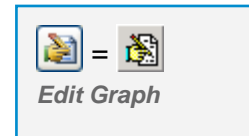
Figure 158: Performance Graph window with three graph lines

4. You can resize the Graph and Legend panels relative to each other by dragging the horizontal panel divider line up or down.

18.4 Editing Graph Settings

You can modify the properties of variables plotted in the Performance Graph window.

1. In the list of graph lines below the graph panel, click the variable that you wish to edit ([Figure 158](#)).
2. Click the **Edit Graph** toolbar button or simply double-click the selected variable.
3. The Graph Properties dialog box opens. Modify the variable properties, as described in the [Specifying Variable Properties](#) section.



Deleting Variables

You can delete individual graph lines from the Performance Graph window. Select the graph line that you wish to delete from the graph list and click the **Delete Graph** toolbar button or pop-up command.



Clearing the Graph Panel

If you click the **Reset All Graphs** toolbar button, MIB Browser will clear the Graph panel and start plotting graph lines with defined parameters from the beginning of the Graph panel.



18.5 Saving Graph Settings to File

After you have added and configured all variables in the Performance Graph window, you can save the settings to file for later use. Furthermore, you can also save the current contents of the Graph panel to a bitmap file.

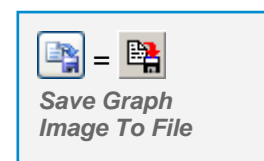
Saving the current set of graph parameters:

1. In the Performance Graph window, click the **Save Graph To File** toolbar button. The Save As dialog box appears.
2. In the Save As dialog box enter the file name.
3. Click the **Save** button and the graph parameters will be saved to a file with the * .mbgx extension. See also the
4. [Appendix: MIB Browser File Formats](#).



Saving the contents of the Graph panel as image:

1. Click the **Save Graph Image To File** toolbar button. The Save As dialog box appears.
2. Make any changes necessary, including the file name or the directory in which the graph shall be saved.
3. Select the desired file type and click the **Save** button.



Example: How to continuously monitor and present in a graph the throughput of a network interface (in octets per second in both directions)?

To open the Performance Graph window, click the **Tools / Performance Graph** command. In the Performance Graph window, click the **New Graph** toolbar button to open the Graph Properties dialog box. Into the **Agent** drop-down list in the Graph Properties dialog box, specify the IP address of the SNMP agent that you wish to query. Click the **Select OID from MIB Tree** toolbar button and in the expanded MIB tree double-click the `ifInOctets` node. In the Select Table Instance window, double-click the index of the instance that you wish to monitor. From the **Show** drop-down list in the **Graph Properties** dialog box, select the **Delta/Sec** option and click the **OK** button. The Graph Properties dialog box closes and MIB Browser starts plotting a graph line. The values of the graph line present the number of octets per second received on the selected interface.

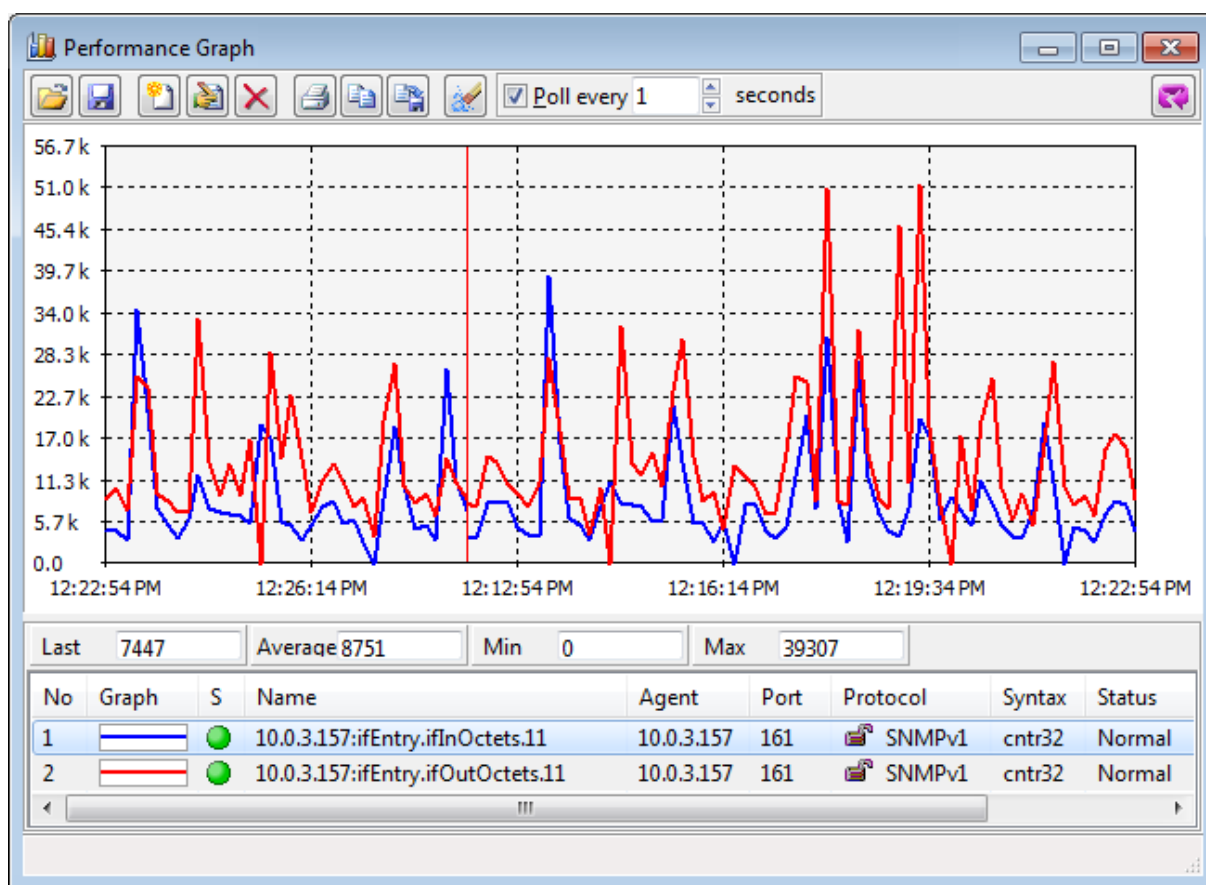


Figure 159: Graphical presentation of the number of octets per second received in (blue line) and transmitted out (red line) of the interface

To present the number of octets per second transmitted out of the interface, click the **New Graph** toolbar button in the Performance Graph window and in the MIB tree double-click the `ifOutOctets` node. To monitor the same interface, select the same index as before in the Select Table Instance(s) window. Choose the **Delta/Sec** option in the Graph Properties dialog box and click the **OK** button. MIB Browser adds a new graph line to the Graph panel and simultaneously monitors and plots the changing value of octets per second transmitted out and received in the interface.

19 RECEIVE SNMP TRAP AND SNMP INFORM NOTIFICATION MESSAGES

MIB Browser can receive SNMP Trap and SNMP Inform notification messages sent from arbitrary SNMP devices or applications on the network. In this section, you will learn how to use the SNMP Trap Ringer Console window to view all received SNMP notification messages, how to search and display only those SNMP notifications that match the search criteria and how to configure MIB Browser's settings to adjust the SNMP trap reception to your preferences.

19.1 Receiving SNMPv1 and SNMPv2c Notification Messages on Standard Ports

To receive SNMPv1 Trap notifications or SNMPv2c Trap and Inform notifications on the standard SNMP Trap ports UDP/IPv4 162 and UDP/IPv6 162, no special setup is required. While running, MIB Browser automatically receives and displays all valid SNMPv1 and SNMPv2c Trap and Inform notification messages sent to the standard Trap ports (i.e., UDP/IPv4 162 and UDP/IPv6 162) of the host computer.

Note: SNMP over IPv6 (including receiving SNMP Trap messages over UDP/IPv6 transport protocol) is available only in the *DOCSIS/DH and better editions of MG-SOFT MIB Browser Pro*.

19.1.1 Viewing Received SNMP Notification Messages

SNMP Trap and Inform notification messages received from SNMP devices on the network are displayed in the SNMP Trap Ringer Console window. To view the received messages:

1. Open the SNMP Trap Ringer Console window by using the **Tools / Trap Ringer Console** command or the **SNMP Trap Ringer Console** toolbar button in the main window.
2. The SNMP Trap Ringer Console window appears displaying the received SNMP Trap and Inform notifications ([Figure 160](#)).

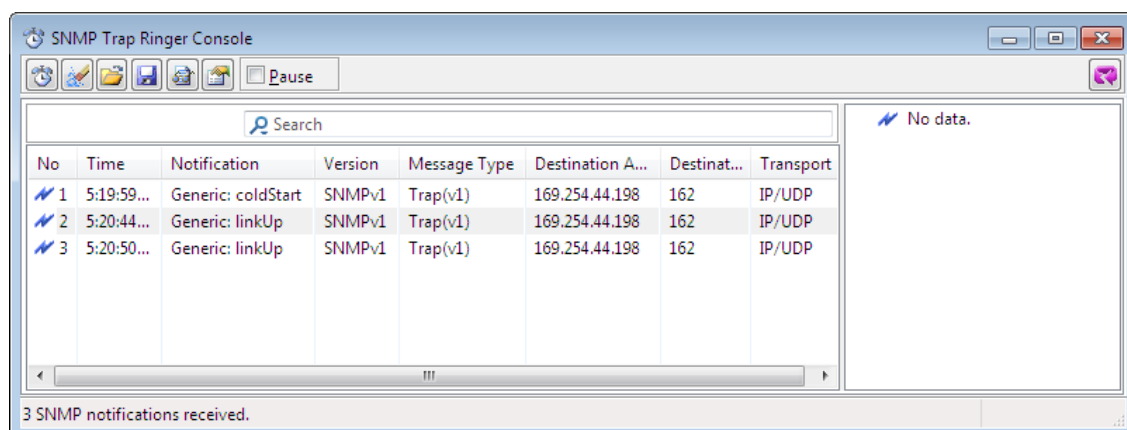


Figure 160: SNMP Trap Ringer Console window with received SNMP notification messages

- To specify which properties of received SNMP notifications should be shown, open the Notification Console Properties dialog box by clicking the **Preferences** button in the SNMP Trap Ringer Console window toolbar and select the desired properties.
- To see details about the received SNMP notification message in a tree structure, with all properties and variable bindings, click the corresponding line in the Trap List (left) panel and the selected message will be displayed in a tree structure in the Trap Details (right) panel (Figure 161).

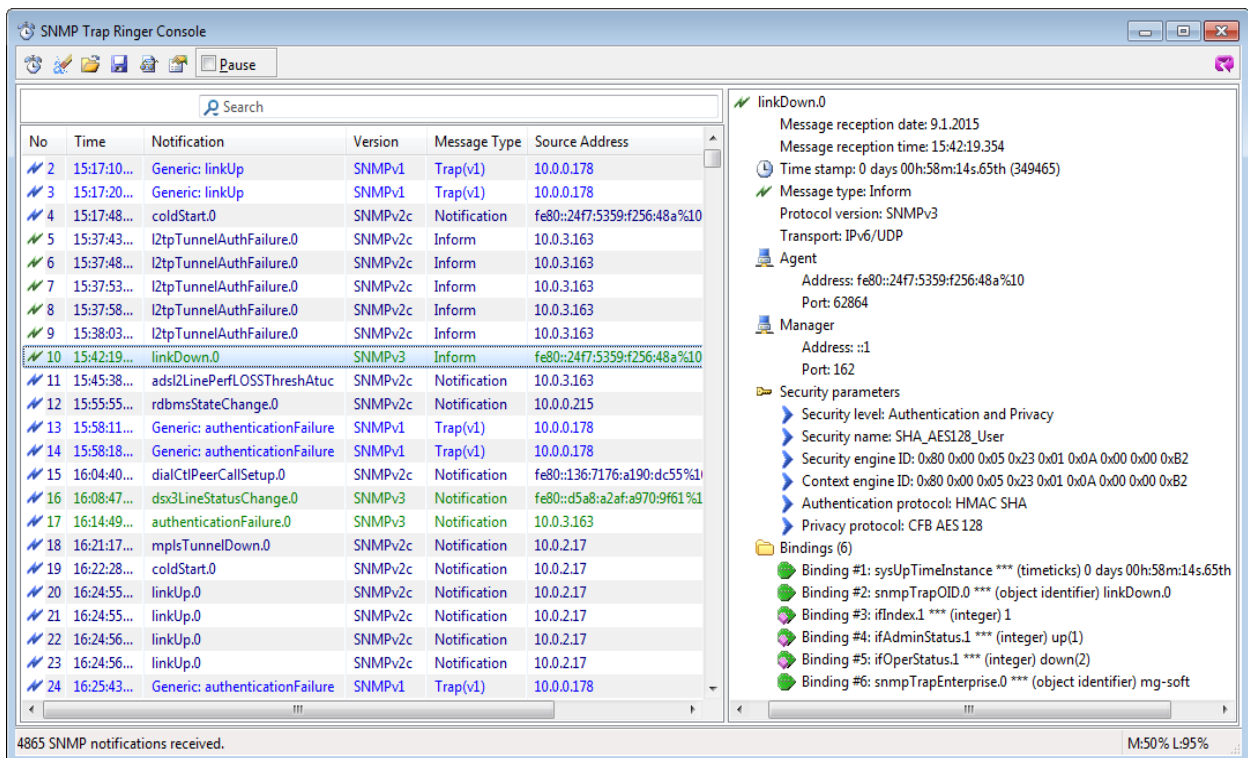
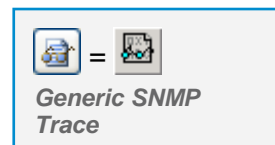


Figure 161: Selected SNMP notification message displayed in a tree structure (right panel)

Note: MIB Browser provides more information about the received SNMP Trap or Inform notification if the MIB module, which defines that SNMP Trap or Inform notification, is loaded in MIB Browser. For instructions on loading MIB modules, see the [Manually Loading MIB Modules](#) section.

- If you want to see the decoded form of received SNMP notification messages, open the Generic SNMP Trace For Trap Ringer window by clicking the **Generic SNMP Trace** button in the SNMP Trap Ringer Console window toolbar.



Note: The SNMP trace feature is available only in the *Developer's* and *Simulator* editions of **MG-SOFT MIB Browser Pro**. For more information on how to use it, see the [Decoding SNMP Notification Messages](#) section.

- Notification messages that are listed in the left panel can be colored (Figure 161) based on the SNMP protocol version and message type (SNMPv1, SNMPv2c, SNMPv3, Trap or Inform messages). Colors can be set in the MIB Browser Preferences dialog box in the Trap Ringer Console Preferences panel (**Tools / MIB Browser Preferences** command / **Trap Ringer** entry), Figure 162.

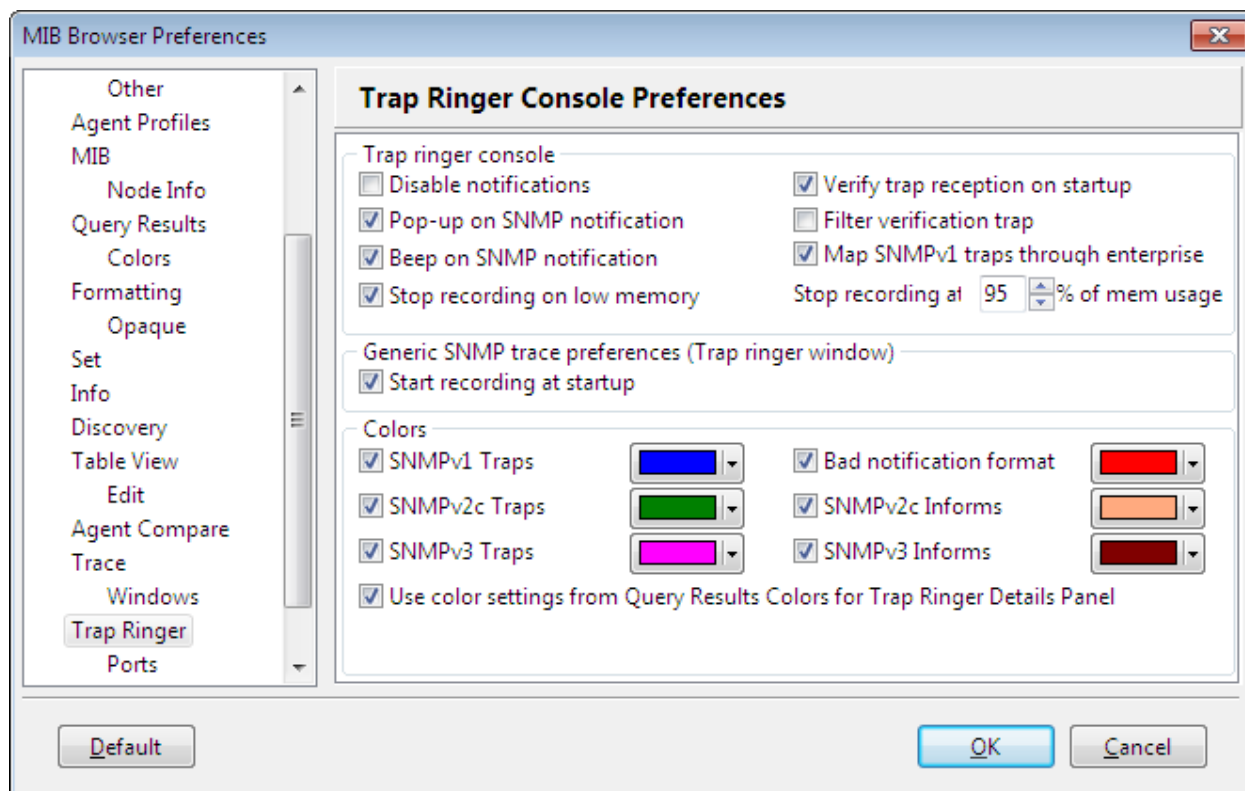


Figure 162: Trap Ringer Console Preferences panel in the MIB Browser Preferences dialog box

19.1.2 Identifying SNMPv1 Trap Notifications through Enterprise OID

MIB Browser can resolve Specific SNMPv1 Trap notifications through the SNMPv1 Trap number value and through the Enterprise OID value.

To resolve SNMPv1 Trap notifications also through enterprise value:

- Select the **View / MIB Browser Preferences** command to open the MIB Browser Preferences dialog box.
- In the MIB Browser Preferences dialog box, switch to the Trap Ringer Console Preferences panel (**Trap Ringer** preferences) and check the **Map SNMPv1 traps through enterprise** checkbox (Figure 162). Click the **OK** button.
- When you click an SNMPv1 Trap notification in the list of notifications, MIB Browser resolves it through enterprise and in the *Specific Trap MIB Lookup Results* folder contains the line displaying the name of the SNMPv1 Trap and the name of the MIB module that defines it (Figure 163).

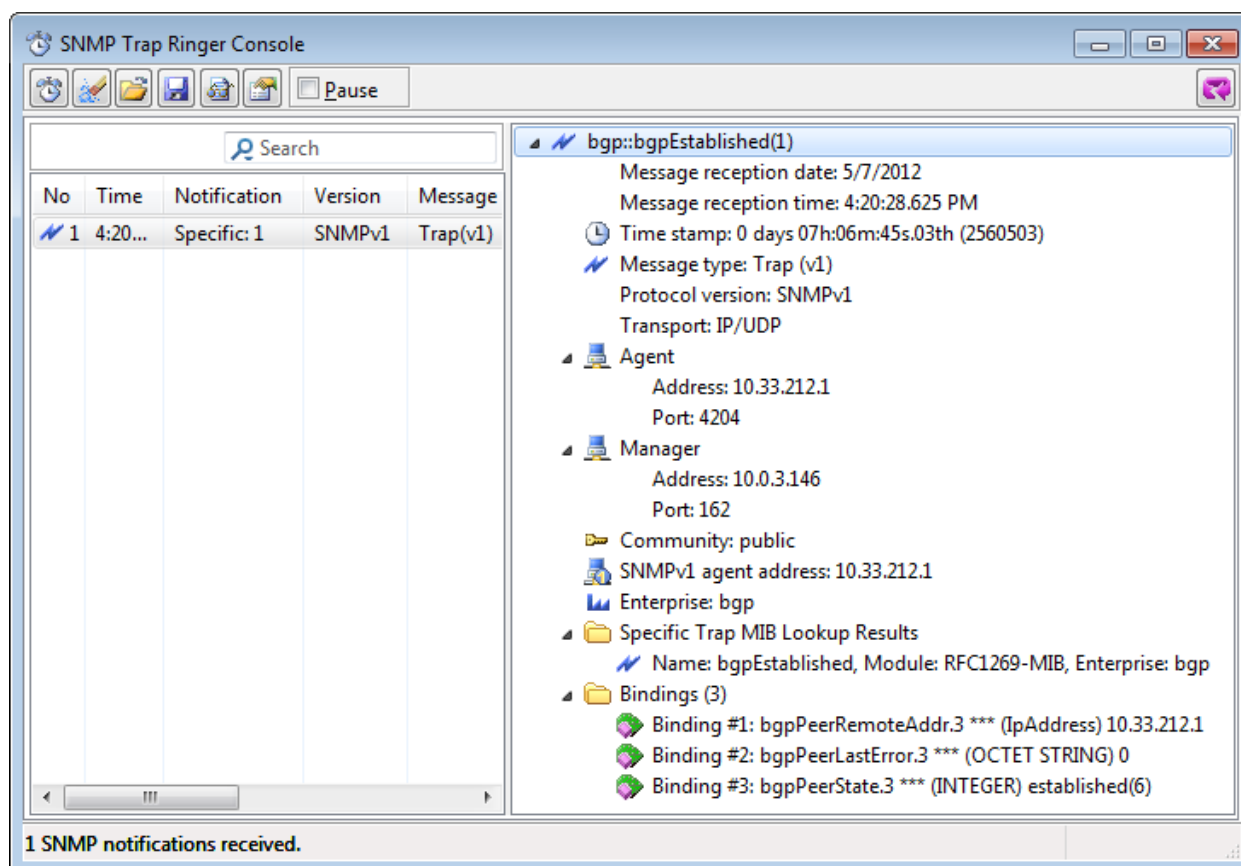


Figure 163: SNMPv1 Trap message resolved through the SNMPv1 Trap number and the Enterprise value

Example:

How to identify the received SNMPv1 Trap also through the Enterprise value?

When a Specific SNMPv1 Trap notification is received, MIB Browser by default identifies it by two parameters: by the SNMPv1 Trap number value (e.g., 1) and by the Enterprise value (e.g., bgp). If any of the loaded MIB modules defines an SNMPv1 Trap with the given Trap number and Enterprise value, the received SNMPv1 Trap is considered identified and its name is displayed in the top row of the Trap Details window panel (Figure 163). Furthermore, the *Specific Trap MIB Lookup Results* folder contains only one line displaying the name of the SNMPv1 Trap and the name of the MIB module that defines it.

To disable trap resolving through enterprise, uncheck the **Map SNMPv1 traps through enterprise** checkbox in the MIB Browser Preferences dialog box in the Trap Ringer Console Preferences panel (**Tools / MIB Browser Preferences** command / **Trap Ringer** entry). In this case, MIB Browser resolves an SNMPv1 Trap notification only through the SNMPv1 Trap number value (e.g., 1) and in the *Specific Trap MIB Lookup Results* folder lists all possible matches, i.e., all SNMPv1 Trap names with this specific SNMPv1 Trap number, defined in loaded MIBs (Figure 164).

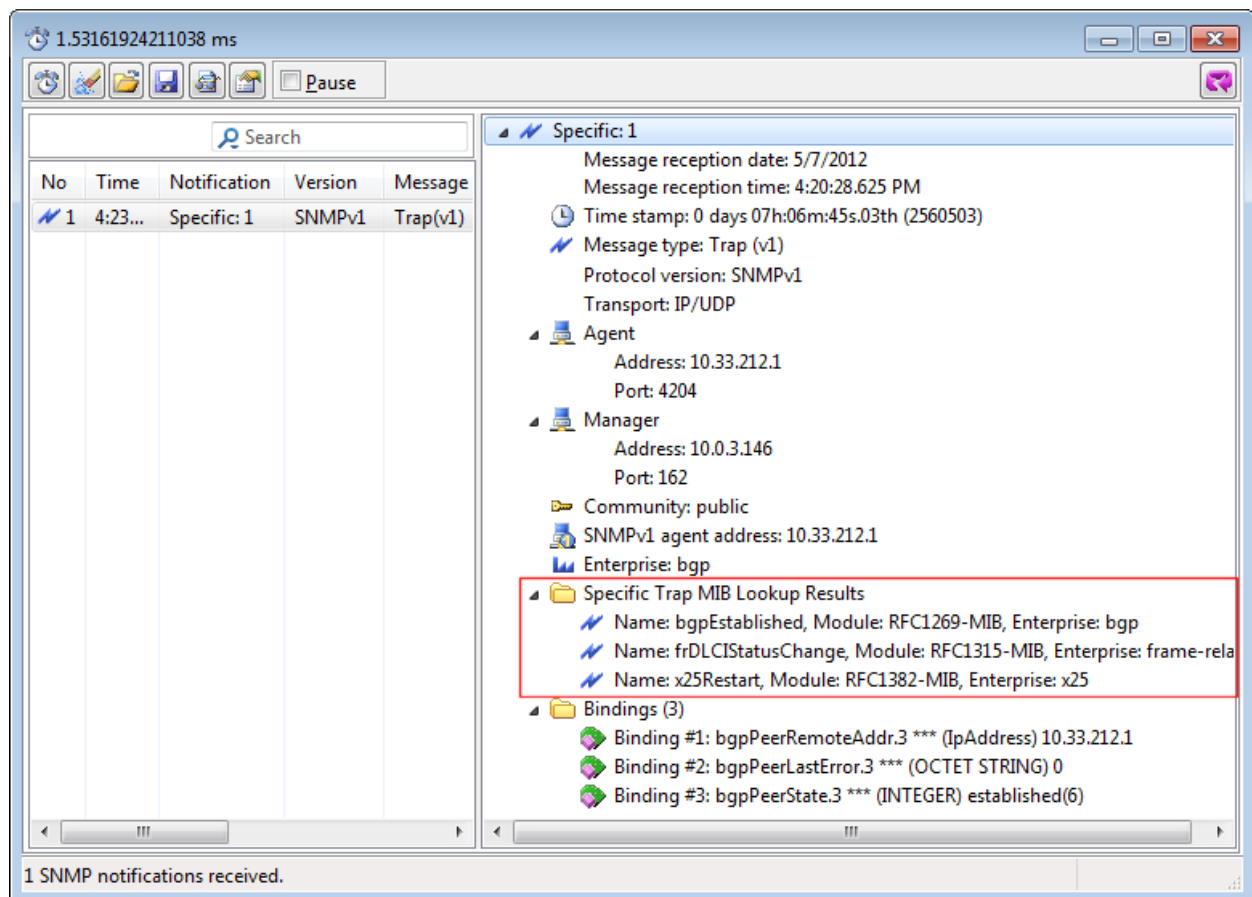


Figure 164: SNMPv1 Trap message resolved only through the SNMPv1 Trap number value

19.2 Receiving SNMPv3 Notification Messages

To enable receiving SNMPv3 Trap and Inform notifications, you need to select or configure an SNMPv3 user profile in the MIB Browser Preferences dialog box, in the Notification SNMPv3 Security Preferences panel (Figure 165). MIB Browser will receive only those SNMPv3 notification messages that match the security parameters of the specified SNMPv3 user profile.

1. To open the MIB Browser Preferences dialog box, select the **View / MIB Browser Preferences** command.
2. Choose the **Trap Ringer / SNMPv3** entry in the navigation tree to display the Notification SNMPv3 Security Preferences panel.
3. To use an already configured SNMPv3 USM user profile, click the **Load User** button and select the desired profile in the [SNMPv3 USM User Profiles](#) window that appears. If no SNMPv3 USM user profile exists yet, you can create it in the SNMPv3 USM user profile window as described in the [Creating New SNMPv3 USM User Profile](#) section.
4. To edit the selected SNMPv3 user profile, click the **Edit User** button. Edit the parameters of the selected user profile in the [SNMPv3 Security Parameters \(USM\)](#) dialog box that appears.
5. Click the **OK** button. The selected SNMPv3 user profile name and security level is displayed in the Notification SNMPv3 Security Preferences panel (Figure 165).

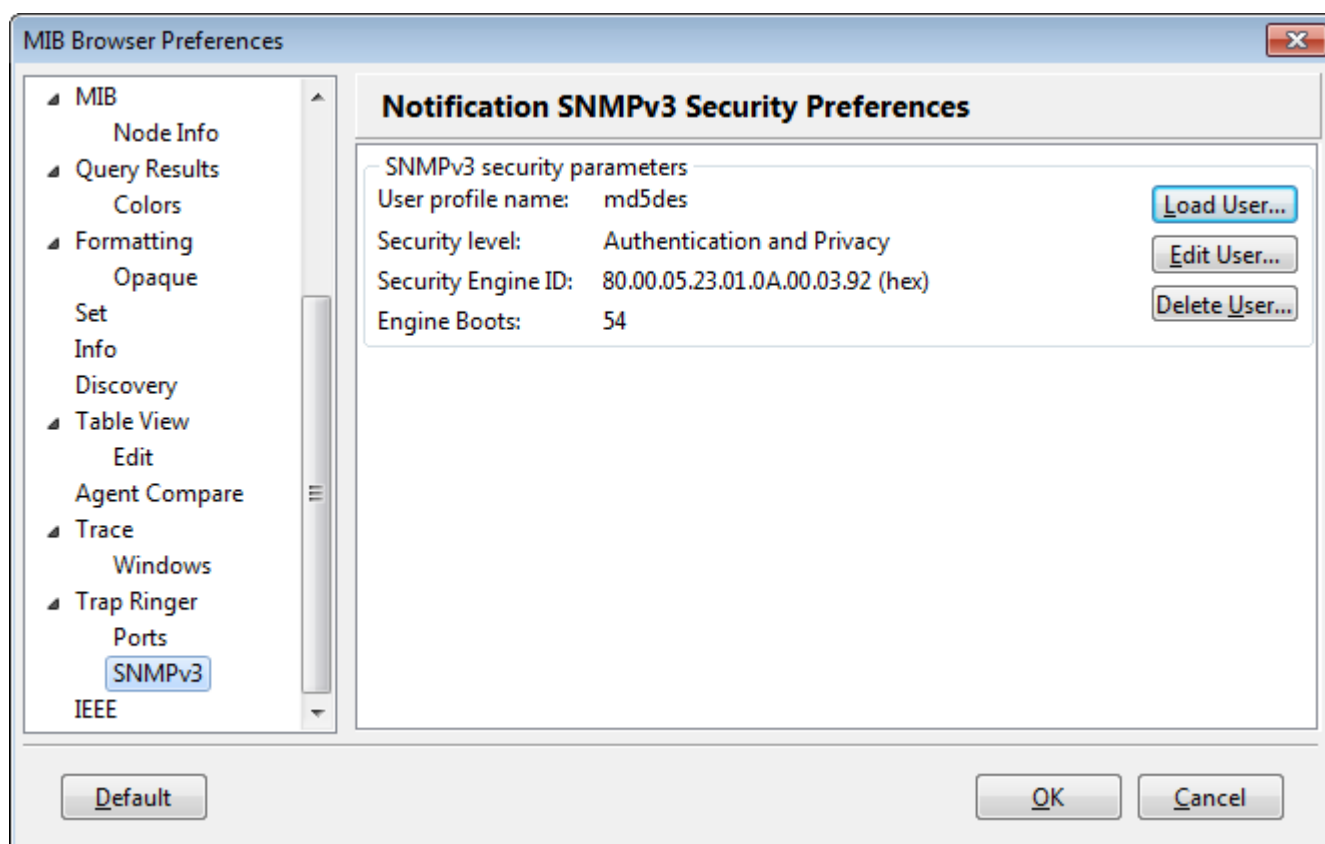


Figure 165: Notification SNMPv3 Security Preferences panel

19.3 Sound Notification on Received SNMP Notification Messages

When an SNMP notification is received, MIB Browser plays the Windows system default beep sound if the **Beep on SNMP notification** checkbox in the MIB Browser Preferences dialog box (Trap Ringer Console Preferences panel) is checked. If you do not hear a beep when you receive an SNMP notification, make sure your speakers are properly connected to your computer and turned on that the volume is adjusted to an appropriate level. If you still do not hear the sound, the system **Default Beep** sound might be disabled. In order to change that (on Windows operating system):


1. Open the Control Panel window (**Start / Settings / Control Panel**).
2. Select the **Sounds and Audio Devices** or the **Sounds** entry (depending on your Windows version) to open the Sounds window. In the **Sounds tab**, select the **Default Beep** event and assign it a *.wav file.
3. Click the **OK** button.

Note: If you check the **Pop-up on SNMP notifications** checkbox in the MIB Browser Preferences dialog box (Trap Ringer Preferences panel), the SNMP Trap Ringer Console window will open automatically (if not already open) when a new SNMP Trap or Inform message is received.

19.4 Acknowledging Received SNMP Notification Messages

1. In the SNMP Trap Ringer Console window, click the **Acknowledge Notifications** toolbar button or use the **Acknowledge Notifications** pop-up command.
2. The program sets an ACK flag to all received SNMP Trap and Inform messages and the alarm clock in the MIB Browser **status bar** (main window) stops “ringing”.

19.5 Searching and Filtering SNMP Notification Messages

MIB Browser offers the convenient **Live search** tool  in the SNMP Trap Ringer Console window. The Live search tool lets you perform incremental text search to quickly find and display only those SNMP notification messages that match the search criteria, i.e., contain the entered text in one or more of the selected search categories.

SNMP notifications can be searched for by virtually any category (property), like the notification name, reception date and time, source address, included variable bindings, etc.

Note that once you enter text into the Live search box, the search is automatically started and it remains active until you cancel it. Active search behaves as a **continuous display filter**, meaning that only those newly received SNMP notifications that match the search criteria are displayed in the SNMP Trap Ringer Console window (until the search is canceled).

To search for and filter SNMP notification messages:

1. Open the SNMP Trap Ringer Console window by using the **Tools / Trap Ringer Console** command or the **SNMP Trap Ringer Console** toolbar button in the main window.
2. The SNMP Trap Ringer Console window appears displaying the received SNMP Trap and Inform notifications ([Figure 160](#)).

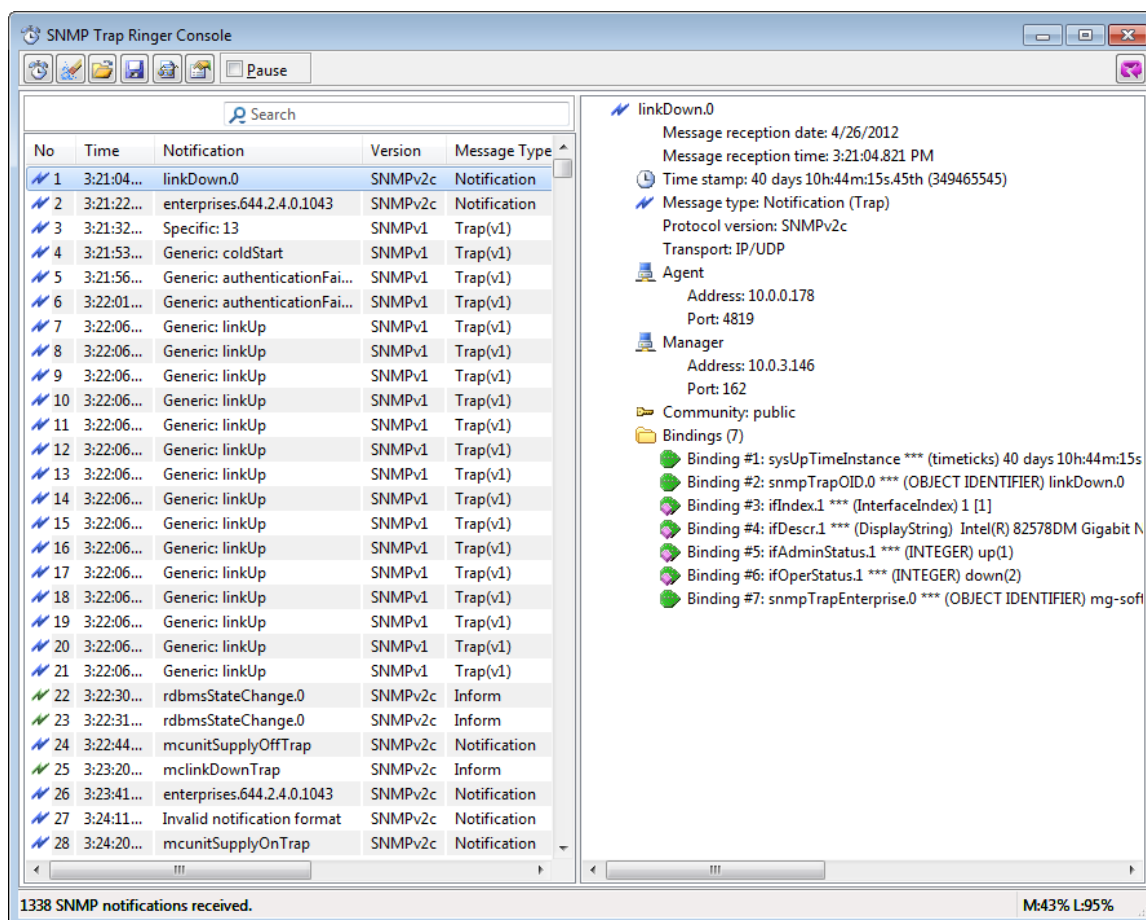


Figure 166: SNMP Trap Ringer Console window displaying all received SNMP notification messages

3. In the **Live search** tool located below the toolbar, click the search symbol (🔍).
4. The **Search Options** drop-down menu is displayed (Figure 89).

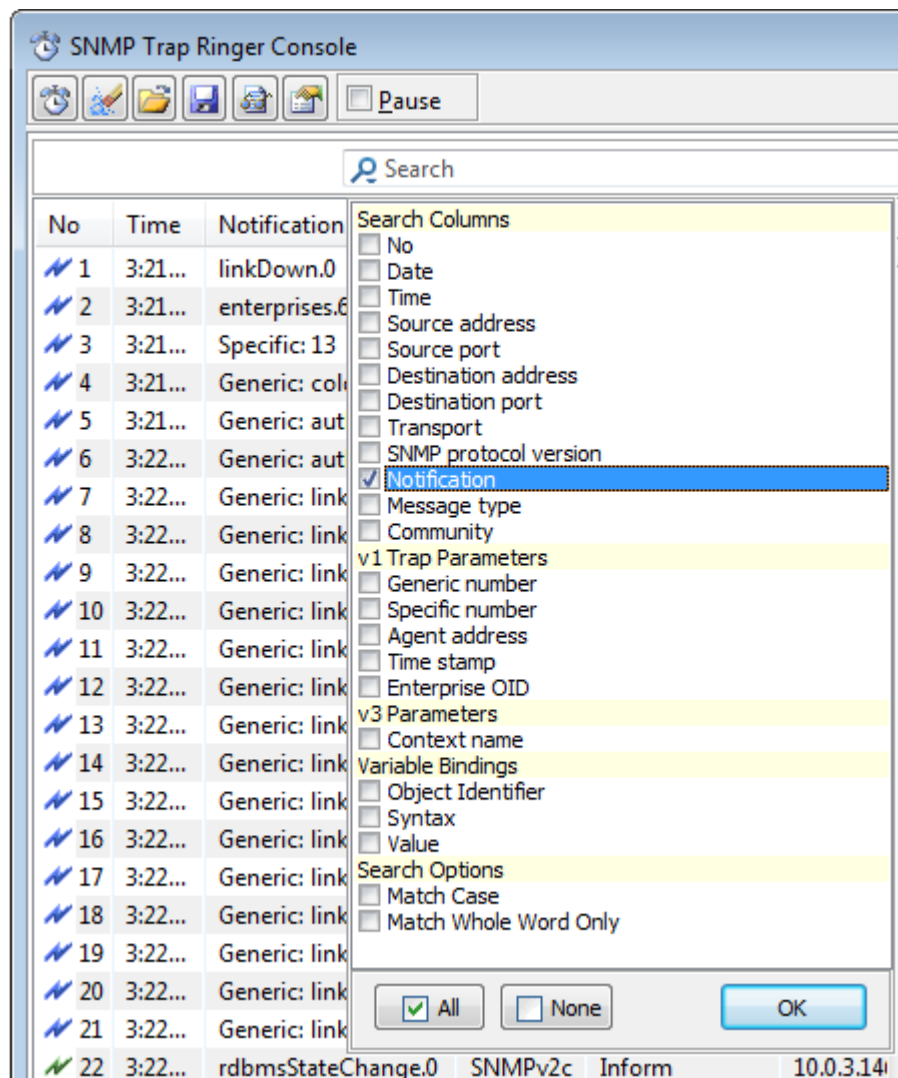


Figure 167: Setting the Live search options in the SNMP Trap Ringer Console

5. In the Search Options drop-down menu, select the desired search options by checking the checkboxes in front of them. Select the columns or other notification properties you wish to search in. For example, to search by the notification names, select the **Notification** item in the Search Columns category (Figure 89). Click the **OK** button at the bottom of the Search Options drop-down menu to close it and apply the changes.

Select the **Match case** search option to make the search case sensitive. If this option is enabled, the search will find only those strings in which the capitalization matches the one used in the search query (e.g., ADSL will find ADSL, but not adsl).

Select the **Match whole word only** search option to find only those strings that are whole words and not part of a larger word (e.g., adsl will find adsl, but not adsl2).

- Click inside the Live search box and start typing the search query. The Live search tool automatically performs incremental search as you type the characters into the search box and progressively updates the list of narrowed results in the Trap List window panel on the left hand-side.

For example, to find all SNMP notifications that **contain** the word `down` in their names, start typing the word “down” into the Live search tool. The SNMP Trap Ringer Console window (left panel) will display all SNMP notification messages that contain the entered text anywhere in the name (Figure 90).

- The search results (total number of matches) is displayed in front of the Live search tool (Figure 90). The entered text functions as a continuous display filter, meaning that newly received SNMP notifications that match the search criteria will be added to the list of search results in the SNMP Trap Ringer Console window and the search result count will increase.

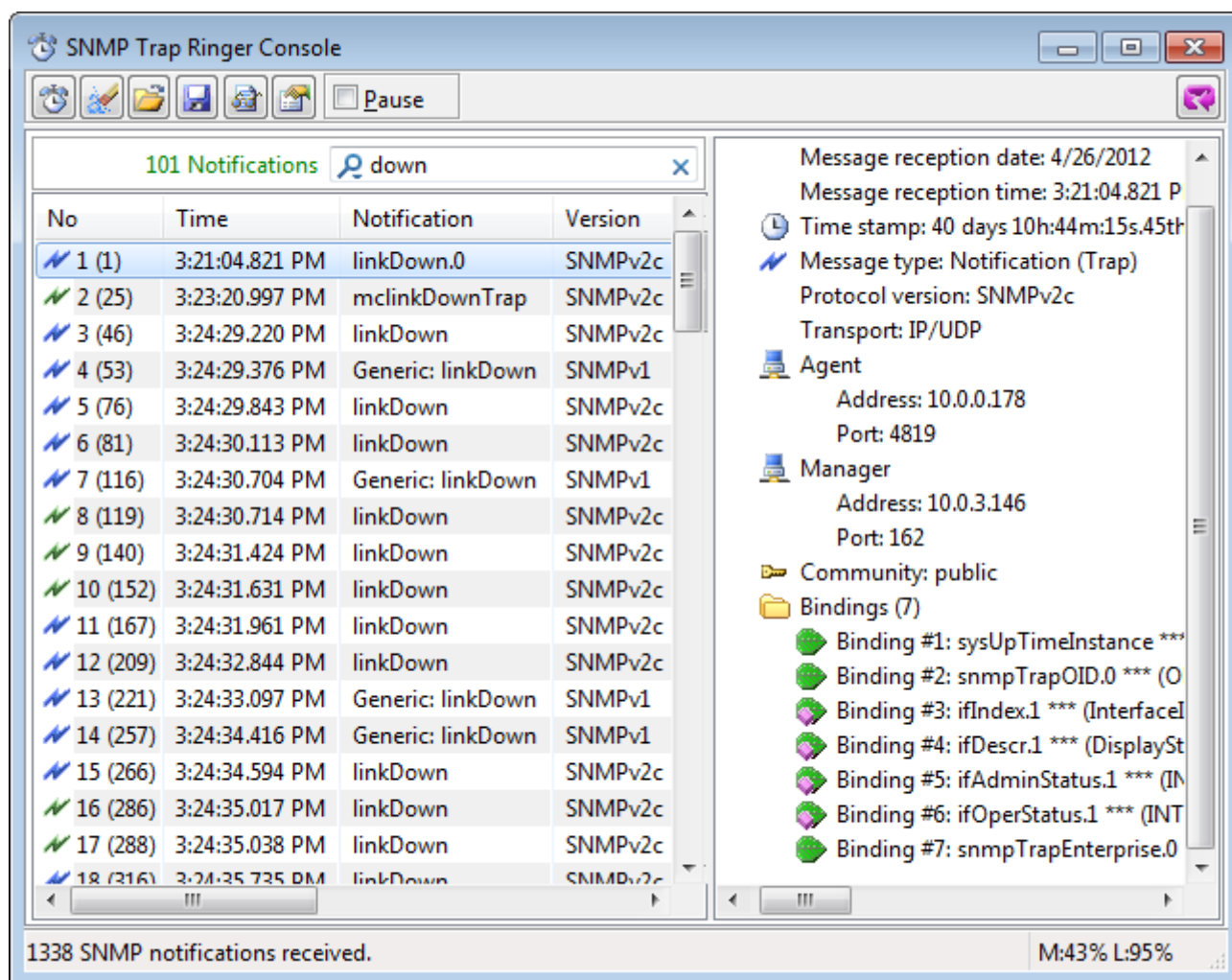


Figure 168: Viewing the Live search results in the SNMP Trap Ringer Console

- To cancel the search, click the **Cancel Current Search** symbol (X) in the Live search box or delete the text from it. All received SNMP notifications are shown in the SNMP Trap Ringer Console window when you cancel the search.

19.6 SNMP Notification Messages on other UDP Ports

MIB Browser can be configured to listen for SNMP Trap and Inform notifications on other, non-standard IPv4/UDP and IPv6/UDP ports, as described in this section.

19.6.1 Configuring a New Listening Port

1. Select the **View / MIB Browser Preferences** command. The MIB Browser Preferences dialog box appears.
2. Choose the **Trap Ringer / Ports** entry in the navigation tree to display the Notification Port Preferences panel, listing the currently registered SNMP notification ports and their statuses.
3. Click the **Add** button in the Notification Port Preferences panel.

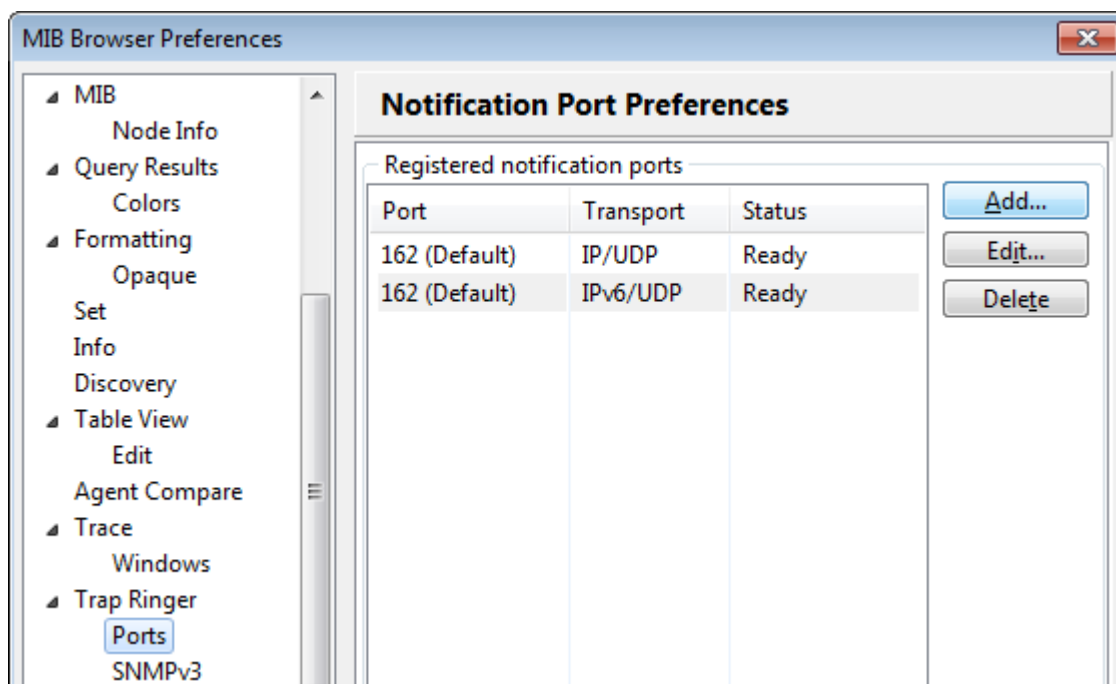


Figure 169: Notification Port Preferences panel

4. The Select Port And Transport dialog box appears.

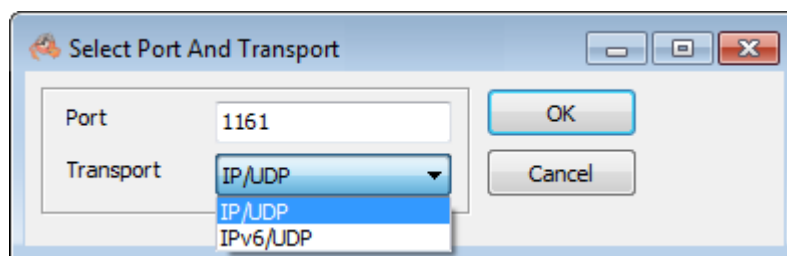


Figure 170: Adding a new port for dialog box

5. Into the **Port** input line, type the number of the new port, select the desired transport protocol and click the **OK** button.
6. A new port is added to the list of ports in the MIB Browser Preferences dialog box and MIB Browser (actually MG-SOFT SNMP Trap Service) starts listening for incoming SNMP notifications also on the newly added port.

19.7 Checking the SNMP Notification Reception Status

You can check the status of ports registered for receiving SNMP notifications in the MIB Browser Preferences dialog box; in the Notification Port Preferences panel ([Figure 169](#)).

1. Select the **View / MIB Browser Preferences** command. The MIB Browser Preferences dialog box appears.
2. Choose the **Trap Ringer / Ports** entry in the navigation tree to display the Notification Port Preferences panel, listing the currently registered SNMP notification ports and their statuses, as follows:
 - ❑ If the **Status** column for a port (e.g., UDP 162) states **Ready**, MIB Browser should successfully receive SNMP notifications on the given port.
 - ❑ If the **Status** column for a port (e.g., UDP 162) states **Down** the SNMP notification reception on this port is not possible, probably because the port is already occupied by some other running process. To solve the problem, you need to terminate this process and restart MG-SOFT SNMP Trap service.

19.8 Copying and Saving SNMP Notification Messages

Information about received SNMP notification messages can be copied to the clipboard (as text) and saved to an XML file, i.e., either Trap Ringer XML (`.trfx`) file format or Multiple Variable Bindings XML (`.mvbx`) file format. A Trap Ringer XML file (`.trfx`) can later be loaded into the Trap Ringer Console window (separate tab) for reviewing or into the Multiple Operations window. A Multiple Variable Binding XML (`.mvbx`) file can be loaded into the Multiple Variable Bindings window and Multiple Operations window, e.g., for sending SNMP notifications to the network.

To save all received SNMP notifications to a Trap Ringer XML file (`.trfx`):

1. In the Trap Ringer Console window toolbar, click the **Save to File** button. The standard Save As dialog box appears.
2. In the Save As dialog box navigate to the folder in which you want save the file.
3. From the **Save as type** drop-down list, select the **Trap Ringer File XML (`.trfx`)** entry.
4. In the **File name** drop-down list, enter the name of the `.trfx` file.
5. Click the **Save** button to create the file and close the Save As dialog box. MIB Browser might prompt you with a dialog asking if you want to save all notifications or only the selected ones. Choose the first option to save all received notifications to a file.

To save a received SNMP notification to a Multiple Variable Bindings XML file (.mvbx):

1. In the Trap Ringer Console left window panel, select the SNMP notification you want to save.
2. Click the **Save to File** toolbar button. The standard Save As dialog box appears.
3. In the Save As dialog box navigate to the folder in which you want save the file.
4. From the **Save as type** drop-down list, select the **Multiple Variable Bindings File XML (.mvbx)** entry.
5. In the **File name** drop-down list, enter the name of the .mvbx file.
6. Click the **Save** button to create the file and close the Save As dialog box. MIB Browser might display a dialog asking if you want to save all notifications or only the selected ones. Choose the first option to save all received notifications to a file.

To copy details about a SNMP notification to the clipboard:

1. In the Trap Ringer Console left window panel, select the SNMP notification whose details you want to copy to the clipboard.
2. Right-click inside the right window panel and choose the **Copy Full Tree** pop-up menu command.
3. MIB Browser copies the displayed information to the clipboard (as text).
4. Open any other application (e.g., Notepad); paste the contents from the clipboard and save it to a desired location.

19.9 Information About SNMP Notification Messages

To obtain more information about SNMP Trap and Inform notifications, view the properties of objects that represent them, as described in this section.

19.9.1 Information About SNMPv2c and SNMPv3 Notifications

SNMPv2 notifications have OID values assigned and are represented in the MIB tree as NOTIFICATION-TYPE nodes (🚩). SNMPv2 notifications are conveyed by means of SNMPv2c and SNMPv3 Trap and Inform messages.

1. In the MIB tree pane of the main window, right-click the NOTIFICATION-TYPE object (🚩) that you wish to read more information about and select the **Properties** pop-up command (Figure 171).

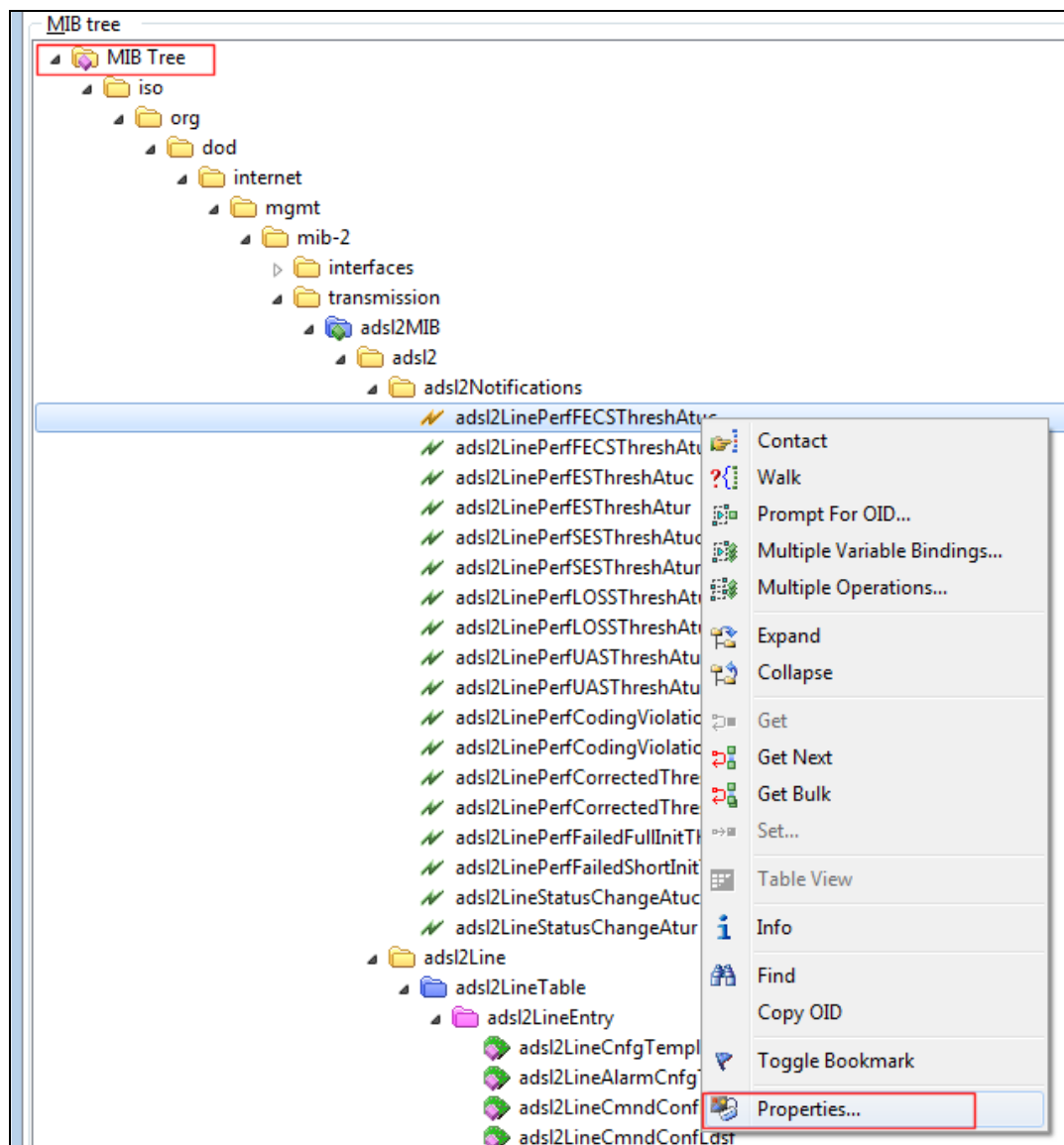


Figure 171: Selecting the Properties pop-up command on a NOTIFICATION-TYPE MIB tree node

2. The MIB Node Properties window appears and displays the properties of the selected NOTIFICATION-TYPE node, including its description [Figure 172](#)).

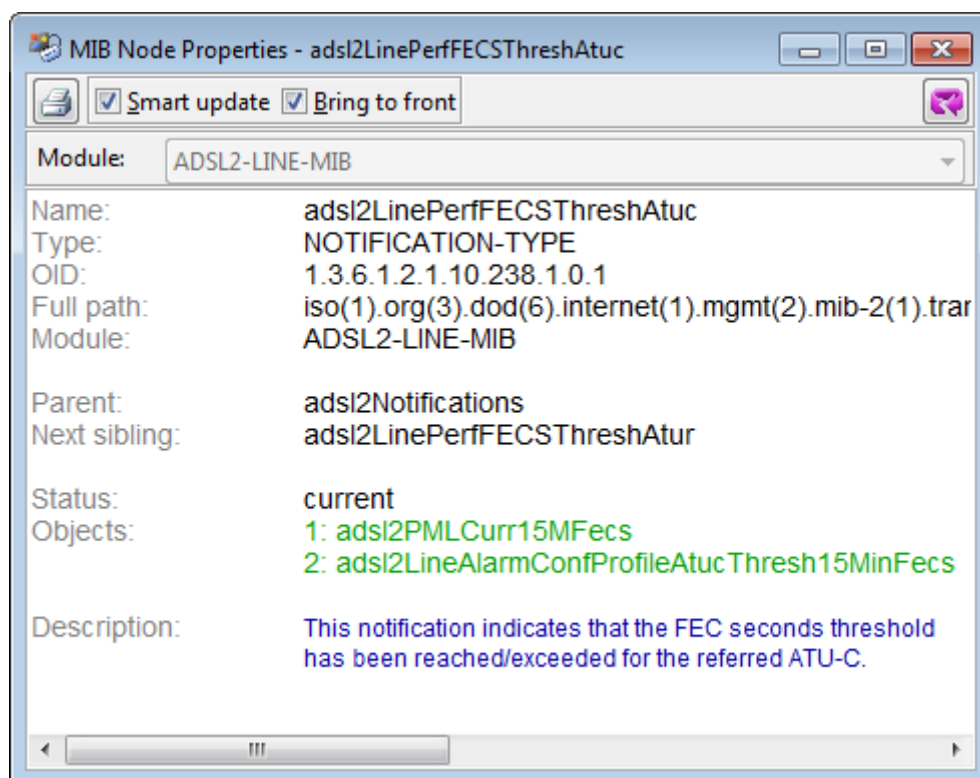


Figure 172: Viewing the properties of a notification-type node

19.9.2 Information About SNMPv1 Trap Notifications

SNMPv1 Traps do not have OID values assigned and cannot be displayed in the regular MIB tree that shows the OID hierarchy. Instead, SNMPv1 Traps are represented by means of TRAP-TYPE nodes (🚩) that are displayed in a separate, **SNMPv1 Traps** tree in the MIB Tree panel.

1. Open the MIB Browser Preferences dialog box (**View / MIB Browser Preferences**) and choose the **MIB** preferences to display the MIB Tree And MIB Modules Preferences panel.
2. Check the **Show SNMPv1 traps** checkbox in the **MIB Tree** frame and click the **OK** button.
3. In the MIB tree panel the **SNMPv1 Traps** tree is displayed below the regular MIB tree ([Figure 173](#)).
4. Expand the **SNMPv1 Traps** tree, navigate to the TRAP-TYPE node that represents the SNMPv1 Trap you are interested in, right-click the node and select the **Properties** pop-up command ([Figure 173](#)).

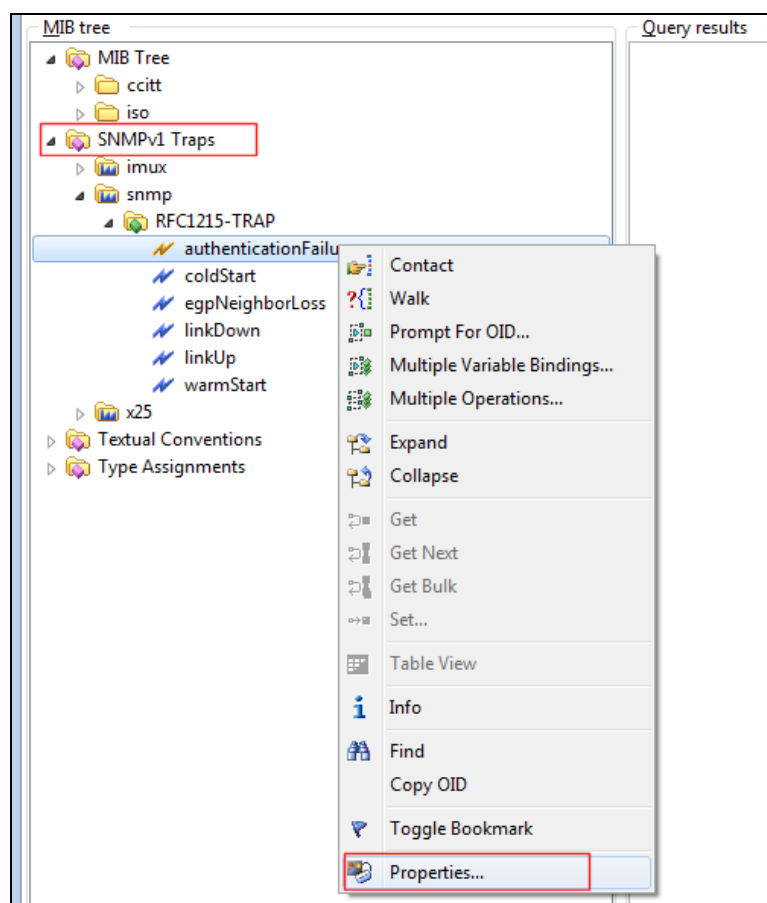


Figure 173: Selecting the Properties pop-up command on a TRAP-TYPE node

5. The MIB Node Properties window appears and displays the properties and description of the selected TRAP-TYPE node (Figure 174).

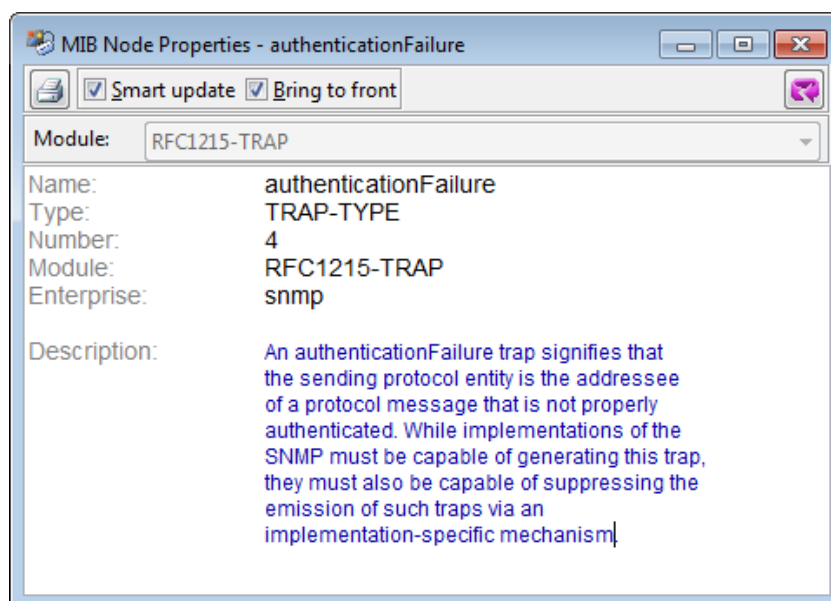


Figure 174: Viewing the description of an SNMPv1 Trap

19.10 Decoding SNMP Notification Messages

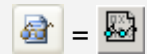
The Generic SNMP Trace For Trap Ringer window enables you to see decoded SNMP notification messages received into the SNMP Trap Ringer Console window, as well as the SNMP messages sent out as response to SNMP Inform notification messages.

To trace SNMP notification messages:

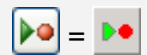
1. Open the SNMP Trap Ringer Console window by using the **Tools / Trap Ringer Console** command in the main menu.
2. When the SNMP Trap Ringer Console window opens, click the **Generic SNMP Trace** toolbar button.
3. The Generic SNMP Trace For Trap Ringer window opens. To activate the recording of SNMP notification messages, click the **Record** toolbar button. The recording of SNMP notification messages will continue until you click the **Pause** toolbar button.
4. When recording is activated, the Generic SNMP Trace For Trap Ringer window records and displays all SNMP notification messages received into the SNMP Trap Ringer Console window ([Figure 175](#)), including SNMP messages sent as responses to SNMP Inform notification messages.
5. For a more detailed explanation about how SNMP messages are displayed and decoded, see the step 7 in the [Tracing and Decoding SNMP Messages](#) section.



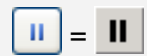
Note: This feature is available only in the **Developer's Edition** and **Simulator Edition** of **MIB Browser Pro**.



Generic SNMP Trace



Record



Pause

Note 1: For receiving SNMP notification messages, MIB Browser uses the MG-SOFT WinSNMP API layer, which by default receives SNMP notification messages through the Microsoft's SNMP Trap service. But at the reception of an SNMP notification message, this service does not provide information about the port number where the message has been received. Therefore, the '**Destination Port**' value for received SNMP notification messages is shown as zero '0'.

If you disable the Microsoft's SNMP Trap service, MIB Browser will receive SNMP notification messages directly through MG-SOFT SNMP Trap Service (MgWTrap3.exe). Because MG-SOFT SNMP Trap Service provides information about the port number on which SNMP notification messages are received, the correct value of the destination port is shown.

Note 2: The recording function slightly decreases the performance of the software; so make sure to switch it off when you do not need it.

The screenshot displays the 'Generic SNMP Trace [Trap Ringer Window]' interface. It features a toolbar with icons for file operations, a search bar, and a 'Compact decoding level' dropdown. Below the toolbar is a table listing SNMP messages with columns: No, Direct..., Time, Version, Type, Source Address, Destination Port, Transport, Community, and Request ID. The table shows five messages, with the last one (No. 2564) being a Trap (v2) from 10.0.0.178 to port 162, with community 'public' and request ID 54.

No	Direct...	Time	Version	Type	Source Address	Destination Port	Transport	Community	Request ID
2560	<	2:15:10...	SNMPv3	Inform	10.0.0.215	162	IP/UDP		0
2561	<	2:15:10...	SNMPv3	Report	10.0.3.146	56769	IP/UDP		0
2562	<	2:20:26...	SNMPv2c	Trap (v2)	10.0.0.178	162	IP/UDP	public	52
2563	<	2:21:04...	SNMPv2c	Trap (v2)	10.0.0.178	162	IP/UDP	public	53
2564	<	2:21:22...	SNMPv2c	Trap (v2)	10.0.0.178	162	IP/UDP	public	54

Below the table is a hex dump of the message data. The bottom section, 'Decoded SNMP Message', provides a detailed breakdown of the message structure:

```

1: SNMP 0000:00/00|FF ***** Simple Network Management Protocol *****
2: SNMP 0000:00/00|FF
3: SNMP 0001:02/00|FF Length 193 [C1 (hex)] (octets)
4: SNMP 0005:01/00|FF Version 1 (SNMPv2c)
5: SNMP 0008:06/00|FF Community public
6: SNMP 0014:01/08|FF Object type 1.0.1.0.0.1.1.1 (TRAP (v2))
7: SNMP 0019:01/00|FF Request ID 53
8: SNMP 0022:01/00|FF Error code 0 (no error)
9: SNMP 0025:01/00|FF Error index 0
10: SNMP 0033:08/00|FF Object ID 1.3.6.1.2.1.1.3.0 (sysUpTime.0) #1
11: SNMP 0041:01/08|FF Object type 0.1.0.0.0.0.1.1 (TimeTicks)
12: SNMP 0043:04/00|FF Value 349465545
13: SNMP 0051:10/00|FF Object ID 1.3.6.1.6.3.1.1.4.1.0 (snmpTrapOID.0) #2
14: SNMP 0061:01/08|FF Object type 0.0.0.0.0.1.1.0 (OBJECT IDENTIFIER)
15: SNMP 0063:10/00|FF Value 1.3.6.1.6.3.1.1.5.3.0
16: SNMP 0077:10/00|FF Object ID 1.3.6.1.2.1.2.2.1.1.1 (ifIndex.1) #3
17: SNMP 0087:01/08|FF Object type 0.0.0.0.0.0.1.0 (INTEGER)
18: SNMP 0089:01/00|FF Value 1
19: SNMP 0094:10/00|FF Object ID 1.3.6.1.2.1.2.2.1.2.1 (ifDescr.1) #4
20: SNMP 0104:01/08|FF Object type 0.0.0.0.0.1.0.0 (OCTET STRING)
  
```

The status bar at the bottom indicates 'Recording' is active, with various counters and a list of message numbers (4878, 1461, 2033, 1384, 0, 676, 692, 1461, 681, 1368).

Figure 175: SNMP notification message received into SNMP Trap Ringer Console window decoded and displayed in the Generic SNMP Trace For Trap Ringer window

20 SEND SNMP TRAP AND INFORM NOTIFICATION MESSAGES

MIB Browser lets you send SNMP Trap and SNMP Inform notifications to arbitrary SNMP entities (applications or devices) on the network. This section describes how to use the Multiple Variable Bindings window to create the SNMPv1/v2c/v3 notification messages and send them to remote SNMP applications or devices.

First, you will learn how to configure the necessary parameters for SNMPv1 Generic and Specific Trap messages and send them to the network using the Multiple Variable Bindings window. Then, the process of creating a typical variable binding list for SNMPv2c/v3 Trap and Inform notification messages is explained. You will also learn how to configure the SNMP protocol preferences for sending SNMPv1, SNMPv2c, and SNMPv3 notification messages.

Tip: MIB Browser ships with the **SENDTRAP** utility, which can be used for sending SNMPv1 and SNMPv2c Trap and Inform notifications from the Command Prompt window.

20.1 Sending SNMPv1 Generic and Specific Trap Notification Messages

The SNMPv1 Trap messages have several parameters written in special PDU fields, which are not present in other SNMP messages. First, there are two parameters defining the type of an SNMPv1 Trap notification. The SNMPv1 Traps are either generic or enterprise specific. Additionally, SNMPv1 Trap messages use several other parameters, i.e., the IP address of the agent associated with the trap, the identification of enterprise associated with the trap, and the time stamp of the Trap message. All these SNMPv1 Trap message parameters can be set within the Multiple Variable Bindings window.

20.1.1 Setting Parameters for SNMPv1 Generic and Specific Trap Notifications

1. Use the **SNMP / Multiple Variable Bindings** command, to open the Multiple Variable Bindings window (Figure 176).

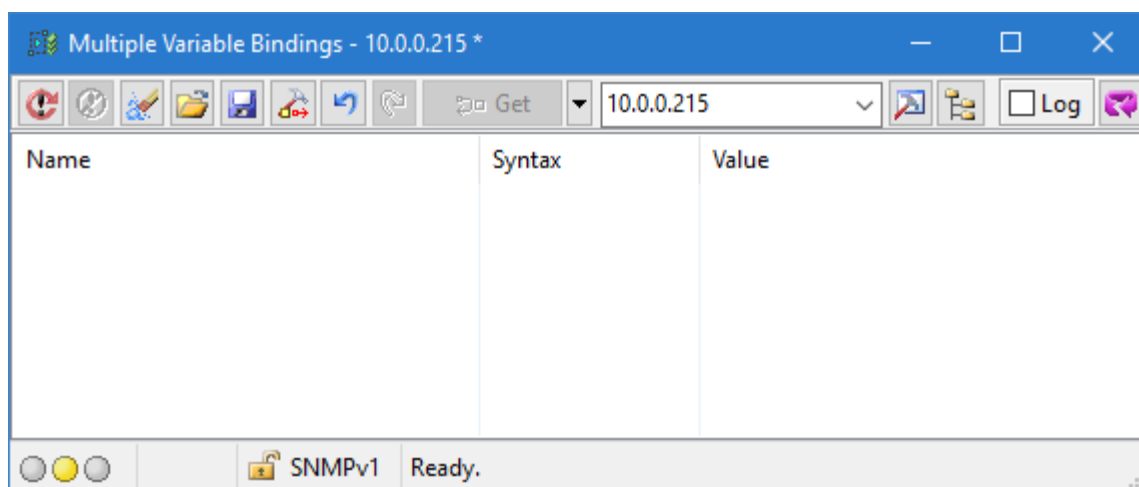


Figure 176: Multiple Variable Bindings window

- Click the **SNMPv1 Trap Preferences** toolbar button to display the SNMPv1 Trap Protocol Parameters dialog box (Figure 177).

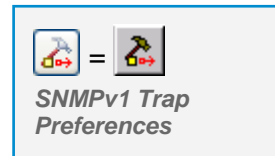
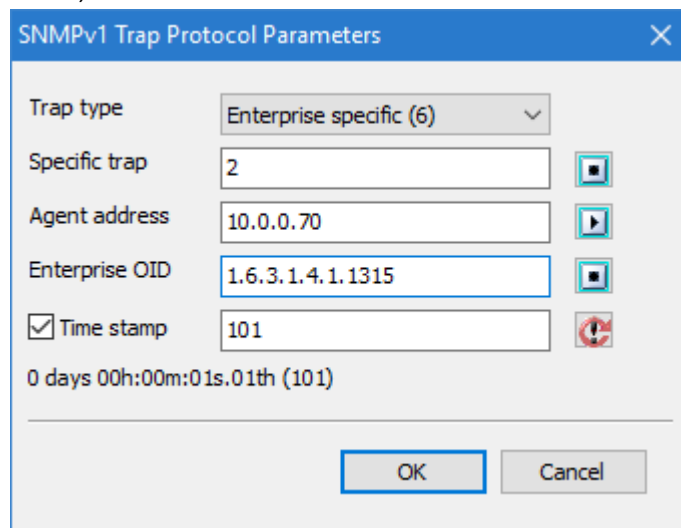


Figure 177: SNMPv1 Trap Protocol Parameters dialog box

- In the **Trap type** drop-down list specify the type of the SNMPv1 Trap. To designate the trap as **enterprise specific**, select the **Enterprise specific** (the last entry). Otherwise, select one of the following **generic** trap types:
 - ☐ Cold start
 - ☐ Warm start
 - ☐ Link down
 - ☐ Link up
 - ☐ Authentication failure
 - ☐ EGP neighbor loss
- If you have selected the **Enterprise specific** trap type entry in step 3, enter its specific number into the **Specific trap** input line. This parameter defines the SNMPv1 enterprise specific traps more precisely.

Note: If you select one of the generic trap types, the **Specific trap** input line and the **Select OID from MIB Tree** toolbar button are disabled.

Tip: You can view the properties of the SNMPv1 traps by clicking the toolbar button next to the **Specific trap** input line, which opens the Select Object Identifier window. This window displays all SNMPv1 traps that are defined by the currently loaded MIB modules. Note that enterprise specific traps are typically defined in private enterprise MIB modules. To view the properties of any of the displayed SNMPv1 Traps, right-click the desired trap and select the **Properties** pop-up menu command. This will open the MIB Node Properties window.

- Into the **Agent Address** input line enter the IP address of the SNMP entity associated with the Trap notification (i.e., in this case this is the IP address of computer running MIB Browser). If you want to use your local IP address as the agent's address, click the **Select Local Address** toolbar button and select the offered IP address from the list that appears.



Note: If more than one IP address is available on the computer running MIB Browser, you can choose any of them from the **Select Local Address** list.

6. Into the **Enterprise OID** input line enter the root OID of the enterprise that will be associated with this Trap notification.

Tip: Alternatively, you can click the toolbar button next to the **Enterprise OID** input line to open the Select Object Identifier window. In this window, you can browse the MIB tree or use the **Find Object in MIB Tree** command to quickly find the desired enterprise root OID. Note that you must load the MIB module, which defines this node in order for MIB Browser to display it in the MIB tree.

7. If you want MIB Browser to enter the time stamp value automatically, uncheck the **Time stamp** checkbox. To manipulate the time stamp value manually, check this checkbox and enter the time stamp value in timeticks or click the **Refresh Time Stamp** button to update this field with MIB Browser current sysUpTime value.

Note: The time stamp value should correspond to the Trap sender sysUpTime value at the time of sending the notification.

8. Close the SNMPv1 Trap Protocol Preferences dialog box by clicking the **OK** button.
9. You can create a multiple variable bindings list for an SNMPv1 Trap message in several ways, as described in the [Making Multiple Variable Bindings List](#) section of this manual.

Note: In general, it is not mandatory to include any variable bindings into an SNMPv1 Trap message. However, the linkUp and linkDown SNMPv1 generic traps typically require at least one variable binding to be included into the Trap message. This variable binding contains an instance of the columnar object ifIndex, which identifies the interface that caused the trap. See the example of a variable binding for the linkUp generic trap in the picture below.

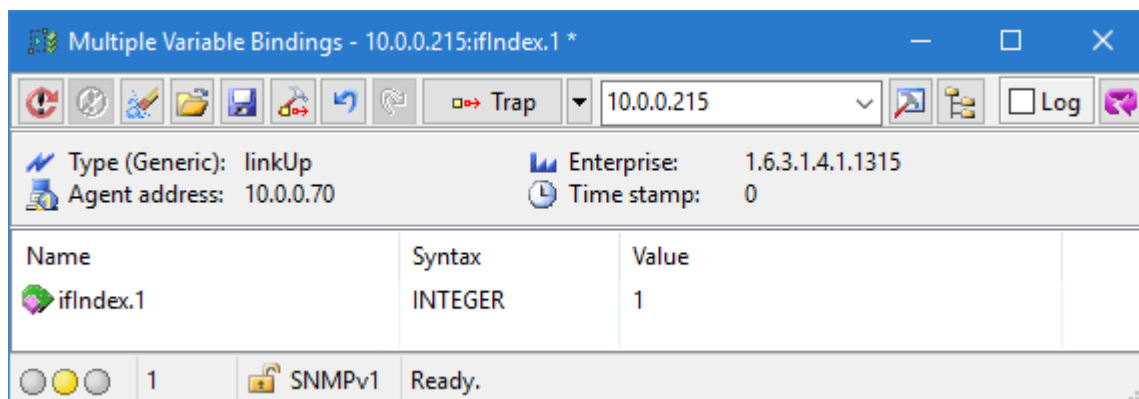


Figure 178: Example of a variable binding for SNMPv1 linkUp Trap

20.1.2 Sending SNMPv1 Trap Messages

After setting the parameters for an SNMPv1 generic or specific Trap message and creating a variable bindings list (if required), you can send the Trap notification to the network in the following way:

1. Into the Multiple Variable Bindings window drop-down list containing IP addresses (Figure 179), specify the IP address of the SNMP entity, to which you are sending this Trap message.

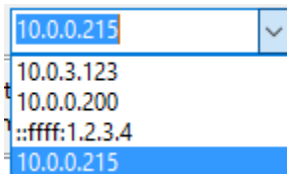


Figure 179: Specifying the trap receiver IP address

2. Click the **SNMP Protocol Preferences** toolbar button to adjust the SNMP protocol parameters for accessing the SNMP entity specified in the previous step. In the SNMP Protocol Preferences dialog box specify the following:

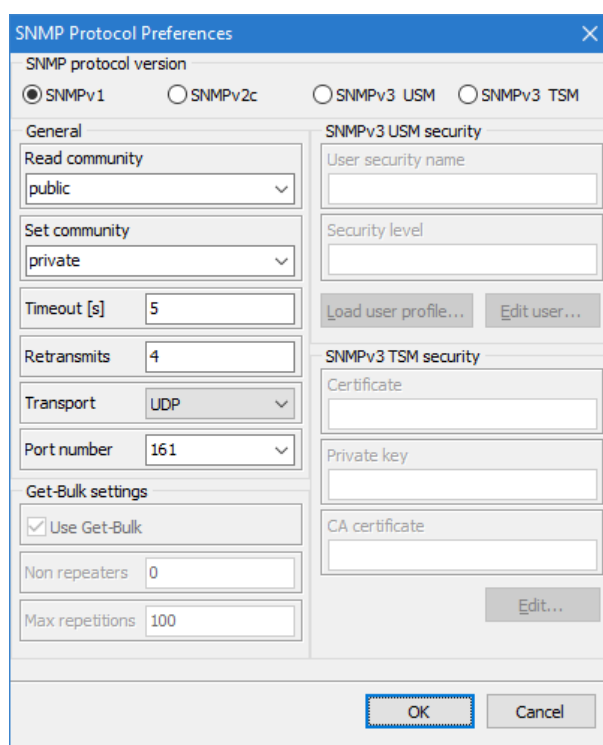
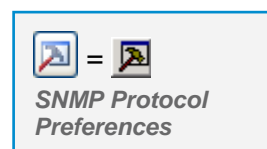


Figure 180: SNMP Protocol Preferences dialog box

- ❑ Select the **SNMPv1** radio button in the SNMP protocol version frame.
- ❑ Into the **Read community** drop-down list specify the community string for accessing this SNMP entity. This community string will be included into the Trap message.

- ❑ Into the **Port number** drop-down list specify the port number on which the trap receiver listens to for incoming traps (default: UDP/162).
 - ❑ Close the SNMP Protocol Preferences dialog box by clicking the **OK** button.
3. Finally, select the **Trap** operation type from the programmable toolbar button and click it (Figure 181).

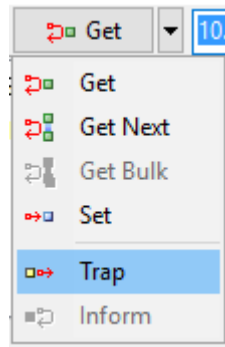
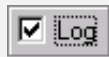


Figure 181: Selecting the Trap entry from the programmable button

4. MIB Browser sends the SNMPv1 Trap notification message (including the variable bindings if present) to the specified remote SNMP entity, e.g., to an SNMP manager.

Note: The status bar of the Multiple Variable Bindings window displays, among others, the date and time of sending the trap. Note that SNMP Trap messages do not trigger any response from the receiver.



Check the **Log** checkbox in the Multiple Variable Bindings window if you want MIB Browser to log its activities in the Query result panel of the main window.

20.2 Sending SNMPv2c/v3 Trap and Inform Notification Messages

The SNMPv2c and SNMPv3 Trap and Inform messages do not have any special PDU fields for storing notification parameters like the SNMPv1 Trap messages. Instead, SNMPv2c and SNMPv3 notification messages carry all information in the multiple variable bindings list.

This section begins with an explanation of differences between the SNMP Trap and Inform notifications. Then, the process of creating a typical variable bindings list for an SNMPv2c or an SNMPv3 notification message is described together with the steps necessary to send SNMPv2c and SNMPv3 notifications to a remote SNMP entity.

20.2.1 Difference between SNMP Trap and Inform Notifications

SNMP Trap messages represent unacknowledged notifications, meaning that they do not initiate any response from the receiver. The SNMP Inform messages, on the other hand, require that the receiver replies with a response message, confirming that the notification has been received.

Both types of SNMP notifications can be sent using the Multiple Variable Bindings window.

20.2.2 Creating Variable Binding List for SNMPv2c/v3 Notification Messages

The figure below shows an example of a variable bindings list for the SNMPv2c or SNMPv3 `linkUp` Trap message. To make a variable bindings list, use any of the procedures described in the [Making Multiple Variable Bindings List](#) section, while considering the guidelines specified below.

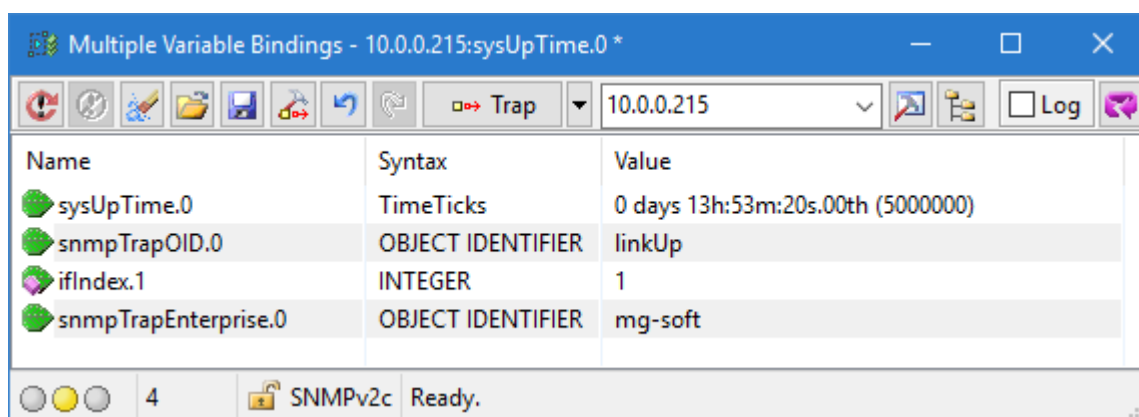


Figure 182: A typical variable binding list used with SNMPv2c/v3 `linkUp` traps

The SNMP specification defines some rules about the variable bindings, which should be included in SNMPv2c/v3 notification messages, as well as the rules about their order in the variable bindings list. These rules are:

1. The first variable binding in an SNMPv2c/v3 notification message should consist of the `sysUpTime.0` object instance and a corresponding value (in timeticks). This value should be equal to the `sysUpTime` value of the entity sending this message, at the time of sending it.
2. The second variable binding in an SNMPv2c/v3 notification message should provide the authoritative identification of the notification being sent. The name of the second variable binding is `snmpTrapOID.0` and the value is an OID, which identifies the Trap or Inform message (e.g., 1.3.6.1.6.3.1.1.5.4 (`linkUp`)).
3. In general, all other variable bindings are optional. However, in case of a `linkUp` or `linkDown` generic SNMPv2c/v3 Trap or Inform message, one of the variable bindings should contain an instance of the columnar object `ifIndex` and the corresponding value, identifying the network interface that caused the trap (similarly as in the SNMPv1 `linkUp` generic trap, described in the previous section).
4. One of the variable bindings should also specify the authoritative identification of the enterprise associated with the trap. If you are mapping an SNMPv1 Trap message to an SNMPv2c/v3 Trap message, this variable binding should occur as the last in the variable binding list. The name of this variable binding is `snmpTrapEnterprise.0` with the OID syntax and the value that identifies the enterprise associated with the Trap or Inform message.

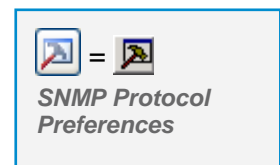
20.2.3 Sending SNMPv2c/v3 Notification Messages

Sending SNMPv2c and SNMPv3 notification messages require different settings in the SNMP Protocol Preferences dialog box. See the instructions below.

Sending SNMPv2c Trap and Inform Messages

To send an SNMPv2c Trap or Inform message containing a prepared variable bindings list (as described in the previous section), do the following:

1. In the **IP Address** drop-down list within the Multiple Variable Bindings window, specify the IP address of the SNMP entity, to which you are sending the SNMPv2c Trap or Inform message (Figure 179).
2. Click the **SNMP Protocol Preferences** toolbar button to adjust the SNMP protocol parameters for sending notifications to the SNMP entity specified in the previous step. In the SNMP Protocol Preferences dialog box specify the following:
 - ❑ Select the **SNMPv2c** radio button in the SNMP protocol version frame.
 - ❑ Specify the read community string in the **Read community** drop-down list. This community string will be included into the notification message.
 - ❑ If you are sending an SNMP Inform message, enter the desired values into the **Timeout** and **Retransmits** input lines as described in [Using SNMPv2c Protocol](#) section. These parameters are ignored when sending SNMP Trap messages.
 - ❑ In the **Port number** drop-down list, specify the port number on which the trap receiver listens to for traps (default: UDP/162).
 - ❑ Click the **OK** button to close the SNMP Protocol Preferences dialog box.
3. Finally, select the **Trap** or **Inform** operation type from the programmable toolbar button and click it to send a Trap or Inform message (Figure 181).
4. MIB Browser sends the SNMPv2c Trap or Inform message to the remote SNMP entity, for example, to a remote SNMP manager. To view the status of a sent notification, check the Multiple Variable Bindings window status bar. If the **Log** checkbox is checked in the Multiple Variable Bindings, this operation is logged in the Query result window.



Note:

The Multiple Variable Bindings window status bar shows the number of variable bindings in a message, SNMP protocol version, and the status of performed SNMP operations (this applies also to sent notifications).

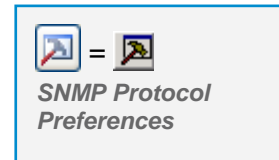
For a sent SNMP Trap notification, it displays the date and exact time of sending in the rightmost status bar field. Note that SNMP Trap notifications are neither acknowledged nor retransmitted. Therefore, in contrast to the SNMP Inform notifications, the **Timeout** and **Retransmits** input lines in the SNMP Protocol Preferences dialog box do not apply to SNMP Trap notifications.

When sending SNMP Inform notification messages, the rightmost status bar field displays the date and exact time of the confirmation response from the remote entity if it is received in the time frame, defined by the **Timeout** and **Retransmits** parameters. Otherwise, a timeout message is displayed and the red light in the status indicator (LED semaphore) is activated.

Sending SNMPv3 Trap and Inform Messages

To send an SNMPv3 Trap or Inform message containing a prepared variable bindings list (as described in the [Creating Variable Binding List for SNMPv2c/v3 Notification Messages](#) section), do the following:

1. In the **IP Address** drop-down list within the Multiple Variable Bindings window, specify the IP address of the SNMP entity, to which you are sending the SNMPv3 Trap or Inform message ([Figure 179](#)).
2. Click the **SNMP Protocol Preferences** toolbar button to adjust the SNMP protocol parameters for sending notification messages to the SNMP entity specified in the previous step. Into the SNMP Protocol Preferences dialog box specify the following:
 - ❑ Select the **SNMPv3** radio button in the SNMP protocol version frame.
 - ❑ Click the **Load User Profile** button and select an SNMPv3 USM user profile as described in the [Using SNMPv3 Protocol](#) section. Selected profile defines the USM user's SNMPv3 security settings that will be used for sending the Trap or Inform message. To create a new SNMPv3 USM user profile, follow the procedure described in the [Creating New SNMPv3 USM User Profile](#) section.



Note: The receiving entity must be configured with exactly the same SNMPv3 user security parameters as specified in MIB Browser **SNMPv3 Security Parameters (USM)** dialog box to be able to receive and process the SNMPv3 notification messages.

- ❑ When sending an SNMPv3 Inform notification, specify the desired values in the **Timeout** and **Retransmits** input lines as described in [Using SNMPv3 Protocol](#) section. These two parameters are ignored when sending SNMPv3 Trap notifications.
 - ❑ In the **Port number** drop-down list specify the port number on which the trap receiver listens for traps (default: UDP 162).
 - ❑ Click the **OK** button to close the SNMP Protocol Preferences dialog box.
3. Select the **Trap** or **Inform** operation type from the programmable toolbar button and click it to send an SNMPv3 Trap or Inform notification message ([Figure 181](#)).
 4. MIB Browser sends the SNMPv3 Trap or Inform message to the remote SNMPv3 entity. To view the status of the sent notification, check the Multiple Variable Bindings window status bar. If you have checked the **Log** checkbox in the Multiple Variable Bindings, you can also view the log of this operation in the Query result window.

21 TAKE AND COMPARE SNMP AGENT SNAPSHOTS

With MIB Browser you can take and view a snapshot of an SNMP agent as well as compare two snapshots side-by-side. An agent snapshot is a MIB tree-like presentation of MIB objects and MIB object instances together with the syntax and values of object instances as retrieved from an SNMP agent at the given time by means of the Walk operation. An agent snapshot can include either all object instances implemented in the SNMP agent, or any segment of object instances (e.g., object instances in a particular OID range or a subtree).

MIB Browser lets you take and examine the agent snapshot either in the Agent Snapshot window or in the Compare Agent Snapshots window. The procedures of taking an agent snapshot are similar in both windows, as described in the following sections.

21.1 Taking and Viewing SNMP Agent Snapshots

In the Agent Snapshot window, you can take and view an agent snapshot displaying a tree-like representation of MIB object instances together with their values and syntaxes as existed on the SNMP agent at the time of taking the snapshot (i.e., retrieving object instances by performing the Walk operation).

To take an agent snapshot in the Agent Snapshot window:

1. Open the Agent Snapshot window by using the **Tools / Agent Snapshot** command.
2. The Agent Snapshot window opens (Figure 184).
3. To take a snapshot of the SNMP agent, specify its address in the **Remote SNMP Agent** drop-down list and adjust the SNMP protocol preferences for accessing the agent if necessary, or select the proper agent profile from the SNMP Agent Profiles window.

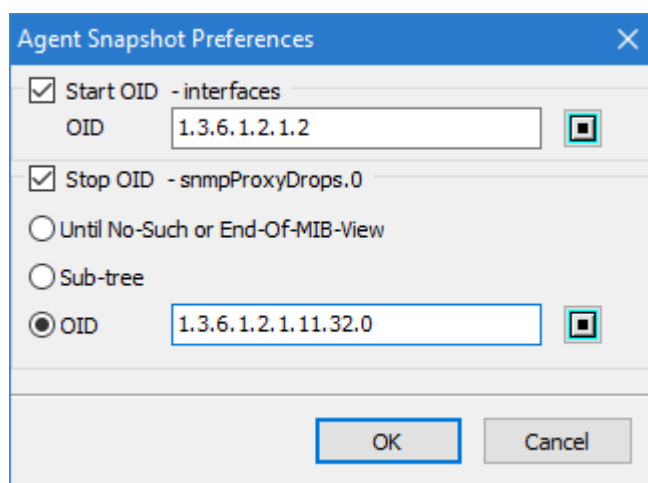
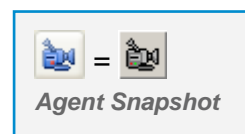


Figure 183: Agent Snapshot Preferences dialog box

4. Click the **Agent Snapshot Preferences** button to open the Agent Snapshot Preferences dialog box (Figure 183) and specify what object instances you want to retrieve from the agent.

- ❑ To take a snapshot of the entire MIB tree implemented in the SNMP agent and retrieve all object instances and their values, simply uncheck the **Start OID** and **Stop OID** checkboxes.
- ❑ To take a snapshot of a particular part of the MIB tree implemented in the SNMP agent and retrieve all object instances and their values in the specified OID range, proceed as follows:
 - ❑ Check the **Start OID** checkbox and enter the start OID value for the Walk operation into the **OID** input line.

Tip: You can also specify the OID value by selecting a corresponding node from the MIB tree. To do that, click the **Select OID from MIB Tree** button next to the start OID input line. The Select Object Identifier window appears (Figure 112). Expand the MIB tree and select the OID by double-clicking the desired node.



Note: If the **Start OID** checkbox is not checked, MIB Browser starts the Walk operation from the OID value of 1 (iso).

- ❑ Check the **Stop OID** checkbox and select one of the following options:
 - ❑ To retrieve all object instances that lexicographically follow the Start OID value, select the **Until No-Such or End-Of-MIB-View** option.
 - ❑ To retrieve all object instances within the subtree specified by the Start OID value, select the **Sub-tree** option.
 - ❑ To retrieve all object instances within the OID range specified by the start and stop OID values, select the **OID** option and specify the OID value at which the Walk operation should stop.

Tip: You can also specify the OID value by selecting a corresponding node from the MIB tree. To do that, click the **Select OID from MIB Tree** button next to the stop OID input line. The Select Object Identifier window appears (Figure 112). Expand the MIB tree and select the OID by double-clicking the desired node.

Note: If the **Stop OID** checkbox is not checked, MIB Browser retrieves all object instances that lexicographically follow the Start OID value.

- ❑ After setting the Start OID and/or Stop OID values, click the **OK** button to apply the changes and close the Agent Snapshot Preferences dialog box.
5. Click the **Refresh** toolbar button to start the Walk operation.
 6. When MIB Browser finishes the Walk operation, it displays the SNMP agent snapshot in the Agent Snapshot window (Figure 184).



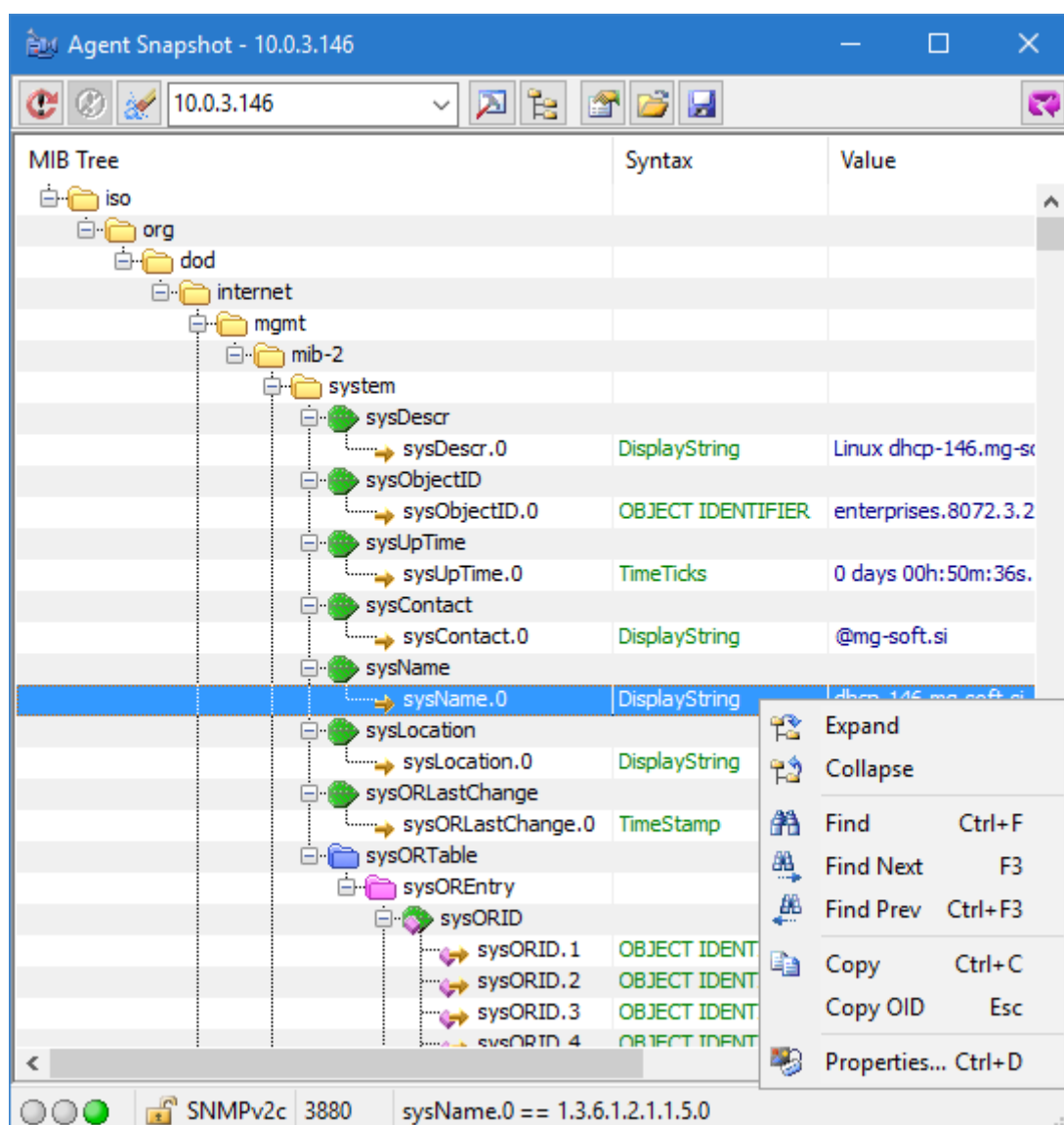


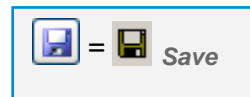
Figure 184: Agent Snapshot window

- To view the properties of a MIB object or a MIB object instance select it in the Agent Snapshot window and choose the **Properties** pop-up command.

21.1.1 Saving and Loading Agent Snapshots

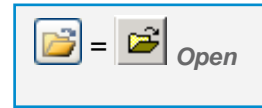
To save an agent snapshot to a file:

- Click the **Save** toolbar button to save the agent snapshot displayed in Agent Snapshot window.
- Specify the agent snapshot file name and save destination in the standard Save As dialog box that appears and click the **Save** button to create a snapshot file and close the dialog box. By default, agent snapshot files obtain the `.asfx` file name extension.



To load an agent snapshot file:

1. Click the **Open** toolbar button in the in Agent Snapshot window to open the standard Open dialog box.
2. In the Open dialog box select the desired agent snapshot file (.asf or .asf) and click the **Open** button.



Tip: You can also load an agent snapshot file that has been saved in the Compare Agent Snapshots window or in the main window (**File / Save Agent Snapshot**).

3. MIB Browser loads the selected agent snapshot file and displays its contents in the Agent Snapshot window. The Agent Snapshot window title bar displays the full path to the opened agent snapshot file.

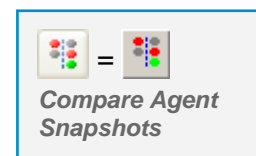
21.2 Comparing SNMP Agent Snapshots

In the Compare Agent Snapshots window you can compare two SNMP agent snapshots side-by-side. Agent snapshots can be taken either from two different SNMP agents or from one SNMP agent at different times. The window shows matches and mismatches between object instance values, 'orphaned' MIB tree nodes and differences in syntax. This section describes how to use the Compare Agent Snapshots window to take and compare agent snapshots.

21.2.1 Opening Compare Agent Snapshots Window

To open the Compare Agent Snapshots window:

1. Use the **Tools / Compare Agent Snapshots** command.
2. The Compare Agent Snapshot window opens ([Figure 185](#)). The window is divided into the left and right part, each part for displaying one SNMP agent snapshot.



MIB Browser can take a snapshot of an SNMP agent by retrieving object instances implemented in that agent, or it can load an already existing agent snapshot from a file. Furthermore, the Compare Agent Snapshots window lets you save and open the compare agent snapshot [sessions](#).

Before taking SNMP agent snapshots, you need to set the agent snapshot preferences to specify what object instances you want to compare, as described in the next section.

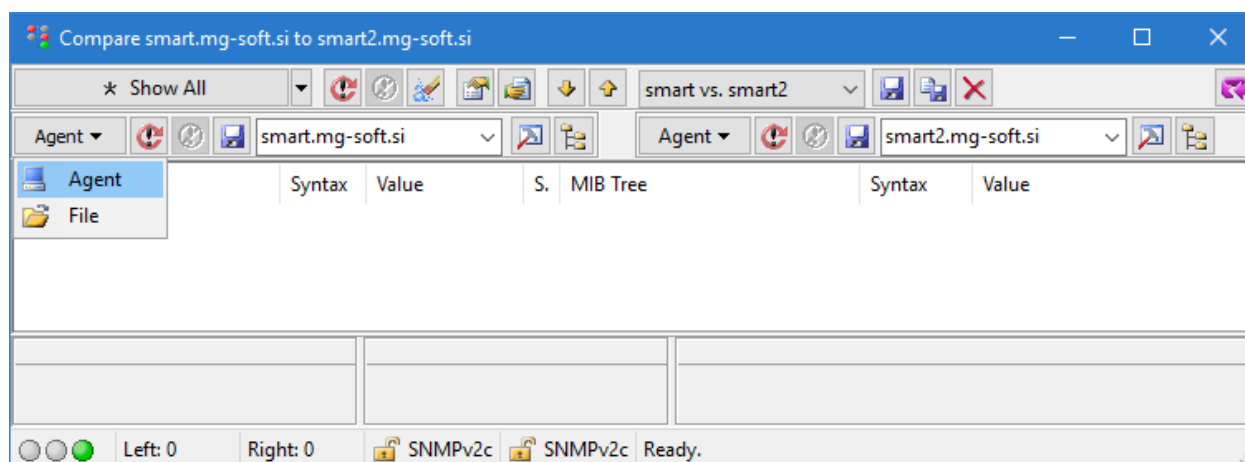
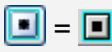


Figure 185: Compare Agent Snapshot window with a displayed Agent/File toolbar switch

21.2.2 Setting Agent Snapshot Preferences

1. Click the **Agent Snapshot Preferences** button to open the Agent Snapshot Preferences dialog box (Figure 183) and specify what object instances you want to retrieve and compare.
2. To take a snapshot of the entire MIB tree implemented in SNMP agents and retrieve all object instances and their values, simply uncheck the **Start OID** and **Stop OID** checkboxes.
3. To take a snapshot of a particular part of the MIB tree implemented in the SNMP agents and retrieve all object instances and their values in the specified OID range, proceed as follows:
 - ❑ Check the **Start OID** checkbox and enter the start OID value for the Walk operation into the **OID** input line.

Tip: You can also specify the OID value by selecting a corresponding node from the MIB tree. To do that, click the **Select OID from MIB Tree** button next to the Start OID input line. The Select Object Identifier window appears (Figure 112). Expand the MIB tree and select the OID by double-clicking the desired node.

 **Select OID from MIB Tree**

Note: If the **Start OID** checkbox is not checked, MIB Browser starts the Walk operation from the OID value of 1 (iso).

- ❑ Check the **Stop OID** checkbox and select one of the following options:
 - ❑ To retrieve all existing object instances that lexicographically follow the Start OID value, select the **Until No-Such or End-Of-MIB-View** option.
 - ❑ To retrieve all existing object instances within the subtree specified by the Start OID value, select the **Sub-tree** option.
 - ❑ To retrieve all object instances within the OID range specified by the start and stop OID values, select the **OID** option and specify the OID value at which the Walk operation should stop.

Tip: You can also specify the OID value by selecting a corresponding node from the MIB tree. To do that, click the **Select OID from MIB Tree** button next to the stop OID input line. The Select Object Identifier window appears (Figure 112). Expand the MIB tree and select the OID by double-clicking the desired node.

Note: If the **Stop OID** checkbox is not checked, MIB Browser retrieves all object instances that lexicographically follow the Start OID value.

4. After setting the Start OID and/or Stop OID values, click the **OK** button to apply the changes and close the Agent Snapshot Preferences dialog box.

21.2.3 Taking SNMP Agent Snapshots

The Compare Agent Snapshots window is vertically divided into two parts (left and right part). Each part of the window can display one SNMP agent snapshot.

To take the snapshots of two SNMP agents you want to compare:

1. Select the **Agent** command from the **Agent/File** toolbar switch in the left part of the Compare Agent Snapshots window (Figure 185).
2. Specify the address of the first SNMP agent in the left **Remote SNMP Agent** drop-down list and adjust the SNMP protocol preferences for accessing the agent if necessary, or select the proper agent profile from the SNMP Agent Profiles window.
3. Repeat steps 1 and 2 for the second SNMP agent in the right part of the Compare Agent Snapshots window.
4. Click the **Refresh (both sides)** toolbar button to start querying both SNMP agents.



Tip: that you can use the **Refresh (left side)** and **Refresh (right side)** toolbar buttons to take the snapshots of SNMP agents independently of one another.

5. The rightmost field of the status bar displays the progress of the agent snapshot operation, i.e., the OIDs currently being retrieved from both SNMP agents.
6. When MIB Browser finishes the agent snapshot (Walk) operation, it displays both agent snapshots side-by-side in the Compare Agent Snapshots window.
7. The status bar displays various information about the agent snapshot operation, i.e., the number of object instances retrieved from each SNMP agent, the SNMP protocol version used to query each agent and the status of the snapshot operation for each agent (e.g., Ready, Timeout, etc.).

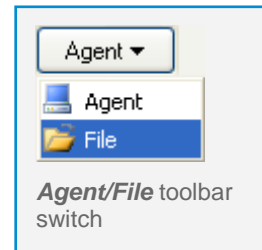
21.2.4 Saving and Loading SNMP Agent Snapshots

SNMP agent snapshots can be saved to files for later usage. The Compare Agent Snapshots window lets you load a saved agent snapshot from a file and compare it to the snapshot retrieved directly from an agent or to another agent snapshot file. Among

others, this allows you to compare snapshots of the same SNMP agent taken at different times.

To save an agent snapshot to a file:

1. Select the **File** command from the **Agent/File** toolbar switch in the left or right part of the Compare Agent Snapshots window.
2. Click the **Save** toolbar button next to the **Agent/File** toolbar switch to save the agent snapshot displayed in that part of the window.
3. Specify the agent snapshot file name and save destination in the standard Save As dialog box that appears and click the **Save** button to create a snapshot file and close the dialog box. By default, agent snapshot files obtain the `.asf` file name extension.
4. Repeat the procedure in the other part of the window to save the agent snapshot displayed in that part of the window.



Tip: To save the configuration for comparing two SNMP agents snapshots in the Compare Agent Snapshots window, proceed as described in the [Saving Compare Agent Snapshots Window Configuration as a Session](#) section.

To load an existing agent snapshot file into the Compare Agent Snapshots window:

1. Select the **File** command from the **Agent/File** toolbar switch in the left or right part of the Compare Agent Snapshots window.
2. Click the **Open** toolbar button next to the **Agent/File** toolbar switch to open the standard Open dialog box.
3. In the Open dialog box select the desired agent snapshot file (`.asfx` or `.asf`) and click the **Open** button.

Tip: You can also load an agent snapshot file that has been saved in the [Agent Snapshot window](#) or in the main window (**File / Save Agent Snapshot**).

4. MIB Browser loads the selected agent snapshot file and displays its contents in the left or right part (depending on your selection) of the Compare Agent Snapshots window.
5. Repeat the procedure in the other part of the window to open another agent snapshot file and compare both snapshots.

21.2.5 Comparing Agent Snapshots

When two SNMP agent snapshots are displayed side-by-side, you can filter the display to specify which similarities or differences between the compared SNMP agent snapshots you want to see. Moreover, you can use the **Find Next Difference** and **Find Previous Difference** commands to quickly locate the next and previous differences in compared agent snapshots.

Setting the Display Filter

- To filter the display of similarities and differences between the snapshots, click the drop-down arrow next to the **Display Filter** button in the window toolbar (Figure 186).

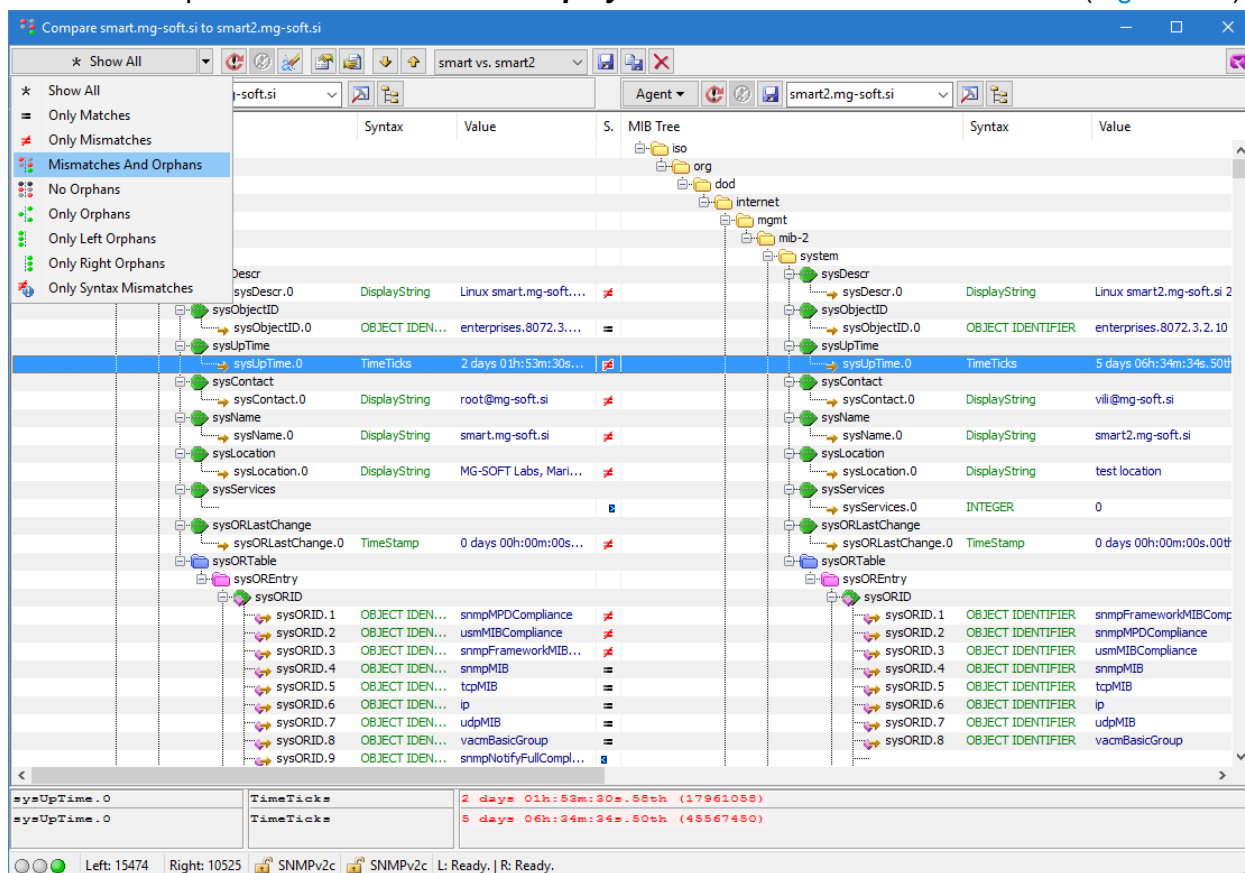
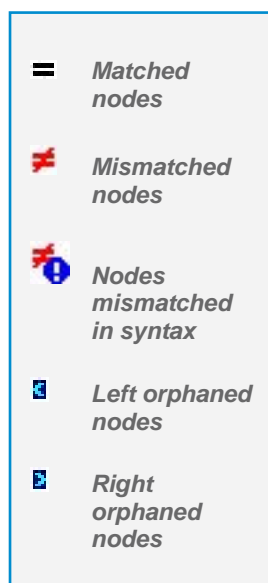


Figure 186: SNMP Agent Snapshot window and Display Filter menu

- When the menu displays, choose among:
 - ☐ **Show All** - Shows the whole MIB tree structure of both SNMP agent snapshots. It shows all matched, mismatched as well as 'orphaned' MIB tree nodes and differences in syntax values.
 - ☐ **Only Matches** - Shows only MIB tree nodes that are present in both SNMP agent snapshots and have the same OID value as well as the object instance value.
 - ☐ **Only Mismatches** - Shows only MIB tree nodes that are present in both SNMP agent snapshots and have the same OID value but different object instance value.
 - ☐ **Mismatches And Orphans** - Shows mismatched MIB tree nodes that have the same OID value but different object instance value, and 'orphaned' MIB tree objects that are present in only one of the compared SNMP agent snapshots.
 - ☐ **No Orphans** - Shows only MIB tree nodes that are present in both SNMP agent snapshots.



- ❑ **Only Orphans** - Shows MIB tree nodes that are present in only one or the other SNMP agent snapshot.
 - ❑ **Only Left Orphans** - Shows MIB tree nodes and their values that are present only in the SNMP agent snapshot displayed in the left part of the window.
 - ❑ **Only Right Orphans** - Shows MIB tree nodes and their values that are present only in the SNMP agent snapshot displayed in the right part of the window.
 - ❑ **Only Syntax Mismatches** - Shows only syntax mismatches between the compared object instances in SNMP agent snapshots.
3. MIB Browser filters the display and shows only selected parts of the MIB tree structure.
 4. If you click a particular MIB tree node in the displayed MIB tree, you can see a detailed textual description and comparison in the bottom panel.

Finding Differences in Agent Snapshots

1. To quickly locate the first difference between compared agent snapshots, click the **Find Next Difference** toolbar button or use the **CTRL+N** keyboard shortcut.
2. MIB Browser expands the MIB tree and selects the first mismatching object instance (node) in the agent snapshot MIB trees.
3. Use the **Find Next Difference** and **Find Previous Difference** toolbar buttons (or the **CTRL+N** and **CTRL+P** keyboard shortcuts) to find and view the next or previous difference between compared agent snapshots.

Note: By default, the **Find Next/Previous Difference** commands do not find the orphaned nodes. To configure MIB Browser to treat the orphan nodes as differences, open the MIB Browser Preferences dialog box (**View / MIB Browser Preferences**), switch to the **Agent Compare** panel and click the **Orphans are differences when searching for differences** checkbox.

21.2.6 Comparison Report

MIB Browser can display a comparison report summarizing differences between the compared SNMP agent snapshots.

To view the report:

1. Click the **Comparison report** toolbar button in the Compare Agent Snapshots window.
2. A Comparison Report window opens. It displays a report of compared SNMP agent snapshots ([Figure 187](#)).



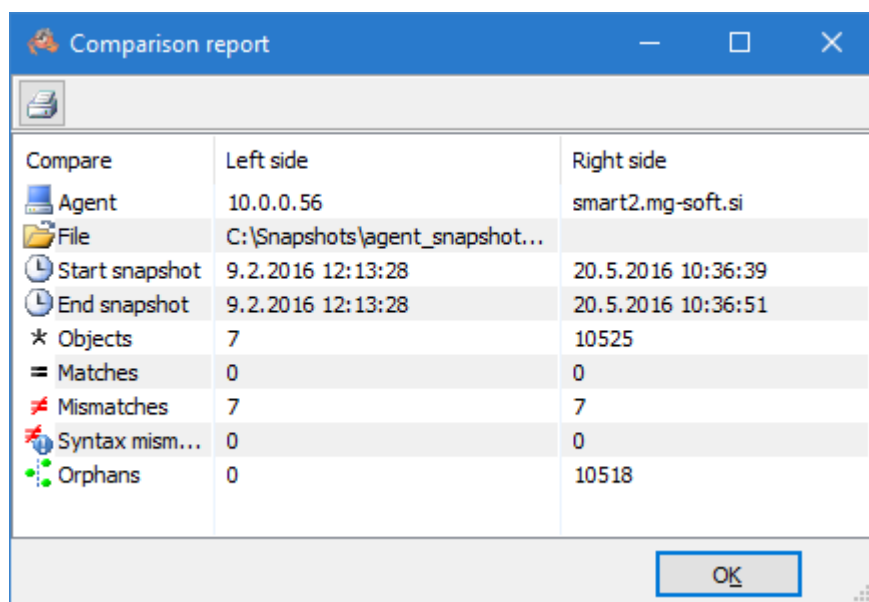


Figure 187: Comparison Report window

3. The SNMP agent snapshot comparison report includes the following information (Figure 187):
 - ❑ IP addresses of compared SNMP agents
 - ❑ Paths to files where the snapshots are saved
 - ❑ Date and the time when the snapshots were taken
 - ❑ Number of object instances retrieved from each SNMP agent
 - ❑ Number of matched object instances
 - ❑ Number of mismatched object instances
 - ❑ Number of syntax mismatches
 - ❑ Number of 'orphaned' object instances in each SNMP agent
4. You can also print the report by clicking the **Print** toolbar button.

21.3 Saving and Loading SNMP Agent Snapshot Sessions

Once you configure all settings for comparing two SNMP agent snapshots in the Compare Agent Snapshots window, you can save such configuration as a session. A session includes information about the addresses of compared SNMP agents, the SNMP access parameters for accessing those agents (or information about loaded agent snapshot files), as well as the Agent Snapshot Preferences and display filter settings. After saving a session, you can quickly take and compare snapshots of the same SNMP agents by selecting the appropriate session from the **Sessions** drop-down list in the Compare Agent Snapshots window.

Note: Saving a session does not save the currently displayed SNMP agent snapshots (MIB trees). To save such snapshots, proceed as described in the [Saving and Loading SNMP Agent Snapshots](#) section.

Saving Compare Agent Snapshots Window Configuration as a Session

1. Click the **Save Session As** toolbar button to open the New Session Name dialog box.

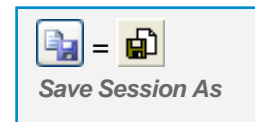
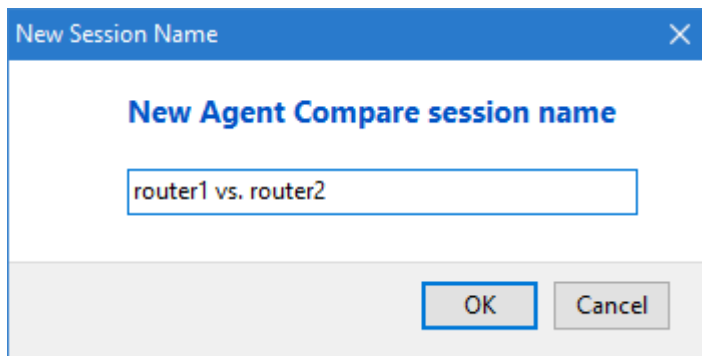
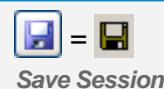


Figure 188: Creating a session in the Compare Agent Snapshot window

2. Specify the compare agent snapshots session name in the New Session Name dialog box and click the **OK** button to save the session and close the dialog box.
3. The new session is added to the **Sessions** drop-down list in the Compare Agent Snapshots window.

Tip: Once the session is saved, simply use the **Save Session** toolbar button to save any subsequent configuration changes in the Compare Agent Snapshots Window under the same session name.



Loading an Existing Session in the Compare Agent Snapshots Window

1. Select the desired session name from the **Sessions** drop-down list in the Compare Agent Snapshots window.

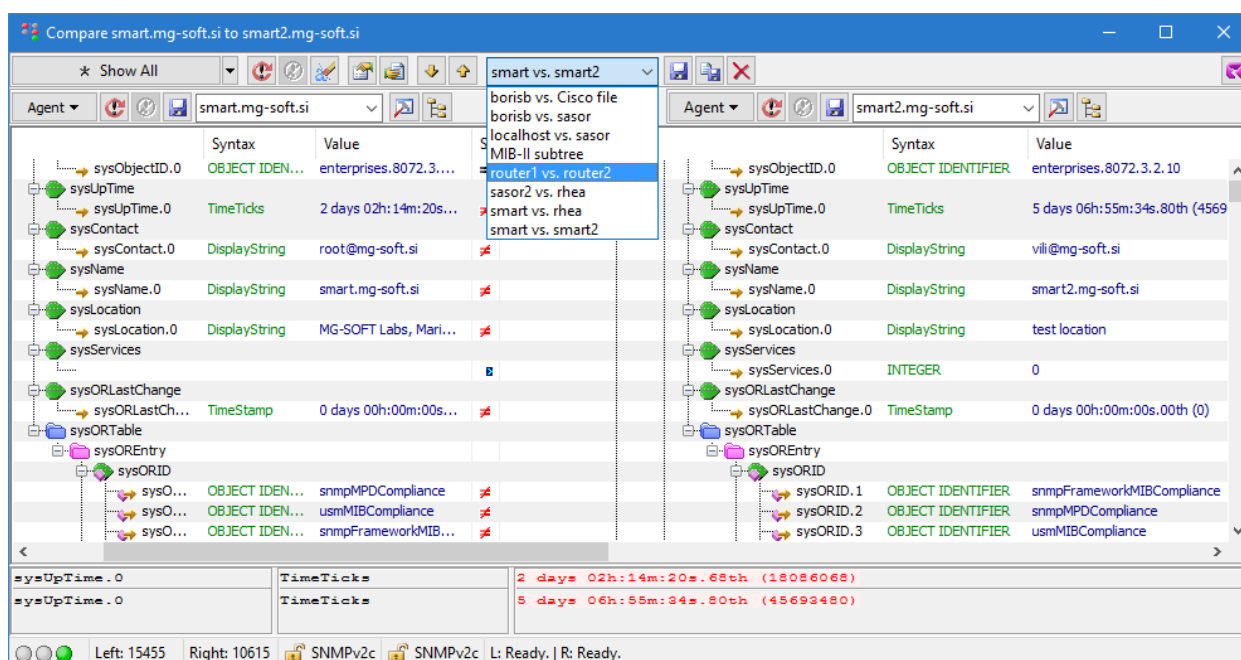


Figure 189: Loading a session in the Compare Agent Snapshot window

2. MIB Browser loads the selected session in the Compare Agent Snapshots window and takes the fresh snapshots of compared SNMP agents or loads and displays agent snapshot files side-by-side (depending on the session settings).

Tip: To configure MIB Browser to automatically load the last used session when you open the Compare Agent Snapshots window, open the MIB Browser Preferences dialog box (**View / MIB Browser Preferences**), display the 'Agent Compare' panel and select the **Browse last session at show** option.

22 MANAGE SNMPV3 USM USERS ON REMOTE SNMP AGENTS

MIB Browser lets you manage SNMPv3 USM user configuration on remote SNMPv3 agents. The user management operations include ‘cloning’ SNMPv3 users, changing secret authentication and privacy keys of SNMPv3 users, as well as enabling, disabling and deleting SNMPv3 users.

All these operations are accomplished through SNMP by setting the appropriate ‘usmUserTable’ object instances on remote SNMP agents as specified in the SNMPv3/USM specification (RFC 3414). Therefore, to be able to successfully perform SNMPv3 user management operations on an SNMP agent, the agent must implement the ‘usmUserTable’ (SNMP-USER-BASED-SM-MIB) and provide write access to it.

22.1 Managing Existing SNMPv3 Users on Remote SNMP Agent

To view and manage the existing SNMPv3 USM users on a remote SNMP agent:

1. Select the **Tools / Manage Agent SNMPv3 USM Users** command.
2. The **Manage Agent SNMPv3 Users** dialog box appears (Figure 190), listing all existing SNMPv3 USM users configured on the given remote SNMP agent (i.e., the SNMPv3 users that exist in the ‘usmUserTable’ implemented in the remote SNMP agent).

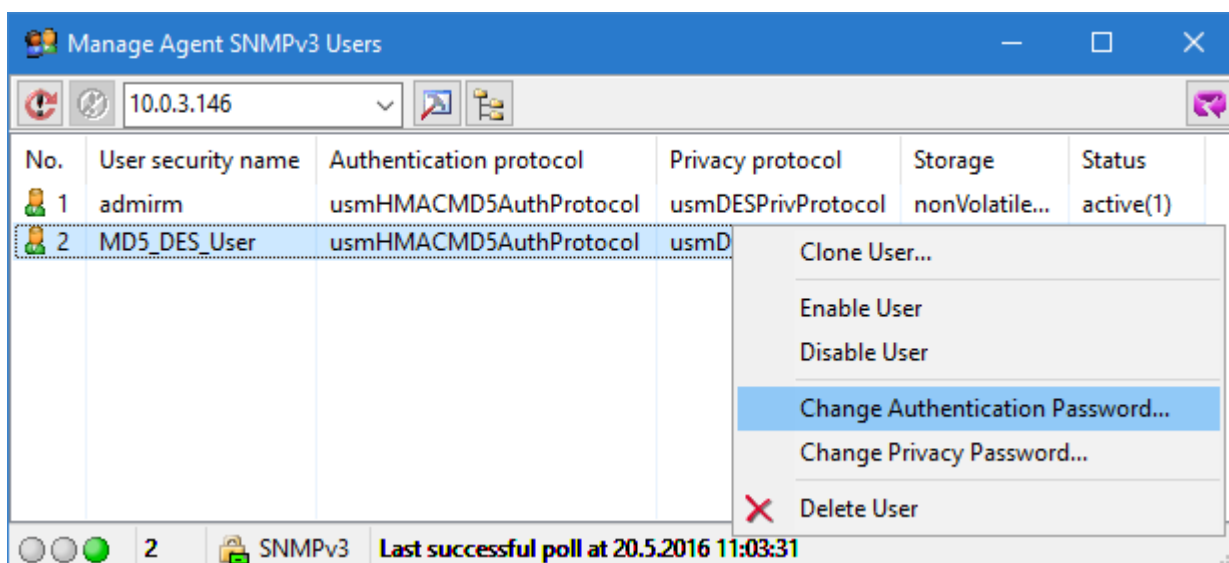


Figure 190: Manage Agent SNMPv3 Users dialog box

3. To view or manage SNMPv3 user configuration on another SNMP agent, specify its address in the **Remote SNMP Agent** drop-down list or select the agent profile from the SNMP Agent Profiles window.
4. The Manage Agent SNMPv3 Users dialog box lets you perform the following operations:
 - ❑ To disable an active SNMPv3 USM user, select the relevant row in the Manage Agent SNMPv3 Users dialog box and use the **Disable** pop-up command. The status of the given row should change from ‘active(1)’ to ‘notInService(2)’, meaning that the SNMPv3 user is disabled.

- ❑ To enable a disabled SNMPv3 USM user, select the relevant row in the Manage Agent SNMPv3 Users dialog box and use the **Enable** pop-up command. The status of the given row should change to 'active(1)', meaning that the SNMPv3 user is enabled.
- ❑ To change the secret authentication key and thus the authentication password of an existing SNMPv3 USM user, select the relevant row and choose the **Change Authentication Password** pop-up command (Figure 190).
- ❑ The Old Password for Authentication Protocol dialog box appears (Figure 191). Enter the existing authentication protocol password of the selected USM user into both input lines and click the **OK** button.

Figure 191: Entering SNMPv3 user's old authentication protocol password

- ❑ The New Password for Authentication Protocol dialog box appears (Figure 192). Enter the new authentication protocol password for the USM user into both input lines and click the **OK** button to close the dialog box and change the authentication password (key) on the remote SNMP agent.

Figure 192: Entering SNMPv3 user's new authentication protocol password

- ❑ To change the secret privacy key and thus the privacy password of an existing SNMPv3 USM user, select the relevant row, choose the **Change Privacy Password** pop-up command and enter the old and new privacy passwords twice into both dialog boxes that appear.
- ❑ To delete an SNMPv3 USM user, select the relevant row in the Manage Agent SNMPv3 Users dialog box and use the **Delete** pop-up command. The given row should disappear from the Manage Agent SNMPv3 Users dialog box.
- ❑ For instructions on 'cloning' SNMPv3 USM users, see the next section.

22.2 Creating New SNMPv3 USM User on Remote SNMP Agent

MIB Browser lets you 'clone' SNMPv3 USM users on remote SNMP agents, i.e., create new SNMPv3 users from the existing ones.

To create a new SNMPv3 USM user on Remote SNMP Agent and change its secret keys:

1. Select the **Tools / Manage Agent SNMPv3 USM Users** command.
2. The Manage Agent SNMPv3 Users dialog box appears (Figure 190), listing all existing SNMPv3 USM users configured on the given SNMP agent (i.e., the USM user information that exists in the 'usmUserTable' implemented in the remote SNMP agent).
3. To view or manage SNMPv3 USM user configuration on another SNMP agent, specify its address in the **Remote SNMP Agent** drop-down list or select the agent profile from the SNMP Agent Profiles window.
4. To create a new SNMPv3 USM user by 'cloning' its properties from an existing user (called the 'template' user), select the existing user and choose the **Clone** pop-up command.

Note: At least one SNMPv3 user must be already configured on the remote SNMP agent (i.e., at least one row must exist in the agent's 'usmUserTable'), otherwise no new SNMPv3 users can be created via SNMP.

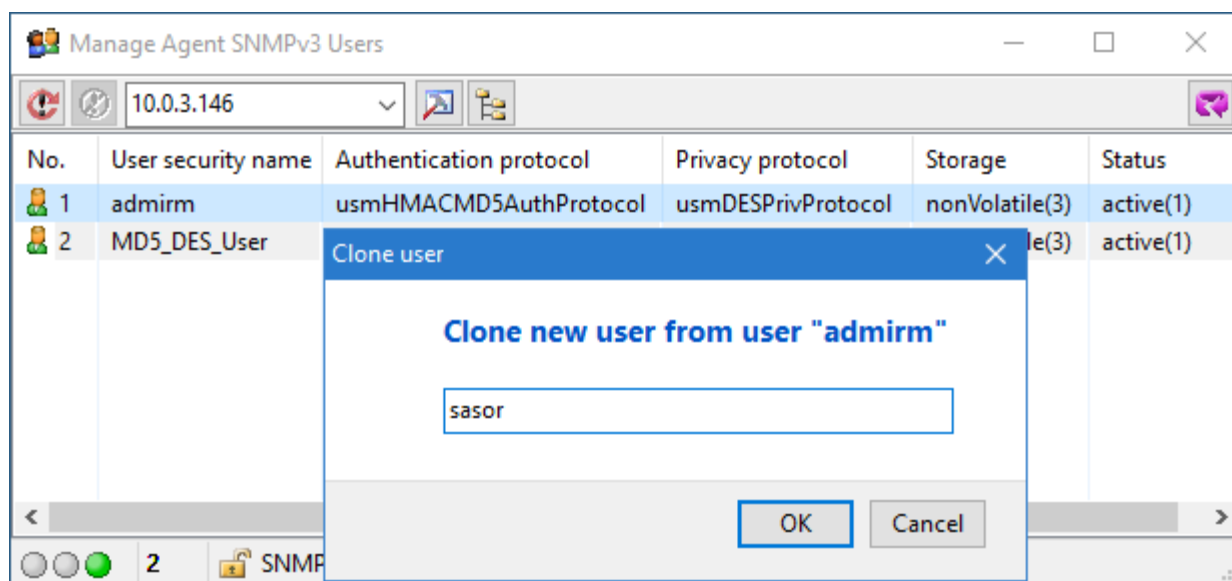


Figure 193: Cloning an SNMPv3 USM user on remote SNMP agent

5. The Clone User dialog box appears, prompting you to enter the user name for the new user, which is to be created (Figure 193). Enter a desired user name and click the **OK** button.
6. MIB Browser sends an SNMP Set request to the SNMP agent to instantiate a new row in the 'usmUserTable' and thus create a new SNMPv3 USM user on the remote SNMP agent. If the SNMP Set operation finishes successfully, a new row appears in the Manage Agent SNMPv3 Users dialog box, representing the new user. The SNMPv3 authentication and privacy parameters (including the secret authentication and privacy keys) of the new user match exactly the parameters of the 'template' user.

No.	User security name	Authentication protocol	Privacy protocol	Storage	Status
1	sasor	usmHMACMD5AuthProtoc...	usmDESPrivProtocol	nonVolatile(3)	active(1)
2	admirm	usmHMACMD5AuthProtoc...	usmDESPrivProtocol	nonVolatile(3)	active(1)
3	MD5_DES_User	usmHMACMD5AuthProtoc...	usmDESPrivProtocol	nonVolatile(3)	active(1)

3 SNMPv2c Last successful poll at 20.5.2016 12:22:14

Figure 194: New SNMPv3 USM user created on remote SNMP agent

7. To change the secret authentication key and thus the authentication password of the new user, select the row representing the new user and choose the **Change Authentication Password** pop-up command (Figure 190).
8. The Old Password for Authentication Protocol dialog box appears (Figure 191). Enter the authentication protocol password of the 'template' user into both input lines and click the **OK** button.
9. The New Password for Authentication Protocol dialog box appears (Figure 192). Enter the new authentication protocol password for the selected user into both input lines and click the **OK** button.
10. MIB Browser computes the new secret authentication key from the given old and new passwords according to the algorithm specified in RFC 3414 and sends an SNMP Set request to the SNMP agent to change the secret authentication key and thus the authentication password of the user. If the operation finishes successfully (check the status line), the secret key is changed and the new password is active.
11. To change the secret privacy key and thus the privacy password of the new user, select the row representing the new user, choose the **Change Privacy Password** pop-up command and enter the old and new privacy passwords twice into both dialog boxes that appear (similar to changing the authentication password).
12. If the new SNMPv3 user is not enabled yet, i.e., if the status column displays the 'notInService(2)' status for the relevant row, select the row and use the **Enable** pop-up command.
13. MIB Browser sends a SNMP Set request to the SNMP agent to change its status to 'active(1)' and thus enable the new user. If the operation finishes successfully, the user is enabled, meaning that the SNMP agent will accept and respond to SNMPv3 requests sent to it on behalf of that user.

Note: On SNMP agents implementing the View-based Access Control Model (RFC 3415), you need to configure the appropriate access rights for the new SNMPv3 USM user, before starting to query and manage the agent on behalf of the new user.

23 DEBUG PROBLEMS IN GENERIC SNMP TRACE WINDOW

During its operations, MIB Browser exchanges a number of SNMP messages with remote SNMP agents in order to retrieve or set certain information.

Sometimes the exchange of information is not possible for whatever reason (e.g., wrong SNMP access parameters may be used and the SNMP agent does not respond, or there can be a bug in the SNMP agent that prevents the exchange of SNMP messages or it behaves in an unexpected fashion).

That is why MIB Browser introduced the Generic SNMP Trace window that can be used for checking the SNMP messages exchanged on the network during any SNMP operation performed in MIB Browser.

The Generic SNMP Trace window shows a list of SNMP request and response messages that were sent to or received from SNMP agents. It also shows the contents of each SNMP message; displayed in hexadecimal format as well as in decoded, human-readable format. Therefore, the Generic SNMP Trace feature is particularly useful for debugging and resolving problems when the SNMP agent does not properly respond to MIB Browser queries.



Note: This feature is available only in the *Developer's Edition* and *Simulator Edition* of *MIB Browser Pro*.

Note: MIB Browser implements the Generic SNMP Trace window in two instances:

- 1) The general **Generic SNMP Trace** window, which traces SNMP messages that are exchanged during operations performed in any MIB Browser window.
- 2) The **Generic SNMP Trace For Trap Ringer** window, which traces *only* SNMP notification messages received into the SNMP Trap Ringer Console window (together with responses to SNMP Inform notifications).

23.1 Tracing Exchanged SNMP Messages

You can use the Generic SNMP Trace window to trace and record SNMP messages exchanged between MIB Browser and SNMP agents while performing SNMP operations in any MIB Browser window.

23.1.1 Select MIB Browser Windows to Be Recorded

By default, the Generic SNMP Trace window traces SNMP packets in two windows: in MIB Browser main widow (Query results panel) and in the Set window. You can configure MIB Browser to trace SNMP packets originating from any other window.

To select windows in which SNMP messages shall be recorded:

1. Open the MIB Browser Preferences dialog box by using the **View / MIB Browser Preferences** command and click the **Windows** entry under the **Trace** entry in the navigation tree (left-hand side of the dialog box).

2. In the **Traced windows** frame (Figure 195), check the checkboxes in front of the names of the windows that shall be traced.
3. When you have specified which MIB Browser windows shall be traced, click the **OK** button. To learn how to trace the SNMP messages in selected windows, see the [Tracing and Decoding SNMP Messages](#) section.

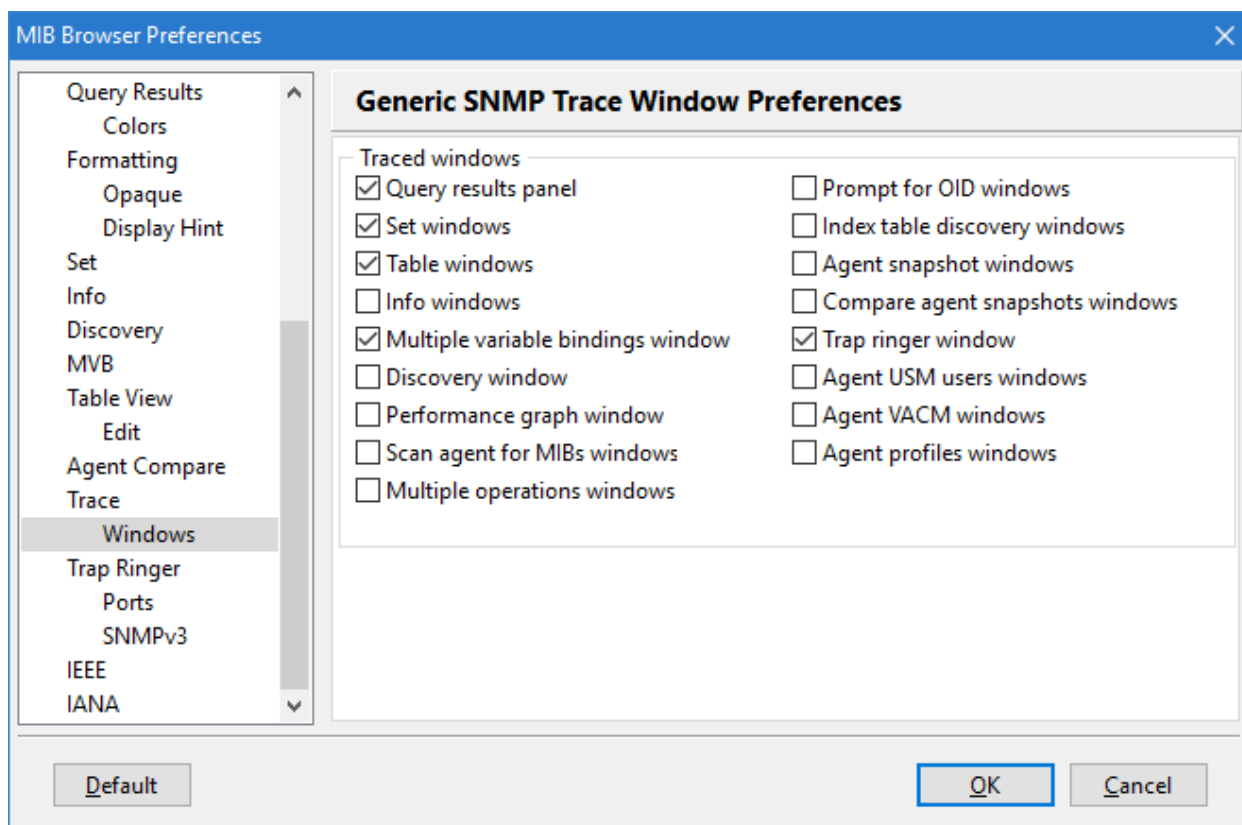
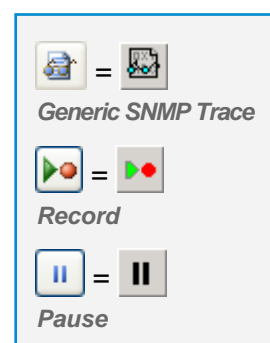


Figure 195: In Generic SNMP Trace Window Preferences panel specify MIB Browser windows to be traced

23.1.2 Tracing and Decoding SNMP Messages

To trace SNMP messages exchanged during operations performed in the selected windows:

1. In the main window, use the **Tools / Generic SNMP Trace** command or click the **Generic SNMP Trace** toolbar button to open the Generic SNMP Trace window.
2. If necessary, click the **Record** toolbar button in the Generic SNMP Trace window to start the recording. The recording of SNMP messages will continue until you click the **Pause** toolbar button.



Note: By default, the recording starts at startup. You can change this, by unchecking the **Start recording at startup** checkbox in the MIB Browser Preferences dialog box (Figure 195).

3. Open the window, whose SNMP messages you wish to record and perform one or more SNMP operations in it. For example, if you have selected to trace the Multiple

Variable Bindings windows, open a [Multiple Variable Bindings window](#) and perform a SNMP Set operation in it.

Note: Make sure the window has been selected in the MIB Browser Preferences dialog box (see the [Select MIB Browser Windows to Be Recorded](#) section).

4. MIB Browser records the SNMP message exchange of the selected window and displays the recorded messages in the Generic SNMP Trace window.
5. To check the contents of the recorded SNMP messages, switch to the Generic SNMP Trace window by using the **Window / Trace Windows / Query Windows** command.
6. The Generic SNMP Trace window opens ([Figure 196](#)). In the first panel, it displays a list of all SNMP messages exchanged on the network during the recorded SNMP session.

Note: The recording function slightly decreases the performance of the software; so make sure to switch it off when you do not need it.

The screenshot shows the 'Generic SNMP Trace [Query Windows]' window. It features a toolbar with icons for file operations, playback, and search. Below the toolbar is a search bar and a table of recorded SNMP messages. The table has columns: No, Direction, Time, Version, Type, Source Address, Destin..., Community, Request ID, and Error Status. Three messages are listed, with the second one (No. 6) selected. Below the table, the 'SNMP Message' section shows the raw hex data of the selected message. The 'Decoded SNMP Message' section shows the parsed fields of the message, including Object ID, Object type, Request ID, Error code, and Value.

No	Direction	Time	Version	Type	Source Address	Destin...	Community	Request ID	Error Status
5	>	4:00:41.928 AM	SNMPv1	GetNext	10.0.3.127	161	public	202	0
6	<	4:00:41.953 AM	SNMPv1	Response	127.0.0.1	62167	public	202	0
7	>	4:00:41.953 AM	SNMPv1	GetNext	10.0.3.127	161	public	203	0

SNMP Message

Size = 0002D(000045)

```

1: 0000(000000) 30 2B 02 01 00 04 06 70 75 62 6C 69 63 A2 1E 02 0+....public...
2: 00010(000016) 02 00 CA 02 01 00 02 01 00 30 12 30 10 06 08 2B .....0.0...+
3: 00020(000032) 06 01 02 01 01 03 00 43 04 04 29 35 A7 .....C..) 5.

```

Decoded SNMP Message

```


1: SNMP 0000:00/00|FF ***** Simple Network Management Protocol *****
2: SNMP 0000:00/00|FF
3: SNMP 0001:01/00|FF Length 43 [2B (hex)] (octets)
4: SNMP 0004:01/00|FF Version 0 (SNMPv1)
5: SNMP 0007:06/00|FF Community public
6: SNMP 0013:01/08|FF Object type 1.0.1.0.0.1.0 (Response)
7: SNMP 0017:02/00|FF Request ID 202
8: SNMP 0021:01/00|FF Error code 0 (no error)
9: SNMP 0024:01/00|FF Error index 0
10: SNMP 0031:08/00|FF Object ID 1.3.6.1.2.1.1.3.0 (sysUpTime.0) #1
11: SNMP 0039:01/08|FF Object type 0.1.0.0.0.1.1 (TimeTicks)
12: SNMP 0041:04/00|FF Value 69809575

```

Recording [S] 16 [1] 16 [2] 0 [3] 0 [4] 0 [5] 8 [6] 0 [7] 0 [8] 0 [9] 0 [10] 0 [11] 0 [12] 0 [13] 0 [14] 0 [15] 0 [16] 0 [17] 0 [18] 0 [19] 0 [20] 0 [21] 0 [22] 0 [23] 0 [24] 0 [25] 0 [26] 0 [27] 0 [28] 0 [29] 0 [30] 0 [31] 0 [32] 0 [33] 0 [34] 0 [35] 0 [36] 0 [37] 0 [38] 0 [39] 0 [40] 0 [41] 0 [42] 0 [43] 0 [44] 0 [45] 0 [46] 0 [47] 0 [48] 0 [49] 0 [50] 0 [51] 0 [52] 0 [53] 0 [54] 0 [55] 0 [56] 0 [57] 0 [58] 0 [59] 0 [60] 0 [61] 0 [62] 0 [63] 0 [64] 0 [65] 0 [66] 0 [67] 0 [68] 0 [69] 0 [70] 0 [71] 0 [72] 0 [73] 0 [74] 0 [75] 0 [76] 0 [77] 0 [78] 0 [79] 0 [80] 0 [81] 0 [82] 0 [83] 0 [84] 0 [85] 0 [86] 0 [87] 0 [88] 0 [89] 0 [90] 0 [91] 0 [92] 0 [93] 0 [94] 0 [95] 0 [96] 0 [97] 0 [98] 0 [99] 0 [100] 0 [101] 0 [102] 0 [103] 0 [104] 0 [105] 0 [106] 0 [107] 0 [108] 0 [109] 0 [110] 0 [111] 0 [112] 0 [113] 0 [114] 0 [115] 0 [116] 0 [117] 0 [118] 0 [119] 0 [120] 0 [121] 0 [122] 0 [123] 0 [124] 0 [125] 0 [126] 0 [127] 0 [128] 0 [129] 0 [130] 0 [131] 0 [132] 0 [133] 0 [134] 0 [135] 0 [136] 0 [137] 0 [138] 0 [139] 0 [140] 0 [141] 0 [142] 0 [143] 0 [144] 0 [145] 0 [146] 0 [147] 0 [148] 0 [149] 0 [150] 0 [151] 0 [152] 0 [153] 0 [154] 0 [155] 0 [156] 0 [157] 0 [158] 0 [159] 0 [160] 0 [161] 0 [162] 0 [163] 0 [164] 0 [165] 0 [166] 0 [167] 0 [168] 0 [169] 0 [170] 0 [171] 0 [172] 0 [173] 0 [174] 0 [175] 0 [176] 0 [177] 0 [178] 0 [179] 0 [180] 0 [181] 0 [182] 0 [183] 0 [184] 0 [185] 0 [186] 0 [187] 0 [188] 0 [189] 0 [190] 0 [191] 0 [192] 0 [193] 0 [194] 0 [195] 0 [196] 0 [197] 0 [198] 0 [199] 0 [200] 0 [201] 0 [202] 0 [203] 0 [204] 0 [205] 0 [206] 0 [207] 0 [208] 0 [209] 0 [210] 0 [211] 0 [212] 0 [213] 0 [214] 0 [215] 0 [216] 0 [217] 0 [218] 0 [219] 0 [220] 0 [221] 0 [222] 0 [223] 0 [224] 0 [225] 0 [226] 0 [227] 0 [228] 0 [229] 0 [230] 0 [231] 0 [232] 0 [233] 0 [234] 0 [235] 0 [236] 0 [237] 0 [238] 0 [239] 0 [240] 0 [241] 0 [242] 0 [243] 0 [244] 0 [245] 0 [246] 0 [247] 0 [248] 0 [249] 0 [250] 0 [251] 0 [252] 0 [253] 0 [254] 0 [255] 0 [256] 0 [257] 0 [258] 0 [259] 0 [260] 0 [261] 0 [262] 0 [263] 0 [264] 0 [265] 0 [266] 0 [267] 0 [268] 0 [269] 0 [270] 0 [271] 0 [272] 0 [273] 0 [274] 0 [275] 0 [276] 0 [277] 0 [278] 0 [279] 0 [280] 0 [281] 0 [282] 0 [283] 0 [284] 0 [285] 0 [286] 0 [287] 0 [288] 0 [289] 0 [290] 0 [291] 0 [292] 0 [293] 0 [294] 0 [295] 0 [296] 0 [297] 0 [298] 0 [299] 0 [300] 0 [301] 0 [302] 0 [303] 0 [304] 0 [305] 0 [306] 0 [307] 0 [308] 0 [309] 0 [310] 0 [311] 0 [312] 0 [313] 0 [314] 0 [315] 0 [316] 0 [317] 0 [318] 0 [319] 0 [320] 0 [321] 0 [322] 0 [323] 0 [324] 0 [325] 0 [326] 0 [327] 0 [328] 0 [329] 0 [330] 0 [331] 0 [332] 0 [333] 0 [334] 0 [335] 0 [336] 0 [337] 0 [338] 0 [339] 0 [340] 0 [341] 0 [342] 0 [343] 0 [344] 0 [345] 0 [346] 0 [347] 0 [348] 0 [349] 0 [350] 0 [351] 0 [352] 0 [353] 0 [354] 0 [355] 0 [356] 0 [357] 0 [358] 0 [359] 0 [360] 0 [361] 0 [362] 0 [363] 0 [364] 0 [365] 0 [366] 0 [367] 0 [368] 0 [369] 0 [370] 0 [371] 0 [372] 0 [373] 0 [374] 0 [375] 0 [376] 0 [377] 0 [378] 0 [379] 0 [380] 0 [381] 0 [382] 0 [383] 0 [384] 0 [385] 0 [386] 0 [387] 0 [388] 0 [389] 0 [390] 0 [391] 0 [392] 0 [393] 0 [394] 0 [395] 0 [396] 0 [397] 0 [398] 0 [399] 0 [400] 0 [401] 0 [402] 0 [403] 0 [404] 0 [405] 0 [406] 0 [407] 0 [408] 0 [409] 0 [410] 0 [411] 0 [412] 0 [413] 0 [414] 0 [415] 0 [416] 0 [417] 0 [418] 0 [419] 0 [420] 0 [421] 0 [422] 0 [423] 0 [424] 0 [425] 0 [426] 0 [427] 0 [428] 0 [429] 0 [430] 0 [431] 0 [432] 0 [433] 0 [434] 0 [435] 0 [436] 0 [437] 0 [438] 0 [439] 0 [440] 0 [441] 0 [442] 0 [443] 0 [444] 0 [445] 0 [446] 0 [447] 0 [448] 0 [449] 0 [450] 0 [451] 0 [452] 0 [453] 0 [454] 0 [455] 0 [456] 0 [457] 0 [458] 0 [459] 0 [460] 0 [461] 0 [462] 0 [463] 0 [464] 0 [465] 0 [466] 0 [467] 0 [468] 0 [469] 0 [470] 0 [471] 0 [472] 0 [473] 0 [474] 0 [475] 0 [476] 0 [477] 0 [478] 0 [479] 0 [480] 0 [481] 0 [482] 0 [483] 0 [484] 0 [485] 0 [486] 0 [487] 0 [488] 0 [489] 0 [490] 0 [491] 0 [492] 0 [493] 0 [494] 0 [495] 0 [496] 0 [497] 0 [498] 0 [499] 0 [500] 0 [501] 0 [502] 0 [503] 0 [504] 0 [505] 0 [506] 0 [507] 0 [508] 0 [509] 0 [510] 0 [511] 0 [512] 0 [513] 0 [514] 0 [515] 0 [516] 0 [517] 0 [518] 0 [519] 0 [520] 0 [521] 0 [522] 0 [523] 0 [524] 0 [525] 0 [526] 0 [527] 0 [528] 0 [529] 0 [530] 0 [531] 0 [532] 0 [533] 0 [534] 0 [535] 0 [536] 0 [537] 0 [538] 0 [539] 0 [540] 0 [541] 0 [542] 0 [543] 0 [544] 0 [545] 0 [546] 0 [547] 0 [548] 0 [549] 0 [550] 0 [551] 0 [552] 0 [553] 0 [554] 0 [555] 0 [556] 0 [557] 0 [558] 0 [559] 0 [560] 0 [561] 0 [562] 0 [563] 0 [564] 0 [565] 0 [566] 0 [567] 0 [568] 0 [569] 0 [570] 0 [571] 0 [572] 0 [573] 0 [574] 0 [575] 0 [576] 0 [577] 0 [578] 0 [579] 0 [580] 0 [581] 0 [582] 0 [583] 0 [584] 0 [585] 0 [586] 0 [587] 0 [588] 0 [589] 0 [590] 0 [591] 0 [592] 0 [593] 0 [594] 0 [595] 0 [596] 0 [597] 0 [598] 0 [599] 0 [600] 0 [601] 0 [602] 0 [603] 0 [604] 0 [605] 0 [606] 0 [607] 0 [608] 0 [609] 0 [610] 0 [611] 0 [612] 0 [613] 0 [614] 0 [615] 0 [616] 0 [617] 0 [618] 0 [619] 0 [620] 0 [621] 0 [622] 0 [623] 0 [624] 0 [625] 0 [626] 0 [627] 0 [628] 0 [629] 0 [630] 0 [631] 0 [632] 0 [633] 0 [634] 0 [635] 0 [636] 0 [637] 0 [638] 0 [639] 0 [640] 0 [641] 0 [642] 0 [643] 0 [644] 0 [645] 0 [646] 0 [647] 0 [648] 0 [649] 0 [650] 0 [651] 0 [652] 0 [653] 0 [654] 0 [655] 0 [656] 0 [657] 0 [658] 0 [659] 0 [660] 0 [661] 0 [662] 0 [663] 0 [664] 0 [665] 0 [666] 0 [667] 0 [668] 0 [669] 0 [670] 0 [671] 0 [672] 0 [673] 0 [674] 0 [675] 0 [676] 0 [677] 0 [678] 0 [679] 0 [680] 0 [681] 0 [682] 0 [683] 0 [684] 0 [685] 0 [686] 0 [687] 0 [688] 0 [689] 0 [690] 0 [691] 0 [692] 0 [693] 0 [694] 0 [695] 0 [696] 0 [697] 0 [698] 0 [699] 0 [700] 0 [701] 0 [702] 0 [703] 0 [704] 0 [705] 0 [706] 0 [707] 0 [708] 0 [709] 0 [710] 0 [711] 0 [712] 0 [713] 0 [714] 0 [715] 0 [716] 0 [717] 0 [718] 0 [719] 0 [720] 0 [721] 0 [722] 0 [723] 0 [724] 0 [725] 0 [726] 0 [727] 0 [728] 0 [729] 0 [730] 0 [731] 0 [732] 0 [733] 0 [734] 0 [735] 0 [736] 0 [737] 0 [738] 0 [739] 0 [740] 0 [741] 0 [742] 0 [743] 0 [744] 0 [745] 0 [746] 0 [747] 0 [748] 0 [749] 0 [750] 0 [751] 0 [752] 0 [753] 0 [754] 0 [755] 0 [756] 0 [757] 0 [758] 0 [759] 0 [760] 0 [761] 0 [762] 0 [763] 0 [764] 0 [765] 0 [766] 0 [767] 0 [768] 0 [769] 0 [770] 0 [771] 0 [772] 0 [773] 0 [774] 0 [775] 0 [776] 0 [777] 0 [778] 0 [779] 0 [780] 0 [781] 0 [782] 0 [783] 0 [784] 0 [785] 0 [786] 0 [787] 0 [788] 0 [789] 0 [790] 0 [791] 0 [792] 0 [793] 0 [794] 0 [795] 0 [796] 0 [797] 0 [798] 0 [799] 0 [800] 0 [801] 0 [802] 0 [803] 0 [804] 0 [805] 0 [806] 0 [807] 0 [808] 0 [809] 0 [810] 0 [811] 0 [812] 0 [813] 0 [814] 0 [815] 0 [816] 0 [817] 0 [818] 0 [819] 0 [820] 0 [821] 0 [822] 0 [823] 0 [824] 0 [825] 0 [826] 0 [827] 0 [828] 0 [829] 0 [830] 0 [831] 0 [832] 0 [833] 0 [834] 0 [835] 0 [836] 0 [837] 0 [838] 0 [839] 0 [840] 0 [841] 0 [842] 0 [843] 0 [844] 0 [845] 0 [846] 0 [847] 0 [848] 0 [849] 0 [850] 0 [851] 0 [852] 0 [853] 0 [854] 0 [855] 0 [856] 0 [857] 0 [858] 0 [859] 0 [860] 0 [861] 0 [862] 0 [863] 0 [864] 0 [865] 0 [866] 0 [867] 0 [868] 0 [869] 0 [870] 0 [871] 0 [872] 0 [873] 0 [874] 0 [875] 0 [876] 0 [877] 0 [878] 0 [879] 0 [880] 0 [881] 0 [882] 0 [883] 0 [884] 0 [885] 0 [886] 0 [887] 0 [888] 0 [889] 0 [890] 0 [891] 0 [892] 0 [893] 0 [894] 0 [895] 0 [896] 0 [897] 0 [898] 0 [899] 0 [900] 0 [901] 0 [902] 0 [903] 0 [904] 0 [905] 0 [906] 0 [907] 0 [908] 0 [909] 0 [910] 0 [911] 0 [912] 0 [913] 0 [914] 0 [915] 0 [916] 0 [917] 0 [918] 0 [919] 0 [920] 0 [921] 0 [922] 0 [923] 0 [924] 0 [925] 0 [926] 0 [927] 0 [928] 0 [929] 0 [930] 0 [931] 0 [932] 0 [933] 0 [934] 0 [935] 0 [936] 0 [937] 0 [938] 0 [939] 0 [940] 0 [941] 0 [942] 0 [943] 0 [944] 0 [945] 0 [946] 0 [947] 0 [948] 0 [949] 0 [950] 0 [951] 0 [952] 0 [953] 0 [954] 0 [955] 0 [956] 0 [957] 0 [958] 0 [959] 0 [960] 0 [961] 0 [962] 0 [963] 0 [964] 0 [965] 0 [966] 0 [967] 0 [968] 0 [969] 0 [970] 0 [971] 0 [972] 0 [973] 0 [974] 0 [975] 0 [976] 0 [977] 0 [978] 0 [979] 0 [980] 0 [981] 0 [982] 0 [983] 0 [984] 0 [985] 0 [986] 0 [987] 0 [988] 0 [989] 0 [990] 0 [991] 0 [992] 0 [993] 0 [994] 0 [995] 0 [996] 0 [997] 0 [998] 0 [999] 0 [1000] 0 [1001] 0 [1002] 0 [1003] 0 [1004] 0 [1005] 0 [1006] 0 [1007] 0 [1008] 0 [1009] 0 [1010] 0 [1011] 0 [1012] 0 [1013] 0 [1014] 0 [1015] 0 [1016] 0 [1017] 0 [1018] 0 [1019] 0 [1020] 0 [1021] 0 [1022] 0 [1023] 0 [1024] 0 [1025] 0 [1026] 0 [1027] 0 [1028] 0 [1029] 0 [1030] 0 [1031] 0 [1032] 0 [1033] 0 [1034] 0 [1035] 0 [1036] 0 [1037] 0 [1038] 0 [1039] 0 [1040] 0 [1041] 0 [1042] 0 [1043] 0 [1044] 0 [1045] 0 [1046] 0 [1047] 0 [1048] 0 [1049] 0 [1050] 0 [1051] 0 [1052] 0 [1053] 0 [1054] 0 [1055] 0 [1056] 0 [1057] 0 [1058] 0 [1059] 0 [1060] 0 [1061] 0 [1062] 0 [1063] 0 [1064] 0 [1065] 0 [1066] 0 [1067] 0 [1068] 0 [1069] 0 [1070] 0 [1071] 0 [1072] 0 [1073] 0 [1074] 0 [1075] 0 [1076] 0 [1077] 0 [1078] 0 [1079] 0 [1080] 0 [1081] 0 [1082] 0 [1083] 0 [1084] 0 [1085] 0 [1086] 0 [1087] 0 [1088] 0 [1089] 0 [1090] 0 [1091] 0 [1092] 0 [1093] 0 [1094] 0 [1095] 0 [1096] 0 [1097] 0 [1098] 0 [1099] 0 [1100] 0 [1101] 0 [1102] 0 [1103] 0 [1104] 0 [1105] 0 [1106] 0 [1107] 0 [1108] 0 [1109] 0 [1110] 0 [1111] 0 [1112] 0 [1113] 0 [1114] 0 [1115] 0 [1116] 0 [1117] 0 [1118] 0 [1119] 0 [1120] 0 [1121] 0 [1122] 0 [1123] 0 [1124] 0 [1125] 0 [1126] 0 [1127] 0 [1128] 0 [1129] 0 [1130] 0 [1131] 0 [1132] 0 [1133] 0 [1134] 0 [1135] 0 [1136] 0 [1137] 0 [1138] 0 [1139] 0 [1140] 0 [1141] 0 [1142] 0 [1143] 0 [1144] 0 [1145] 0 [1146] 0 [1147] 0 [1148] 0 [1149] 0 [1150] 0 [1151] 0 [1152] 0 [1153] 0 [1154] 0 [1155] 0 [1156] 0 [1157] 0 [1158] 0 [1159] 0 [1160] 0 [1161] 0 [1162] 0 [1163] 0 [1164] 0 [1165] 0 [1166] 0 [1167] 0 [1168] 0 [1169] 0 [1170] 0 [1171] 0 [1172] 0 [1173] 0 [1174] 0 [1175] 0 [1176] 0 [1177] 0 [1178] 0 [1179] 0 [1180] 0 [1181] 0 [1182] 0 [1183] 0 [1184] 0 [1185] 0 [1186] 0 [1187] 0 [1188] 0 [1189] 0 [1190] 0 [1191] 0 [1192] 0 [1193] 0 [1194] 0 [1195] 0 [1196] 0 [1197] 0 [1198] 0 [1199] 0 [1200] 0 [1201] 0 [1202] 0 [1203] 0 [1204] 0 [1205] 0 [1206] 0 [1207] 0 [1208] 0 [1209] 0 [1210] 0 [1211] 0 [1212] 0 [1213] 0 [1214] 0 [1215] 0 [1216] 0 [1217] 0 [1218] 0 [1219] 0 [1220] 0 [1221] 0 [1222] 0 [1223] 0 [1224] 0 [1225] 0 [1226] 0 [1227] 0 [1228] 0 [1229] 0 [1230] 0 [1231] 0 [1232] 0 [1233] 0 [1234] 0 [1235] 0 [1236] 0 [1237] 0 [1238] 0 [1239] 0 [1240] 0 [1241] 0 [1242] 0 [1243] 0 [1244] 0 [1245] 0 [1246] 0 [1247] 0 [1248] 0 [1249] 0 [1250] 0 [1251] 0 [1252] 0 [1253] 0 [1254] 0 [1255] 0 [1256] 0 [1257] 0 [1258] 0 [1259] 0 [1260] 0 [1261] 0 [1262] 0 [1263] 0 [1264] 0 [1265] 0 [1266] 0 [1267] 0 [1268] 0 [1269] 0 [1270] 0 [1271] 0 [1272] 0 [1273] 0 [1274] 0 [1275] 0 [1276] 0 [1277] 0 [1278] 0 [1279] 0 [1280] 0 [1281] 0 [1282] 0 [1283] 0 [1284] 0 [1285] 0 [1286] 0 [1287] 0 [1288] 0 [1289] 0 [1290] 0 [1291] 0 [1292] 0 [1293] 0 [1294] 0 [1295] 0 [1296] 0 [1297] 0 [1298] 0 [1299] 0 [1300] 0 [1301] 0 [1302] 0 [1303] 0 [1304] 0 [1305] 0 [1306] 0 [1307] 0 [1308] 0 [1309] 0 [1310] 0 [1311] 0 [1312] 0 [1313] 0 [1314] 0 [1315] 0 [1316] 0 [1317] 0 [1318] 0 [1319] 0 [1320] 0 [1321] 0 [1322] 0 [1323] 0 [1324] 0 [1325] 0 [1326] 0 [1327] 0 [1328] 0 [1329] 0 [1330] 0 [1331] 0 [1332] 0 [1333] 0 [1334] 0 [1335] 0 [1336] 0 [1337] 0 [1338] 0 [1339] 0 [1340] 0 [1341] 0 [1342] 0 [1343] 0 [1344] 0 [1345] 0 [1346] 0 [1347] 0 [1348] 0 [1349] 0 [1350] 0 [1351] 0 [1352] 0 [1353] 0 [1354] 0 [1355] 0 [1356] 0 [1357] 0 [1358] 0 [1359] 0 [1360] 0 [1361] 0 [1362] 0 [1363] 0 [1364] 0 [1365] 0 [1366] 0 [1367] 0 [1368] 0 [1369] 0 [1370] 0 [1371] 0 [1372] 0 [1373] 0 [1374] 0 [1375] 0 [1376] 0 [1377] 0 [1378] 0 [1379] 0 [1380] 0 [1381] 0 [1382] 0 [1383] 0 [1384] 0 [1385] 0 [1386] 0 [1387] 0 [1388] 0 [1389] 0 [1390] 0 [1391] 0 [1392] 0 [1393] 0 [1394] 0 [1395] 0 [1396] 0 [1397] 0 [1398] 0 [1399] 0 [1400] 0 [1401] 0 [1402] 0 [1403] 0 [1404] 0 [1405] 0 [1406] 0 [1407] 0 [1408] 0 [1409] 0 [1410] 0 [1411] 0 [1412] 0 [1413] 0 [1414] 0 [1415] 0 [1416] 0 [1417] 0 [1418] 0 [1419] 0 [1420] 0 [1421] 0 [1422] 0 [1423] 0 [1424] 0 [1425] 0 [1426] 0 [1427] 0 [1428] 0 [1429] 0 [1430] 0 [1431] 0 [1432] 0 [1433] 0 [1434] 0 [1435] 0 [1436] 0 [1437] 0 [1438] 0 [1439] 0 [1440] 0 [1441] 0 [1442] 0 [1443] 0 [1444] 0 [1445] 0 [1446] 0 [1447] 0 [1448] 0 [1449] 0 [1450] 0 [1451] 0 [1452] 0 [1453] 0 [1454] 0 [1455] 0 [1456] 0 [1457] 0 [1458] 0 [1459] 0 [1460] 0 [1461] 0 [1462] 0 [1463] 0 [1464] 0 [1465] 0 [1466] 0 [1467] 0 [1468] 0 [1469] 0 [1470] 0 [1471] 0 [1472] 0 [1473] 0 [1474] 0 [1475] 0 [1476] 0 [1477] 0 [1478

7. Click a line in the list of SNMP messages. MIB Browser displays information contained in the selected SNMP message in other two panels, in the Hex Dump panel in the middle and in the Decoder panel at the bottom ([Figure 196](#)).
8. In the Hex Dump panel, information in SNMP messages is displayed in the HEX dump format ([Figure 201](#)). In the Decoder panel, the same SNMP message is displayed in decoded, human-readable format that can be easily understood by the user.

Tip: In a drop-down list in the Generic SNMP Trace toolbar, you can select the decoding level of SNMP messages shown in the Decoder panel at the bottom of the Generic SNMP Trace window. You can choose between the *Standard decoding level*, *Compact decoding level* and *No decoding*.

9. To check the contents of another SNMP message, select another line in the list of SNMP messages.
10. To quickly find one or more SNMP messages that match the search criteria, use the [Live search tool](#)  Search in the Generic SNMP Trace window.
11. You can switch to one of the traced windows and perform another SNMP operation. Then you can return to the Generic SNMP Trace window and view the messages.



Show Encrypted SNMPv3 Messages in Decrypted Form

Note: When the SNMPv3 privacy is used, the SNMP messages exchanged on the network are encrypted. MIB Browser will decrypt the encrypted PDUs if you click the **Decrypt** toolbar button. In this way, you can view the contents of SNMPv3 messages in unencrypted form.

In the Generic SNMP Trace Preferences dialog box ([Figure 197](#)), which opens by clicking the **Preferences** toolbar button in the Generic SNMP Trace window, you can specify which parameters of the recorded SNMP messages will be displayed in the topmost panel of the Generic SNMP Trace window.

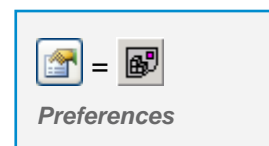
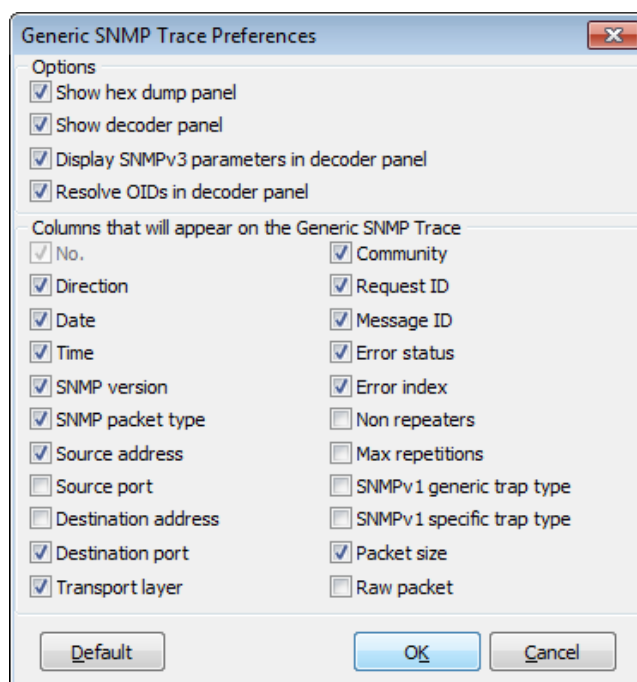




Figure 197: Generic SNMP Trace Preferences dialog box

23.1.3 Searching and Filtering SNMP Messages

The Live search tool  in the Generic SNMP Trace window lets you perform incremental text search to quickly find and display only those SNMP messages that match the search criteria, i.e., contain the entered text in one or more of the selected search categories (Generic SNMP Trace window columns).

Note that once you enter the query into the Live search box, the search is automatically started and it remains active until you cancel it. Active search behaves as a **continuous display filter**, meaning that it applies also to newly recorded SNMP messages, i.e., only those newly recorded messages that match the search criteria will be displayed in the Generic SNMP Trace window (until the search is canceled).

For example, to find all SNMP Set messages:

1. Click the search symbol () in the **Live search** tool.
2. In the **Search Options** drop-down menu that appears, deselect all options and select only the **Type** entry to enable searching in the message type column and click the **OK** button to close the Search Options drop-down menu.

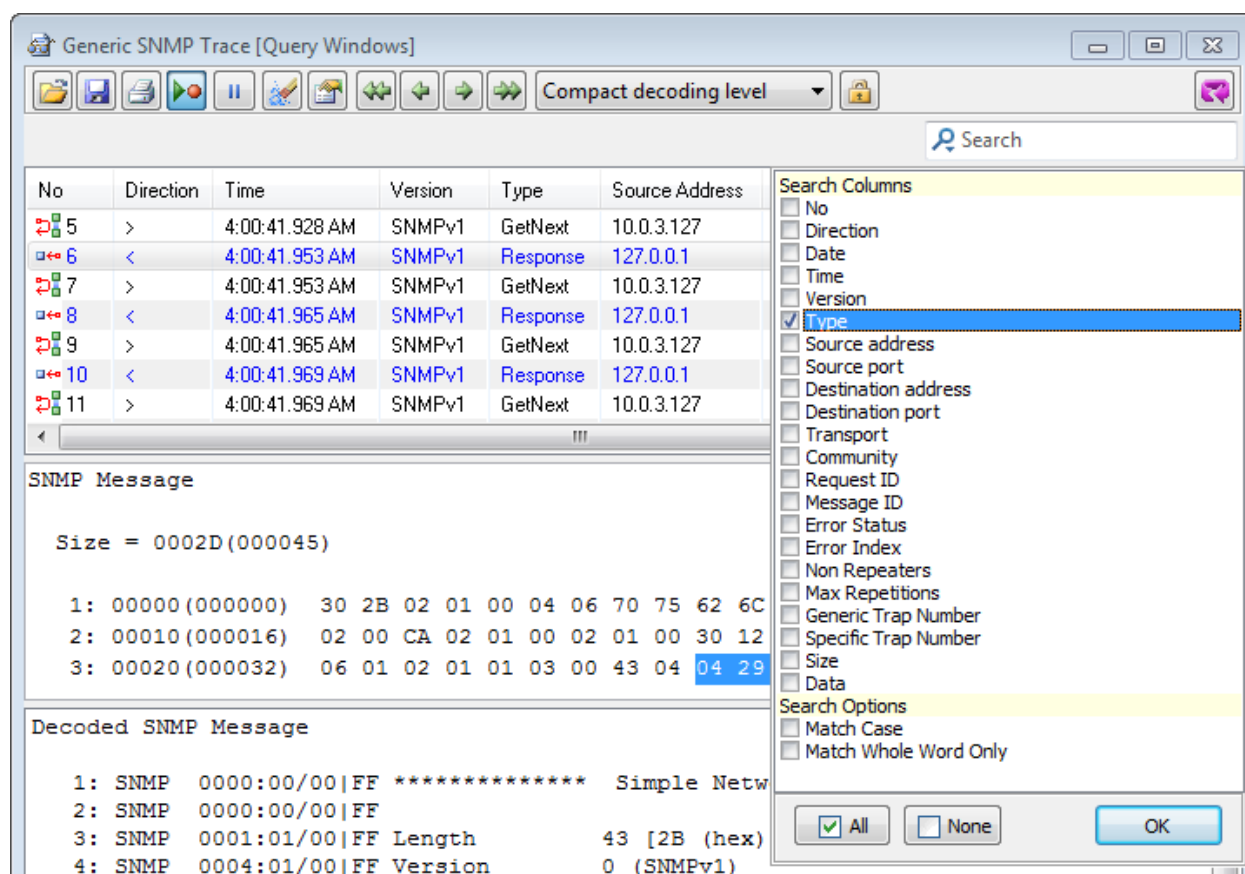


Figure 198: Selecting the Live search options in the Generic SNMP Trace window

3. Click inside the Live search box and type in the **set** query. The Live search tool automatically performs the search as you type the characters into the search box and displays only SNMP Set messages in the Generic SNMP Trace window – upper panel. Select the message in the upper panel to view its contents in the middle and lower panels.

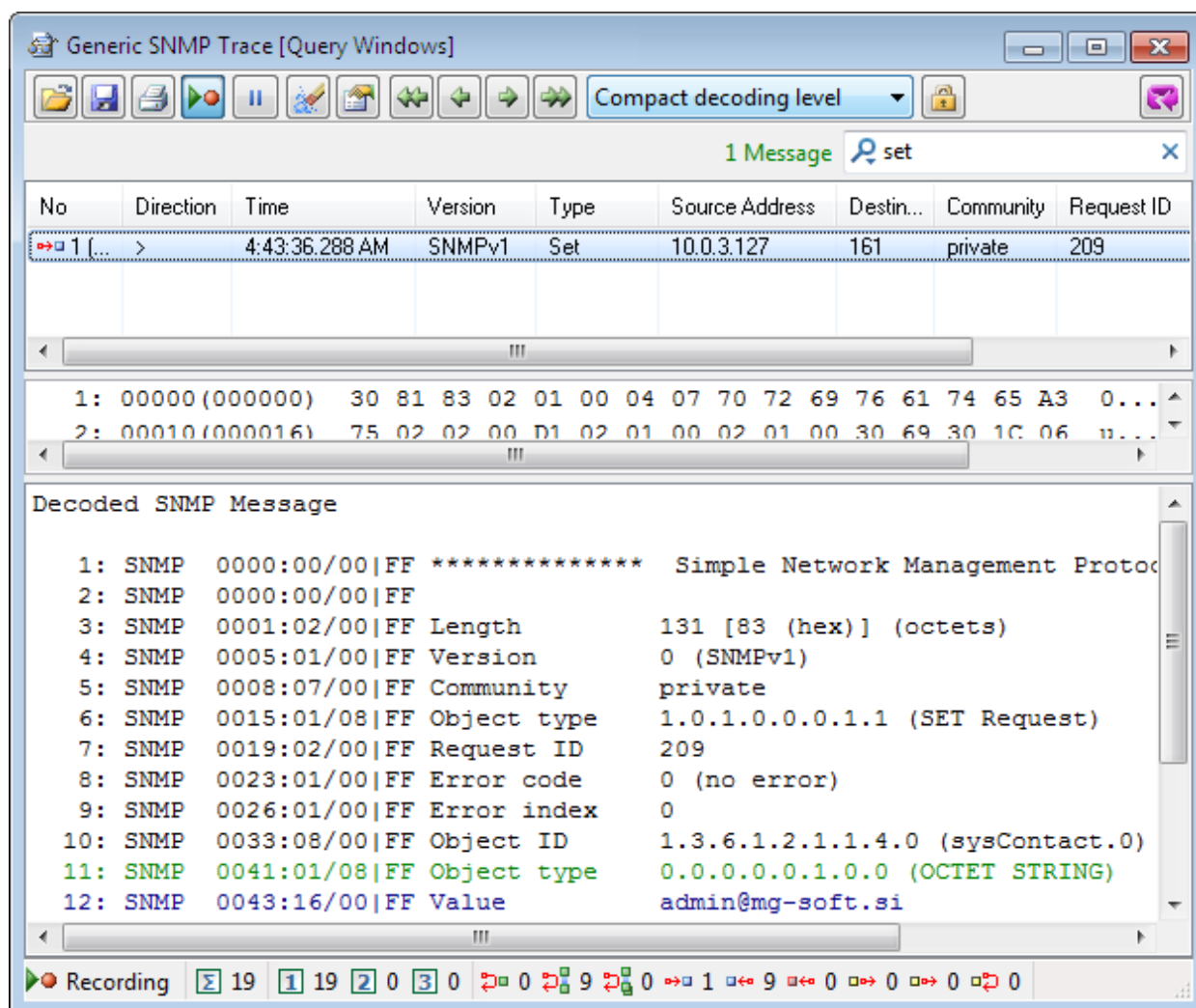


Figure 199: Viewing Live search results in the Generic SNMP Trace window

- The search results (total number of matches) is displayed in front of the Live search tool (Figure 90). Note that the entered query (*set*) functions as continuous display filter, meaning that newly recorded SNMP messages will also be filtered and only those that match the search criteria (i.e., SNMP Set messages) will be displayed in the Generic SNMP Trace window.
- To cancel the search, click the **Cancel Current Search** symbol (X) in the Live search box or delete the text from it. After you cancel the search, the Generic SNMP Trace window displays all recorded SNMP messages.

23.2 Troubleshooting in Generic SNMP Trace Window

The Generic SNMP Trace window allows you to see the contents of SNMP messages and can therefore be used for troubleshooting. In the Hex Dump panel ([Figure 201](#)), the contents of an SNMP message are displayed in hexadecimal format and in the Decoder panel, in the human-readable format ([Figure 202](#)). When you are using the SNMPv3 protocol, the Decoder panel displays also the SNMPv3 message parameters ([Figure 200](#)).

SNMPv3 Message Parameters

```
Security model:          USM
Security level:         Authentication and privacy
Context name:           public [70.75.62.6C.69.63 (hex)]
Context engine ID:      12.34.EF (hex)
Security name:          SHA_DES_User [53.48.41.5F.44.45.53.5F.55.73.65.72 (hex)]
Security engine ID:     80.00.05.23.01.D4.1E.49.46 (hex)
Local engine boots:     79 [4F (hex)]
Local engine time:      2239334 [222B66 (hex)]
Remote engine boots:    79 [4F (hex)]
Remote engine time:     2239334 [222B66 (hex)]
Authentication protocol: HMAC-SHA
Authentication key:     56.69.D8.49.4C.10.49.48.77.D4.4F.F7.51.24.2E.7E.E3.AA.23.BD
(hex)
Localized authentication key:
C9.ED.87.CA.A4.6F.16.89.23.2B.51.3F.A8.F0.55.CB.AF.B2.EF.6F (hex)
Privacy protocol:       CBC-DES
Privacy key:            D0.46.D0.9C.4A.44.75.D3.43.B6.5B.7A.DB.D0.6A.C0.71.F2.D5.FC
(hex)
Localized privacy key:  0E.DE.E9.13.74.D6.8D.A9.B3.CE.ED.4E.AD.6B.2D.86.87.58.98.83
(hex)
```

Figure 200: SNMPv3 message parameters displayed in the Decoder panel

SNMP Packet (Decrypted)

Size = 00085(000133)

```
00000(000000): 30 81 82 02 01 03 30 0E 02 01 05 02 03 00 FF F0 0.....0.....
00010(000016): 04 01 03 02 01 03 04 3B 30 39 04 09 80 00 05 23 .....;09.....#
00020(000032): 01 D4 1E 49 46 02 01 4F 02 03 22 2B 66 04 0C 53 ...IF..O.."+f..S
00030(000048): 48 41 5F 44 45 53 5F 55 73 65 72 04 0C EF ED DB HA_DES_User.....
00040(000064): D7 BC D6 CF 0C 47 B1 F8 EB 04 08 00 00 00 C8 00 .....G.....
00050(000080): 00 AC 81 04 30 30 2C 04 03 12 34 EF 04 06 70 75 ....00,...4...pu
00060(000096): 62 6C 69 63 A2 1D 02 01 04 02 01 00 02 01 00 30 blic.....0
00070(000112): 12 30 10 06 08 2B 06 01 02 01 01 03 00 43 04 0D .0...+.....C..
00080(000128): 58 F4 45 00 00 X.E..
```

Figure 201: The contents of an SNMP message displayed in the Hex Dump panel

The contents of an SNMP message that is in the Hex Dump panel displayed in hexadecimal format is decoded in the Decoder panel, e.g.:

In the Hex Dump panel ([Figure 201](#)):

```
00000(000000): 30 81 82 02 01 03 30 0E 02 01 05 02 03 00 FF F0 0.0
```

In the Decoder panel (Figure 202):

SNMP 0000:01/21|20 Simple type _._.1._._._._. (no)

Decoded SNMP Packet (Decrypted)

```

SNMP 0000:00/00|FF ***** Simple Network Management Protocol *****
SNMP 0000:00/00|FF
SNMP 0000:01/08|FF Tag 0.0.1.1.0.0.0.0 (30 hex)
SNMP 0000:01/02|C0 Class 0.0._._._._._. (universal)
SNMP 0000:01/21|20 Simple type _._.1._._._._. (no)
SNMP 0000:01/08|DF Object type 0.0._.1.0.0.0.0 (sequence [of])
SNMP 0001:02/00|FF Length 130 (octets)
SNMP 0003:00/00|00
SNMP 0003:01/08|FF Tag 0.0.0.0.0.0.1.0 (02 hex)
SNMP 0003:01/02|C0 Class 0.0._._._._._. (universal)
SNMP 0003:01/21|20 Simple type _._.0._._._._. (yes)
SNMP 0003:01/08|DF Object type 0.0._.0.0.0.1.0 (integer)
SNMP 0005:01/00|FF Version 3 (SNMPv3)
SNMP 0006:00/00|00
SNMP 0006:01/08|FF Tag 0.0.1.1.0.0.0.0 (30 hex)
SNMP 0006:01/02|C0 Class 0.0._._._._._. (universal)
SNMP 0006:01/21|20 Simple type _._.1._._._._. (no)
SNMP 0006:01/08|DF Object type 0.0._.1.0.0.0.0 (sequence [of])
SNMP 0008:00/00|00
SNMP 0008:01/08|FF Tag 0.0.0.0.0.0.1.0 (02 hex)
SNMP 0008:01/02|C0 Class 0.0._._._._._. (universal)
SNMP 0008:01/21|20 Simple type _._.0._._._._. (yes)
SNMP 0008:01/08|DF Object type 0.0._.0.0.0.1.0 (integer)
SNMP 0010:01/00|FF Message ID 5
SNMP 0011:00/00|00
SNMP 0011:01/08|FF Tag 0.0.0.0.0.0.1.0 (02 hex)
SNMP 0011:01/02|C0 Class 0.0._._._._._. (universal)
SNMP 0011:01/21|20 Simple type _._.0._._._._. (yes)
SNMP 0011:01/08|DF Object type 0.0._.0.0.0.1.0 (integer)
SNMP 0013:03/00|FF Max size 65520 (octets)

```

Figure 202: The contents of an SNMP message decoded and displayed in the Decoder panel

The descriptor (e.g., 0000:01/02|C0) placed before the description and the actual value (e.g., Simple type _._.1._._._._. (no)) defines the location, length and mask of bytes in an SNMP message that are used to produce this particular decoded line.

The 0000:01/21|20 descriptor has the following meaning:

<offset>:<byteLength>/<bits>|<bitMask>

- ❑ '0000' designates the offset of the decoded information in the SNMP message.
- ❑ '01' designates the length of the decoded information in the SNMP message.
- ❑ '21' designates the bit offset and the number of bits in the decoded information in the SNMP message. In this particular example, it means that only the third bit within the byte is used to produce the decoded line (bit offset is 2, bit length is 1).
- ❑ '20' is a bit mask.

Tip: For better understanding of how an SNMP message is encoded, double-click a line in the Decoder panel. Byte(s) encoding the double-clicked line will be highlighted in the Hex Dump panel. Note that one byte can encode more than one line displayed in the Decoder panel.

Example:

How to use the Generic SNMP Trace window to debug a problem when MIB Browser cannot contact an SNMP agent when using the SNMPv3 protocol?

If MIB Browser cannot contact an SNMP agent, it receives an error message in response (e.g., `usmStatUnknownUserNames.0`) and displays it in the Query results panel.

When you are using the SNMPv3 protocol, the problem might be, for example, wrongly specified SNMPv3 security parameters. Therefore, you can use the Generic SNMP Trace window to check the contents of SNMP messages exchanged between MIB Browser and the SNMP agent, and debug the problem.

In order to do this, click the **Generic SNMP Trace** toolbar button in the main window. When the Generic SNMP Trace window opens, click the **Clear All** toolbar button to delete all recorded SNMP messages. Click the **Record** toolbar button. Switch to the main window and try to contact the SNMP agent again by using the **Contact** pop-up command. The Generic SNMP Trace window records all SNMP messages exchanged during this operation.

If MIB Browser cannot contact the SNMP agent and the agent returns the `usmStatUnknownUserNames.0` message, the security name of the user is not correct.

To check the security name, return to the Generic SNMP Trace window by using the **Windows / Trace Windows / Main Window** command. In the list of SNMP messages displayed in the upper panel, click the last returned SNMPv3 Report message. MIB Browser decodes its contents and displays it in the last (Decoder) panel ([Figure 203](#)).

SNMPv3 Message Parameters

```

Security model:      USM
Security level:      None
Context name:        (zero-length)
Context engine ID:   (zero-length)
Security name:        SHA_DES_User[53.48.41.5F.44.45.53.5F.55.73.65.72..20(hex)]
Security engine ID:   80.00.05.23.01.D4.1E.49.46 (hex)
Local engine boots:   0 [0 (hex)]
Local engine time:    0 [0 (hex)]
Remote engine boots:  0 [0 (hex)]
Remote engine Time:   0 [0 (hex)]

```

Figure 203: SNMPv3 message parameters displayed in the Decoder panel

In the Decoder panel, check the value of the `Security name` SNMPv3 parameter:

```
Security name: SHA_DES_User[53.48.41.5F.44.45.53.5F.55.73.65.72..20 (hex)]
```

In the hexadecimal format of the security name, you can see that the last value is `.20`, which is a blank character. A blank is normally not visible, but because of it, the security name of the user is not correct.

To correct the mistake, open the SNMP Protocol Preferences dialog box, click the **Edit User** toolbar button and erase the blank space in the security user name. Click the **OK** button and close the SNMP Protocol Preferences dialog box. If there are no other problems, MIB Browser will now successfully contact the SNMP agent.

24 PERFORM MULTIPLE OPERATIONS

The Multiple Operations window is used for performing arbitrary series of SNMP operations on a selected SNMP agent. This can be useful, for example, when testing or configuring SNMP agents, etc.

This section describes how to use the Multiple Operations window.

24.1 About Multiple Operations Window

To open the Multiple Operations window, select the **SNMP / Multiple Operations** command or click the **Multiple Operations** toolbar button.

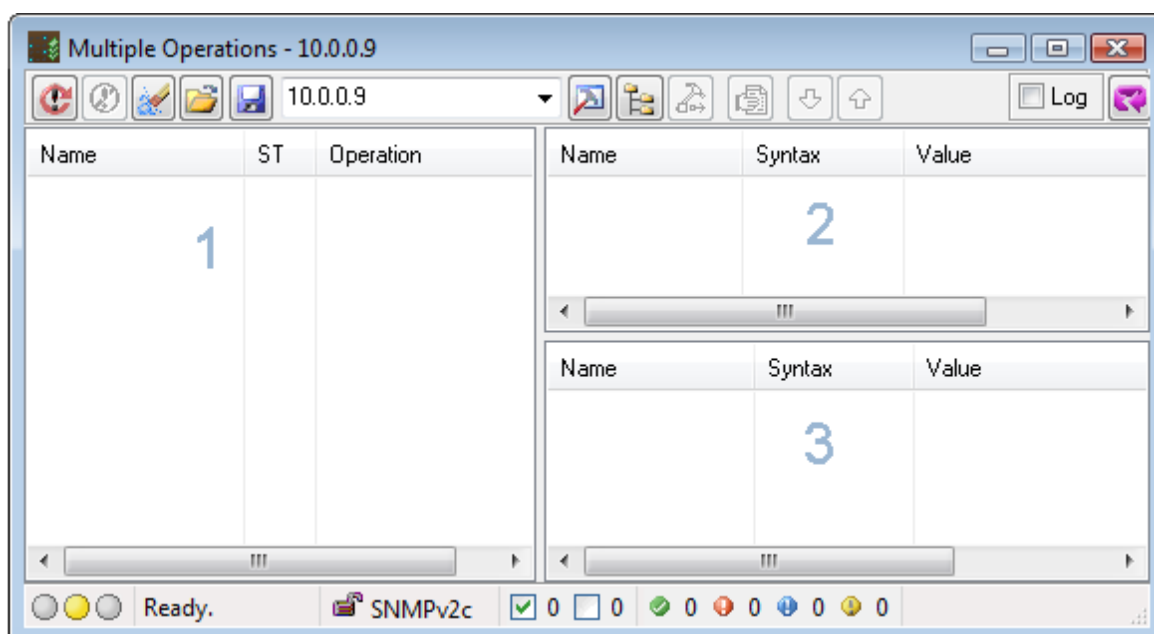
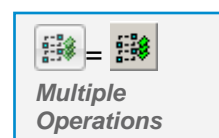


Figure 204: Empty Multiple Operations window

The Multiple Operations window contains 3 panels (Figure 204):

1. Operations (left panel)
2. Send (upper-right panel)
3. Response (lower-right panel)

The Operations panel displays a configurable list of SNMP operations to be performed against the selected SNMP agent. This list can be considered as a script containing a sequence of SNMP operations (Get, GetNext, Set, Trap, etc.). When the operations execution is started, MIB Browser performs the listed SNMP operations top-down one after another. The list may also contain timers, i.e., elements that cause MIB Browser to wait a configured amount of time (e.g., 100ms, 1s, 5s, etc.) before performing the subsequently listed SNMP operations.

The Send (upper-right) panel displays a variable bindings list that will be/was included into the outgoing SNMP message that corresponds to the operation selected in the Operations panel.

The Response (lower-right) panel displays the results of the operation selected in the Operations panel, i.e., a variable bindings list included in the received SNMP Response message that corresponds to the operation selected in the Operations panel.

24.2 Configuring SNMP Operations in Multiple Operations Window

24.2.1 Adding Operations to Multiple Operations Window

SNMP operations and associated variable bindings can be added to the Multiple Operations window in several ways, as described in this section.

In context of the Multiple Operations window, a valid SNMP operation has a certain name (label), is of a certain type (Get, GetNext, GetBulk, Set, Trap (v1), Trap (v2), Inform), and has a variable bindings list with one or more variable bindings (except for the SNMPv1 Trap operation, which may have an empty variable bindings list).

To Manually Add Operations

1. Adding Operations

The contents of the Operations panel, i.e., the number and type of SNMP operations (Get, GetNext, Set, etc.), their order and names, as well as timers and their properties, can be configured.

1. Right-click the Operations panel on the left hand side and select the **New Operation** pop-up command. This adds a new operation to the Operations panel.

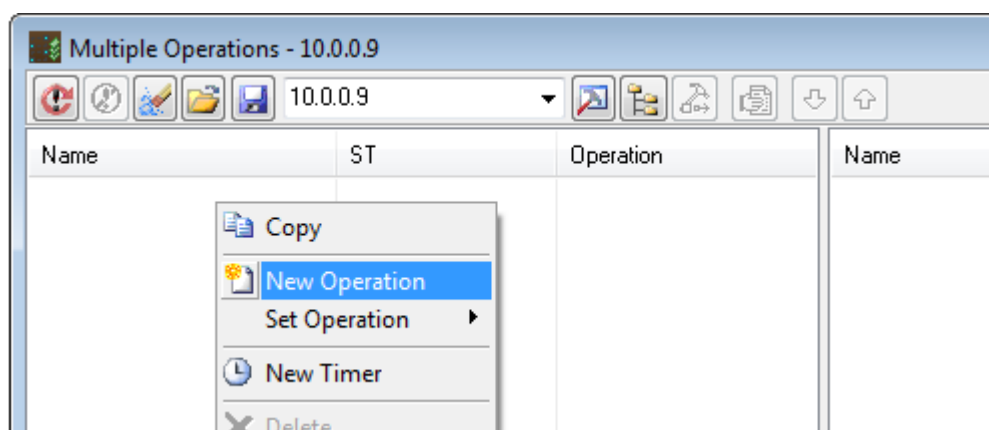


Figure 205: Adding a new operation to the Multiple Operations window

2. Click the **Operation** field and select the operation type (e.g., Get, GetNext, Set, Trap, etc.) from the drop-down list that is displayed (Figure 206).

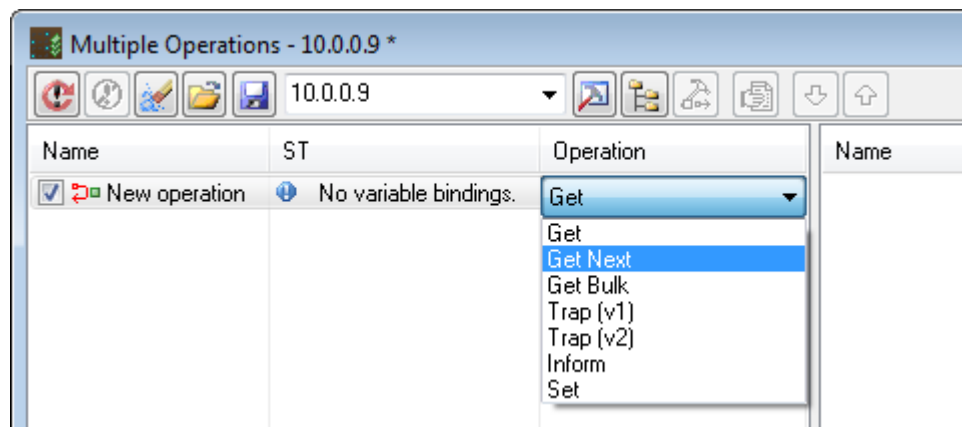


Figure 206: Selecting the operation type

3. To specify a meaningful name for the operation (e.g., 'Get sysName'), right-click the operation, select the **Rename** pop-up command and edit the name of the operation.
4. To add additional operations to the operations list, repeat the steps 1-3.
5. To change the order of operations, select individual operations and use the **Move Up** or **Move Down** pop-up commands.

2. Adding Variable Bindings to Operations

The variable bindings list for a SNMP operation can be populated in several ways. One can either:

- ❑ Manually add variable bindings by using the **New** pop-up menu command.
- ❑ Manually add variable bindings by dragging&dropping individual objects from the MIB tree (main window) to the Send (upper-right) panel of the Multiple Operations window.
- ❑ **Automatically insert** operations and variable bindings by selecting a node in the MIB tree (main window) and choosing the Multiple Operations command.
- ❑ **Load operations** and variable bindings from a Multiple Operations XML (. mofx) file or Agent Snapshot XML (.asfx) file.
- ❑ Use a combination of the methods above.

This section describes the first method listed above.

1. In the Operations panel, select the operation you want to add variable bindings to. The Send (upper-right) panel displays an empty variable bindings list of the selected operation (Figure 207).

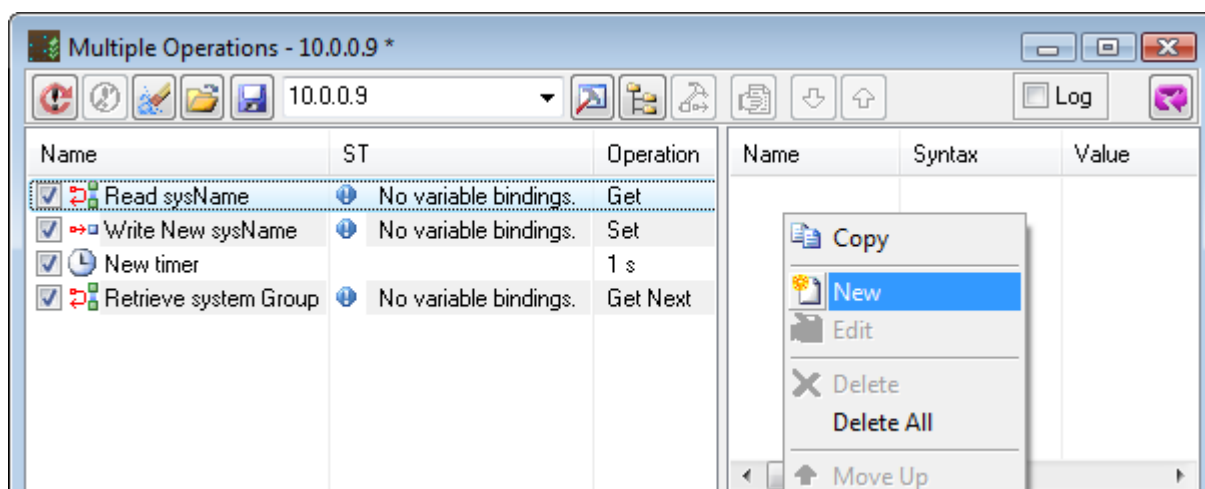


Figure 207: Adding a new binding to selected operation in the Multiple Operations window

2. Right-click within the upper-right panel and select the **New** pop-up command. The Select dialog box appears (Figure 208).

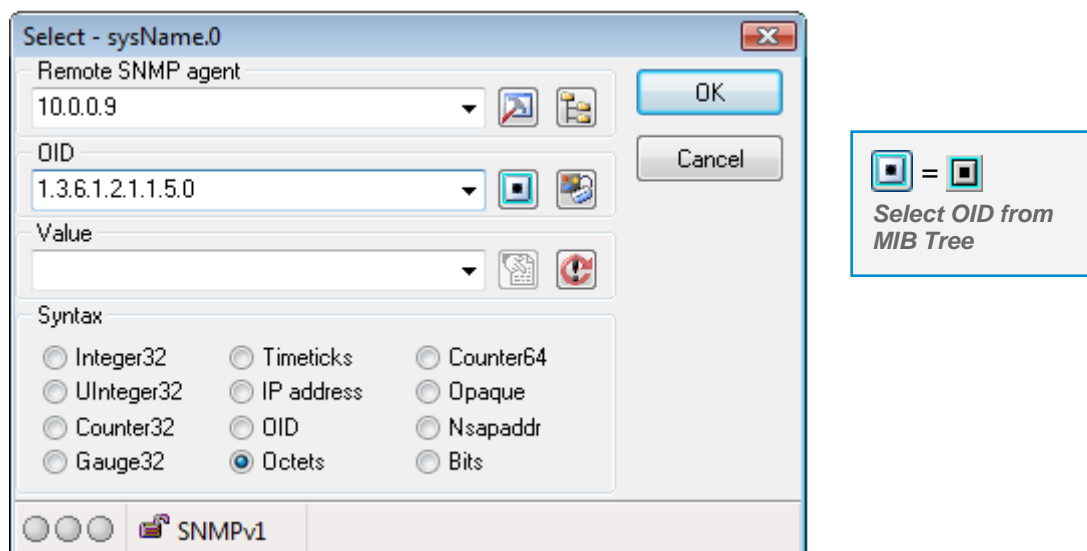


Figure 208: Select dialog box

3. In the **OID** input line, specify the OID of the variable binding.

Tip: You can also specify the OID value by selecting a corresponding node from the MIB tree. To do that, click the **Select OID from MIB Tree** button next to the stop OID input line. The Select Object Identifier window appears (Figure 112). Expand the MIB tree and select the OID by double-clicking the desired node.

4. Depending on the operation type, specify the value of variable binding in the **Value** input line (for querying operations (Get, GetNext, GetBulk) you can leave this input line empty).
5. Choose the appropriate syntax of variable binding in the **Syntax** frame. If you select OID from the MIB tree, the correct syntax is selected automatically.

- Click the **OK** button. The dialog box closes and the specified variable binding is inserted into the variable bindings list (Figure 209).

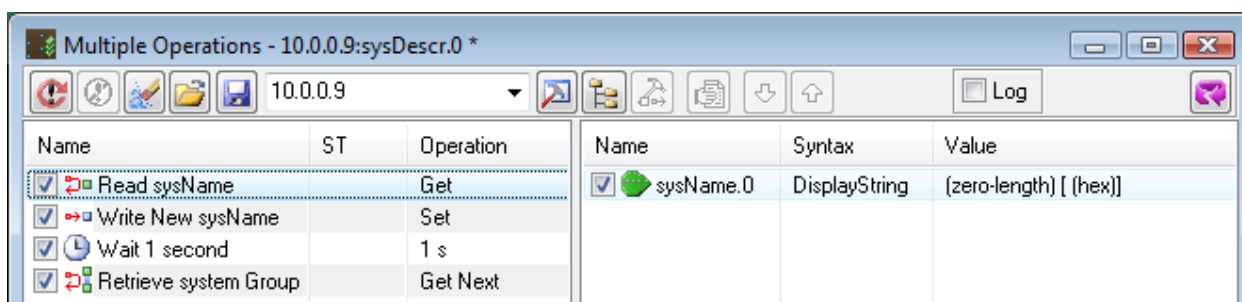


Figure 209: A new variable binding in the Multiple Operations window (Send panel)

- To add additional variable bindings to the same variable bindings list, repeat steps 1-6 or use [alternative methods \(drag&drop, load\)](#).
- Add variable bindings to the remaining operations in the Multiple Operations window, as described in steps 1-7.

To Automatically Insert Operations

- Right-click the MIB Tree node in the MIB Browser main window, which has one or more subordinated MIB object instances that you want to retrieve or modify and select the **Multiple Operations** pop-up command (Figure 210). Alternatively, select the desired MIB tree node and choose the **SNMP / Multiple Operations** main menu command or click the **Multiple Operations** toolbar button.

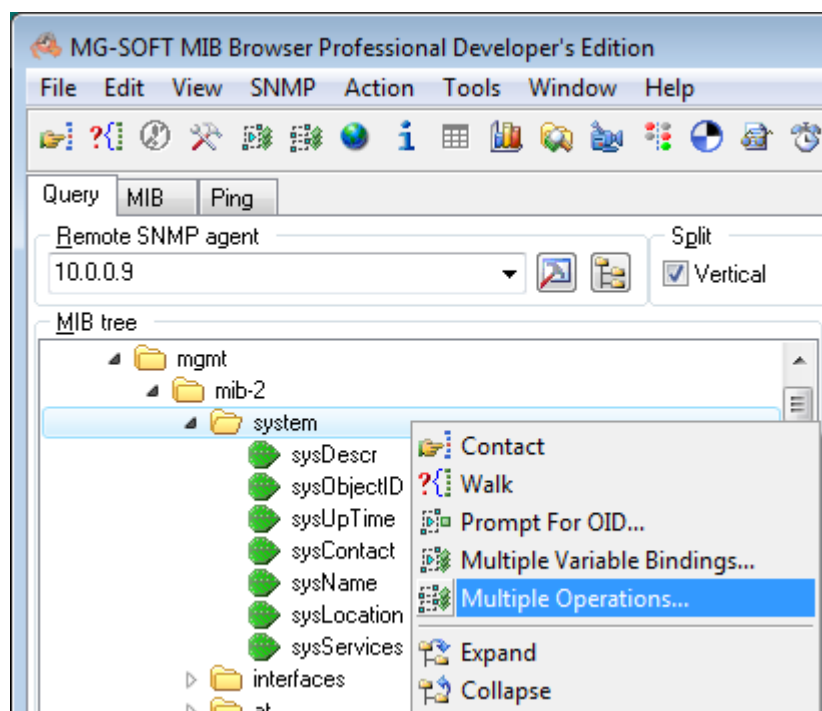


Figure 210: Selecting the *Multiple Operations* command from the MIB tree pop-up menu

2. This opens the Multiple Operations window and automatically populates it with operations that let you retrieve object instances from the selected MIB subtree or MIB object. For example:

- ❑ If the 'sysUpTime' **scalar node** was selected in the MIB tree, a SNMP Get operation with one variable binding for retrieving the only instance of the 'sysUpTime' scalar object (i.e., 'sysUpTime.0') is automatically inserted into the Multiple Operations window.
- ❑ If the 'system' **subtree node** was selected in the MIB tree (Figure 210), a SNMP Get operation with multiple variable bindings for retrieving all scalar object instances in the 'system' group is automatically inserted into the Multiple Operations window (Figure 215).

Name	ST	Operation	Name	Syntax	Value
<input checked="" type="checkbox"/> 1: system		Get	<input checked="" type="checkbox"/> sysDescr.0	DisplayString	(zero-length) [(hex)]
			<input checked="" type="checkbox"/> sysObjectID.0	OBJECT ID...	null
			<input checked="" type="checkbox"/> sysUpTime.0	TimeTicks	0 days 00h:00m:00s.
			<input checked="" type="checkbox"/> sysContact.0	DisplayString	(zero-length) [(hex)]
			<input checked="" type="checkbox"/> sysName.0	DisplayString	(zero-length) [(hex)]
			<input checked="" type="checkbox"/> sysLocation.0	DisplayString	(zero-length) [(hex)]
			<input checked="" type="checkbox"/> sysServices.0	INTEGER	0

Figure 211: Operation for retrieving the scalar object instances of the MIB-2 'system' group

- ❑ If the 'ifTable' **table node** was selected in the MIB tree, a SNMP GetNext operation with multiple variable bindings for retrieving the first instance of all columnar objects in the 'ifTable' is automatically inserted into the Multiple Operations window.
- ❑ If the 'interfaces' **subtree node** was selected in the MIB tree, two SNMP operations are automatically inserted into the Multiple Operations window: one SNMP Get operation for retrieving the only scalar object instance in the 'interfaces' group ('ifNumber.0') and one SNMP GetNext operation with multiple variable bindings for retrieving the first instance of all columnar objects in the 'ifTable'.
- ❑ If the 'mib-2' **subtree node** (which has many subordinated subtrees containing scalar and table objects) was selected in the MIB tree, a number of SNMP Get and GetNext operations is automatically inserted into the Multiple Operations window: SNMP Get operations with one or more bindings are inserted for retrieving all scalar object instances within the 'mib-2' subtree, while SNMP GetNext operations with multiple variable bindings for retrieving the first instance of columnar objects in tables within the 'mib-2' subtree, etc.

Name	ST	Operation	Name	Syntax	Value
<input checked="" type="checkbox"/> 1: system		Get	<input checked="" type="checkbox"/> ipAdEntAddr	IpAddress	0.0.0.0
<input checked="" type="checkbox"/> 2: interfaces		Get	<input checked="" type="checkbox"/> ipAdEntIfIndex	INTEGER	0
<input checked="" type="checkbox"/> 3: ifEntry		Get Next	<input checked="" type="checkbox"/> ipAdEntNetMask	IpAddress	0.0.0.0
<input checked="" type="checkbox"/> 4: atEntry		Get Next	<input checked="" type="checkbox"/> ipAdEntBcastAddr	INTEGER	0
<input checked="" type="checkbox"/> 5: ip		Get	<input checked="" type="checkbox"/> ipAdEntReasmMaxSize	INTEGER	0
<input checked="" type="checkbox"/> 6: ipAddrEntry		Get Next			
<input checked="" type="checkbox"/> 7: ipRouteEntry		Get Next			
<input checked="" type="checkbox"/> 8: ipNetToMediaE...		Get Next			
<input checked="" type="checkbox"/> 9: icmp		Get			
<input checked="" type="checkbox"/> 10: tcp		Get			
<input checked="" type="checkbox"/> 11: tcpConnEntry		Get Next			
<input checked="" type="checkbox"/> 12: udp		Get			
<input checked="" type="checkbox"/> 13: udpEntry		Get Next			
<input checked="" type="checkbox"/> 14: egp		Get			
<input checked="" type="checkbox"/> 15: egpNeighEntry		Get Next			
<input checked="" type="checkbox"/> 16: dot3StatsEntry		Get Next			
<input checked="" type="checkbox"/> 17: dot3CallEntry		Get Next			

Figure 212: Operations for retrieving object instances form the MIB-2 subtree

- Once you have the automatically inserted operations and variable bindings into the Multiple Operations window, you can further manipulate them in various ways:
 - To add additional operations to the Operations panel, proceed as described in the [To Manually Add Operations](#) section.
 - To delete one or more operations from the Operations panel, select the operations you want to delete (use the SHIFT key to select adjacent operations and CTRL key to select non-adjacent operations) and choose the **Delete** pop-up menu command.
 - To edit operations (e.g., rename, enable/disable operations, change the order of operations, change operation type, edit variable bindings list, etc.) select operation(s) and choose the appropriate command from the pop-up menu (please refer to “Multiple Operations Window” section of the MIB Browser Help documentation for more information on this).
- Once you have finished configuring operations and variable bindings in the Multiple Operations window, you can save them to a file by clicking the **Save Operations to File** toolbar button and specifying the location and name of the resulting .mofx file in the standard Save As dialog box that appears. A saved multiple operations XML file (.mofx) can later be loaded into the Multiple Operations window via the **Load Operations from File** feature.

24.3 Running SNMP Operations in Multiple Operations window

After you have configured the operations in the Multiple Operations window (as described in the preceding section), you can start executing them as follows:

- In the **Agent Address** drop-down list specify the address of the SNMP agent the operations should be performed against.

- Click the **SNMP Protocol Preferences** toolbar button to open the SNMP Protocol Preferences dialog box and **specify the SNMP protocol settings** for accessing the selected agent.



Tip: Instead of step 1 and 2, click the **SNMP Agent Profiles** button and **select the proper profile** from the SNMP Agent Profiles window if the profile for the target agent already exists.



- Click the **Refresh** toolbar button to start executing operations. MIB Browser performs all operations listed in the Operations panel top-down one after another and displays the status of executed operations ("Status" column) and the values retrieved (lower-right panel).

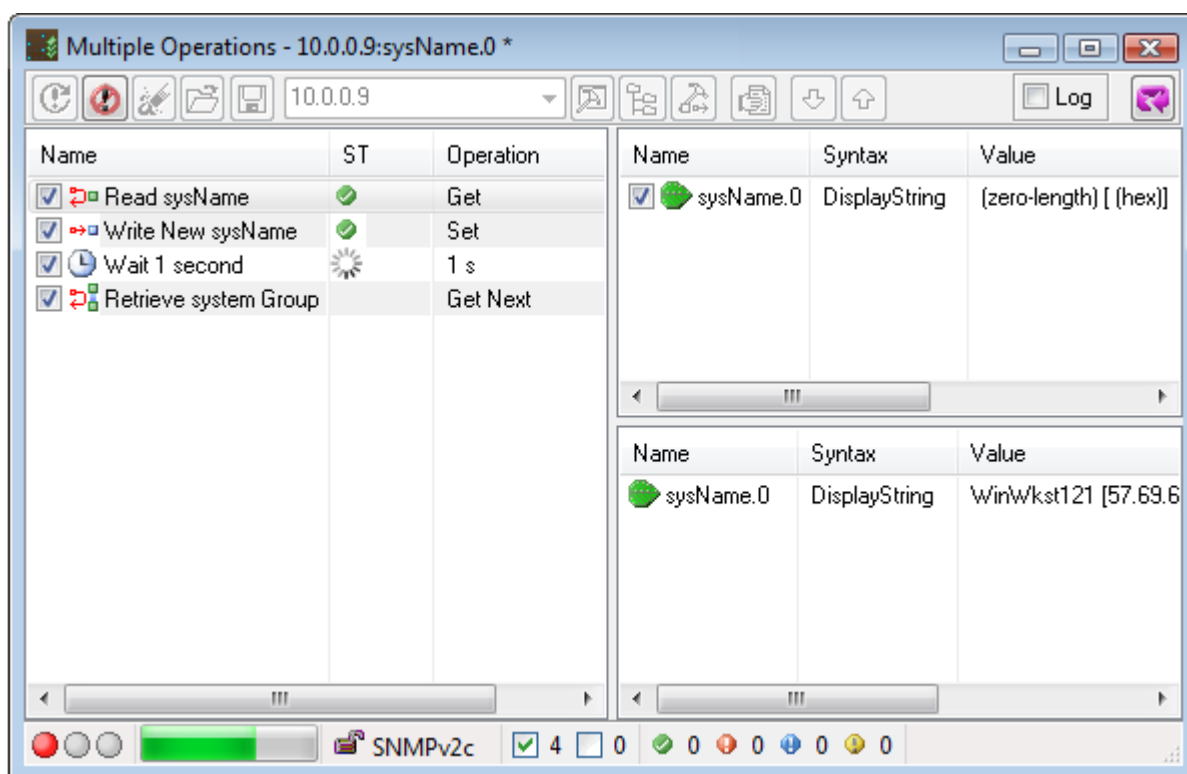


Figure 213: Performing operations in the Multiple Operations window

- When all operations have been carried out, you can review the status and results of individual operations. The "Status" column in Operations panel indicates the status of performed operations using of the following symbols:

Symbol: Meaning:



Operation completed successfully



Operation ended in error (includes a short error description)



No variable bindings are associated with the operation (operation was skipped)



Operation is incompatible with the SNMP protocol version (operation was skipped)

The Multiple Operations window status bar also displays the number of enabled operations, the number of disabled operations, the number of operations completed successfully, and the number of failed operations.

5. Click the **Next Error** toolbar button to quickly locate and select the first operation that ended in error (if any). Use the **Next Error** and **Previous Error** buttons to quickly step forward and backward through the remaining errors (if any).
6. If an operation ended in error, you can modify the operation (e.g., change the operation type) or its variable bindings list (e.g., change the OID or instance of the variable bindings, syntax or value), or the SNMP protocol Preferences and then re-run the operations by clicking the **Refresh** toolbar button again.

25 SIMULATE SNMP AGENT


MIB Browser lets you create a snapshot of an SNMP agent on the network and then simulate this agent on the computer where MIB Browser runs.


Simulating means that MIB Browser runs a separate process, which listens for SNMP queries on selected network interface(s) and port(s) and responds to SNMP queries, returning exactly the same OIDs and values as the "real" SNMP agent would (at the time of taking its snapshot). MIB Browser can simulate an agent that 'speaks' SNMP over UDP and SNMP over TCP over IPv4 and IPv6 protocol. SNMPv3 over TLS over TCP and SNMPv3 over DTLS over UDP (both over IPv4 and IPv6 transport) are also supported.

This section describes how to use the SNMP Agent Simulator window to load an agent snapshot XML file (.asfx), configure agent simulation preferences and start simulating an SNMP agent.

Note: This feature is available only in the *Simulator Edition* of *MIB Browser Pro*.

Note: Before being able to simulate an SNMP agent, one needs to **take a snapshot** of it and **save the snapshot** to MIB Browser agent snapshot XML file (*.asfx), as described in the preceding sections.

1. In the main window, use the **Tools / SNMP Agent Simulator** command or click the **SNMP Agent Simulator** toolbar button () to open the SNMP Agent Simulator window ([Figure 214](#)).
2. In the SNMP Agent Simulator window, click the **Load** button next to the **Agent snapshot** input line to display the standard Open dialog box. In the Open dialog box, select the agent snapshot XML file (*.asfx) of the SNMP agent you want to simulate and click the Open button. The full path of the selected agent snapshot appears in the **Agent snapshot file** input line.

Tip: To view or edit the selected agent snapshot, click the **Edit Snapshot** button ().

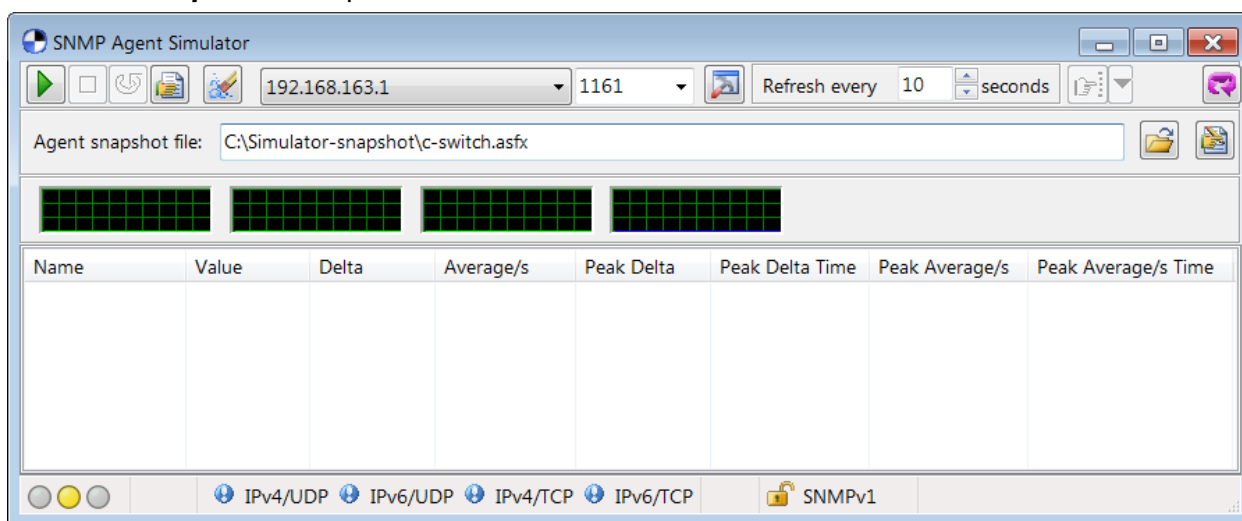


Figure 214: SNMP Agent Simulator window (simulation is not running)

- From the **Binding Interface** drop-down list select the network interface, i.e., its IPv4, or IPv6 address on which the simulated agent will listen and respond to SNMP queries. Select the option "Any" for simulator to listen and respond on all available interfaces, IPv4 and IPv6 addresses, and transports (UDP and TCP) (Figure 215).

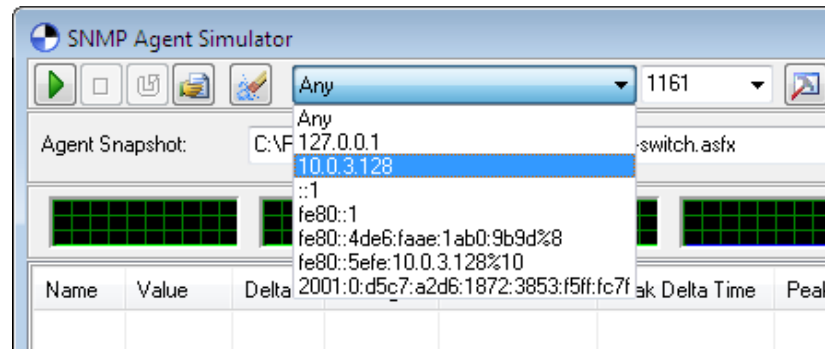

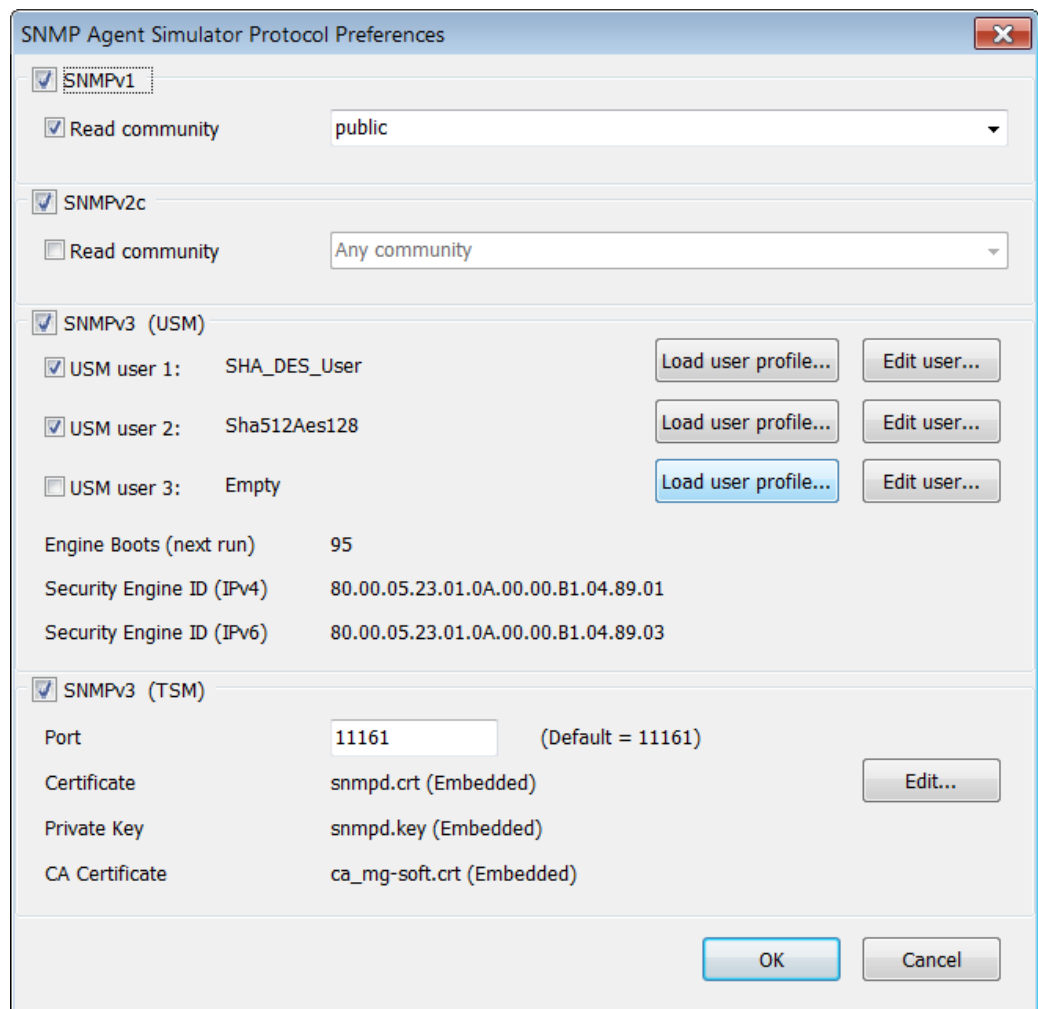


Figure 215: Selecting a binding interface in the SNMP Agent Simulator window

- Into the accompanying **Port** drop-down list specify the port number on which the simulated agent will listen to SNMP queries (e.g., 1161). The specified port applies to SNMP over UDP and SNMP over TCP, but not to SNMP over (D)TLS. The latter is configured separately in the SNMP Agent Simulator Protocol Preferences dialog box.
- Click the **SNMP Agent Simulator Protocol Preferences** toolbar button () to open the SNMP Agent Simulator Protocol Preferences dialog box (Figure 216), where you can configure the SNMP protocol parameters for agent simulation, as follows:
 - ❑ Check the **SNMPv1** checkbox if you want the simulated agent to respond to SNMPv1 queries regardless of the community name used. To configure the simulated agent to respond only to SNMPv1 queries containing a specific community name, check the **Read community** checkbox in the SNMPv1 frame and enter the desired community name into the accompanying drop-down list.
 - ❑ Check the **SNMPv2c** checkbox if you want the simulated agent to respond to SNMPv2c queries regardless of the community name used. To configure the simulated agent to respond only to SNMPv2c queries containing a specific community name, check the **Read community** checkbox in the SNMPv2c frame and enter the desired community name into the accompanying drop-down list.



The dialog box is titled "SNMP Agent Simulator Protocol Preferences". It contains several sections for configuring different SNMP protocols:

- SNMPv1:** A checked checkbox. Below it, "Read community" is checked and set to "public".
- SNMPv2c:** A checked checkbox. Below it, "Read community" is unchecked and set to "Any community".
- SNMPv3 (USM):** A checked checkbox. It contains three rows for USM users:
 - USM user 1: SHA_DES_User (checked). Buttons: "Load user profile...", "Edit user..."
 - USM user 2: Sha512Aes128 (checked). Buttons: "Load user profile...", "Edit user..."
 - USM user 3: Empty (unchecked). Button: "Load user profile..."
- Below the USM section, three fields are displayed:
 - Engine Boots (next run): 95
 - Security Engine ID (IPv4): 80.00.05.23.01.0A.00.00.B1.04.89.01
 - Security Engine ID (IPv6): 80.00.05.23.01.0A.00.00.B1.04.89.03
- SNMPv3 (TSM):** A checked checkbox. It contains four fields:
 - Port: 11161 (Default = 11161)
 - Certificate: snmpd.crt (Embedded) with an "Edit..." button.
 - Private Key: snmpd.key (Embedded)
 - CA Certificate: ca_mg-soft.crt (Embedded)

At the bottom right are "OK" and "Cancel" buttons.

Figure 216: Setting the agent simulator protocol preferences

- ❑ Check the **SNMPv3 (USM)** checkbox if you want the simulated agent to respond to SNMPv3 USM queries. At least one USM user must be selected and enabled in the SNMPv3 (USM) frame to be able to successfully query the simulated agent via the SNMPv3 USM protocol. To configure the simulated agent to respond only to SNMPv3 queries sent on behalf of a given USM user, check the first USM user checkbox and click the **Load user profile** button next to it. This opens the SNMPv3 USM User Profiles window, where you can select an existing SNMPv3 user profile (Figure 217). You can view or customize the SNMP protocol settings of a selected user by clicking the **Edit user** button. You can select or configure up to 3 different USM users in this frame. The SNMPv3 (USM) frame also displays the EngineBoots and EngineID (IPv4 and IPv6) values of the simulated agent.

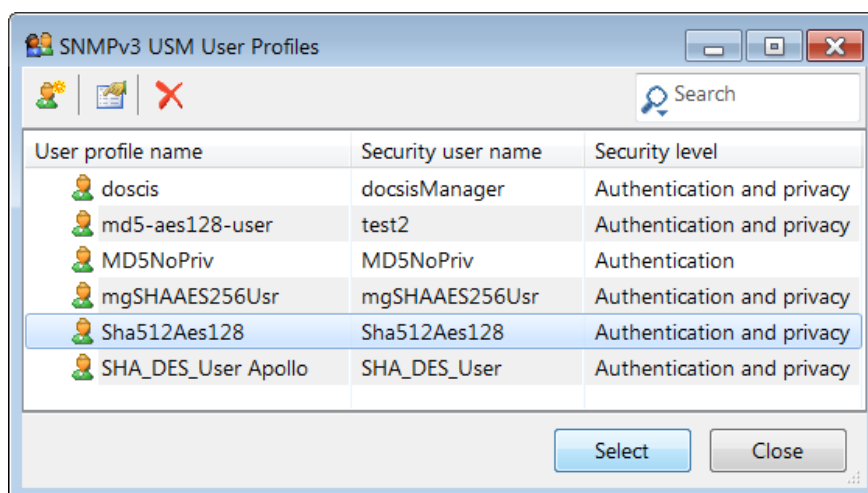


Figure 217: Selecting a SNMPv3 USM user profile for the agent simulator

- ❑ Check the **SNMPv3 (TSM)** checkbox if you want the simulated agent to respond to SNMPv3 TSM queries (i.e., SNMPv3 over TLS/DTLS) and specify the following parameters:
 - ❑ Into the **Port** input line in the SNMPv3 (TSM) frame, enter the port on which the simulated agent will listen to for incoming SNMP over TLS and SNMP over DTLS requests (e.g., 11161).
 - ❑ Click the **Edit** button in the SNMPv3 (TSM) frame to open the **SNMPv3 Security Parameters (TSM)** dialog box and specify the corresponding agent (server) TSM parameters, as follows:

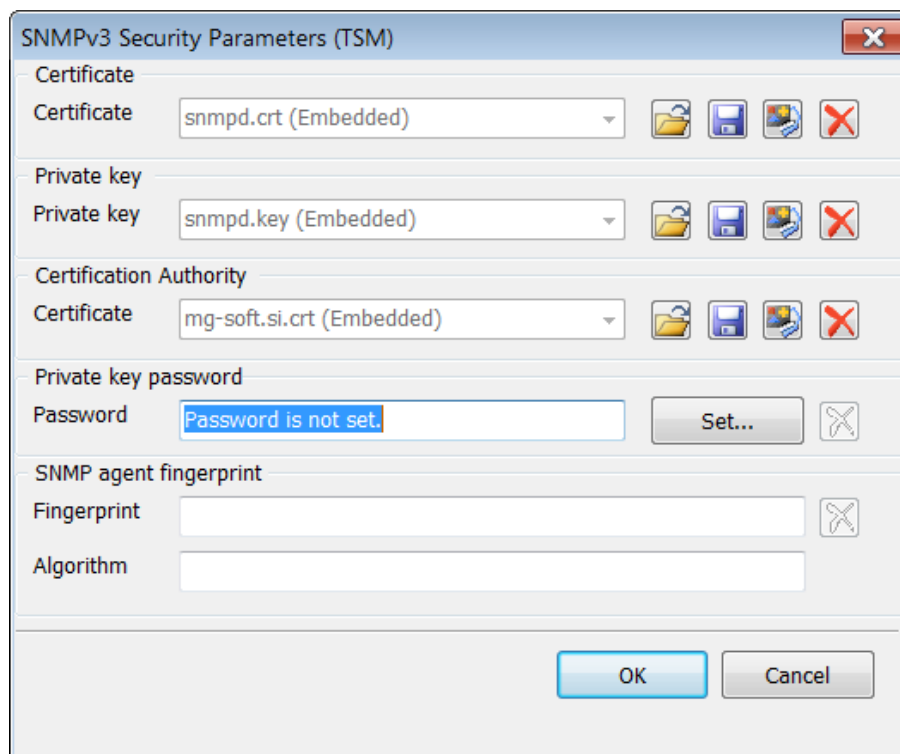







Figure 218: Specifying SNMPv3 TSM details for the agent simulator

- ❑ In the **Certificate** frame, click the **Load** button () to open the standard Open dialog box and select the file containing the X.509 digital certificate file that contains the **agent (server) public key**.
- ❑ In the **Private key** frame, click the **Load** button () to open the standard Open dialog box and select the file containing the **agent private key** in PEM format (e.g., .key or .pem) from disk.

Tip: Click the Properties button () next to the **Certificate** or **Private key** input line to view full details of the loaded digital certificate or private key, respectively.

- ❑ In the **Certification Authority** frame, click the **Load** button () to open the standard Open dialog box and select the X.509 digital certificate file (in PEM format), containing the **CA authority public key**. This certificate will be used for verifying the manager certificate. If the manager uses a self-signed certificate, leave this input line empty.
 - ❑ To enter the password for decrypting the agent private key (if encrypted), click the **Set** button in the **Private key password** frame, and enter the corresponding password twice into the dialog box that appears.
 - ❑ The **Fingerprint** and **Algorithm** are two read-only text fields that get automatically populated after establishing a TLS connection with the manager and accepting its certificate (when no CA certificate is provided). Fingerprint is a cryptographic hash of the certificate in hexadecimal (unique identification of the certificate) and algorithm is the name of algorithm used for producing the fingerprint (e.g., sha1, md5, sha256, etc.).
 - ❑ Click the **OK** button to apply the settings and close the **SNMPv3 Security Parameters (TSM)** dialog box.
 - ❑ After configuring the SNMP protocol preferences for the simulated agent, click the **OK** button to apply the settings and close the **SNMP Agent Simulator Protocol Preferences** dialog box.
6. Into the **Refresh every X seconds** input line in the SNMP Agent Simulator window, enter the number (X) that controls how frequently (in seconds) the statistics and mini graphs will be updated during a simulation.
 7. After you have configured all the settings, you can start simulating the agent by clicking the **Start** toolbar button ().
 - ❑ MIB Browser starts a separate SNMP agent simulation process. While running, this process listens on the user-selected network interface(s) and port(s) (e.g., 1161) for SNMP queries and responds to SNMP queries, returning those OIDs and values that are specified in the loaded agent snapshot XML file.
 - ❑ The Statistics list in the central section of the window displays SNMP statistics of the running agent simulation, i.e., the number of SNMP packets received and sent by the simulated agent, the number of requested and returned OIDs, the number of received and sent octets in SNMP PDUs, the number of received SNMP Get, GetNext, GetBulk and Set requests and the number of sent SNMP Response messages, etc. For each statistical variable, the columns display the total value, delta (value difference of two consecutive polls), average (delta

divided by the refresh interval in seconds), peak delta value and time, peak average value and time (Figure 219).

- ❑ SNMP statistics of the running agent simulation is displayed also in four mini graphs. Right-click on a mini graph to display a pop-up menu with the selection of statistical variables that can be monitored (total values only) in a given mini graph. A toggle tick mark in front of a variable name denotes that the variable is being graphed. The color of the variable name in the pop-up menu is the color of the graph line used for depicting that variable.

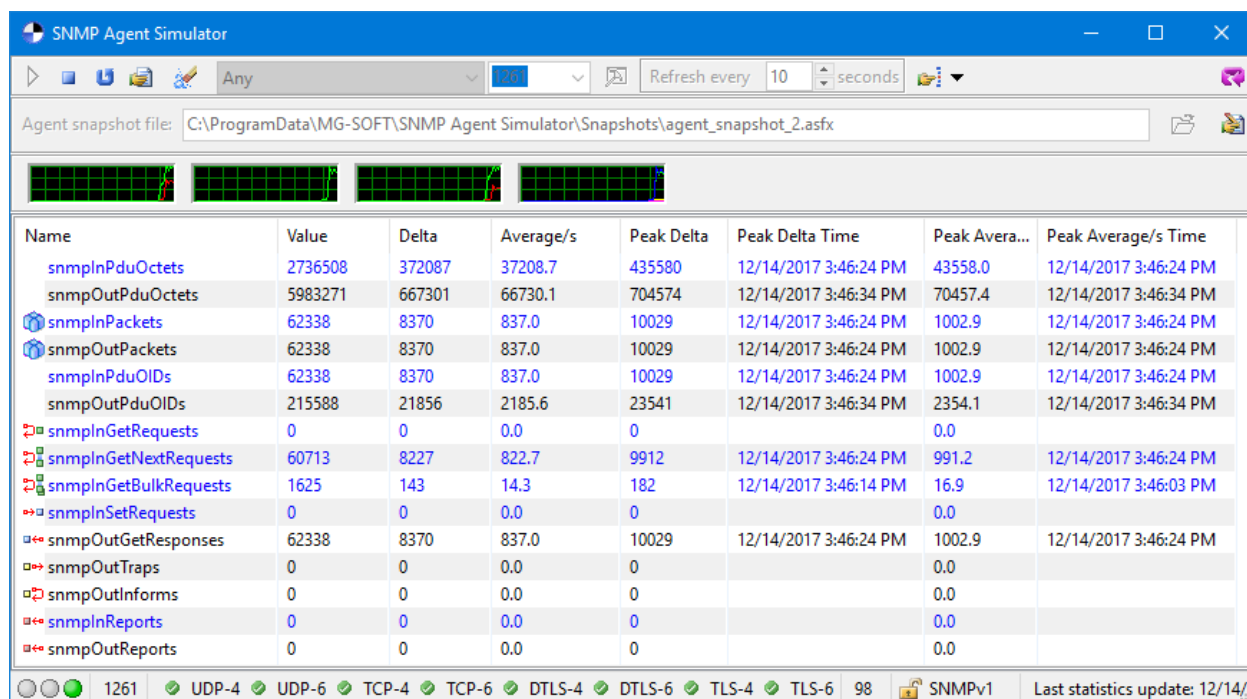


Figure 219: SNMP Agent Simulator window - simulation is running

- To verify if the simulated agent responds to SNMP queries, click the **Contact** toolbar button (🔍) in the SNMP Agent Simulator window. MIB Browser performs the **Contact** operation using the SNMP protocol settings configured in this window and displays the value of the retrieved object instance in the Query results panel of the main window.
- To view the agent simulator status information, click the **Status Report** toolbar button (📄). This displays a report in the SNMP Agent Status Report window (Figure 220).

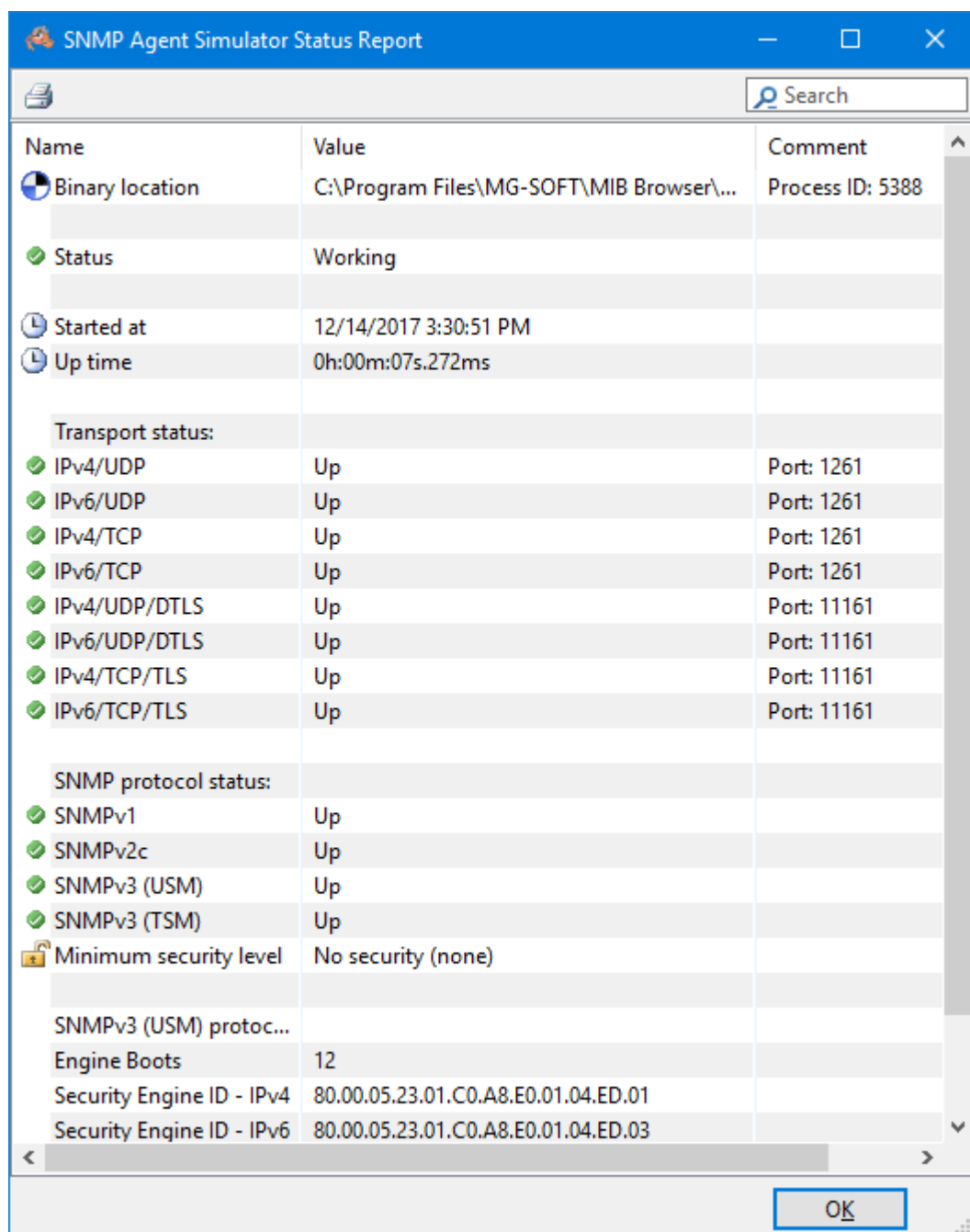


Figure 220: SNMP Agent Simulator Status Report window

10. To stop simulating the agent, click the **Stop** toolbar button () , which terminates the SNMP agent simulation process.

INDEX

A

about

- MG-SOFT Corporation 13
- MIB Browser 14
- MIB Browser file formats 253
- MIB Browser main features 15
- MIB Browser manual 17

adding

- IPv4/UDP or IPv6/UDP ports 191
- MIB modules to MIB Browser 166
- objects to multiple variable bindings list 147
- OID values monitored in Info window 158
- row to an SNMP table 169
- SNMPv3 USM user profile 64, 88

address

- IPv4/v6 39

agents, SNMP

- comparing SNMP agent snapshots 213
- contacting 38
 - IPv4/v6 address* 39
 - selecting binding interface* 41
- discovering 152–56
- problems with contacting 231
- scanning for implemented MIB modules 163–66

authentication security protocol 65, 90

B

binding interface

- select 41

bulk, SNMP GetBulk operation 50, 58–61

C

columnar objects

- selecting object instances 122

Command line interface (CLI) 126

community

- set community string 55, 57, 82, 84, 137

comparing SNMP agents 213

compiling MIB files 109

contacting

- an SNMP agent 38
 - problems with contacting* 223–48
 - example* 231
- MG-SOFT Corporation 13

D

decoding

- exchanged SNMP messages 226

desktop

- MIB Browser 34
- MIB Compiler 109

dialog boxes

- Add New Table Instance 170
- Binary Key For Auth/Priv Protocol 68
- Generic SNMP Trace Preferences 226
- Info Window Properties 158
- Instance To Query 120, 123
- MIB Browser Preferences 48
- Password For Auth/Priv Protocol 65
- Prompt For OID 134
- Scan Agent For Implemented MIB Modules Preferences 164
- Search Compiled MIB Modules To Resolve OID 48
- Select 145
- Select Bits Value 139
- Select Object Identifier 135
- Select OID To Query 158
- Select SNMP Agent Port And Transport 191
- Select Value 139
- Set 138, 140
- SNMP Agent Profiles 79
- SNMPv3 Security Parameters 69, 99, 221

Diffie-Hellman key exchange 69

discovering

- MIBs implemented in SNMP agents 163
 - example* 165
- SNMP agents 152–56
 - example* 156

DOCSIS based SNMPv3 agents 69

- Diffie-Hellman key exchange 69

DTLS75

E

editing

adding row to an SNMP table169
 SNMP tables in a table view141

F

features, MIB Browser.....15

file formats, supported.....253

G

Get operationSee SNMP operations

GetBulk operationSee SNMP operations

GetNext operationSee SNMP operations

graphical representation

creating a graph line.....175
 editing a graph line179
 example180
 starting graphing operation.....171

H

help file35

I

informing

sound notification on received SNMP
 notification messages187
 with SNMP notification messages181–98

informs.....See SNMP notification messages

installing the software

on Linux operating system23
 on Mac OS X operating system.....24
 on Solaris operating system.....25
 on Windows operating system22

IPv4/v6 address.....39

K

key exchange, Diffie-Hellman method69

L

Linux operating system

installing MIB Browser.....23
 Linux version of MIB Browser20
 starting MIB Browser.....30
 uninstalling MIB Browser.....27

Live search

Generic SNMP Trace widow227
 MIB tab in main window112
 SNMP Trap Ringer Console188

loading MIB modules

automatically, during SNMP Walk48
 manually111, 166
 from a MIB group114

logging the retrieved values.....161

M

Mac OS X operating system

installing MIB Browser.....24
 starting MIB Browser.....32
 uninstalling MIB Browser.....27

making

a list of multiple variable bindings.....144

manager random number.....69

manual

usage instructions17

**max-repetitions.... 58, 76, 84, See also SNMP
 GetBulk**

MG-SOFT Corporation

about.....13

MIB Browser Professional Edition

desktop34
 different editions14
 file formats.....253
 installing the software
 on Linux operating system22
 on Mac OS X operating system.....24
 on Solaris operating system.....25
 on Windows operating system.....23
 main features15
 software requirements20
 starting the software
 on Linux operating system30
 on Mac OS X operating system.....32
 on Windows operating system.....29

uninstalling the software
 on Linux operating system 27
 on Mac OS X operating system 27
 on Solaris operating system 28
 on Windows operating system 26

MIB Compiler
 compiling MIB files 109
 starting MIB Compiler 109

MIB files/modules
 compiling MIB files 109
 loading MIB modules in MIB Browser.. 111,
 166
 saving MIB modules to a MIB group 114
 scanning SNMP agents for implemented MIB
 modules 163–66
 example 165

MIB group 114

MIB nodes *See Nodes, MIB tree*

MIB tree
 comparing SNMP agents 213
 selecting MIB nodes 44
 walking
 step-by-step 134
 whole MIB tree in one step 47

modifying object instance values
 with SNMP Set operation 137–50
 directly in table view 141
 example 140

modifying SNMP table values 141

modules, MIB *See MIB modules*

monitoring SNMP agents
 in Info window
 logging the retrieved values 161
 in Performance Graph window 171
 example 180
 in Table View window 167

multiple variable bindings in PDU
 modifying values with SNMP Set
 example 149
 retrieving values with SNMP GetBulk
 example 59–61

N

network card
 select 41

nodes, MIB tree
 properties 52, 115
 selecting 44
 SNMP Walk operation 46

non-repeaters 58, 76, 84, *See also* SNMP
 GetBulk

notifying
 SNMP Trap and Inform messages 181–98, *See*
 also SNMP notification messages
 sound notification on received messages 187

O

object instance
 selecting 122

operations
 SNMP *See* SNMP operations
 ways of accessing 17

P

passwords, SNMPv3 security 66

polling SNMP tables 167

ports
 receiving SNMP notification messages
 on non-standard ports 191
 specifying SNMP port number 54, 191

privacy security protocol 65, 90
 decrypting encrypted SNMPv3 messages 226

properties
 MIB node 52
 MIB node 115

protocols, SNMP *See* SNMP protocols

Q

querying object instances
 monitoring
 graphical representation 171
 tabular representation 167
 SNMP Get operation
 example 121
 SNMP GetBulk operation
 example 58
 SNMP GetNext operation 122
 SNMP Walk operation 46
 example 49

Step-by-Step SNMP Walk operation 134
example 136

R

receiving

SNMP notification messages..... 181

recording

exchanged SNMP messages..... 224
 SNMP notification messages..... 197

remote SNMP agent.....*See Agents, SNMP*

representation

graphical 171
 tabular 167

requirements

software 20

resolving OID values 48

retransmits 57

retrieving

object instance values... *See Querying object instances*
 OID values
 all in one step (SNMP Walk)..... 46
 Step-by-Step SNMP Walk..... 134

S

scanning

SNMP agents for implemented MIBs 163–66

scope ID 40

searching

for active SNMP agents..... 152
 for implemented MIB modules 163–66
 for MIB modules to resolve OID 48

security

Diffie-Hellman key exchange 69
 passwords and security keys..... 66
 SNMPv3 security parameters.. 63–66, 63–66
 SNMPv3, authentication security protocol 65, 90
 SNMPv3, privacy security protocol 65, 90
 decrypting encrypted SNMPv3 messages
 226

selecting

an object instance 122
 in Multiple Variable Bindings window 146

binding interface 41
 MIB tree nodes..... 44

sending

SNMP notification messages 199

Set operation.....*See SNMP operations*

setting values in SNMP agents 137–50

 in table view 141
 problems with setting values..... 151
 selecting and setting pre-defined values . 139
 when SNMP syntax is BITS..... 139

shortcuts in MIB Browser 17

Simulating SNMP agents..... 241

SNMP agent.....*See Agents, SNMP*

SNMP notification messages

acknowledging 187
 listening on non-standard ports 191
 more information about..... 194
 receiving
 SNMPv1/v2c notifications
 on standard SNMP Trap ports 181
 SNMPv3 notifications 186
 sending 199–206
 SNMPv1 notification messages..... 199
 SNMPv2c/v3 notification messages..... 203
 SNMPv3 notification messages..... 206
 SNMPv1/v2c notifications 181
 sound notification..... 187
 tracing and decoding 197

SNMP operations

 difference between SNMP Get and GetNext
 operation..... 124
 SNMP Get 117, 126, 131
 SNMP GetBulk 50, 58–61, 132
 SNMP GetNext 122–25, 129, 131
 SNMP Set..... 137–50
 SNMP Walk 46–53, 130
 Step-by-Step SNMP Walk..... 134–36
 with SNMP GetBulk requests..... 50
 tracing exchanged SNMP messages..... 225
 tracing SNMP notification messages 197

SNMP protocols

SNMPv1 55
 SNMPv2c 56
 SNMPv3 *See also Security, See also Security*
 SNMPv3 TSM with DTLS 75
 SNMPv3 TSM with TLS 71
 SNMPv3 USM 62–70
 specifying SNMP protocol parameters 54

SNMP tables..... *See* **Tables**

SNMP transport protocols

select binding interface.....41

SNMPv3 agents, DOCSIS based69

Diffie-Hellman key exchange69

software requirements20

Solaris operating system

installing MIB Browser.....25

Solaris version of MIB Browser.....21

uninstalling MIB Browser28

sound notification

on received SNMP notification messages187

specifying

multiple variable bindings in PDU146

SNMP protocol parameters54

SNMPv3 passwords and security keys.....66

SNMPv3 security parameters.....64, 89

starting

MIB Browser.....29

on Linux operating system 30

on Mac OS X operating system..... 32

on Windows operating system..... 29

MIB Compiler109

status bar35

System requirements

Mac OS X version of Trap Ringer21

T

tables

adding rows169

modifying SNMP tables141

viewing and polling SNMP tables.....167

tabular display of SNMP tables167

timeout.....56, 57, 82, 85

TLS - Transport Layer Security protocol.71

tracing

exchanged SNMP messages.....223

SNMP notification messages.....197

transport, SNMP

select binding interface.....41

traps.....*See* **SNMP notification messages**

traversing MIB tree

Step-by-Step Walk operation134

Walk operation.....38

troubleshooting

in Generic SNMP Trace window229

TSM - Transport Security Model for SNMP

.....71

U

uninstalling the software

on Linux operating system.....27

on Mac OS X operating system27

on Solaris operating system28

on Windows operating system26

using

MIB Browser manual.....17

W

Walk operation.....*See* **SNMP operations**

windows

About MG-SOFT MIB Browser29

Compare Agent Snapshot.....207, 210

Comparison Report215

Generic SNMP Trace223, 225

Generic SNMP Trace For Trap Ringer ...197

Info157

Manage Agent SNMPv3 Users219

MIB Browser desktop34

MIB Browser Preferences183, 186

MIB Compiler desktop.....109

MIB Node Properties52, 116, 194

Multiple Operations232

Multiple Variable Bindings.....60, 144, 149

Performance Graph174

Remote SNMP Agent Discovery152

Scan Agent For Implemented MIB Modules

.....164

Select Table Instance(s)120, 137

SNMP Agent Simulator241

SNMP Trap Ringer Console182

Table View167

Windows operating system

installing MIB Browser.....22

starting MIB Browser.....29

uninstalling MIB Browser.....26

Windows version of MIB Browser20

APPENDIX: MIB BROWSER FILE FORMATS

Following is the list of **file formats supported by MG-SOFT MIB Browser 2018, Version 16.x**, both 32-bit (x86) and 64-bit (x86_64) build.

Saving files to deprecated file formats should be avoided, as the future versions of MIB Browser might stop supporting the deprecated formats.

Extension	Description	Type	Status	x86		x86_64		Comment
				Load	Save	Load	Save	
.asfx	Agent Snapshot File XML	XML	Current	✓	✓	✓	✓	
.mbgx	Graph File XML	XML	Current	✓	✓	✓	✓	
.mbmx	Monitor File XML	XML	Current	✓	✓	✓	✓	
.mvbx	Multiple Variable Bindings File XML	XML	Current	✓	✓	✓	✓	
.mofx	Multiple Operations File XML	XML	Current	✓	✓	✓	✓	
.trfx	Trap Ringer File XML	XML	Current	✓	✓	✓	✓	
.apfx	Agent Profiles File XML	XML	Current	✓	✓	✓	✓	
.mqsx	Query Set File XML	XML	Current	✓	✓	✓	✓	New in v13
.qcsx	Color Scheme File XML	XML	Current	✓	✓	✓	✓	New in v13
.asf	Agent Snapshot File	BIN	Deprecated	✓	✓	✗	✗	
.mbg	Graph File	XML	Deprecated	✓	✓	✓	✓	
.mbm	Monitor File	BIN	Deprecated	✓	✓	✗	✗	
.mvb	Multiple Variable Bindings File	BIN	Deprecated	✓	✓	✗	✗	
.apf	Agent Profiles File	XML	Deprecated	✓	✓	✗	✗	
.mqs	Query Set File	BIN	Deprecated	✓	✓	✓	✗	Note 1
.qcs	Color Scheme File	INI	Deprecated	✓	✓	✓	✓	

Note 1: The Query Set File XML (.mqsx) format used for storing the Info window settings has been introduced in MIB Browser Version 13.0 and the 64-bit (x86_64) build of MIB Browser v14 still supports loading the old file format (.mqs) for conversion to .mqsx. Support for .mqs format will end in the next version of MIB Browser x86_64.