

AutoPilot[®] for IBM DataPower

Version 1.2.0

Installation and User's Guide

CONFIDENTIALITY STATEMENT: THE INFORMATION WITHIN THIS MEDIA IS PROPRIETARY IN NATURE AND IS THE SOLE PROPERTY OF NASTEL TECHNOLOGIES, INC. ALL PRODUCTS AND INFORMATION DEVELOPED BY NASTEL ARE INTENDED FOR LIMITED DISTRIBUTION TO AUTHORIZED NASTEL EMPLOYEES, LICENSED CLIENTS, AND AUTHORIZED USERS. THIS INFORMATION (INCLUDING SOFTWARE, ELECTRONIC AND PRINTED MEDIA) IS NOT TO BE COPIED OR DISTRIBUTED IN ANY FORM WITHOUT THE EXPRESSED WRITTEN PERMISSION FROM NASTEL TECHNOLOGIES, INC.

PUBLISHED BY:

RESEARCH & DEVELOPMENT
NASTEL TECHNOLOGIES, INC.
88 SUNNYSIDE BLVE, SUITE 101
PLAINVIEW, NY 11803

COPYRIGHT © 2017. ALL RIGHTS RESERVED. NO PART OF THE CONTENTS OF THIS DOCUMENT MAY BE PRODUCED OR TRANSMITTED IN ANY FORM, OR BY ANY MEANS WITHOUT THE WRITTEN PERMISSION OF NASTEL TECHNOLOGIES.

DOCUMENT TITLE: **AUTOPILOT® FOR IBM DATAPOWER INSTALLATION AND USER'S GUIDE**

VERSION: **1.2.0**

DOCUMENT RELEASE DATE: **AUGUST 2017**

NASTEL DOCUMENT NUMBER: **DP 120.004**

CONFIDENTIALITY STATEMENT: THE INFORMATION WITHIN THIS MEDIA IS PROPRIETARY IN NATURE AND IS THE SOLE PROPERTY OF NASTEL TECHNOLOGIES, INC. ALL PRODUCTS AND INFORMATION DEVELOPED BY NASTEL ARE INTENDED FOR LIMITED DISTRIBUTION TO AUTHORIZED NASTEL EMPLOYEES, LICENSED CLIENTS, AND AUTHORIZED USERS. THIS INFORMATION (INCLUDING SOFTWARE, ELECTRONIC AND PRINTED MEDIA) IS NOT TO BE COPIED OR DISTRIBUTED IN ANY FORM WITHOUT THE EXPRESSED WRITTEN PERMISSION FROM NASTEL TECHNOLOGIES, INC.

ACKNOWLEDGEMENTS:

THE FOLLOWING TERMS ARE TRADEMARKS OF NASTEL TECHNOLOGIES CORPORATION IN THE UNITED STATES OR OTHER COUNTRIES OR BOTH: TRANSACTIONWORKS, M6 AUTOPILOT, AUTOPILOT/IT, AUTOPILOT/ENTERPRISE, M6 FOR WMQ, AUTOPILOT/WMQ, M6 WEB SERVER, M6 WEB CONSOLE, AUTOPILOT/WEB, MQCONTROL, MQCONTROL EXPRESS, AUTOPILOT/TRANSACTION ANALYZER, AUTOPILOT/WAS, AUTOPILOT/TRANSACTION MONITOR, AUTOPILOT/OS MONITOR

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

THE FOLLOWING TERMS ARE TRADEMARKS OF HEWLETT-PACKARD IN THE UNITED STATES OR OTHER COUNTRIES OR BOTH: OPENVIEW, HP-UX

COMPAQ, THE COMPAQ LOGO, ALPHASERVER, COMPAQ INSIGHT MANAGER, CDA, DEC, DECNET, TRUCLUSTER, ULTRIX, AND VAX REGISTERED IN U.S. PATENT AND TRADEMARK OFFICE. ALPHA AND TRU64 ARE TRADEMARKS OF COMPAQ INFORMATION TECHNOLOGIES GROUP, L.P IN THE UNITED STATES AND OTHER COUNTRIES

SNMPC, SNMPC, WORKGROUP, AND SNMPC ENTERPRISE ARE TRADEMARKS OF CASTLE ROCK COMPUTING IN THE UNITED STATES OR OTHER COUNTRIES, OR BOTH.

SUN, SUN MICROSYSTEMS, THE SUN LOGO, IFORCE, JAVA, NETRA, N1, SOLARIS, SUN FIRE, SUN RAY, SUNSPECTRUM, SUN STOREDGE, SUNTONE, THE NETWORK IS THE COMPUTER, ALL TRADEMARKS AND LOGOS THAT CONTAIN SUN, SOLARIS, OR JAVA, AND CERTAIN OTHER TRADEMARKS AND LOGOS ARE TRADEMARKS OR REGISTERED TRADEMARKS OF SUN MICROSYSTEMS, INC. IN THE UNITED STATES AND OTHER COUNTRIES.

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/](http://www.apache.org/)). THE "JAKARTA PROJECT" AND "TOMCAT" AND THE ASSOCIATED LOGOS ARE REGISTERED TRADEMARKS OF THE APACHE SOFTWARE FOUNDATION

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.

"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.

SCO CUSA, SCO DOCTOR, SCO DOCTOR FOR NETWORKS, SCO DOCTOR LITE, SCO GLOBAL ACCESS, SCO MPX, SCO MULTIVIEW, SCO NIHONGO OPENSER, SCO OK, THE SCO OK LOGO, SCO OPENSER, SCO OPEN SERVER, SCO PORTFOLIO, SCO POS SYSTEM, SCO TOOLWARE, AND THE WORLD NEVER STOPS ARE TRADEMARKS OR REGISTERED TRADEMARKS OF CALDERA INTERNATIONAL, INC. IN THE U.S.A. AND OTHER COUNTRIES, ALL RIGHTS RESERVED.

ORACLE® IS A REGISTERED TRADEMARK OF ORACLE CORPORATION AND/OR ITS AFFILIATES

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

Contents

CHAPTER 1: INTRODUCTION	1
1.1 HOW THIS GUIDE IS ORGANIZED	1
1.2 HISTORY OF THIS DOCUMENT	1
1.3 RELATED DOCUMENTS.....	1
1.4 RELEASE NOTES.....	1
1.5 INTENDED AUDIENCE.....	2
1.5.1 <i>User Feedback</i>	2
1.6 TECHNICAL SUPPORT	2
1.7 TERMS AND ABBREVIATIONS	2
1.8 CONVENTIONS.....	2
CHAPTER 2: ABOUT DATAPOWER.....	3
CHAPTER 3: INSTALLATION, DEPLOYMENT, AND CONFIGURATION	5
3.1 BEFORE INSTALLATION	5
3.1.1 <i>Technical Documents</i>	5
3.1.2 <i>Installation Requirements</i>	5
3.2 INSTALLATION	5
3.3 DEPLOYMENT.....	6
3.4 AUTOPILOT EXPERT CONFIGURATION	7
3.4.1 <i>SNMP Expert</i>	7
3.4.2 <i>SNMP Trap Expert</i>	9
3.4.3 <i>Syslog Expert</i>	10
3.5 METRIC COLLECTION.....	12
3.6 DATAPOWER CONFIGURATION	12
3.6.1 <i>DataPower SNMP Configuration</i>	14
3.6.2 <i>DataPower SNMP Trap Configuration</i>	16
3.6.3 <i>DataPower Syslog Data Capture</i>	17
3.6.4 <i>DataPower WSDM Data Capture</i>	18
CHAPTER 4: DELETED	19
CHAPTER 5: TROUBLESHOOTING SERVER CONFIGURATION ISSUES.....	21
APPENDIX A: REFERENCES	23
A.1 NASTEL DOCUMENTATION.....	23
A.2 OTHER DOCUMENTATION	23
APPENDIX B: CONVENTIONS.....	25
B.1 TYPOGRAPHICAL CONVENTIONS.....	25
APPENDIX C: SAMPLE APPLICATION XSD.....	27
GLOSSARY	33

Figures

FIGURE 2-1. BASIC AUTOPILOT ARCHITECTURE	3
FIGURE 3-1. CEP SERVER POPUP MENU	6
FIGURE 3-2. CREATE DATAPOWERSERVERS DIALOG BOX	6
FIGURE 3-3. DEPLOYMENT CONFIRMATION DIALOG BOX	6
FIGURE 3-4. DEPLOYMENT SUCCESSFUL DIALOG BOX	7
FIGURE 3-5. DATAPOWER APPLIANCES	7
FIGURE 3-6. SNMP CONFIGURATION	8
FIGURE 3-7. SNMP TRAPS PROPERTIES – SNMP	9
FIGURE 3-8. SNMP TRAPS PROPERTIES – TRAPS	10
FIGURE 3-9. SYSLOGSERVER PROPERTIES – SYSLOG OPTIONS	11
FIGURE 3-10. METRIC COLLECTION.....	12
FIGURE 3-11. DATAPOWER REGISTRY POPUP MENU.....	12
FIGURE 3-12. SERVER PROFILE DIALOG BOX	13
FIGURE 3-13. CONFIGURE SNMP SETTINGS – MAIN TAB.....	14
FIGURE 3-14. CONFIGURE SNMP SETTINGS – ENTERPRISE MIBs TAB	15
FIGURE 3-15. CONFIGURE SNMP SETTINGS – SNMPv1/v2c COMMUNITIES TAB.....	15
FIGURE 3-16. CONFIGURE SNMP SETTINGS – TRAP AND NOTIFICATION TARGETS TAB	16
FIGURE 3-17. CONFIGURE SNMP SETTINGS – TRAP EVENT SUBSCRIPTIONS TAB	16
FIGURE 3-18. CONFIGURE LOG TOPIC – MAIN TAB	17
FIGURE 3-19. CONFIGURE LOG TOPIC – MAIN TAB	18

Tables

TABLE 1-1. DOCUMENT HISTORY	1
TABLE 3-1. SNMP SETTINGS.....	8
TABLE 3-2. SNMP TRAPS PROPERTIES – SNMP	9
TABLE 3-3. SNMP TRAPS PROPERTIES – TRAPS	10
TABLE 3-4. SYSLOGSERVER PROPERTIES – SYSLOG OPTIONS	11
TABLE 3-5. SERVER PROFILE SETTINGS.....	13
TABLE A-1. NASTEL DOCUMENTATION	23
TABLE B-1. TYPOGRAPHICAL CONVENTIONS	25

Chapter 1: Introduction

Welcome to the *Nastel AutoPilot for IBM DataPower Installation and User's Guide*. This guide describes installation, configuration, and deployment. Please review this guide carefully before installing and using the product.

1.1 How This Guide is Organized

- [Chapter 1:](#)** Identifies the users and history of the document as well as supplying support and reference information.
- [Chapter 2:](#)** A brief overview of AutoPilot for IBM DataPower.
- [Chapter 3:](#)** Describes AutoPilot for IBM DataPower installation, deployment, and configuration.
- [Chapter 4:](#)** Deleted
- [Chapter 5:](#)** Describes server configuration issues.
- [Appendix A:](#)** Provides a list of reference information for using AutoPilot for IBM DataPower.
- [Appendix B:](#)** Contains conventions used in this document.
- [Appendix C:](#)** Provides a sample application XSD.
- [Glossary:](#)** Contains a listing of unique and common acronyms and words and their definition.

1.2 History of this Document

Release Date	Document Number	AutoPilot for DataPower Version	Summary
November 2011	DP 100.001	1.0.2	Initial release
February 2014	DP 120.001	1.2.0	Mantis 8219 – include instructions on configuring SNMP DataPower Collection. Mantis 8490 – DataPower version 6 support
August 2015	DP 120.002	1.2.0	Errata
April 2017	DP 120.003	1.2.0	Remove Chapter 4
August 2017	DP 120.004	1.2.0	Update Nastel's phone numbers and address

1.3 Related Documents

A complete listing of related and referenced documents is in [Appendix A](#) of this guide.

1.4 Release Notes

See the **README.htm** files on your installation media or AutoPilot for DataPower installation directory. Release notes and updates are also available through the Nastel Resource Center at: <http://customers.nastel.com>.

1.5 Intended Audience

This document is intended for personnel installing, configuring, and using AutoPilot for DataPower.

1.5.1 User Feedback

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

1.6 Technical Support

If you need additional technical support, you can contact Nastel 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 **001-516-801-2100**.
- To contact Nastel technical support by e-mail, send a message to support@nastel.com.
- To contact Nastel technical support through the support website (user ID and password are required), go to <http://support.nastel.com>, or visit the Nastel Resource Center at: <http://www.nastel.com/resources>.

Contact your local AutoPilot for DataPower administrator for further information.

1.7 Terms and Abbreviations

A list of terms and abbreviations used in all AutoPilot documents is located in the [Glossary](#).

1.8 Conventions

Refer to [Appendix B](#) for typographical and naming conventions used in all AutoPilot documentation.

Chapter 2: About DataPower

The following IBM products are complete hardware platforms for delivering highly manageable, secure, and scalable integration solutions:

- WebSphere® DataPower® Integration Appliance XI50/XI52
- WebSphere DataPower Integration Blade XI50B
- WebSphere DataPower Integration Appliance for zEnterprise (XI50z).

For more information, visit IBM at <http://www-01.ibm.com/software/integration/datapower/xi50/>.

Architecture Review

The diagram below shows the basic AutoPilot architecture. DataPower information is collected as both environmental and transactional data.

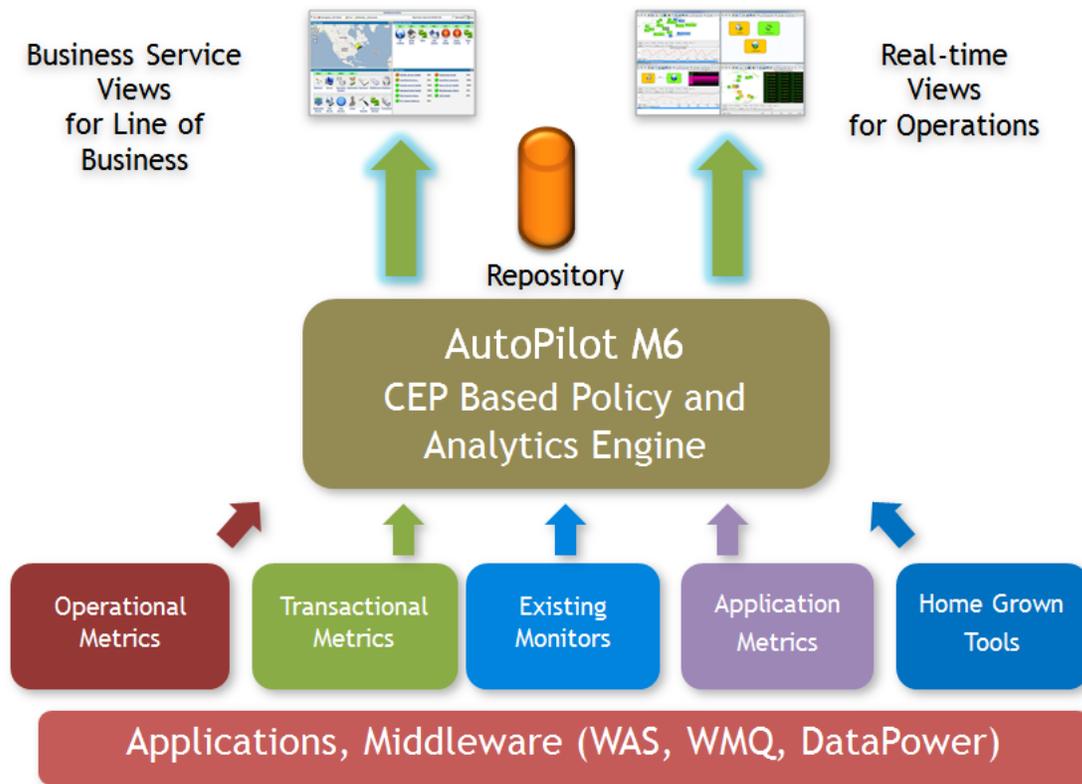


Figure 2-1. Basic AutoPilot Architecture

This page intentionally left blank.

Chapter 3: Installation, Deployment, and Configuration

This chapter provides information on the following topics:

- [Section 3.1](#) Setup requirements
- [Section 3.2](#) Installation
- [Section 3.3](#) Deployment
- [Section 3.4](#) AutoPilot Expert Configuration
- [Section 3.5](#) Metric Collection
- [Section 3.6](#) DataPower Configuration

3.1 Before Installation

The procedures in this chapter cover the installation of the AutoPilot for DataPower.

3.1.1 Technical Documents

Prior to installation you should review all text files and installation procedures. You should print, as needed, all of the installation-related materials to give yourself quick access to any required information during any installation procedures. Additional sets of printed documents are available from your Nastel representative or Nastel Support.

3.1.2 Installation Requirements

In order to install the product, the following pre-requisite products must be installed:

- AutoPilot with SU20
- Group Expert Framework 2.3.2 (AP_CORE_GEF-2.3.2.pkg)
- DataPower firmware 6.0 or higher.

3.2 Installation

1. Copy the package file to <APHOME>/updates.
2. Stop the CEP Server instance and other AutoPilot M6 services on the server.
3. Run package manager to install the pre-requisites and the expert.

For example:

```
<APHOME>/bin/pkgman <APHOME>/updates/AP_DATAPOWER-<version>.pkg
```

4. Restart the CEP Server instance and other AutoPilot M6 services on the server.

3.3 Deployment

1. Start the AutoPilot Enterprise Manager.
2. Right click the CEP Server and select **Deploy Expert > DataPower > DataPowerServers**.

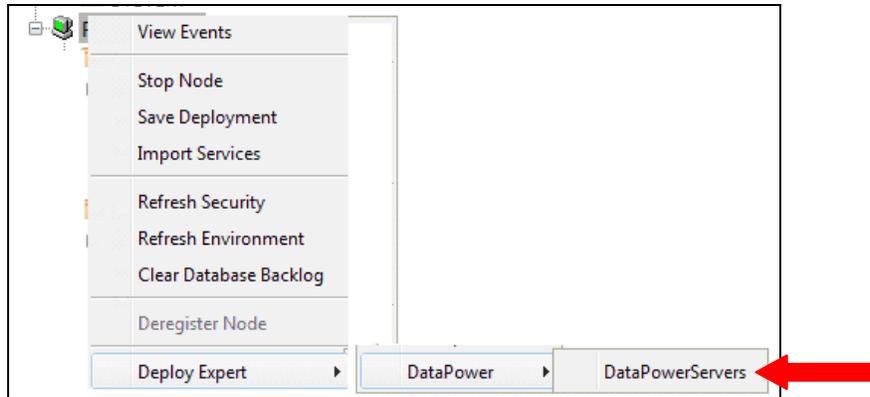


Figure 3-1. CEP Server Popup Menu

3. The *Create DataPowerServers* dialog box is displayed.

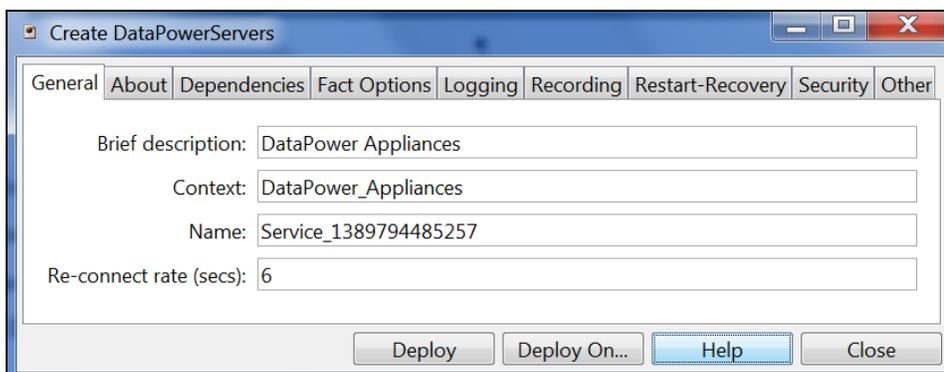


Figure 3-2. Create DataPowerServers Dialog Box

4. Leave all the defaults except for:
 - **Name** – can be changed to a more meaningful value
 - **Re-connection rate(secs)** – adjust to 1 minute or as required
5. Click **Deploy**. A confirmation window is displayed.

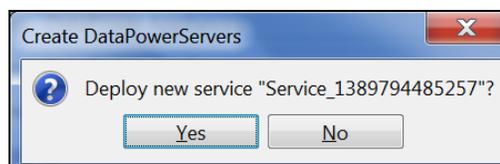


Figure 3-3. Deployment Confirmation Dialog Box

6. Click **Yes** to deploy or **No** to cancel. If you clicked **Yes**, a dialog box confirms the action.

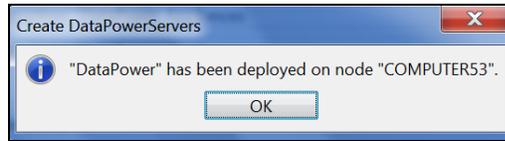


Figure 3-4. Deployment Successful Dialog Box

7. Click **OK**.

3.4 AutoPilot Expert Configuration

In addition to the DataPower Expert installed in [section 3.3](#), the following additional experts are required to capture additional facts from DataPower. If desired, they can be deployed with the Category and Name combinations indicated in Figure 3-5.

- SNMP Expert ([section 3.4.1](#))
- SNMP Trap Expert ([section 3.4.2](#))
- Syslog Expert ([section 3.4.3](#)).

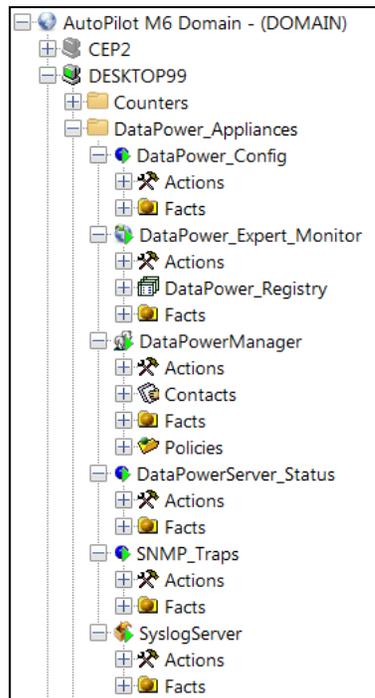


Figure 3-5. DataPower Appliances

3.4.1 SNMP Expert

- Deploy the SNMP Expert (refer to the AutoPilot M6 for SNMP Installation and User's Guide)
- Configure the expert ([section 3.4.1.1](#))
- SNMP must be enabled in DataPower ([section 3.6.1](#)).

	<p>NOTE:</p>	<p>The steps below are used for two types of SNMP traps for config mib or status mib. Either, or both, can be deployed, depending on requirements.</p>
--	---------------------	--

3.4.1.1 Configuring the SNMP Expert

1. Right click **DataPower_Config** and select **Properties**.
2. The *DataPower_Config Properties* dialog box is displayed.

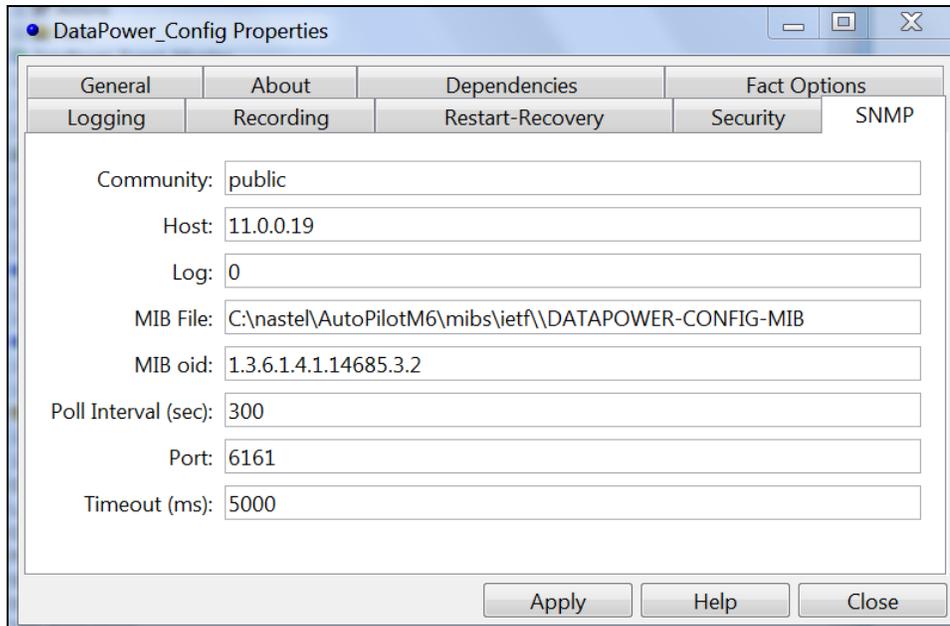


Figure 3-6. SNMP Configuration

Table 3-1. SNMP Settings

Field	Description
Community	SNMP Read Community. This value comes from DataPower. (See Figure 3-15 .)
Host	SNMP host where SNMP agent is located
Log	Whether to log to System.out or not (0 = do not log, 1 = log)
MIB File	Location of MIB file. This is the file where you saved the MIBs downloaded from Figure 3-14 . You must save the MIB using its full name, e.g. DATAPOWER-CONFIG-MIB or DATAPOWER-STATUS-MIB. The mibs can be extracted from the DataPower device, but must be saved as these names.
MIB oid	Start scanning at this OID, that is where to start in the tree – “walk the mib”. For the config MIB, value shown is the required value. For the status MIB, the oid is the one ending in 3.1.
Poll Interval (sec)	Interval to poll the SNMP server
Port	Port to poll SNMP host
Timeout (ms)	SNMP socket timeout intervals in ms

3.4.2 SNMP Trap Expert

- Deploy the SNMP Trap expert (refer to the AutoPilot M6 for SNMP Installation and User's Guide)
- Configure the expert ([section 3.4.2.1](#))
- SNMP must be setup in DataPower ([section 3.6.1](#)).

3.4.2.1 Configuring the SNMP Trap Expert

1. Right click **SNMP_Traps** and select **Properties**.
2. The *SNMP_Traps Properties* dialog box is displayed.

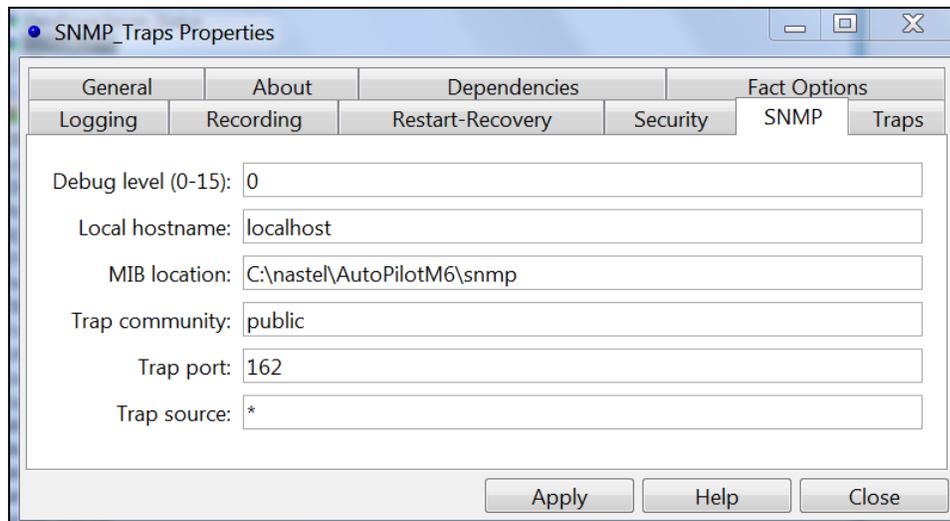


Figure 3-7. SNMP Traps Properties – SNMP

Field	Description
Debug level (0-15)	SNMP debug level, 0 is the lowest
Local hostname	Name of localhost (optional)
MIB location	Comma separated list of directories where MIBs are located
Trap community	Receiving trap community name. This value comes from DataPower. (See Figure 3-15.)
Trap port	Listening trap port number
Trap source	Trap source mask

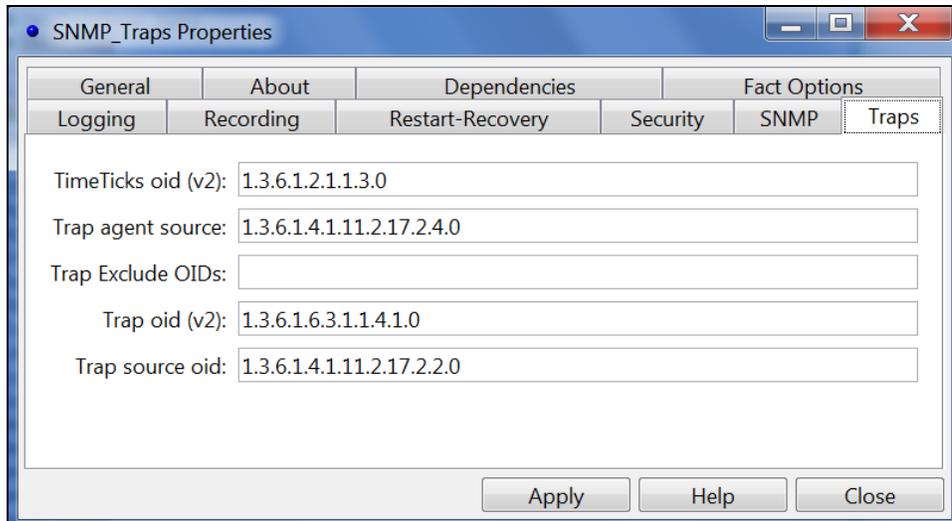


Figure 3-8. SNMP Traps Properties – Traps

Table 3-3. SNMP Traps Properties – Traps	
Field	Description
TimeTicks oid (v2)	OID that contains the values of timeticks (SNMP v2)
Trap agent source	Variable containing the source of the agent sending the trap
Trip Exclude OIDs	trap OID exclude list(comma or so semi-colon separated)
Trap oid (v2)	OID that contains the real OID of the trap (SNMP v2)
Trap source oid	Variable containing the real source of the trap

3.4.3 Syslog Expert

- Deploy the AIM Syslog Expert (refer to the AutoPilot M6 User's Guide)
- Configure the expert ([section 3.4.3.1](#))
- Syslog Data Capture must be setup in DataPower ([section 3.6.2](#)).

3.4.3.1 Configuring the Syslog Expert

1. Right click **SyslogServer** and select **Properties**.
2. The *SyslogServer Properties* dialog box is displayed.

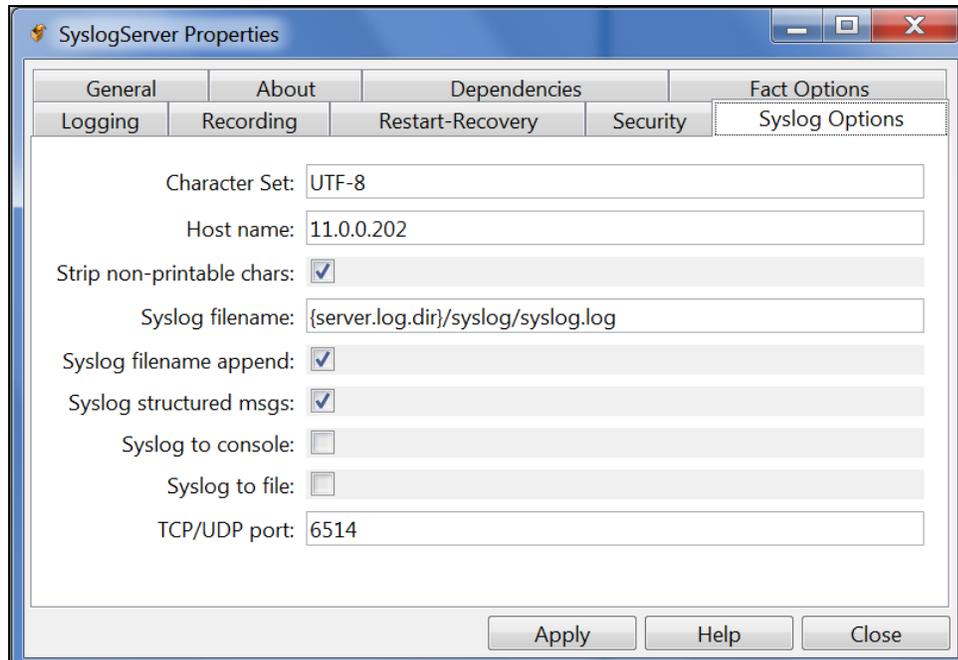


Figure 3-9. SyslogServer Properties – Syslog Options

Table 3-4. SyslogServer Properties – Syslog Options	
Field	Description
Character Set	The character set for received messages
Host name	Host name or IP address to be used for binding syslog server
Strip non-printable chars	Enable to automatically strip non-printable characters from event messages
Syslog filename	File where all syslog messages are recorded
Syslog filename append	Enable to append syslog messages on restart; otherwise clean restart
Syslog structured msgs	Enable to support syslog structured event messages
Syslog to console	Enable syslog output to a stdout (console)
Syslog to file	Enable syslog output to a logfile
TCP/UDP port	TCP/UDP port number to be used by syslog server (using TCP and UDP transports)

3.5 Metric Collection

The data shown will be presented by the DataPower Expert. This will be published each time the expert polls the DataPower device and the facts represent the last interval of data. Fact recording can be used to record a collection history.

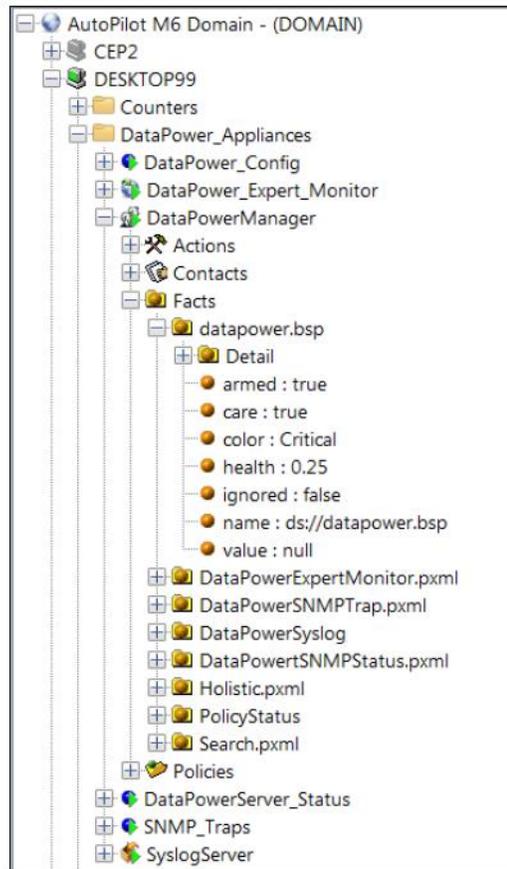


Figure 3-10. Metric Collection

3.6 DataPower Configuration

1. Right click **DataPower_Registry** and select **Add Server**.

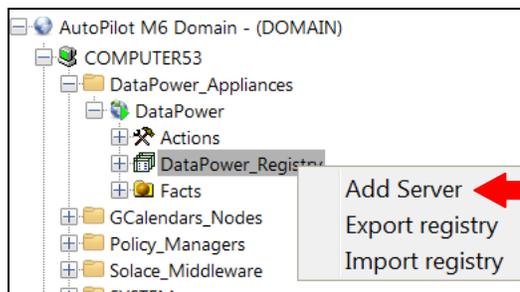


Figure 3-11. DataPower Registry Popup Menu

- The *Server profile* dialog box is displayed.

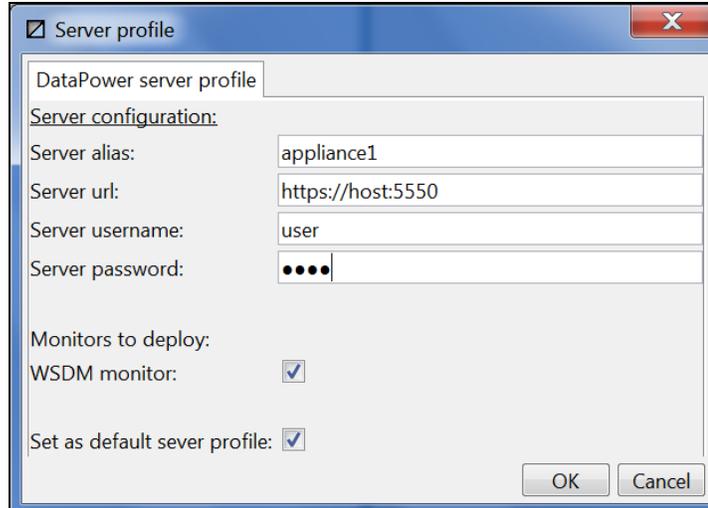


Figure 3-12. Server Profile Dialog Box

- Enter data per Table 3-5 and click **OK** to save your settings.

Table 3-5. Server Profile Settings	
Field	Description
Server alias	Name of the DataPower device as shown in AutoPilot fact tree. Required.
Server url	Connection string to connect to the DataPower Device XML Management Interface. NOTE: This is not the admin console URL. The default DataPower XML Management Interface port is 5550. Required.
Server username	The username of a user for the DataPower server with the following access rights: */*/?*Access=r Required.
Server password	The password for the administrative user for the DataPower server. Required.
Monitors to deploy: WSDM monitor	Identifies the type of service that will be used to collect the data. (Additional monitors may be added in the future.) Required.
Set as default server profile	Select to save this profile as the default for future server instances added. Optional.

3.6.1 DataPower SNMP Configuration

In order to collect data, the SNMP feature must be enabled on the DataPower appliance as shown in the figure below.

1. Navigate to the *Configure SNMP Settings* page by:

Admin > Access > SNMP Settings

2. On the **Main** tab, the following fields are required:

- **Administrative State** – select **enable**
- **Local IP Address**
- **Local Port**

The remainder fields are optional depending on your requirements. The Local IP Address can be configured specifically for management traffic or a standard IP can be used.

3. Click **Apply**.

The screenshot shows the 'Configure SNMP Settings' page with the 'Main' tab selected. The 'Administrative State' is set to 'enabled'. The 'Local IP Address' is 'ix52' and the 'Local Port' is '161'. Other fields include 'Comments' (SNMP Management Enabled), 'SNMPv3 Users' (empty), 'SNMPv3 Security Level' (Authentication, Privacy), and 'SNMPv3 Access Level' (read-only). The 'Apply' button is visible at the top left of the form area.

Figure 3-13. Configure SNMP Settings – Main Tab

You can also use the **Enterprise MIBs** tab (Figure 3-14) to download the MIBs used by DataPower which will need to be installed on the AutoPilot Server.

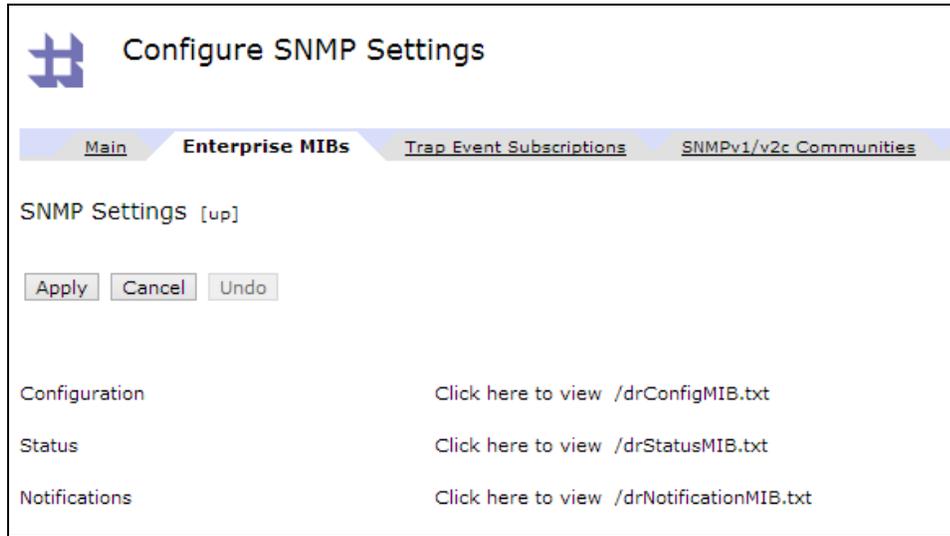


Figure 3-14. Configure SNMP Settings – Enterprise MIBs Tab

On the **SNMPv1/v2c Communities** tab define a public community that provides access to the management data as shown in the figure below. A **Remote Host Address** of 0.0.0.0/0 in the example below means anybody can connect.

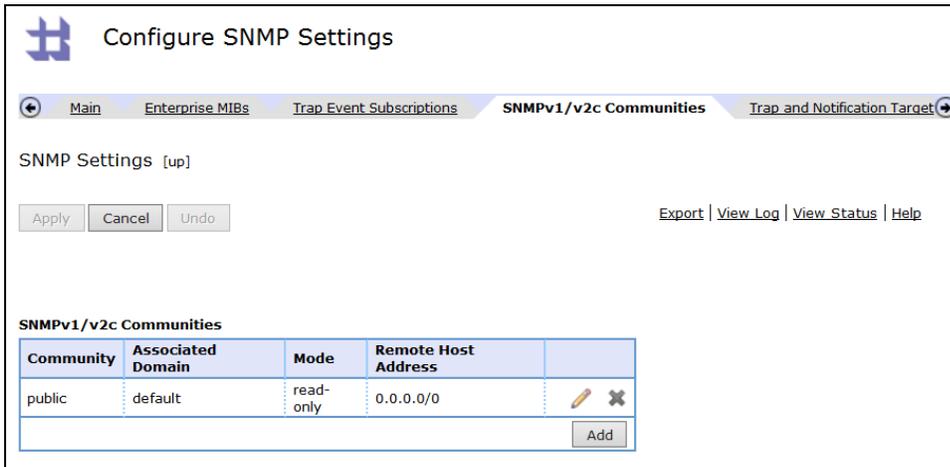


Figure 3-15. Configure SNMP Settings – SNMPv1/v2c Communities Tab

3.6.2 DataPower SNMP Trap Configuration

Optionally, the DataPower server can be configured to send SNMP traps to the AutoPilot server. When this is required, use the **Trap and Notification Targets** tab.



Figure 3-16. Configure SNMP Settings – Trap and Notification Targets Tab

The specific SNMP traps must also be configured. Alternatively, the syslog feature can be used to send similar log events. (Refer to [section 3.6.3.](#))

The **Trap Event Subscriptions** tab lists the traps that get sent.

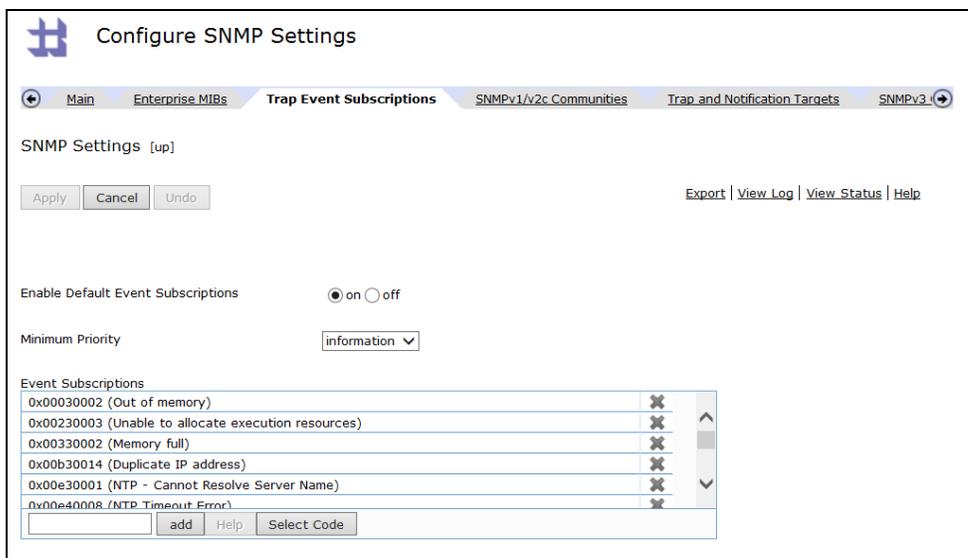


Figure 3-17. Configure SNMP Settings – Trap Event Subscriptions Tab

3.6.3 DataPower Syslog Data Capture

In order to collect data, a log target must be enabled on the DataPower appliance as shown in the figure below. The specific events required must also be configured.

1. Navigate to the *Configure Log Target* page by:

Admin > Miscellaneous > Manage Log Targets to display the *Configure Log Target* screen and click **Add**.

The screenshot shows the 'Configure Log Target' web interface. At the top, there is a navigation bar with tabs: 'Main', 'Event Filters', 'Object Filters', 'IP Address Filters', 'Event Triggers', and 'Event Subscriptions'. The 'Main' tab is selected. Below the navigation bar, the title 'Configure Log Target' is displayed, followed by a message: 'This configuration has been modified, but not yet saved.' Below this message, there are buttons for 'Apply', 'Cancel', 'Delete', and 'Undo'. The main configuration area is divided into three sections: 'General Configuration', 'Source Configuration', and 'Destination Configuration'. In the 'General Configuration' section, 'Administrative State' is set to 'enabled', 'Comments' is 'AutoPilot Log', 'Target Type' is 'syslog', 'syslog Facility' is 'user', 'Rate Limit' is '100 events/second', 'Feedback Detection' is 'off', 'Identical Event Detection' is 'on', and 'Event Suppression Period' is '10 seconds'. In the 'Source Configuration' section, 'Local IP Address' is 'mgmtinterface' and 'Local Identifier' is 'XI52Syslog'. In the 'Destination Configuration' section, 'Remote Host' is '11.0.0.202' and 'Remote Port' is '6514'.

Figure 3-18. Configure Log Topic – Main Tab

3.6.4 DataPower WSDM Data Capture

WSDM data capture uses the management interface to the appliance and collects some overlapping and some unique data compared to using SNMP alone.

To enable this feature:

1. Navigate to the *Configure XML Management* page by:
Network > Management > XML Management Interface
2. Enable **AMP Endpoint** and **WSDM Endpoint** in addition to any other currently enabled services.
3. Click **Apply**.

Configure XML Management Interface

main Advanced SLM

XML Management Interface [up]

Apply Cancel Undo

Administrative State
 enabled disabled

Local IP Address
mgmtinterface Select Alias *

Port Number
5550 *

Access Control List
xml-mgmt

Comments

Enabled Services

- SOAP Management URI
- SOAP Configuration Management
- SOAP Configuration Management (v2004)
- AMP Endpoint
- SLM Endpoint
- WS-Management Endpoint
- WSDM Endpoint
- UDDI Subscription
- WSRR Subscription

Figure 3-19. Configure Log Topic – Main Tab

Chapter 4: Deleted

This page intentionally left blank.

Chapter 5: Troubleshooting Server Configuration Issues

The following is a list of errors/issues and their meaning.

Issue: Error_msg: SOAP Fault = rejected by policy

Indicates that the username/password used are invalid or may not have sufficient permission for the expert to collect the data required.

Issue: Connection Timed out: connect

Confirm that the URL specified for the DataPower device is correct and has the correct port specified.

Issue: No error, but sampler_connected and sampler_sampling stay "true"

Confirm that the port specified is the XML Management port, not the administration port.

This page intentionally left blank.

Appendix A: References

A.1 Nastel Documentation

The following table provides a list of reference information for using the AutoPilot.

Table A-1. Nastel Documentation	
Document Number (or higher)	Title
APM6/INS 623.001	<i>AutoPilot M6 Installation Guide</i>
APM6/USR 624.001	<i>AutoPilot M6 User's Guide</i>
M6/SNMP 600.002	<i>AutoPilot M6 for SNMP Installation and User's Guide</i>
M6WMQ/ADM 658.001	<i>AutoPilot M6 for WebSphere MQ Administrator's Guide</i>
M6WMQ/INS 658.001	<i>AutoPilot M6 for WebSphere MQ Installation Guide</i>
M6WMQ/SM 656.001	<i>AutoPilot M6 for WebSphere MQ Security Manager User's Guide</i>

A.2 Other Documentation

Refer to the IBM web page for more information and documentation on DataPower.

<http://www-01.ibm.com/software/integration/datapower/datapower-library/>

This page intentionally left blank.

Appendix B: Conventions

B.1 Typographical Conventions

Table 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 .
<i>Italic Print</i>	Used to place emphasis on a title, menu, screen name, or other category.
Monospaced bold	Used to identify keystrokes/data entries, file names, directory names, etc.
<i>Monospaced italic</i>	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.

This page intentionally left blank.

Appendix C: Sample Application XSD

```

<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:annotation>
    <xs:documentation>
      This schema defines the format of XML messages to use in reporting
      tracking events for processing by TransactionWorks Direct Feed Probe.
    </xs:documentation>
  </xs:annotation>

  <!-- Definition for Data Formats -->
  <xs:simpleType name="DataFormats">
    <xs:restriction base="xs:string">
      <xs:enumeration value="base64Binary">
        <xs:annotation>
          <xs:documentation>
            Data is binary, in base64 encoding
          </xs:documentation>
        </xs:annotation>
      </xs:enumeration>

      <xs:enumeration value="hexBinary">
        <xs:annotation>
          <xs:documentation>
            Data is binary, represented as a hex string
          </xs:documentation>
        </xs:annotation>
      </xs:enumeration>

      <xs:enumeration value="string">
        <xs:annotation>
          <xs:documentation>
            Data is a string of characters
          </xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <!-- Precision of durations and numeric timestamps -->
  <xs:simpleType name="TimeUnits">
    <xs:annotation>
      <xs:documentation>
        Set of internally-supported precision units for field data.
      </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
      <xs:enumeration value="Seconds"/>
      <xs:enumeration value="Milliseconds"/>
      <xs:enumeration value="Microseconds"/>
    </xs:restriction>
  </xs:simpleType>

  <!-- Definition for date/time fields -->
  <xs:complexType name="DateTimestamp">
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="datatype" use="optional" default="Timestamp">

```

```

<xs:simpleType>
  <xs:restriction base="xs:string">
    <xs:enumeration value="DateTime">
      <xs:annotation>
        <xs:documentation>
          Value is a date, time, or date/time expression with a
          specific format.
        </xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="Timestamp">
      <xs:annotation>
        <xs:documentation>
          Value is a numeric value representing a date/time in the
          specified resolution.
        </xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="format" type="xs:string" use="optional"/>
<xs:attribute name="units" type="TimeUnits" use="optional"
  default="Milliseconds"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<!-- Definition for data fields -->
<xs:complexType name="DataField">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="format" type="DataFormats" use="optional"
        default="string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<!-- Root of tracking event tree -->
<xs:element name="tracking_event">
  <xs:complexType>
    <xs:all>
      <xs:element name="HostName" type="xs:string" minOccurs="1">
        <xs:annotation>
          <xs:documentation>
            Host Alias name of server where tracking event occurred.
          </xs:documentation>
        </xs:annotation>
      </xs:element>

      <xs:element name="HostIp" type="xs:string" minOccurs="0">
        <xs:annotation>
          <xs:documentation>
            IP Address of server where tracking event occurred.
          </xs:documentation>
        </xs:annotation>
      </xs:element>

      <xs:element name="HostInfo" type="xs:string" minOccurs="0">
        <xs:annotation>

```

```
<xs:documentation>
  String identifying information (e.g. type, version) about
  system where tracking event occurred.
</xs:documentation>
</xs:annotation>
</xs:element>

<xs:element name="Service" type="xs:string" minOccurs="1">
  <xs:annotation>
    <xs:documentation>
      Name of Service associated with the tracking event.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="User" type="xs:string" minOccurs="0">
  <xs:annotation>
    <xs:documentation>
      Name of User associated with the tracking event.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Domain" type="xs:string" minOccurs="1">
  <xs:annotation>
    <xs:documentation>
      Name of Domain associated with the tracking event.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Policy" type="xs:string" minOccurs="1">
  <xs:annotation>
    <xs:documentation>
      Name of Policy associated with the tracking event.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Rule" type="xs:string" minOccurs="1">
  <xs:annotation>
    <xs:documentation>
      String identifying the operation (e.g. function/method name)
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="EventType" minOccurs="0" default="OTHER">
  <xs:annotation>
    <xs:documentation>
      Type of operation associated with the tracking event.
    </xs:documentation>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="OTHER"/>
      <xs:enumeration value="START"/>
      <xs:enumeration value="OPEN"/>
      <xs:enumeration value="SEND"/>
      <xs:enumeration value="RECEIVE"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
```

```
<xs:enumeration value="CLOSE"/>
<xs:enumeration value="END"/>
<xs:enumeration value="INQUIRE"/>
<xs:enumeration value="SET"/>
<xs:enumeration value="CALL"/>
<xs:enumeration value="URL"/>
<xs:enumeration value="BROWSE"/>
</xs:restriction>
</xs:simpleType>
</xs:element>

<xs:element name="Correlator" type="xs:string" minOccurs="0">
  <xs:annotation>
    <xs:documentation>
      Identifier used to correlate/relate tracking event entries to
      group them into logical tasks.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Signature" type="xs:string" minOccurs="0">
  <xs:annotation>
    <xs:documentation>
      Unique identifier for message in tracking event (message with
      same signature are treated as same message).
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Tag" type="xs:string" minOccurs="0">
  <xs:annotation>
    <xs:documentation>
      User-defined label to associate with message, used for
      searching.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="StartTime" type="DateTimeStamp" minOccurs="0">
  <xs:annotation>
    <xs:documentation>
      Start time of the tracking event, in specified format.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="EndTime" type="DateTimeStamp" minOccurs="0">
  <xs:annotation>
    <xs:documentation>
      End time of the tracking event, in specified format.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ElapsedTime" minOccurs="0" default="0">
  <xs:annotation>
    <xs:documentation>
      Elapsed time of the tracking event in specified units (default:
      microseconds).
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

```
</xs:annotation>
<xs:complexType>
  <xs:simpleContent>
    <xs:extension base="xs:nonNegativeInteger">
      <xs:attribute name="units" type="TimeUnits" use="required"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
</xs:element>

<xs:element name="ErrorCode" minOccurs="0" default="SUCCEEDED">
  <xs:annotation>
    <xs:documentation>
      Error/status code for the tracking event.
    </xs:documentation>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="SUCCEEDED"/>
      <xs:enumeration value="WARNING"/>
      <xs:enumeration value="FAILED"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<xs:element name="ErrorSubCode" type="xs:integer" minOccurs="0"
default="0">
  <xs:annotation>
    <xs:documentation>
      Numeric reason/sub-error code associated with the tracking
      event.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ErrorMsg" type="xs:string" minOccurs="0">
  <xs:annotation>
    <xs:documentation>
      Error/exception message associated with the tracking event.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="MsgData" type="DataField" minOccurs="0">
  <xs:annotation>
    <xs:documentation>
      Message data (payload).
    </xs:documentation>
  </xs:annotation>
</xs:element>
</xs:all>
</xs:complexType>
</xs:element>
</xs:schema>
```

This page intentionally left blank.

Glossary

Application: A logical collection of software components that perform a business function, running on a specific server.

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

AutoPilot M6/Message Tracking (AP/MT): Nastel's AutoPilot/Message Tracking plug-in that enables AutoPilot to intercept message exits and forward the statistical data to an AutoPilot expert.

AutoPilot M6/WebSphere Message Queue Integrator (AP/WMQI): Formerly AP/MQSI.

AutoPilot TransactionWorks (AP/TW): Nastel Technologies' transaction and application performance monitoring product.

BCI: *See* Byte Code Instrumentation.

Binary Large Object (BLOB): A collection of binary data stored as a single entity in a database management system. Blobs are typically images, audio or other multimedia objects, though sometimes binary executable code is stored as a blob. Database support for blobs is not universal.

BLOB: *See* Binary Large Object.

BSV: *See* Business Views.

Business Transaction: A collection of related Transactions that comprise a user defined business function (for example, purchase a book, return merchandize, purchase stock). Each of the business activities may be comprised of various workloads.

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

Byte Code Instrumentation (BCI): The process of adding small portions of Java byte code around methods of a Java class. The added code performs tasks such as time spent or CPU utilization within the monitored class.

CEP: *See* Complex Event Processing.

CEP Server: A container that can host any number of AutoPilot services such as experts, managers, policies, etc. (called *managed node* prior to AutoPilot M6 Service Update 6).

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

Common Object Request Broker Architecture (CORBA): A standard defined by the Object Management Group that enables software components written in multiple computer languages and running on multiple computers to work together. It can be invoked from a Web browser using CGI scripts or applets.

Complex Event Processing (CEP): primarily an event processing concept that deals with the task of processing multiple events from an event cloud with the goal of identifying the meaningful events within the event cloud. CEP employs techniques such as detection of complex patterns of many events, event correlation and abstraction, event hierarchies, and relationships between events such as causality, membership, and timing, and event-driven processes.

Composite Application: A collection of applications that collaborate or communicate with each other (have related sessions).

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

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 used by Internet Information Services (IIS) for a connection to an ODBC data source, (for 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.

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

Derby Database Server: A relational database management system that is based on Java and SQL. It will run in any certified Java Virtual Machine.

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.

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

EVT: Event Log file extension (for example, **sample.evt**).

Expert: Services that monitor specific applications such as an applications server, Web server, or specific components within the applications (for example, channels in WMQ.) 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.

Heap: In Java programming, a block of memory that the Java virtual machine uses at run time to store Java objects. Java heap memory is managed by a garbage collector, which automatically de-allocates Java objects that are no longer in use.

IIS: *See* Internet Information Services.

Instrumentation: Modifies a program by adding code at particular program points to capture dynamic information. For example, a program could be instrumented to count how many times each method is called.

Internet Information Services (IIS): 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.

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

Java Authentication and Authorization Service (JAAS): The JAAS is a standard extension to the security in the J2SE Development Kit 5.0. JAAS (pronounced "jazz") provides the ability to enforce access controls based on user identity. JAAS is provided in WebLogic Server as an alternative to the JNDI authentication mechanism.

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 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.

Java Management Extensions (JMX): An open technology for management and monitoring that can be deployed wherever management and monitoring are needed. By design, this standard is suitable for adapting legacy systems, implementing new management and monitoring solutions and plugging into those of the future.

Java Messaging Service (JMS): A Java Message Oriented Middleware API for sending messages between two or more clients.

Java Naming and Directory Interface (JNDI): Unified interface to multiple naming and directory services for applications based on Java technology.

Java Platform, Enterprise Edition (Java EE): The industry standard for developing portable, robust, scalable and secure server-side Java applications. Building on the solid foundation of Java SE, Java EE provides Web services, component model, management, and communications APIs that make it the industry standard for implementing enterprise class service-oriented architecture (SOA) and Web 2.0 applications.

Java Run-time Environment (JRE): The minimum core Java required to run Java programs.

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.

JMS: *See* Java Messaging Service.

JMX: *See* Java Management Extensions.

JNDI: *See* Java Naming and Directory Interface.

JRE: Java Run-time Environment.

JSP: *See* Java Server Pages.

JVM: *See* Java Virtual Machine.

Logical Unit of Work (LUW): A collection of operations and messages within a session that should be considered to be a single unit of work (all or nothing property). These are generally delimited by BEGIN/COMMIT calls.

LUW: *See* Logical Unit of Work.

M6 for WMQ: Nastel Technologies' WebSphere MQ management solution. Re-designated as M6 for WMQ (formally known as AutoPilot M6 for WMQ) with release 6.0. Prior releases retain either AP/WMQ for version 4.0 or MQControl trademark for version 3.0 and prior.

M6 Web Server: M6 Web Server is 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 services such as experts, managers, policies, etc. (Managed node changed to CEP Server with AutoPilot M6 Service Update 6.)

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: A physical message being transported through the TPN.

Message-Oriented Middleware (MOM): A category of inter-application communication software that relies on asynchronous message passing as opposed to a request/response metaphor.

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.

MOM: *See* Message-Oriented Middleware.

MQControl: Nastel Technologies' MQSeries management product. Re-designated as AutoPilot/MQ with release 4.0, prior releases retain the MQControl trademark.

MQI: *See* Message Queue Interface.

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 installation on any Managed Node.

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.

Resource: An entity on which transactions are executed or a medium of exchange. Examples include Queue, DB table, file, JMS topic.

Resource Manager: An entity that is managing a collection of resources. Examples include a WMQ Queue Manager, Application Server, Database Server.

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.

Server: A physical or virtual node within a TPN that hosts all transaction processing activity.

Service Level Agreement (SLA): A formal written agreement made between two parties: the service provider and the service recipient. The SLA itself defines the basis of understanding between the two parties for delivery of the service itself. The document can be quite complex, and sometimes underpins a formal contract. The contents will vary according to the nature of the service itself, but usually includes a number of core elements, or clauses.

Session: A specific period of execution of an application. Examples include the interval during which a database or queue manager connection is active.

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.

SMTP: *See* Simple Mail Transfer Protocol.

Speed Manager: Type of manager which allows loading of policies from a “Speed Folder” which automatically loads all .bsv and .bsp files located in the folder upon manager’s start.

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

TPN: *See* Transaction Processing Network.

Transaction: A group of activities targeted at achieving a common goal or a task; collection of related sessions and LUWs.

Transaction Processing Network (TPN): A collection of servers engaged in transaction processing activity.

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.

WebLogic: A Java EE compatible application server platform which enables support for multiple programming models, which includes advanced administration tools and is the ideal foundation for Service Oriented Architecture (SOA).

WebSphere MQ: IBM’s message queuing product; formerly known as MQSeries.

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.

This page intentionally left blank.