15.4 RELEASE NOTES

OVERVIEW

These release notes outline in broad terms some of the changes that have been made since release 15.3 of our products. Note that this list is not exhaustive for every product on every platform. If you have questions, please refer to the product-specific documentation or contact SNMP Research's support staff.

OPERATING SYSTEMS

SNMP Research's products have been updated to support newer versions of existing supported platforms. For a current list of supported platforms, please visit our Web site at `www.snmp.com`. The most recent additions to our supported platforms are listed below:

- Added support for Windows XP for all products, both manager and agent.
- Added support for the *sysAppl MIB* on Windows for CIAgent.
- Added support for HP/UX 11i (itanium) for agent products (EMANATE, EMANATE Lite, MAb/SADK).

NEW DIRECTORY NAMES

The following directory names have been changed so that “noexport” is now “5D992b1” and “export” is now “other.”
The contents of the directories named “5D992b1”correspond to Part 774 Section 5D992 (b) 1 of the United States Export Administration Regulations (EAR) and are subject to export controls for U.S. origin data and technology. As of this writing, these data cannot be exported or re-exported to any entity on the denied persons list or any destination associated with the following seven countries: Cuba, Iran, Iraq, North Korea, Libya, Sudan, Syria, per Supplement number 1 of Part 738 of the Export Administration Regulations, and may be subject to further controls.

It is the customer’s responsibility to comply with the terms of the License Agreement which states with regard to export and re-export (the exact wording of your agreement may vary somewhat):

> The Licensee agrees to comply with any and all pertinent laws and regulations of the United States, including the regulations of the United States Department of Commerce with respect to the export of United States origin technical data and commodities.
>
> Regardless of any disclosure made by Licensee to SNMP Research of the ultimate destination of the Program or Derivative Works thereof, the Licensee shall not export, re-export, or transfer, directly or indirectly, any portion of the Program or any system containing any portion of the Program, if those portions are subject to export restrictions in the then current regulations of the United States Department of Commerce or any other agency or department of the United States Government, without first obtaining export licenses as may be required, if any, under the applicable laws and regulations.

The contents of the directories named “other” are not subject to AT1 export controls of the United States but may be subject to other export controls. In addition, this product may be subject to re-export regulations of other nations, import regulations, and use restrictions in various governmental jurisdictions.

UPGRADES FOR CORE LIBRARIES

Core Libraries are source code tools that provide the foundational routines used as the building blocks for other products. Core Libraries are written to support SNMPv1, SNMPv2, SNMPv3, and all MIB variables that conform to the Internet Standard Structure of Management Information (SMI). The following list of items reflects a brief overview of some of the more significant updates that affect SNMP Research’s core libraries.

- Improved handling of an empty snmpinfo.dat file, or calling GetMIBNodeFromOID() before the snmpinfo.dat file is read. A non-empty snmpinfo.dat file is handled correctly.

- Fixed problem where thirty-two bit MIB objects were being read with a sixty-four bit format on sixty-four bit architecture machines (Sun Ultra and HPUX PA Risc 2.0). This caused problems with integer values greater than 2147483647.
- Updated base MIB documents.

UPGRADES FOR AGENT PRODUCTS

SNMP Research provides agent products for end-users and Original Equipment Manufacturers (OEMs). Agent products are available for both open and embedded systems. SNMP Research's agent products are built upon the world's leading EMANATE® agent technology. We offer such options as Web accessibility to agent information, run-time extensibility, and compile-time extensibility. The following list of items reflects a brief overview of some of the more significant updates that affect SNMP Research's agent products.

- The notification filter storage type, notification profile storage type and notification parameter storage types are now correctly initialized to nonvolatile. Now, rows no longer disappear in the snmpNotifyFilterProfileTable, snmpNotifyFilterTable, and snmpTargetParamsTable across reboots.
- Improved NVT string handling. Routines no longer accept embedded newlines in NVT strings.
- Corrected initialization failure in vacmAccessTable that could cause vacmAccessEntries created via SNMP to be unmatchable.
- In 32-bit and 64-bit Solaris MIB-2, now, the agent will not return non-IP routing entries from the routing table. Cached and broadcast entries are returned in the proper format.
- Modified the code used with "-vbdump" option to correctly handle authPriv packets that cannot be parsed because SNMPv3 user is unknown.
- Added check in GetNext request processing to handle modifications to dispatch table due to subagent registration/deregistration in the middle of request processing.
- Proxy agent: Added code to tack on the necessary varbinds when forwarding SMIv1 style traps to SMIv2 targets.
- Added new debug tracing messages for SET processing.

EMANATE AND EMANATE/LITE

EMANATE is a run-time extensible SNMP agent. The EMANATE system includes the world's leading subagent development kit, which automates subagent development. Based on a Master Agent/Subagent architecture, EMANATE allows subagents to be loaded and unloaded dynamically at run-time.

EMANATE/Lite is a monolithic agent, which includes an easy-to-use development toolkit for adding MIB extensions to the agent at compile time. EMANATE/Lite provides access to management information for each of the managed protocol layers within the network

element. The upgrades for EMANATE, EMANATE/Lite, and other EMANATE-based agents include the items listed in the Core Libraries section, as well as the following items:

- Configuration File Parser Support in postmosy.

  In earlier releases, the -parser command line argument generated some additional code for MIB tables to allow the saving of tabular data to a text file. Also, MIB tables could be populated by loading tabular data from a text file.

  In Release 15.4, the -parser command line works with scalar MIB objects in addition to tables. Also, Counter64 objects can be stored in the text file in a numeric format.

- DisplayString Support in postmosy.

  There is a new command line argument to support the DisplayString Textual Convention: -defval_c_string. This argument causes postmosy to treat the value of the DEFVAL clause like a C-string, interpreting the values "\0", "\n", "\r", "\a", "\b", "\t", "\v", and "\f" as escape sequences for null (NUL), linefeed (LF), carriage return (CR), alert (BEL), backspace (BS), horizontal tab (HT), vertical tab (VT), and formfeed (FF), respectively. This corresponds to RFC 2579, Page 4, which says, "NUL, LF, CR, BEL, BS, HT, VT and FF have the special meanings specified in RFC 854". Note that -defval_c_string does not yet appear in the Developer Documentation.

RMON

The RMON Agent is an implementation of the Remote Network Monitoring MIB, RFC 1757. When real-time reporting of the traffic that passes through a specific point in the network is needed, then the open-standard RMON MIB can deliver this information to any SNMP-based manager. The following improvement has been made to the RMON Agent:

- Data is now appropriately cached, avoiding any minor data coherence inconsistencies.

UPGRADES FOR MANAGEMENT STATIONS AND APPLICATIONS

SNMP Research provides management stations and applications for end-users and Original Equipment Manufacturers (OEMs). Management stations and applications enable administrators to monitor and control networks, systems, and applications. Options, such as Web and java-based interfaces and policy-based management, are also available. The following list reflects a brief overview of some of the more significant updates that affect SNMP Research's management stations and applications:

- Modified gettab to more closely match the behavior of other command line utilities, particularly with respect to error and report handling.
- Fixed a problem where the timeout signal handling was not being reasserted on SYSV systems and AIX (which in this respect follows SYSV behavior). This would cause command line utility timeouts to return rather than retry.

ARL

The Asynchronous Request Library (ARL) provides an API for building SNMP manager applications or for integrating SNMP manager capabilities into an existing application. The ARL makes it easy to write manager applications that take advantage of the SNMP management framework without requiring the developer to have SNMP expertise or programming capabilities. The upgrades for ARL and ARL-based management stations and applications include the items listed in the Core Libraries section and in the following list:

- The table management code under ArlGetTable() was vastly improved, and deals effectively with agent with small maximum packet size, agents that return objects out of lexicographic order, and requests from management applications to return varying numbers of rows at a time.
- Improved and centralized deleted request management. There were certain situations were stale data were inadvertently accessed in processing responses to requests that had been deleted.

BRASS

The Bilingual Request and Security Subsystem (BRASS) is a Management Application Toolkit designed to provide facilities for creating SNMP management applications. It provides a C programming API that allows one or many management applications to access a single, shared SNMP stack and security database. BRASS optimizes the management station platform by providing full SNMP functionality, management application extensibility, support for SNMPv1, SNMPv2c, and SNMPv3, and simplified security configuration. BRASS also allows for efficient memory usage when there are multiple management applications. The upgrades for BRASS include the items listed in the ARL section as well as the items in the following list:

- A command line option -pkt_size allows the BRASS server to allow one to modify the maximum packet size to be other than the default (2048).
- BRASS servers now ignore the -d qualifier in a non-daemonizing (i.e. Windows) environment.

EPIC

The EMANATE Protocol Interface Component (EPIC) Subsystem provides a solution for interfacing non-UDP and non-SNMP protocols with EMANATE and EMANATE/Lite multilingual agents (combinations of SNMPv1, SNMPv2, and SNMPv3). An EPIC application allows one foreign management protocol to submit get-requests and set-requests into the agent with or without the use of SNMP or UDP. The entire EPIC Subsystem is made up of one or more EPIC applications and the EPIC Adaptation Layer (EAL). The EAL allows for multiple foreign protocol transactions, including CLI, CORBA, XML, Java, etc., and is the layer at which an EPIC integrates into various SNMP Research products. The EPIC API is consistent across all products, and operating system-

specific instrumentation (such as the transport interface) is handled at the EAL level. Using the EAL, the EPIC Subsystem integrates the foreign management protocol engine with the EMANATE or EMANATE/Lite Agent. Regardless of which protocols are used, the application programmer is generally insulated from these concerns by the EAL. EPIC provides you with the EPIC Adaptation Layer for either EMANATE or EMANATE/Lite SNMP Agent (licensed separately). The upgrades to EPIC include the following items:

- EPIC is avalible on several new platforms, including Solaris, Windows, Linux, OSE, netbsd, and aix.
- EPIC is avalible for use with MAb/SADK.
- All EPIC API calls that EPIC clients use to communicate with EMANATE master agents should be thread-safe.
- New examples of EPIC clients are in the top level epic directory. These examples mirror our standard command line utilities in the utility directory.
- EPIC clients are now able to receive notifications from the SNMP agent they are currently connected to. All SNMP agents that are EPIC enabled will send notifications to all connected EPIC clients when the destination address is 127.0.0.1 (loopback).
- EMANATE Lite - EPIC runs more smoothly on platforms that use signals. It now ignores SIGPIPE signals.

DR-WEB

DR-Web Manager integrates our SNMP libraries with a well-engineered interface to an HTTP server. Using this approach, Web browsers may retrieve and display information available from SNMP agents. This interface makes it possible to talk to any SNMP agent using a Web browser. By making SNMP-based management available via Web browsers, DR-Web Manager enables you to access SNMP-based management information without modifications to either the browser or the associated SNMP agents. The upgrades to the DR-Web include the following items:

- Added support for DR-WEB Agent on Nucleus.
- Added support to DR-WEB Manager to receive SNMPv3 notifications.
- Modified code used with "-vbdump" option to correctly handle authPriv packets that cannot be parsed because SNMPv3 user is unknown.
- Added check in GetNext request processing to handle modifications to dispatch table due to subagent registration/deregistration in the middle of request processing.

SNMP SECURITY PACK

SNMP Security Pack enables SNMP Manager applications with built-in support for only SNMPv1 or SNMPv2c to use SNMPv3 with security and administration. By providing SNMPv3, the SNMP Security Pack offers the benefits of a comprehensive approach to management security, including authentication, authorization, access control, data

integrity, key management, and encryption options. The upgrades to SNMP Security Pack include the following items:

- Added support for SHA-based authentication.
- Improved handling of SNMPv2c agent's TOO_BIG error response.
- Improved /KEEP option: The /KEEP option's updates are effective when credentials are changed (for example, changing passwords). Previously, the /KEEP option in overloaded community strings had been ignored when a successful operation had already taken place to an agent using a previous set of credentials.

FOR MORE INFORMATION

For full descriptions of all of our products and their features, please visit our Web site at `www.snmp.com`.