NASTEL™
TECHNOLOGIES, INC.

M6/SNMP 600.002

Nastel AutoPilot M6 for SNMP

Version 6.0.1

Installation and User's Guide

PUBISHED BY:
RESEARCH AND DEVELOPMENT DEPARTMENT
NASTEL TECHNOLOGIES, INC.
48 SOUTH SERVICE ROAD, SUITE 205
MELVILLE, NY 11747

DOCUMENT TITLE: **NASTEL AUTOPILOT M6 FOR SNMP**
DOCUMENT RELEASE DATE: **JANUARY 2009**
NASTEL DOCUMENT NUMBER: **M6/SNMP 600.002**

ACKNOWLEDGEMENTS:

THE FOLLOWING TERMS ARE TRADEMARKS OF NASTEL TECHNOLOGIES CORPORATION IN THE UNITED STATES OR OTHER COUNTRIES OR BOTH: AUTOPILOT/IT, AUTOPILOT/WEB, AUTOPILOT/MQ

THE FOLLOWING TERMS ARE TRADEMARKS OF THE IBM CORPORATION IN THE UNITED STATES OR OTHER COUNTRIES OR BOTH: IBM, MQ, WIN-OS/2, AS/400, OS/2, DB2, AND AIX, WEBSPHERE

JAVA AND THE JAVA LOGOS ARE TRADEMARKS OF SUN MICROSYSTEMS INC. IN THE UNITED STATES OR OTHER COUNTRIES, OR BOTH.

INSTALLANYWHERE IS A REGISTERED TRADEMARK OF ZEROG SOFTWARE IN THE UNITED STATES OR OTHER COUNTRIES, OR BOTH.

THIS PRODUCT INCLUDES SOFTWARE DEVELOPED BY THE APACHE SOFTWARE FOUNDATION (HTTP://WWW.APACHE.ORG/). THE JAKARTA PROJECT" AND "TOMCAT" AND THE ASSOCIATED LOGOS ARE REGISTERED TRADEMARKS OF THE APACHE SOFTWARE FOUNDATION.

THIS PRODUCT MAKES USE OF SNMP STACK SOFTWARE DEVELOPED BY WESTHAWK (HTTP://SNMP.WESTHAWK.CO.UK).

INTEL, PENTIUM AND INTEL486 ARE TRADEMARKS OR REGISTERED TRADEMARKS OF INTEL CORPORATION IN THE UNITED STATES, OR OTHER COUNTRIES, OR BOTH

MICROSOFT, WINDOWS, WINDOWS NT, WINDOWS XP, AND THE WINDOWS LOGOS ARE REGISTERED TRADEMARKS OF THE MICROSOFT CORPORATION.

UNIX IS A REGISTERED TRADEMARK IN THE UNITED STATES AND OTHER COUNTRIES LICENSED EXCLUSIVELY THROUGH X/OPEN COMPANY LIMITED.

MAC, MAC OS, AND MACINTOSH ARE TRADEMARKS OF APPLE COMPUTER, INC., REGISTERED IN THE U.S. AND OTHER COUNTRIES.

"LINUX" AND THE LINUX LOGOS ARE REGISTERED TRADEMARKS OF LINUS TORVALDS, THE ORIGINAL AUTHOR OF THE LINUX KERNEL. ALL OTHER TITLES, APPLICATIONS, PRODUCTS, AND SO FORTH ARE COPYRIGHTED AND/OR TRADEMARKED BY THEIR RESPECTIVE AUTHORS.

OTHER COMPANY, PRODUCT, AND SERVICE NAMES, MAY BE TRADEMARKS OR SERVICE MARKS OF OTHERS

Table of Contents

Figures

Tables

This page intentionally left blank

Chapter 1: Introduction

Welcome to the AutoPilot/SNMP Plug-in Guide. This guide describes installation and use of the plug-in. Please review this guide carefully before installing the product.
This plug-in is designed to work with AutoPilot, its components and other plug-ins, and run simultaneously without interference or performance degradation.

1.1 How This Guide is Organized

Chapter 1: Identifies the users and history of the document. System requirements for this plug-in are outlined. All other system and platform information is listed in the AutoPilot/IT Installation and User's Guides.
Chapter 2: Contains a brief description of AutoPilot/SNMP Plug-in.
Chapter 3: Provides instructions for new installations of the AutoPilot/SNMP Plug-in.
Chapter 4: Provides instruction for using the AutoPilot/SNMP Plug-in.
Chapter 5: Defines the AutoPilot/SNMP configuration metrics.
Appendix A: Provides a detailed list of all reference information required for the installation of AutoPilot.
Appendix B: Contains conventions used in AutoPilot/IT and documents typographical conventions.
Glossary: Contains a listing of unique and common acronyms and words and their definitions.

1.2 History of This Document

1-1. Document History

Release Date:	Document Number	For AutoPilot Version	Summary
March 2006	AP/SNMP 400.001	AP/IT 4.0 or higher	Initial document release.
August 2008	M6/SNMP 600.001	M6	Update for M6.
January 2009	M6/SNMP 600.002	M6	Added acknowledgment of use of Westhawk SNMP software and updated Chapters 2 and 4.

1.2.1 User Feedback

Nastel encourages all Users and Administrators of AutoPilot M6 to submit comments, suggestions, corrections and recommendations for improvement for all AutoPilot M6 documentation. Please send your comments via Post/Mail, or by e-mail. Send messages to: support@nastel.com. You will receive a written response, along with status of any proposed change, update, or correction.

1.3 Related Documents

The complete listing of related and referenced documents is listed in Appendix A of this guide.

1.4 Intended Audience

The AutoPilot/SNMP Plug-in Guide is intended for use by installers and administrators of Nastel's AutoPilot M6 and AutoPilot WebSphere MQ. There are three user groups defined for the purpose of installation and use.

- **Installer:** The installer should be familiar with Java Run Time Environment 1.4.1 (JRE 1.4.1) or higher (included in AutoPilot/IT 4.0 for Solaris, AIX, HP-UX and Linux). Procedures for installing software on the target platform such as Windows and/or UNIX. Basic understanding of TCP/IP.
- **Administrator:** The administrator should have a working knowledge of middleware, TCP/IP, and system management. The Administrator should also have an understanding of Java Runtime Environment (JRE) and TCP/IP. Installation procedures for the platform where AutoPilot is installed (for example, Windows NT, UNIX, etc.)
- **User:** Requires only local operating system operations knowledge and basic knowledge of AutoPilot M6.

1.5 System Requirements

This section defines system and platform prerequisite support requirements for AutoPilot/SNMP.

1.5.1 Platforms

AutoPilot/SNMP is compatible with the following platforms:

- Windows NT/2000/XP
- Unix (Solaris, AIX, HP-UX, Linux)

1.5.2 Other Requirements

AutoPilot/SNMP requires the following conditions:

- AutoPilot M6 Service Pack 7 or higher.
- An SNMP agent must already be installed in order to publish facts.
- Target operating system environment.
- AutoPilot/SNMP Plug-in installation requires less than 1MB of disk space.

1.6 Terms and Abbreviations

A list of Terms and Abbreviations used in this document is located in the Glossary.

1.7 Technical Support

If you need additional technical support, you can contact Nastel Technologies by telephone or by e-mail. To contact Nastel technical support by telephone, call **(800) 963-9822 ext. 1**, if you are calling from outside the United States dial **001-631-761-9190.** To contact Nastel technical support by e-mail, send a message to mailto:support@nastel.com. To access the Nastel automated support system (user id and password required), go to http://support.nastel.com/. Contact your local AutoPilot Administrator for further information.

1.8 Conventions

Refer to Appendix B for conventions used in this guide.

Chapter 2: About AutoPilot/SNMP

This chapter describes Nastel's AutoPilot/SNMP Plug-in and its application with AutoPilot. The SNMP plug-in is used to monitor SNMP-enabled devices. The SNMP Trap Monitor receives events and notifies the SNMP Manager when information is received or an error is present. The SNMP Poll Monitor proactively goes out and polls for Get and Get-Next messages. It also maps the object identifier (OID) to the string. The Management Information Base (MIB) interprets the SNMP messages and provides the readable name of the variable and sometimes interprets its value.

2.1 Introduction to SNMP

SNMP is based on the manager/agent model consisting of a manager, an agent, a database of management information, managed objects and the network protocol. The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device(s) being managed. The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description. A long numeric tag or OID is used to distinguish each variable uniquely in the MIB and in SNMP messages.

2.2 How SNMP Handles Alarm Messages

SNMP uses five basic messages to communicate between the manager and the agent.

- Get
- Get-Next
- Get-Response
- Set
- Trap

The Get and Get-Next messages, used by the SNMP Poll Monitor, allow the manager to request information for a specific variable. (See Figure 2-1.) The agent, upon receiving a Get or Get-Next message, will issue a Get-Response message (simply called a response in version 2) to the manager with either the information requested or an error indication as to why the request cannot be processed.

A Set message allows the manager to request a change be made to the value of a specific variable in the case of an alarm remote that will operate a relay. The agent will then respond with a Get-Response message indicating the change has been made or an error indication as to why the change cannot be made.

The Trap message allows the agent to spontaneously inform the manager of an "important" event. Most of the messages (Get, Get-Next, and Set) are only issued by the SNMP manager. The Trap message is the only message capable of being initiated by an agent. This notifies the SNMP manager as soon as an alarm condition occurs, instead of waiting for the SNMP manager to ask.

2.3 Understanding a MIB

Each SNMP agent has management variables. Each management variable has a unique object identifier (OID) consisting of numbers separated by decimal points (for example: 1.3.6.1.4.1.2682.1). These object identifiers are structured in the form of a tree called a MIB. The MIB associates each OID with a readable label and various other parameters related to the object. The MIB then serves as a data dictionary or codebook that is used to assemble and interpret SNMP messages. When an SNMP manager wants to know the value of an object/characteristic, such as the state of an alarm point, the system name, or the element uptime, it will assemble a GET packet that includes the OID for each management variable of interest. The agent receives the request and looks up each OID in its code book (MIB). If the OID is found (the object is managed by the agent), a response packet is assembled and sent with the current value of the management variable included. If the OID is not found, a special error response is sent that identifies the unmanaged object. When an agent sends a trap packet, it can include OID and value information (bindings) to define the event. SNMP managers will also generally display the readable management variable labels to facilitate user understanding and decision-making.

2.4 Architecture

Figure 2-1 below illustrates the architecture of AutoPilot and SNMP plug-in and the flow of messages.

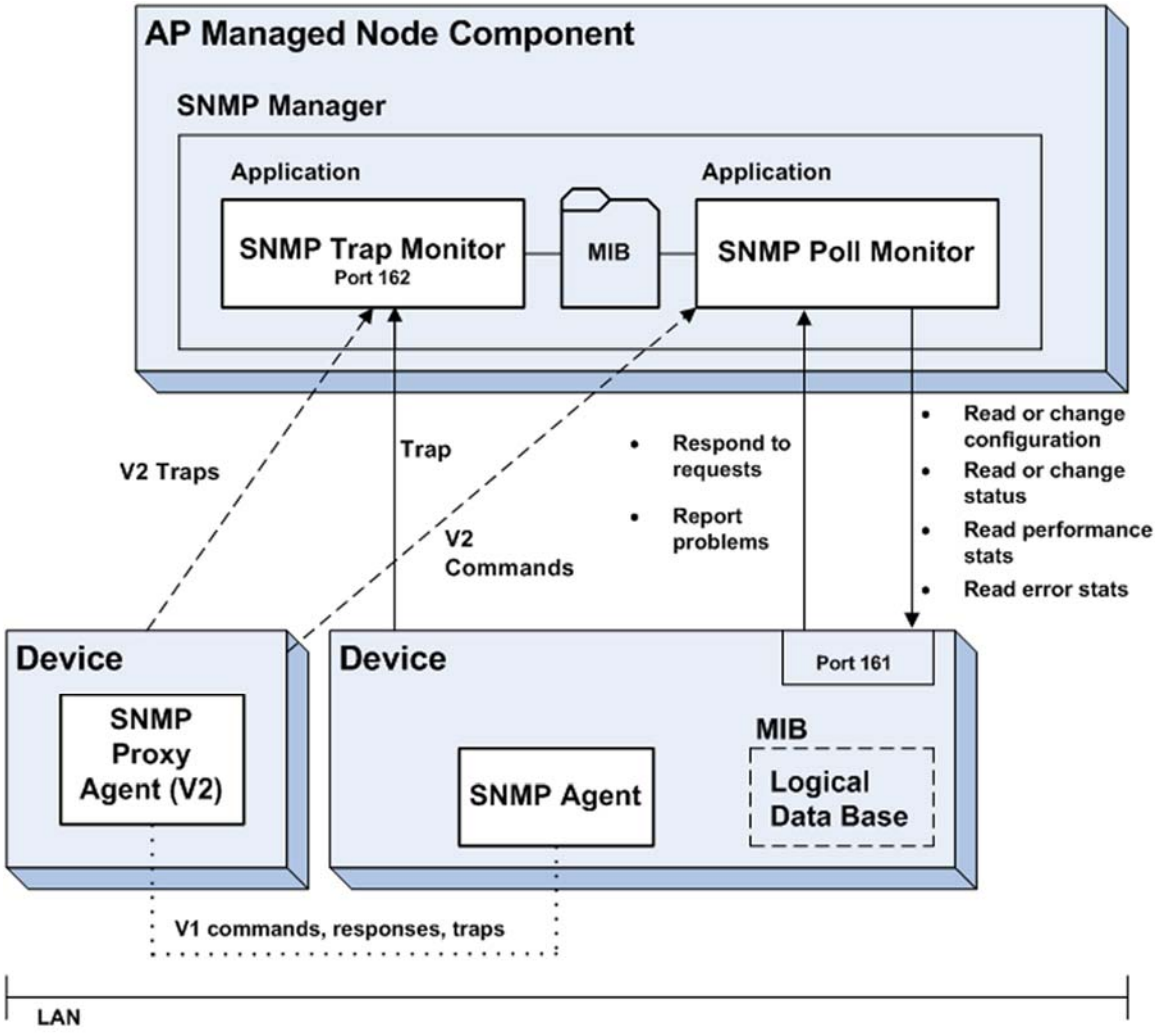

Figure 2-1. SNMP Flow Diagram

Some devices have an SNMP agent and MIB database co-resident in the device being monitored and controlled. Some devices provide indirect access using a proxy management agent. The SNMP manager interacts with the proxy, requesting and receiving information and traps. The proxy has a separate interaction with the actual device. In SNMP V2, proxies are used to relay information between V1 and V2 environments.

The AutoPilot SNMP plug-in supports the following:

- SNMP regular and proxy agents
- SNMP V1, V2 and V3.

Chapter 3: Installation

3.1 Installation Preparation

This section contains general information related to preparing for and installing the installation of AutoPilot/SNMP software.

3.1.1 Installation Materials

The installation can be automatically initiated, then continues using the installation wizard, or manually installed from the installation media. The installation media contains all required AutoPilot M6 components for Java 2 platforms.

3.1.1.1 Technical Documents

Prior to installation, review all text files and installation procedures provided on the installation media. It is recommended that all installation related materials are printed to allow the installer to review prior to installation, and better follow the detailed instructions within. The following files are included on the AutoPilot/SNMP installation media:

- INSTALL.TXT
- README.TXT
- LICENSE.TXT
- Installation and User's Guide: AutoPilot/SNMP 400.001.

3.1.2 Licensing Information

A copy of the standard Licensing Agreement is imbedded in the installation software and is provided on the Nastel Resource Center. The formal licensing agreement has been furnished in the purchase agreement package.

3.2.3 Download the AutoPilot/SNMP Plug-in

Download the AutoPilot/SNMP Plug-in from the Nastel Resource Center.

3.2 Installing the Plug-in

1. Save your work and logoff AutoPilot or AutoPilot/WMQ.

	NOTE:	There are no specific logoff procedures required to exit AutoPilot/IT Console

2. Stop the Nodes and/or Domain Servers that will be updated as specified in the AutoPilot M6 User's Guide.
3. Copy `AP_SNMP_6.0.1.pkg` into the `[`*`AUTOPILOT_HOME`*`]\updates` directory.
4. At the command prompt run:
   `[`*`AUTOPILOT_HOME`*`]\bin\pkgman ..\updates\AP_SNMP_6.0.1.pkg`
5. Verify plug-in installation: `[`*`AUTOPILOT_HOME`*`]\bin\pkgman –libinfo`. The details of the library are listed. Verify that the following files have been copied into the lib directory:

   ```
   snmpbase.jar
   snmpi.jar
   snmpplg.jar
   ```

	NOTE:	Make sure there are no errors posted at the bottom of the screen.

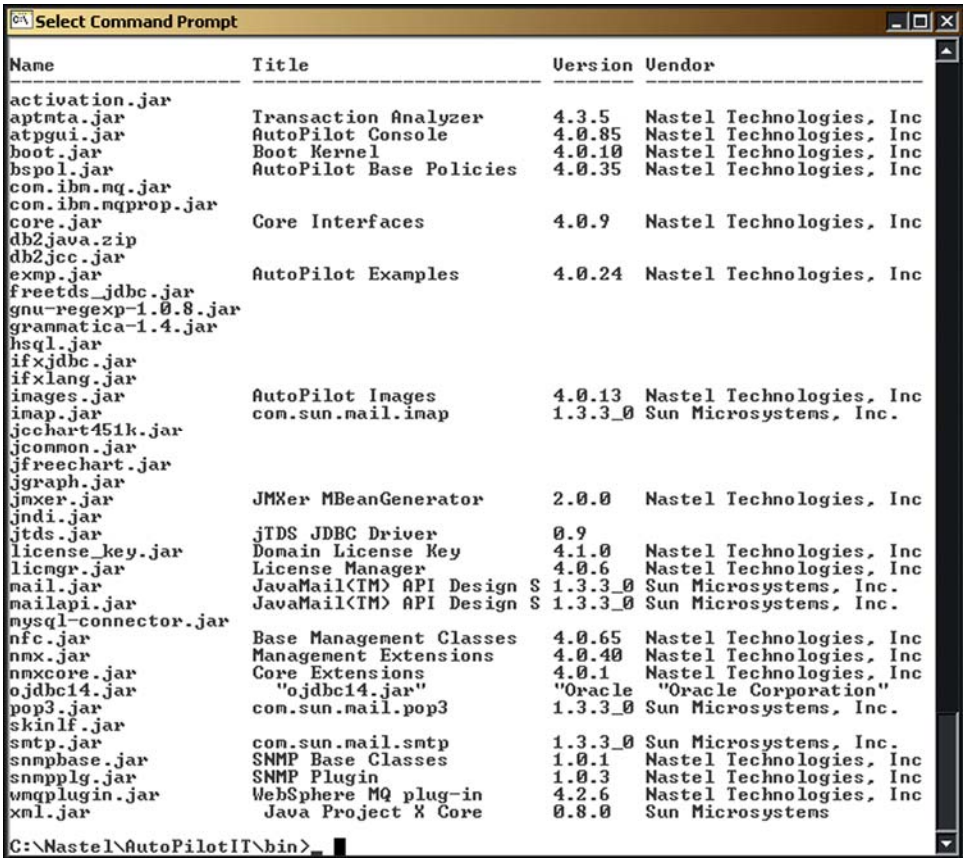

Figure 3-1. Detail of Installed Library List

6. Extract default MIBs to your [*AUTOPILOT_HOME*] folder.

Chapter 4: Using AutoPilot/SNMP

For each device type (for example, Cisco Router Model XYZ, Cisco Bridge Model ABC) to be monitored, a separate pair of SNMP Trap and Poll monitors must be deployed. One trap monitor will manage all devices of the same type, but one poll monitor is needed per device instance. (The device network address is a configuration parameter. See Host field in Table 4-11 and Figure 4-15, SNMP Poll Monitor Expert.)

4.1 Deploying SNMP Expert SNMP Trap Monitor

The following procedure is used to configure the SNMP expert within the AP managed node.

1. Open your AutoPilot Console.
2. Right-click managed node where the SNMP monitors will be displayed.
3. Click **Deploy Expert>SNMP Monitors>SNMP Trap Monitor**.

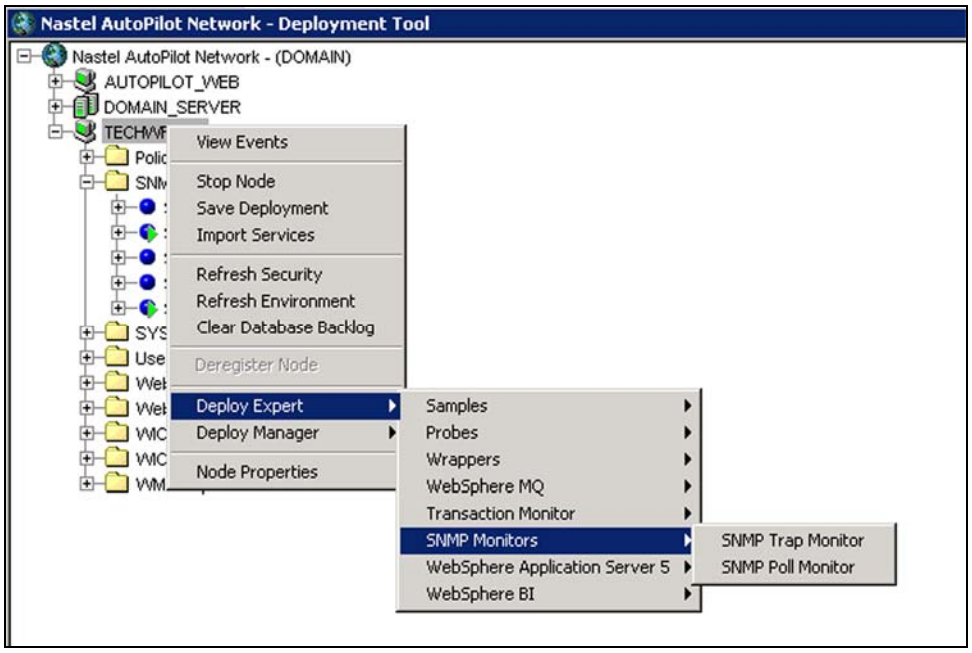

Figure 4-1. Deploy SNMP Expert: Trap Monitor

4. Create your SNMP Trap Monitor as described in the following tables. It is recommended that you change the default *Name* property to something that will uniquely identify your agent.

4-1. SNMP Trap Expert: General	
Property	**Description**
Brief Description	A short description of the service.
Context	A user defined category that will be registered with the domain server. Default displayed.
Name	A user-defined name that uniquely defines the service in the domain. The default name is system assigned with the word service and twelve random digits (Example: Service_123456789012). You can change the name to anything that suites your needs, such as CISCO Router 132A Trap Monitor.

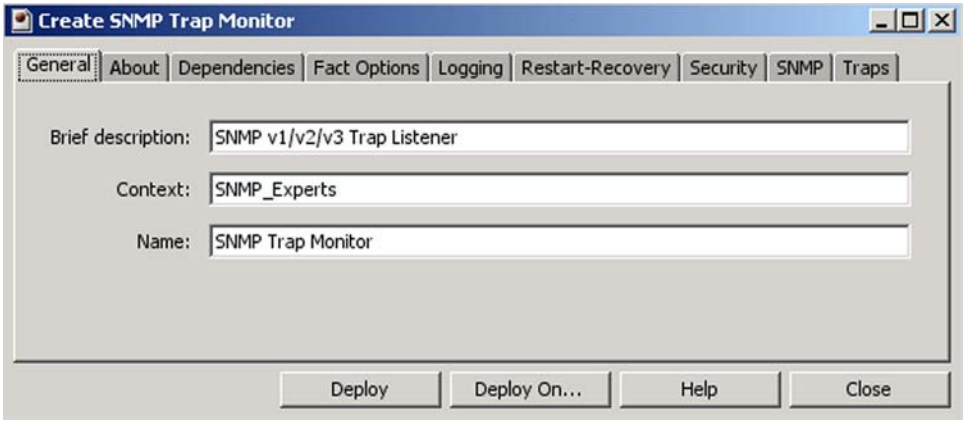

Figure 4-2. SNMP Trap Expert: General

5. Click *About* tab to display information about the package. You cannot change the defaults.

4-2. SNMP Trap Expert: About	
Property	**Description**
Package Title	Implementation title of the source package.
Package vendor	Name of the implementation vendor.
Package version	Package version as assigned by the vendor.

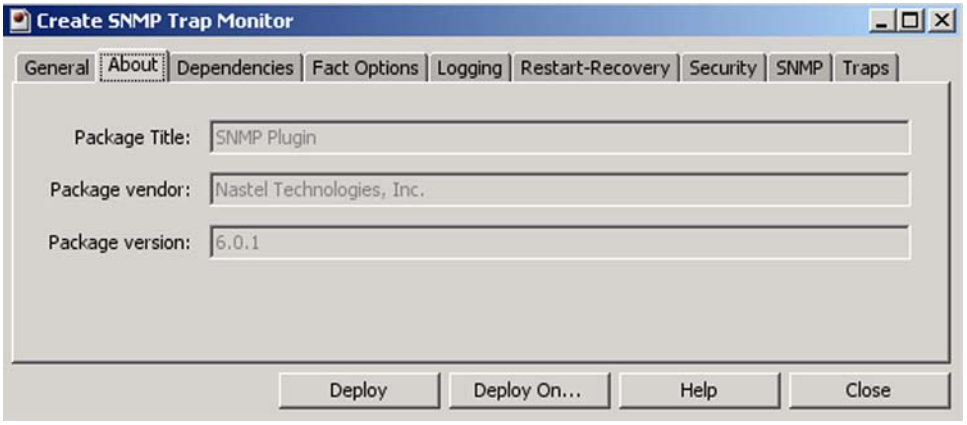

Figure 4-3. SNMP Trap Expert: About

6. Click *Dependencies* tab to identify and format dependencies as defined in the table. These parameters are common to all experts.

4-3. SNMP Trap Expert: Dependencies	
Property	**Description**
Platform dependencies	Comma separated list of operating system platforms this expert is dependent on.
Service dependencies	Comma separated list of other AP services that must be running before this SNMP monitor service can be started.

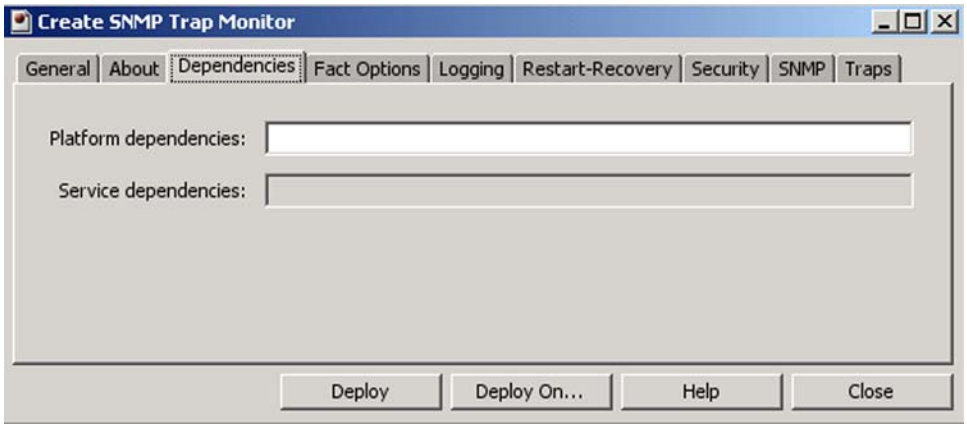

Figure 4-4. SNMP Trap Expert: Dependencies

7. Click *Fact Options* tab to enter your Fact options as defined in the table. These parameters are common to all experts.

4-4. SNMP Trap Expert: Fact Options	
Property	**Description**
Exclude Fact Filters	Comma separated list of fact paths to exclude during publishing.
Expire Facts(ms)	Automatically expires facts that have not been updated in the specified time (ms).
Fact History Size	Automatically maintains the specified number of samples for each published fact in memory.
Fact History Time(ms)	Automatically maintains fact history not exceeding specified time (ms).
Include Fact Filters	Comma separated list of fact paths to include during publishing.

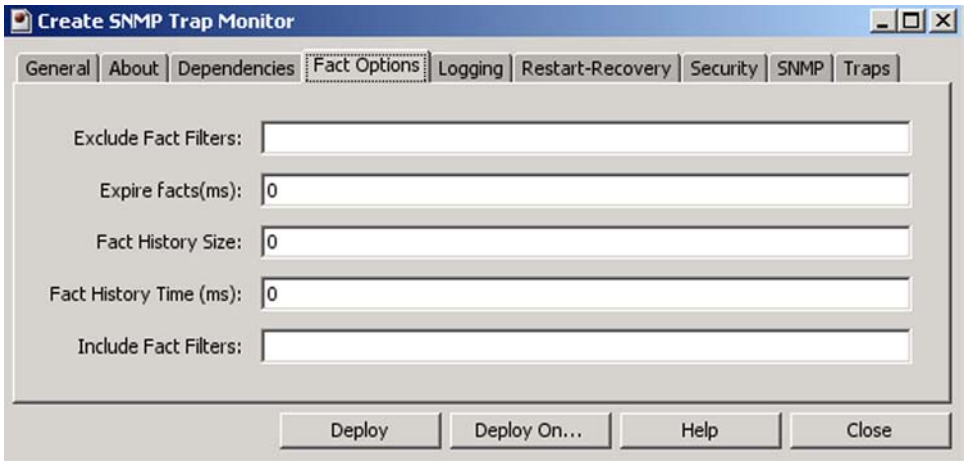

Figure 4-5. SNMP Trap Expert: Fact Options

8. Click *Logging* tab to identify and format logging requirements as defined in the table. These parameters are common to all experts.

4-5. SNMP Trap Expert: Logging	
Property	**Description**
Audit	Check to enable service audit trace. Default is disabled.
Log name	Log name associated with the service.
Log service activity	Check to enable service activity trace. Default is disabled.
Log size (bytes)	Log size in bytes. Real log size is the maximum value of properties server.log.size and logsize. The default value is 200000.
Record Facts	Check to enable fact recording for this service. Default is enabled. Managed node records all facts produced by this service into an .fct file which can be played back using the apfact utility. Recording occurs only when managed node is started with -logfacts option or the environmental variable property server.service.fact.logging=true is defined in global.properties or node.properties.

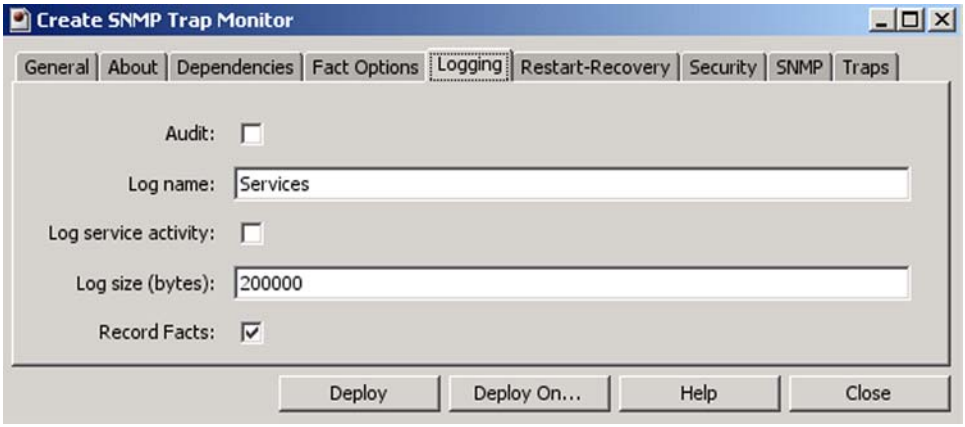

Figure 4-6. SNMP Trap Expert: Logging

9. Click *Restart-Recovery* tab to enable/disable requirements as defined in the table. These parameters are common to all experts.

4-6. SNMP Trap Expert: Restart-Recovery	
Property	**Description**
Automatic start	Check to enable automatic start. Default is enabled
Save in registry	Check to enable saving persistent services in registry .xml file. Default is enabled.
Synchronous Control	Check to enable synchronous service initiation. Default is disabled.

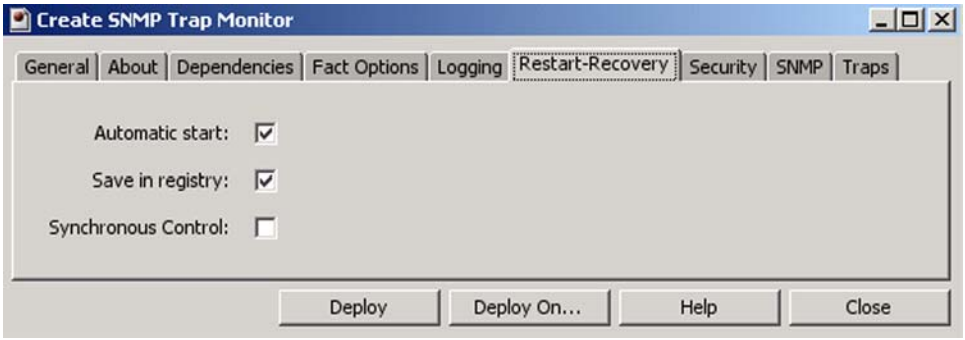

Figure 4-7. SNMP Trap Expert: Restart-Recovery

10. Click *Security* tab to enter or enable requirements as defined in the table. These parameters are common to all experts.

4-7. SNMP Trap Expert: Security

Property	Description	
Inherit Permission from Owner	Enable/disable inherit permission from owner's permission masks. Default is enabled.	
Owner	User that owns the object.	
Permissions	Permissions for users in the same group and users in other groups. Enable/disable as required.	
	Group	**Others**
Read	Group members may read/view attributes of an object.	Other users may read/view attributes of an object.
Change	Group members may change the attributes of an object.	Other users may change the attributes of an object.
Delete	Group members may delete the object.	Other users may delete the object.
Control	Group members may execute control actions such as start, stop, and disable.	Other users may execute control actions such as start, stop, and disable.
Execute	Group members may execute operational commands on the object.	Other users may execute operational commands on the object.

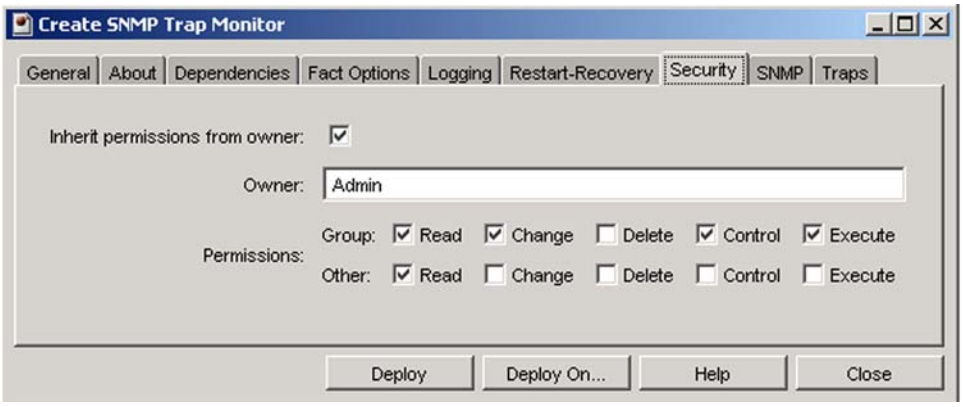

Figure 4-8. SNMP Trap Expert: Security

11. Click *SNMP* tab to enter requirements as defined in the table.

4-8. SNMP Trap Expert: SNMP	
Property	**Description**
Debug level (0-15)	SNMP debug level from 0 to 15; 0 is the lowest level. Extra debug messages will be printed to stdout.
Local hostname	Name of the local host. This is optional.
MIB location	Comma separated list of the directories where the Management Information Bases (MIBs) are located.
Trap community	Name of community (group) for receiving traps. This is a security feature in SNMP v1 to prevent unauthorized monitoring of your devices or generating spoofed traps.
Trap port	Port number of the trap listener; typically 162. (Used by AutoPilot Trap Monitor.)
Trap source	The OID mask of the traps to monitor, ending with a wildcard asterisk character. Example: 1.3.6.1.4.1.2682.*. An asterisk alone, means monitor all traps.

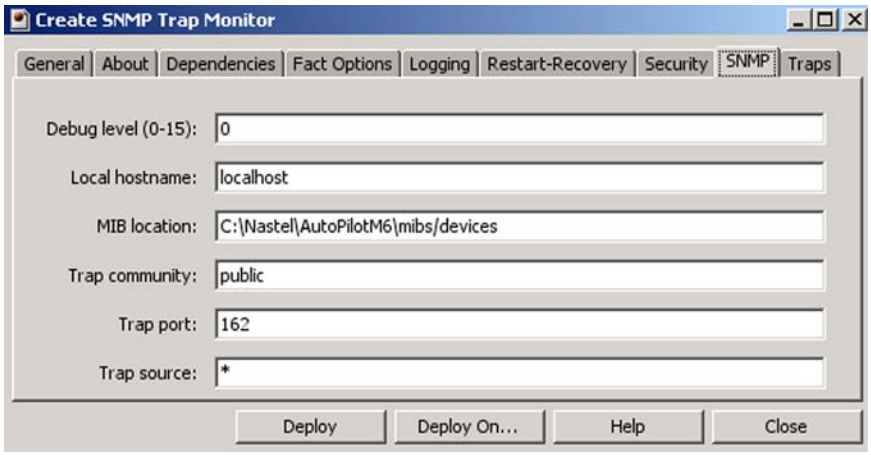

Figure 4-9. SNMP Trap Expert: SNMP

12. Click *Traps* tab to identify trap information as defined in the table.

4-9. SNMP Trap Expert: Traps	
Property	**Description**
TimeTicks oid (v2)	Object Identifier (OID) of trap variable that contains value of TimeTicks (SNMP v2). (TimeTicks is the time in tenths of a second since agent was last activated. This is sysUptime variable.)
Trap agent source	OID of trap variable containing source of the agent sending the trap.
Trap oid (v2)	OID of the SNMP Trap OID variable binding parameter that contains the type of trap (for example: generic coldStart, warmStart or some enterprise specific trap.
Trap source oid	OID of trap variable containing source of the trap (for example: the proxy agent node name or IP address.

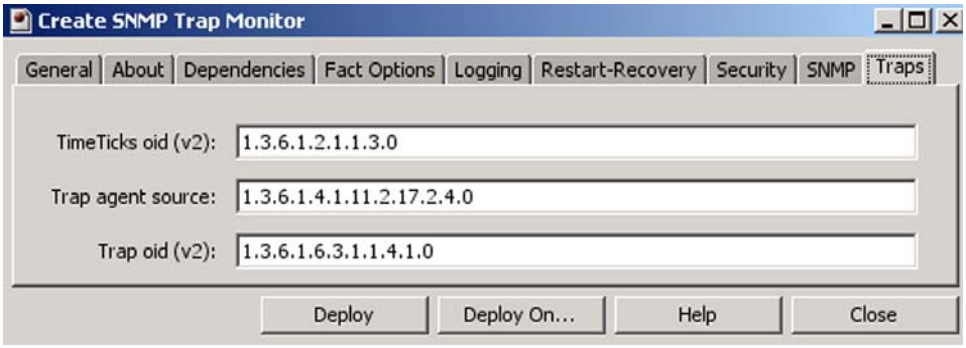

Figure 4-10. SNMP Trap Expert: Traps

13. Click Dep**loy**. The deployment message will confirm the name and location of the expert. Click **OK**.

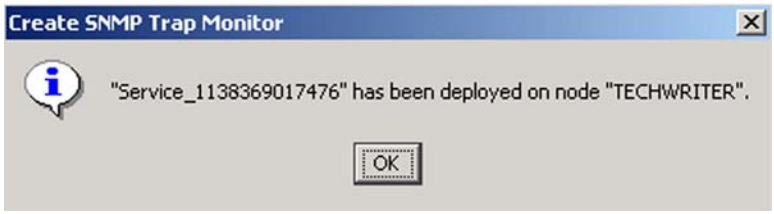

Figure 4-11. Service Deployed

Or, click **Deploy On** to deploy on multiple managed nodes.

14. The deployed expert will be displayed under the node they were deployed on, as in the sample below. The facts produced by each expert are defined in Chapter 5: *AutoPilot/SNMP Configuration Metrics.*

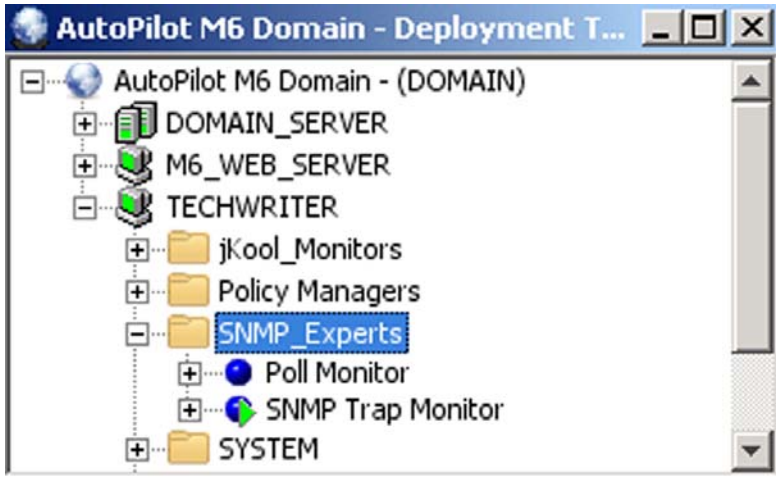

Figure 4-12. Deployed Experts

4.2 Deploying SNMP Poll Monitor Expert

The following procedure is used to configure the SNMP expert within the AP managed node.

1. Open your AutoPilot Console.
2. Right-click managed node that has the SNMP agent installed.
3. Click **Deploy Expert>SNMP Monitors>SNMP Poll Monitor**.

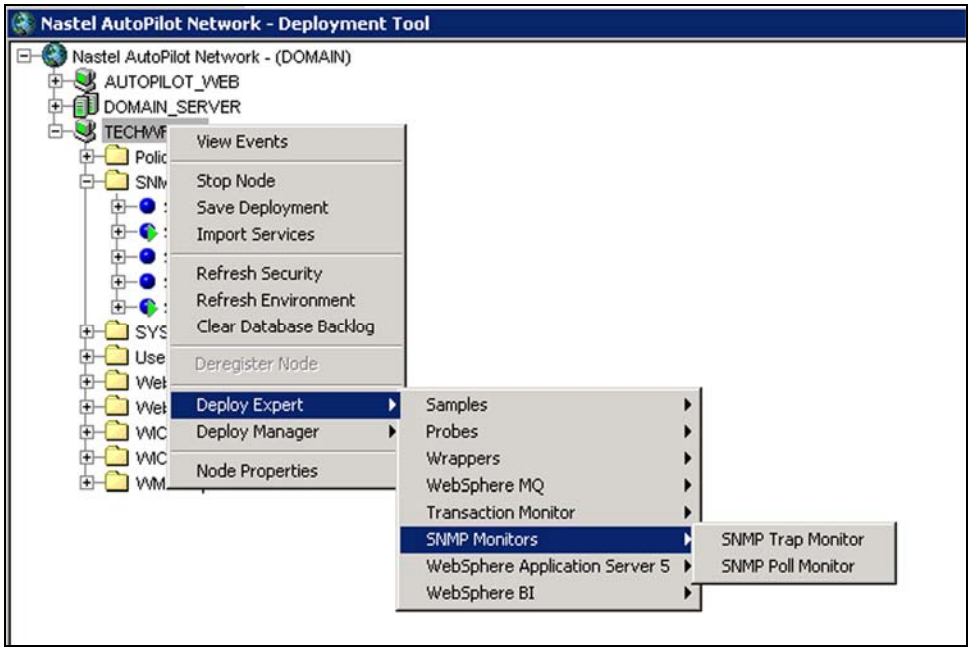

Figure 4-13 Deploy SNMP Expert: Poll Monitor

4. Create your SNMP Poll Monitor as described below. It is recommended that you change the default *Name* property to something that will uniquely identify your agent.

4-10. SNMP Poll Monitor Expert : General

Property	Description
Brief description	A short description of the service.
Context	A user defined category that will be registered with the domain server. Default displayed.
Name	A user-defined name that uniquely defines the service in the domain. The default name is system assigned with the word service and twelve random digits (For example: Service_123456789012). You can change the name to anything that suites your needs; such as CISCO Router 132A Poll Monitor.

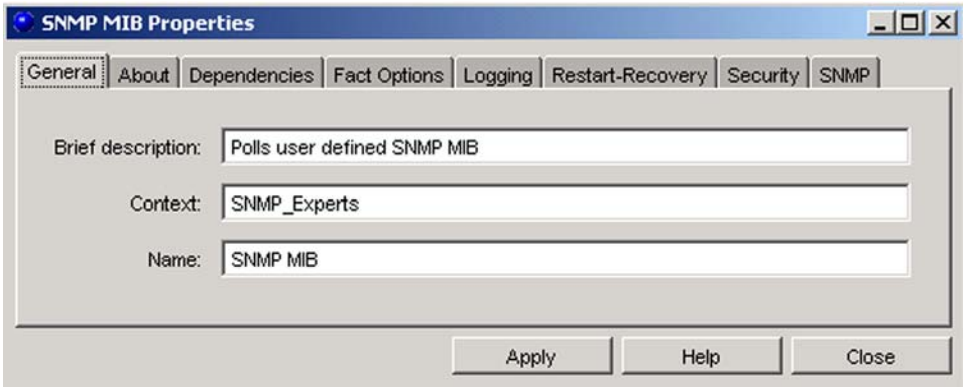

Figure 4-14. SNMP Poll Monitor Expert: General

5. The next six tab properties are identical to the properties for the Trap Monitor.
6. Click *SNMP* tab to enter requirements as defined in the table.

4-11. SNMP Poll Monitor Expert: SNMP	
Property	**Description**
Community	SNMP read-write community name (to be passed to an agent to allow reading and writing of management variables.
Host	SNMP host where SNMP agent is located.
Log	Whether to log to System.out or not (0=no log, 1=log)
MIB File	Directory path to the MIB for the device being monitored.
MIB oid	OID to start scanning from in the MIB.
Poll Interval (sec)	Interval to poll the SNMP agent (in seconds).
Port	Port to poll SNMP agent; typically 161.

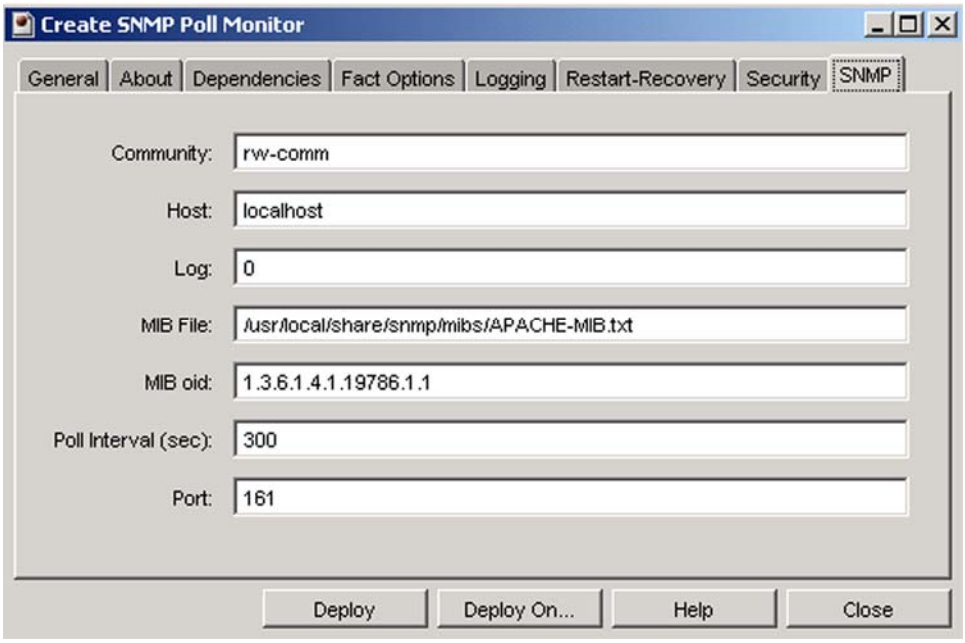

Figure 4-15. SNMP Poll Monitor Expert: SNMP

7. Click **Deploy**. The deployment message will confirm the name and location of the expert. Click **OK**. Or, click **Deploy On** to deploy on multiple managed nodes.
8. The deployed expert will be displayed under the node they were deployed on, as in the sample below. The facts produced by each expert are defined in Chapter 5: *AutoPilot/SNMP Configuration Metrics*.

4.2.1 Getting SNMP Facts from M6-WMQ SNMP Agent

An example of using the SNMP Poll monitor to obtain facts from the M6-WMQ SNMP Agent is described in the following procedure:

1. Set the MIB file to `[AUTOPILOT_HOME]\mibs\nsqMQSeries.mib`
2. Set the MIB OID to an object identifier value that determines the MIB objects that will be displayed.

Each MIB OID starts with the *common* OID path 1.3.6.1.4.1.1796, which is shown in the following table. Refer to `[APWMQ_HOME]\trapd.imq` and `nsqMQSeries.mib` to see the trap and object OID's, respectively.

4-12. MIB OID Description and Text Path

MIB OID	Description	Text Path
<*common*>	Display all events and objects in the MIB	iso.org.dod.internet.private.enterprises.Nastel
<*common*>.1.1.1.1.1.1	Event trap generation control: true or false	.nsMiddleware.nsMessaging.nsMqSeries.nsMIBObjects .nsMIBTransient.nsMqControlTrap
<*common*>.1.1.1.1.1.2	WMQ and AP-M6 WMQ events	.nsMiddleware.nsMessaging.nsMqSeries.nsMIBObjects . nsMIBTransient.nsMqEvent
<*common*>.1.1.1.1.2	Properties of workgroup manager	.nsMiddleware.nsMessaging.nsMqSeries.nsMIBObjects . nsManager
<*common*>.1.1.1.1.3	Properties of workgroup nodes	.nsMiddleware.nsMessaging.nsMqSeries.nsMIBObjects . nsMqNode
<*common*>.1.1.1.1.4	Properties of all queue managers of all nodes	.nsMiddleware.nsMessaging.nsMqSeries.nsMIBObjects . nsMqMgr
<*common*>.1.1.1.1.5	Properties of all channels	.nsMiddleware.nsMessaging.nsMqSeries.nsMIBObjects . nsMqChannel
<*common*>.1.1.1.1.6	Properties of all process definitions	.nsMiddleware.nsMessaging.nsMqSeries.nsMIBObjects . nsMqProcess

4.2.2 To get MIB-2 Standard System Information

Use the following MIB OID to get MIB-2 system information:

1.3.6.1.2.1.1 (iso.org.dod.internet.mgmt.mib-2.system)

4.3 Monitoring SNMP Agents with AP/SNMP Plug-in

Use the following steps to begin monitoring SNMP device:

1. Configure device with SNMP Agent.
2. Obtain MIB and place in MIB directory on AutoPilot.
3. Configure and deploy the Trap Monitor and Poll Monitor experts as described in Sections 4.1 and 4.2.

Chapter 5: AP/SNMP Configuration Metrics

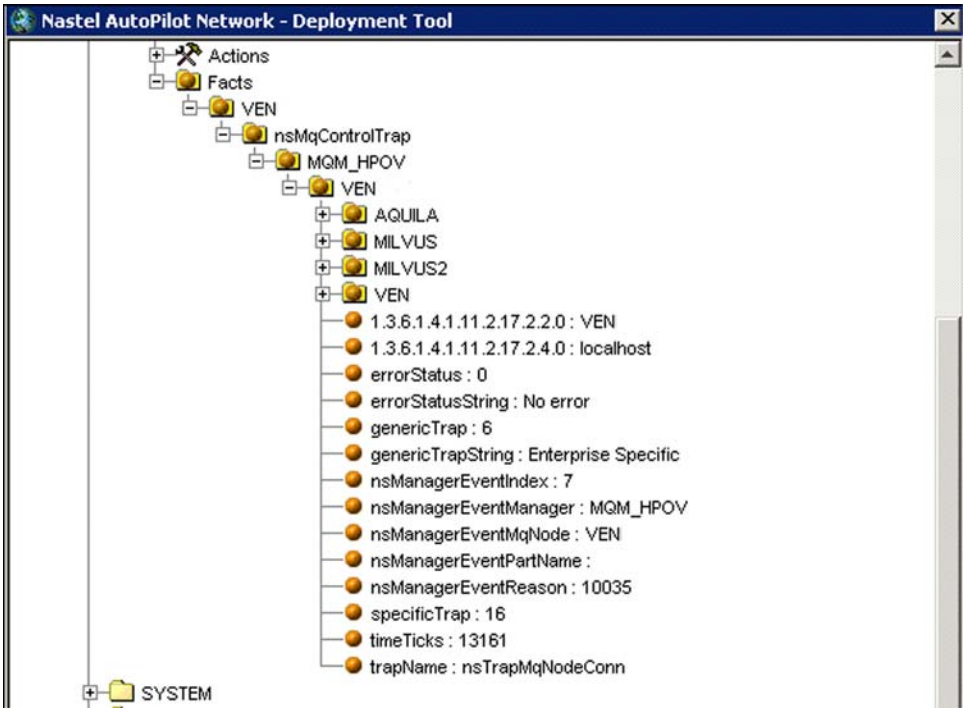

Figure 5-1. Example of SNMP Expert Facts

Metrics published by SNMP Poll and Trap monitors depend on the type of SNMP device and MIB definitions. Figure 5-1 above illustrates metrics collected for an event (Reason Code 10035) in the database of an AutoPilot/WMQ workgroup server running with workgroup named MQM_HPOV on node VEN.

This page intentionally left blank

Appendix A: References

A.1 Nastel Documentation

M6/USR 600.007 *Nastel AutoPilot M6 User's Guide*
M6/INS 600.007 *Nastel AutoPilot M6 Installation Guide*
M6WMQ/ADM 600.002 *Nastel AutoPilot M6 for WebSphere MQ Administrator's Guide*
M6WMQ/SM 600.002 *Nastel AutoPilot M6 for WebSphere MQ Security Manager User's Guide*
M6WMQ/WMMF 600.001 *Nastel AutoPilot M6 for WebSphere MQ Web Message Management Facility User's Guide*
M6WMQ 600.001 *WebSphere MQ Plug-in for AutoPilot M6*

A.2 Java™

http://java.sun.com/products/JavaManagement/reference/docs/index.html
http://www.hp.com/products1/unix/java/infolibrary/index.html
http://developer.java.sun.com/developer/technicalArticles/Servlets/corba/

This page intentionally left blank

Appendix B: Conventions

B.1 Typographical Conventions

B-1. Typographical Conventions

Convention	Description
Blue/Underlined	Used to identify links to referenced material or websites. Example: support@nastel.com
Bold Print	Used to identify topical headings, glossary entries, and toggles or buttons used in procedural steps. Example: Click **EXIT**.
Italic Print	Used to place emphasis on titles, menus, screen names, or other categories.
Monospaced Bold	Used to identify keystrokes/data entries, file names, directory names etc.
Monospaced Italic	Used to identify variables in an address location. Example: `[C:\AUTOPILOT_HOME]\documents`, where the portion of the address in brackets [ ] is variable.
Monospaced Text	Used to identify addresses, commands, scripts, etc.
Normal Text	Typically used for general text throughout the document.
Table Text	Table text is generally a smaller size to conserve space. 10, 9, and 8 point type is used in tables through the AutoPilot product family documents.

This page intentionally left blank

Glossary

This appendix contains a list of reference material and documents relevant to M6-WMQ and other related Nastel products.

AutoPilot M6: Nastel Technologies' Enterprise Application Management Platform. AutoPilot M6 monitors and automates the management of *e*Business integration components such as middleware application, application servers and user applications.

AP-WMQ: Nastel Technologies' WebSphere MQ management solution. Re-designated as AutoPilot for WebSphere MQ with release 4.0. Abbreviated as AP-WMQ and AP-WMQ.

AutoPilot/WebSphere (AP/WS): AutoPilot/WebSphere Server enables AutoPilot M6 to monitor and manage *e*Business applications for continuous operations in addition to its standard features.

AutoPilot/WebSphere Message Queue Integrator (AP-WMQI): Formerly AP/MQSI.

BSV: *see* Business Views.

Business View (BSV): A collection of rules that define a desired state of an *e*Business environment. Business Views can be tailored to presents information in the form most suited to a given user, as defined by the user.

CEP Server: A container that can host any number of AutoPilot M6 services such as experts, managers, policies etc. Unlike managed nodes, it is a physical process.

Client: Any programming component that uses the AutoPilot M6 infrastructure; for example, the AutoPilot M6 Console.

Common Object Request Broker Architecture (CORBA): A Common Object Request Broker Architecture (CORBA) object can be invoked from a Web browser using CGI scripts or applets.

Console: The console acts as the graphical interface for AutoPilot M6.

Contacts: A subordinate to a given Manager or Expert.

CORBA: *see* Common Object Request Broker Architecture.

Data Source Name: A Data Source Name (DSN) is the logical name that is used by Open Database Connectivity (ODBC) to refer to the drive and other information that is required to access data. The name is use by Internet Information Services (IIS) for a connection to an ODBC data source, (Example: Microsoft SQL Server database). The ODBC tool in Control Panel is used to set the DSN. When ODBC DSN entries are used to store the connection string values externally, you simplify the information that is needed in the connection string. This makes changes to the data source completely transparent to the code itself.

Dependent WebSphere MQ Node: WebSphere MQ nodes that are not directly managed by M6-WMQ. Because dependent nodes do not run an MQ WMQ Agent, they must be managed by proxy.

Deploy: To put to use, to position for use or action.

Domain Server: A specialized managed node that maintains the directory of managed nodes, experts etc. The domain server is also capable of hosting experts, managers etc.

DSN: *see* Data Source Name

EVT: Event Log file extension (e.g.: *sample.evt*).

Event: An *Event* is something that happens to an object. Events are logged by AutoPilot M6 and are available for use by AutoPilot M6 Policies or the user.

Expert: Services that monitor specific applications such as an applications server, web-server or specific components within the applications. (Example, channels in WebSphere MQ.) Experts generate facts.

Fact: Facts are single pieces of data that has a unique name and value. One or more facts are used to determine the health of the object, application or server.

Graphical User Interface (GUI): A type of environment that represents programs, files, and options by means of icons, menus, and dialog boxes on the screen. The user can select and activate these options by pointing and clicking with a mouse or, often, with the keyboard. Because the graphical user interface provides standard software routines to handle these elements and report the user's actions (such as a mouse click on a particular icon or at a particular location in text, or a key press); applications call these routines with specific parameters rather than attempting to reproduce them from scratch.

GUI: *see* Graphical User Interface.

Independent WebSphere MQ Node: A WebSphere MQ node that runs a WMQ Agent and which is managed directly by a workgroup server. Independent nodes can be used as proxy nodes for managing dependent nodes.

IIS: *See* Internet Information Services.

Internet Information Services: Microsoft's brand of Web server software, utilizing HTTP to deliver World Wide Web documents. It incorporates various functions for security, allows CGI programs, and also provides for Gopher and FTP services.

JCL: *See* Job Control Language

Java: A platform-independent, object-oriented programming language developed and made available by Sun Microsystems.

Java Developer's Kit (JDK): A set of software tools developed by Sun Microsystems, Inc., for writing Java applets or applications. The kit, which is distributed free, includes a Java compiler, interpreter, debugger, viewer for applets, and documentation.

JDBC: *See* Java Database Connectivity.

Java Database Connectivity (JDBC): The JDBC API provides universal data access from the Java programming language. Using the JDBC 2.0 API, you can access virtually any data source, from relational databases to spreadsheets and flat files. JDBC technology also provides a common base on which tools and alternate interfaces can be built. The JDBC *Test Tool* that was developed by Merant and Sun Microsystems may be used to test drivers, to demonstrate executing queries and getting results, and to teach programmers about the JDBC API.

Java Server Pages (JSP): JSP technology enables rapid development of web-based applications that are platform independent. Java Server Pages technology separates the user interface from content generation enabling designers to change the overall page layout without altering the underlying dynamic content. Java Server Pages technology is an extension of the Java™ Servlet technology.

Java Virtual Machine (JVM): The "virtual" operating system that JAVA-written programs run. The JVM is a hardware- and operating system-independent abstract computing machine and execution environment. Java programs execute in the JVM where they are protected from malicious programs and have a small compiled footprint.

JDBC: *See* Java Database Connectivity

JDK: *See* Java Developer's Kit.

Job Control Language (JCL): Most commonly used in larger computer systems, JCL is any control language that controls the execution of applications. The syntax is usually strict; not permitting the addition or deletion or spaces or characters where they are not expected.

JRE: JAVA Run-time Environment. The minimum core JAVA required to run JAVA Programs.

JSP: *See* Java Server Pages

JVM: *see* JAVA Virtual Machine.

M6 for WMQ: Nastel Technologies' WebSphere MQ management solution. Re-designated as M6 for WMQ with release 6.0, prior releases retain the AP-WMQ or MQControl trademark.

M6 Web: A browser-based interface that provides monitoring and operational control over managed resources and applications.

Managed Node: A container that can host any number of AutoPilot M6 services such as experts, managers, policies etc. Unlike managed nodes, it is a physical process. Renamed CEP Server in M6 with Service Pack 6.

Management Information Base (MIB): A specification that describes the properties and behavior of a network device. Network managers use MIBs to interact with SNMP-compatible devices. Each MIB is part of a directory structure that specifies where objects are found on the network.

Manager: Managers are the home or container for policies. All business views must reside on managers, and manager must be deployed prior to deploying a business view or policy.

Message Management Facility (MMF): Nastel's message management service.

Message Queue Interface: The Message Queue Interface (MQI) is part of IBM's Networking Blueprint. It is a method of program-to-program communication suitable for connecting independent and potentially non-concurrent distributed applications.

MIB: *see* Management Information Base

MMF: *see* Message Management Facility

MOM: *see* Message-Oriented Middleware.

MQControl: Nastel Technologies' MQSeries management product. Re-designated as AP-WMQ with release 4.0 and M6 for WMQ with release 6.0. Prior releases retain the MQControl trademark.

MQI: *see* Message Queue Interface

MQSC: See WebSphere MQ Commands

MQSeries: IBM's message queuing product. Renamed by IBM as WebSphere MQ.

Naming Service: A common server records "names" of objects and associates them with references, locations and properties

ORB: Object Request Broker.

Orbix: CORBA product distributed by IONA Technologies.

Package Manager: The command line utility that allows users to list, install, uninstall, verify and update AutoPilot M6 installation on any Managed Node.

PCF: See Programmable Command Format

PKGMAN: *see* Package Manager

Policy/Business Views: Business views are a collection of one or more sensors. Business views are used to visually present the health and status of the different systems as well as automatically issue remedial actions.

Programmable Command Format (PCF): A set of programmable commands that M6-WMQ uses to manage WebSphere MQ. PCF includes data definitions for items such as integers, strings, and lists. The commands can be submitted directly to a queue manager. PCF is comparable to MQSC, except for the fact that MQSC cannot be programmed.

Proxy Management: The indirect management of MQ objects by an intermediate entity. For example, a proxy queue manager might be used to handle another queue manager.

Sensor: A rule that is used to determine the health of an object or application based on one or more facts. Actions can then be issued, based on the health. Sensors are definable in business views by use of the sensor wizard.

Simple Mail Transfer Protocol (SMTP): A TCP/IP protocol for sending messages from one computer to another on a network. This protocol is used on the Internet to route e-mail. *See also* communications protocol, TCP/IP. *Compare* CCITT X series, Post Office Protocol.

Simple Network Management Protocol (SNMP): A de facto standard for managing hardware and software devices on a network. Each device is associated with a Management Information Base (MIB) that describes its properties and behavior.

SMTP: *see* Simple Mail Transfer Protocol

SNMP: *see* Simple Network Management Protocol

SNMP Master Agent: An implementation of the SNMP protocol. It includes a definition of the standard MIB. The master agent routes SNMP requests from subagent to subagent.

SNMP Subagent: The implementation of an MIB for a particular device. The MIB describes the device's desired behavior; the SNMP subagent carries it out.

TCP/IP: *see* Transmission Control Protocol/Internet Protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP): A protocol developed by the Department of Defense for communications between computers. It is built into the UNIX system and has become the de facto standard for data transmission over networks, including the Internet.

Virtual Machine: Software that mimics the performance of a hardware device, such as a program that allows applications written for an Intel processor to be run on a Motorola chip. *Also See* Java Virtual Machine.

WebSphere MQ: IBM's message queuing product. Formally known as MQSeries.

WebSphere MQ Commands: A command-line language used to configure WebSphere MQ.

Websphere_MQ_Manager: A specialized manager capable of hosting one or more WebSphere MQ specific policies, apart from the regular policies.

Wireless Application Protocol (WAP): An open global specification that is used by most mobile telephone manufacturers. WAP determines how wireless devices utilize Internet content and other services. WAP enables devices to link diverse systems contents and controls.

z/OS: *see* Z Series Operating System.

Z Series Operating System: IBM architecture for mainframe computers and peripherals. The zSeries family of servers uses the z/Architecture. It is the successor to the S/390 and 9672 family of servers.