Tivoli® IBM Tivoli Composite Application Manager
Version 7.1.0.1

Agent for WebSphere Applications Installation and Configuration Guide

IBM

SC27-2818-00

Tivoli® IBM Tivoli Composite Application Manager
Version 7.1.0.1

Agent for WebSphere Applications Installation and Configuration Guide

IBM

SC27-2818-00

Note

Before using this information and the product it supports, read the information in “Notices” on page 299.

2010

This 2010 edition applies to ITCAM for Application Diagnostics 7.1.0.1 and all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures vii

Tables ix

About this publication xi
Intended audience xi
Publications xi
ITCAM for Application Diagnostics library . . . xi
Related publications xii
Accessing terminology online xiii
Accessing publications online xiii
Ordering publications. xiv
Accessibility xiv
Tivoli technical training xiv
Support information xiv
Conventions used in this publication xv
Typeface conventions xv
Variables for directories xv

Part 1. Introduction to ITCAM Agent for WebSphere Applications. 1

Chapter 1. IBM Tivoli Composite Application Manager Agent for WebSphere Applications 3
Overview of the monitoring and diagnostic capabilities 3
Components of the Agent 5
Prerequisites to installation 6
System and software prerequisites 7

Part 2. Installing and Configuring ITCAM Agent for WebSphere Applications on Windows 9

Chapter 2. Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Windows 11
System and software prerequisites 11
Required tasks before installation 11
Permissions 11
Adjusting for ports being blocked by your firewall or being used by other applications . . 11
WebSphere Global Security: setting the user name and password in client properties files . . 12
What to do next 13

Chapter 3. Installing and configuring ITCAM Agent for WebSphere Applications on Windows 15
Installing ITCAM Agent for WebSphere Applications on Windows 15
Step 1: Invoke setup.exe 16
Step 2: Accept the product license 17
Step 3: Choose the destination folder for the installation files 18
Step 4: Enter the IBM Tivoli Monitoring encryption key 19
Step 5: Select the product components you want to install 21
Step 6: Select Windows program folder 21
Step 7: Verify selected features 22
Step 8: Select the items to configure 23
Configuring ITCAM Agent for WebSphere Applications on Windows 25
Configure the monitoring agent connection to the monitoring server 26
Configure Monitoring Agent settings 28
Configure the Data Collector to monitor application server instances 32
Unconfigure the Data Collector for application server instances 47
Configure Data Collector communication with the Managing Server 53
Upgrading monitoring to Data Collector 7.1 . . 60
Changing Data Collector maintenance level. . . 69
Removing a Data Collector maintenance level . . 76
Installing application support on Windows 81
Ensuring that the Eclipse server has been configured. 84
Enabling history collection 86
Silent installation and configuration on Windows. . 87
Performing a silent installation or uninstallation on Windows 87
Performing a silent configuration on Windows . 89
Additional steps for configuring the Data Collector on Windows 91
Setting up a secure connection to the Managing Server 91
JDK 1.4.2 J9: enabling Java core dumps and heap dumps 91
IBM JDK 1.4.2: removing the -Xnoclassgc argument 92
Completing and verifying Data Collector configuration 93
Uninstalling ITCAM Agent for WebSphere Applications on Windows 93
Installing and uninstalling a Language Pack on Windows 94
Installing a Language Pack on Windows. . . . 94
Uninstalling a Language Pack on Windows. . . 95

Part 3. Installing and Configuring ITCAM Agent for WebSphere Applications on UNIX and Linux . . 97

Chapter 4. Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Linux and UNIX systems 99
System and software prerequisites 99
What to do next 99
Required tasks before installation 99
Permissions 99
Adjusting for ports being blocked by your firewall or being used by other applications . . 100
HP-UX: tuning HotSpot JVM garbage collection 101
Making sure there are no invalid mounted file systems 101
WebSphere Global Security: setting the user name and password in client properties files . . 101
AIX 5.3: Prerequisite APAR 102
Linux: timezone setting for historical data collection 103
HP-UX: Mounting the Agent installation DVD 103
What to do next 103

Chapter 5. Installing and configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems. 105
Installing ITCAM Agent for WebSphere Applications on Linux and UNIX systems 105
Step 1: Invoke the installer 106
Step 2: Supply the name of the installation directory 106
Step 3: Select installation options 106
Step 4: Accept the product license agreement 107
Step 5: Enter the IBM Tivoli Monitoring encryption key 107
Step 6: Install prerequisites and specify the component to install 107
Step 7: Install the product software 109
Deep dive diagnostics only installation: disabling Monitoring Agent autostart 109
What to do next 109
Configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems 110
Configuring the Agent using command line . . 110
Configuring the Agent using GUI 133
Starting ITCAM Agent for WebSphere Applications 189
Installing application support on Linux and UNIX systems 190
Ensure that the Eclipse server has been configured 196
Enabling history collection 196
Silent installation and configuration on Linux and UNIX systems 196
Silent installation 197
Silent configuration 198
Additional steps for configuring the Data Collector on Linux and UNIX systems 200
Data Collector installed on IBM WebSphere Application Server 6.0.2 on SLES 9 (64-bit): enabling heap dumps 200
JDK 1.4.2 J9: enabling Java core dumps and heap dumps 201
IBM JDK 1.4.2: removing the -Xnoclassgc argument 201
Generating your own .jks key files and trust files 202
If you used the root ID for the Data Collector installation and the application server is not owned and operated by the root ID 202
Completing and verifying Data Collector configuration 202
Uninstalling ITCAM Agent for WebSphere Applications on Linux and UNIX systems 203
Installing and uninstalling a Language Pack on Linux and UNIX systems 203
Installing a Language Pack on Linux and UNIX systems 204
Uninstalling a Language Pack on Linux and UNIX systems 204

Part 4. Installing and Configuring ITCAM Agent for WebSphere Applications on a Remote Computer 207

Chapter 6. Installing and configuring ITCAM Agent for WebSphere Applications remotely. 209
Installing, upgrading and configuring ITCAM Agent for WebSphere Applications remotely using command line 209
Installing ITCAM Agent for WebSphere Applications remotely using Tivoli Enterprise Portal 213
Configuring ITCAM Agent for WebSphere Applications remotely using Tivoli Enterprise Portal 214

Part 5. Advanced configuration of the Agent 215

Chapter 7. Customization and advanced configuration for the Data Collector 217
Properties files for the Data Collector 217
Tuning Data Collector performance and monitoring scope 218
Data Collector internal buffering and turbo mode settings 219
Enabling instrumentation and monitoring of RMI/IIOP requests between application servers . 220
Disabling various types of Byte Code Instrumentation for J2EE APIs 221
Controlling instrumentation of application classes for lock analysis, memory leak analysis, and method profiling and tracing 223
Defining custom requests 230

Enabling Asynchronous Bean request monitoring 232
Customizing monitoring of custom MBeans . . 233
Modifying Performance Monitoring Infrastructure settings 235
Enabling Performance Monitoring Infrastructure settings for the Service Integration Bus 236
Enabling and disabling instrumentation of Web Services as new request types 237
Enabling and disabling memory monitoring . . . 237
Configuring the Data Collector after changing the application server version 238
Steps to perform if the IP address of the application server host is to be changed 238
Moving the Data Collector to a different host computer 239
Installing Memory Dump Diagnostic for Java with IBM Support Assistant 239
Where to install IBM Support Assistant and Memory Dump Diagnostic for Java 240
Downloading, installing, configuring, and launching IBM Support Assistant and Memory Dump Diagnostic 240
Setting the Heap Dump scan interval 240
Configuring a Data Collector for multiple network interfaces 241
Customizing RMI garbage collection interval . . . 241
Customizing CICS transaction correlation 242
Modifying the garbage collection log path 243
Suppressing verbose garbage collection output in Data Collectors with a Sun JDK 244
What to do when deleting an application server profile 244
Integrating the Data Collector with ITCAM for Transactions 245
Enabling and disabling TTAPI on the Data Collector 245
Tracing the integration of TTAPI with the Data Collector 246
Overriding the Data Collector autoconfiguration 246
Properties for communication with a Deployment Manager 247

Part 6. Appendixes 249

Appendix A. Setting up security . . . 251

Node Authentication 251
Script to run if your SSL certificates have expired 251
Node Authentication on the Managing Server 251
Data Collector custom properties file changes 252
Node Authentication related properties in the Port Consolidator 252
Keystore management and populating certificates 252
Secure Socket Layer communications 255
Password encryption and Kernel property file encryption 256
Enabling Secure Socket Layer at the Data Collector level 256
Verifying secure communications 257
Privacy filtering 258
Enabling privacy filtering 258
Script to run if your SSL certificates have expired 258
Settings for the Data Collector if Java 2 security is enabled 260

Appendix B. Starting and stopping the monitoring environment 263

Disabling and re-enabling a Data Collector . . . 263
Restarting the application server 263
Restarting the application server in a non-Network Deployment environment . . . 264
Restarting the application server in a Network Deployment environment 264
Starting the application server 265
Starting the application server in a non-Network Deployment environment 265
Starting the application server in a Network Deployment environment 266
Stopping the application server 266
Stopping the application server in a non-Network Deployment environment . . . 267
Stopping the application server in a Network Deployment environment 267

Appendix C. Using regular expressions 269

Regular expression library 269
Frequently used regular expressions 269
Specifying exclusions with the bang (!) operator (Quality of Service listening policies only) 270

Appendix D. Manual changes to application server configuration for the Data Collector 271

Restoring the application server configuration after a failed Data Collector configuration 271
Manually configuring the Data Collector to monitor an application server instance 272
Manually removing Data Collector configuration from an application server instance 275

Appendix E. Attribute groups and sizing information for historical warehousing. 277

Appendix F. Port Consolidator reference and configuration 281

Configuring a Data Collector to use the Port Consolidator 281
Reconfiguring the Data Collector to bypass the Port Consolidator 282

Appendix G. Support information. . . 285

Searching knowledge bases. 285
Finding Release Notes 285

Searching the information center on your local system or network. 286
Searching the Internet 286
Obtaining fixes 286
Receiving Weekly support updates 287
Contacting IBM Software Support 287
Determining the business impact of your problem 288
Describing your problem and gathering background information 288
Submitting your problem to IBM Software Support 288
Tivoli Support Technical Exchange 289

Appendix H. Accessibility 291

Index 293

Trademarks 297

Notices 299

Figures

1. Agent interaction with IBM Tivoli Monitoring 4
2. Agent interaction with ITCAM for Application Diagnostics Managing Server 5
3. Installation Welcome window 16
4. Prerequisites window 17
5. Software License Agreement window 18
6. Choose Destination Location window 19
7. User Data Encryption Key window 20
8. Encryption Key confirmation window. . . . 20
9. Select Features window 21
10. Select Program Folder window 22
11. Selected features verification window 23
12. Setup Type window. 24
13. TEMS connection configuration window 25
14. The Agent Configuration window 26
15. Configuring the monitoring agent connection to the monitoring server 27
16. Configuring Communication to the monitoring agent, window 1 29
17. Configuring Communication to the Monitoring Agent, window 2 30
18. Configuring Communication to the monitoring agent, window 3 31
19. Configuring Communication to the monitoring agent, window 4 32
20. Configuring the Data Collector to monitor application server instances, window 1 . . . 33
21. Configuring the Data Collector to monitor application server instances, window 2 . . . 34
22. Configuring the Data Collector to monitor application server instances, window 3 . . . 35
23. Configuring the Data Collector to monitor application server instances, window 4 . . . 36
24. Configuring the Data Collector to monitor application server instances, window 5 . . . 37
25. Configuring the Data Collector to monitor application server instances, window 6 . . . 38
26. Configuring the Data Collector to monitor application server instances, window 7 . . . 39
27. Configuring the Data Collector to monitor application server instances, window 8 . . . 40
28. Configuring the Data Collector to monitor application server instances, window 9 . . . 41
29. Configuring the Data Collector to monitor application server instances, window 10 . . . 43
30. Configuring Communication to the monitoring agent, window 11 45
31. Configuring the Data Collector to monitor application server instances, window 12 . . . 46
32. Configuring the Data Collector to monitor application server instances, window 13 . . . 47
33. Unconfiguring the Data Collector for application server instances, window 1 . . . 48
34. Unconfiguring the Data Collector for application server instances, window 2 . . . 50
35. Unconfiguring the Data Collector for application server instances, window 3 . . . 51
36. Unconfiguring the Data Collector for application server instances, window 4 . . . 52
37. Unconfiguring the Data Collector for application server instances, window 5 . . . 53
38. Configuring Data Collector communication with the Managing Server, window 1 55
39. Configuring Data Collector communication with the Managing Server, window 2 56
40. Configuring Data Collector communication with the Managing Server, window 3 57
41. Configuring Data Collector communication with the Managing Server, window 4 58
42. Configuring Data Collector communication with the Managing Server, window 5 59
43. Configuring Data Collector communication with the Managing Server, window 5 60
44. Upgrading monitoring to Data Collector 7.1, window 1 61
45. Upgrading monitoring to Data Collector 7.1, window 2 62
46. Upgrading monitoring to Data Collector 7.1, window 3 64
47. Upgrading monitoring to Data Collector 7.1, window 4 65
48. Upgrading monitoring to Data Collector 7.1, window 5 66
49. Upgrading monitoring to Data Collector 7.1, window 6 67
50. Upgrading monitoring to Data Collector 7.1, window 7 68
51. Upgrading monitoring to Data Collector 7.1, window 8 69
52. Changing Data Collector maintenance level, window 1 70
53. Changing Data Collector maintenance level, window 2 71
54. Changing Data Collector maintenance level, window 3 73
55. Changing Data Collector maintenance level, window 4 74
56. Changing Data Collector maintenance level, window 5 75
57. Changing Data Collector maintenance level, window 6 76
58. Uninstalling a Data Collector maintenance level, window 1 77
59. Uninstalling a Data Collector maintenance level, window 2 78
60. Uninstalling a Data Collector maintenance level, window 3 79
61. Uninstalling a Data Collector maintenance level, window 4 80
62. Uninstalling a Data Collector maintenance level, window 5 81

63. Configuring the Eclipse server 85
64. Defining the port number for the Eclipse Help Server 85
65. Specifying Eclipse help server startup type 86
66. Manage Tivoli Enterprise Monitoring Services window on UNIX and Linux 133
67. Agent Configuration window 134
68. Configuring Communication to the monitoring agent, window 1 135
69. Configuring Communication to the Monitoring Agent, window 2 136
70. Configuring Communication to the monitoring agent, window 3 137
71. Configuring Communication to the monitoring agent, window 4 138
72. Configuring Communication to the monitoring agent, window 5 139
73. Configuring the Data Collector to monitor application server instances, window 1 . . . 141
74. Configuring the Data Collector to monitor application server instances, window 2 . . . 142
75. Configuring the Data Collector to monitor application server instances, window 3 . . . 143
76. Configuring the Data Collector to monitor application server instances, window 4 . . . 144
77. Configuring the Data Collector to monitor application server instances, window 5 . . . 145
78. Configuring the Data Collector to monitor application server instances, window 6 . . . 146
79. Configuring the Data Collector to monitor application server instances, window 7 . . . 147
80. Configuring the Data Collector to monitor application server instances, window 8 . . . 148
81. Configuring the Data Collector to monitor application server instances, window 9 . . . 149
82. Configuring the Data Collector to monitor application server instances, window 10 . . 151
83. Configuring Communication to the monitoring agent, window 11 153
84. Configuring the Data Collector to monitor application server instances, window 12 . . 154
85. Configuring the Data Collector to monitor application server instances, window 13 . . 155
86. Unconfiguring the Data Collector for application server instances, window 1 . . . 156
87. Unconfiguring the Data Collector for application server instances, window 2 . . . 158
88. Unconfiguring the Data Collector for application server instances, window 3 . . . 159
89. Unconfiguring the Data Collector for application server instances, window 4 . . . 160
90. Unconfiguring the Data Collector for application server instances, window 5 . . . 161
91. Configuring the Data Collector to monitor application server instances, window 1 . . . 163
92. Configuring Data Collector communication with the Managing Server, window 2 . . . 164
93. Configuring Data Collector communication with the Managing Server, window 3 . . . 165
94. Configuring Data Collector communication with the Managing Server, window 4 . . . 166
95. Configuring Data Collector communication with the Managing Server, window 5 . . . 167
96. Configuring Data Collector communication with the Managing Server, window 5 . . . 168
97. Upgrading monitoring to Data Collector 7.1, window 1. 169
98. Upgrading monitoring to Data Collector 7.1, window 2. 170
99. Upgrading monitoring to Data Collector 7.1, window 3. 172
100. Upgrading monitoring to Data Collector 7.1, window 4. 173
101. Upgrading monitoring to Data Collector 7.1, window 5. 174
102. Upgrading monitoring to Data Collector 7.1, window 6. 175
103. Upgrading monitoring to Data Collector 7.1, window 7. 176
104. Upgrading monitoring to Data Collector 7.1, window 8. 177
105. Changing Data Collector maintenance level, window 1. 178
106. Changing Data Collector maintenance level, window 2. 179
107. Changing Data Collector maintenance level, window 3. 181
108. Changing Data Collector maintenance level, window 4. 182
109. Changing Data Collector maintenance level, window 5. 183
110. Changing Data Collector maintenance level, window 6. 184
111. Uninstalling a Data Collector maintenance level, window 1. 185
112. Uninstalling a Data Collector maintenance level, window 2. 186
113. Uninstalling a Data Collector maintenance level, window 3. 187
114. Uninstalling a Data Collector maintenance level, window 4. 188
115. Uninstalling a Data Collector maintenance level, window 5. 189

Tables

1. Default locations for *ITM_home* xvi
2. Communications protocol settings 27
3. Fields for establishing Data Collector and application server communication 42
4. Fields for establishing Data Collector and application server communication 49
5. Comparison of ways to disable Data Collector communication to the Managing Server. . . . 54
6. Fields for establishing Data Collector and application server communication 63
7. Fields for establishing Data Collector and application server communication 72
8. Agent installation response file properties 88
9. Default temporary directories for the InstallShield portion of the installation program 100
10. Comparison of ways to disable Data Collector communication to the Managing Server. . . 122
11. Fields for establishing Data Collector and application server communication. 150
12. Fields for establishing Data Collector and application server communication. 157
13. Comparison of ways to disable Data Collector communication to the Managing Server. . . 162
14. Fields for establishing Data Collector and application server communication. 171
15. Fields for establishing Data Collector and application server communication. 180
16. Agent installation response file properties 197
17. Adding lines to toolkit_custom.properties 221
18. Modifying lines in toolkit_custom.properties 222
19. Byte Code Instrumentation configuration files 223
20. Parameters for the memory leak diagnosis configuration file 227
21. Parameters for the Level 3 method entry and exit analysis configuration file 229
22. Parameters for the custom requests configuration file 231
23. Parameters for the JMX MBean configuration file 233
24. Default Performance Monitoring Infrastructure instrumentation settings . . . 236
25. Procedures to customize instrumentation of the Performance Monitoring Infrastructure. . 236
26. JVM options for garbage collection logging 243
27. Location of the CYND4051I message 257
28. Classification of the data processed on the CommandAgent channel. 257
29. Restarting the application server 264
30. Starting the application server.. 265
31. Stopping the application server. 267
32. Syntax of the restoreConfig command in a non-Network Deployment environment. . . . 271
33. Syntax of restoreConfig command, Network Deployment environment 272
34. Values for the application server platform designation 273
35. 274
36. Information for historical warehousing 277
37. Command for starting the Port Consolidator 281
38. Location of the CYND4051I message 282
39. Entering the proxyserverctrl_ws command 282
40. Entering the proxyserverctrl_ws command 282
41. Entering the proxyserverctrl_ws command 283
42. Entering the proxyserverctrl_ws command 283
43. Criteria for assessing the business impact of your problem 288

About this publication

This publication provides information about installing, customizing, starting, and maintaining IBM® Tivoli® Composite Application Manager Agent for WebSphere® Applications on Windows®, Linux®, and UNIX® systems.

For information about installing, customizing, starting, and maintaining IBM Tivoli Composite Application Manager Agent for WebSphere Applications on IBM z/OS®, see IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide for z/OS.

For information about installing, customizing, starting, and maintaining IBM Tivoli Composite Application Manager Agent for WebSphere Applications Data Collector on IBM i, see IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Data Collector Installation and Configuration Guide for IBM i.

Intended audience

This publication is for administrators or advanced users wanting to install or modify the configuration of ITCAM Agent for WebSphere Applications. The publication assumes that readers are familiar with maintaining operating systems, administering Web servers, maintaining databases, and general information technology (IT) procedures. Specifically, readers of this publication must have some knowledge of the following topics:

- Operating systems on which you intend to install product components
- Web servers, such as IBM HTTP Server and Apache HTTP Server
- Web application servers, such as IBM WebSphere
- Internet protocols such as HTTP, HTTPS, TCP/IP, Secure Sockets Layer (SSL), and Transport Layer Security (TLS)
- Digital certificates for secure communication

Publications

This section lists publications in the product library and related documents. It also describes how to access Tivoli publications online and how to order Tivoli publications.

ITCAM for Application Diagnostics library

The following publications are included in the ITCAM for Application Diagnostics library, available at http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamfad.doc_7101/ic-homepage.html:

- *IBM Tivoli Composite Application Manager for Application Diagnostics: Prerequisites*

  Provides the hardware and software requirements for installing ITCAM for Application Diagnostics components.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: User's Guide*

  Provides the user overview, user scenarios, and Helps for every ITCAM for Application Diagnostics component.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: Planning an Installation*

Provides the user with a first reference point for a new ITCAM for Application Diagnostics installation or upgrade.

- ITCAM Agent for WebSphere Applications Installation and Configuration Guides:
  - *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide*
  - *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide for z/OS*
  - *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Data Collector Installation and Configuration Guide for IBM i*

  Provide installation instructions for setting up and configuring ITCAM Agent for WebSphere Applications on distributed, z/OS, and IBM i systems.
- ITCAM Agent for J2EE Applications Installation and Configuration Guides:
  - *IBM Tivoli Composite Application Manager: Agent for J2EE Data Collector Installation and Configuration Guide*
  - *IBM Tivoli Composite Application Manager: Agent for J2EE Monitoring Agent Installation and Configuration Guide*

  Provide installation instructions for setting up and configuring ITCAM Agent for J2EE.
- *IBM Tivoli Composite Application Manager: Agent for HTTP Servers Installation and Configuration Guide*

  Provides installation instructions for setting up and configuring ITCAM Agent for HTTP Servers.
- *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*

  Provides installation instructions for setting up and configuring ITCAM for Application Diagnostics Managing Server.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: Troubleshooting Guide*

  Provides instructions on problem determination and troubleshooting for ITCAM for Application Diagnostics.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: Messaging Guide*

  Provides information about system messages received when installing and using ITCAM for Application Diagnostics.

Related publications

The following documentation also provides useful information:

- IBM Tivoli Documentation Central:

  Information about IBM Tivoli Documentation is provided on the following Web site:

  http://www.ibm.com/tivoli/documentation.html
- IBM WebSphere Application Server:

  Information about IBM WebSphere Application Server is provided on the following Web site:

  http://www.ibm.com/software/webservers/appserv/was/library
- IBM DB2®:

  Information about IBM DB2 is provided on the following Web site:

  http://www.ibm.com/software/data/sw-library/

- IBM Tivoli Enterprise Console®:

  Information about IBM Tivoli Enterprise Console is provided on the following Web site:

  http://submit.boulder.ibm.com/tividd/td/EnterpriseConsole3.9.html
- IBM Tivoli Data Warehouse:

  Information about IBM Tivoli Data Warehouse is provided on the following Web site:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.tivoli.tdwi.doc/toc.xml
- IBM Tivoli Change and Configuration Management Database:

  Information about IBM Tivoli Change and Configuration Management Database is provided on the following Web site:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?toc=/com.ibm.ccmdb.doc/ccmdb_ic.xml
- IBM Support Assistant:

  Information about IBM Support Assistant is provided on the following Web site:

  http://www.ibm.com/software/support/isa/index.html?rcss=rtlrre

Accessing terminology online

The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available at the following Tivoli software library Web site:

http://publib.boulder.ibm.com/tividd/glossary/tivoliglossarymst.htm

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology

Accessing publications online

The documentation CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli software information center Web site. Access the Tivoli documentation center at the following Web address:

https://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home

Access the Tivoli Information Center for ITCAM for Application Diagnostics at the following Web address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamfad.doc_7101/ic-homepage.html

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File** → **Print** window that enables Adobe® Reader to print letter-sized pages on your local paper.

The IBM Software Support Web site provides the latest information about known product limitations and workarounds in the form of technotes for your product. You can view this information at the following Web site:

http://www.ibm.com/software/support

Ordering publications

You can order many Tivoli publications online at the following Web site:

http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following Web site:

   http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see Appendix H, “Accessibility,” on page 291.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site:

http://www.ibm.com/software/tivoli/education/

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online

Go to the IBM Software Support at the following Web site:

http://www.ibm.com/software/support/

Follow the instructions.

IBM Support Assistant

The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, see the instructions for installing ISA in the Data Collector installation guide.

Troubleshooting Guide

For more information about resolving problems, see the corresponding part in *IBM Tivoli Composite Application Manager for Application Diagnostics: Troubleshooting Guide*.

Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Variables for directories

This guide refers to the following variables:

- *ITM_home*: the top level directory for installation of IBM Tivoli Monitoring components, including ITCAM Agent for WebSphere Applications. The following table shows the default locations:

Table 1. Default locations for ITM_home

UNIX or **Linux systems**	`/opt/IBM/ITM`
Windows	`C:\IBM\ITM`

- *DC_home* and *ITCAM_home*: the directory where the Data Collector files are installed. The location is `*ITM_home*\TMAITM6\wasdc\7.1.0.1` on Windows, `*ITM_home*/*architecture_code*/yn/wasdc/7.1.0.1` on Lunix and UNIX systems..
- *AppServer_home*: the directory where the application server core product files are installed.

  Examples:

  – on Windows, `C:\Program Files\IBM\WebSphere\AppServer`

  – on Linux and UNIX systems, `/opt/IBM/WebSphere/AppServer6`

Part 1. Introduction to ITCAM Agent for WebSphere Applications

Chapter 1. IBM Tivoli Composite Application Manager Agent for WebSphere Applications

This chapter introduces the ITCAM Agent for WebSphere Applications and explains how it can help you monitor, administer, and diagnose your systems that run IBM WebSphere Application Server.

Overview of the monitoring and diagnostic capabilities

IBM Tivoli Composite Application Manager Agent for WebSphere Applications is a component of ITCAM for Application Diagnostics, Version 7.1.0.1. It is also a component of ITCAM for Applications Version 6.2.3. If you are using ITCAM for Applications, the Managing Server (deep dive) functionality is not available; please ignore all references to this functionality in this document.

ITCAM Agent for WebSphere Applications can function within two different infrastructures: IBM Tivoli Monitoring and ITCAM for Application Diagnostics Managing Server.

The IBM Tivoli Monitoring environment places this agent into the context of the IBM Tivoli Monitoring family, a suite of products used to monitor a mixed-systems environment. With IBM Tivoli Monitoring, the user can:

- Monitor for alerts on the managed systems
- Trace the causes leading up to an alert
- Monitor processing time for various requests within WebSphere applications
- Establish your own performance thresholds
- Create custom situations, which are conditions that IBM Tivoli Monitoring automatically monitors
- Create and send commands to control system monitoring using the Take Action feature
- Create comprehensive reports about system conditions
- Define your own queries, using the attributes provided with ITCAM Agent for WebSphere Applications, to monitor conditions of particular interest to you

The Tivoli Enterprise Portal is the user interface for the IBM Tivoli Monitoring environment. It provides an overall view of the enterprise network; from this view, the user can "drill down" to examine components of the environment more closely. The Portal includes information from different agents that monitor various parts of the environment; ITCAM Agent for WebSphere Applications is one of them.

For details on capabilities of IBM Tivoli Monitoring, and information on deploying the IBM Tivoli Monitoring infrastructure, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Figure 1 on page 4 shows how ITCAM Agent for WebSphere Applications interacts with other IBM Tivoli Monitoring components.

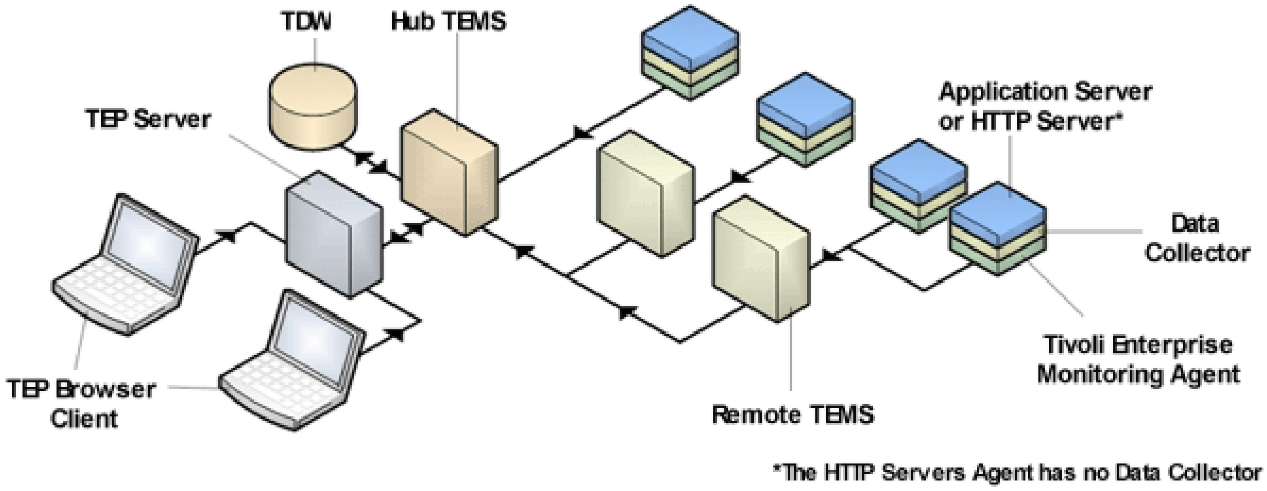


Figure 1. Agent interaction with IBM Tivoli Monitoring

The Managing Server is a component of ITCAM for Application Diagnostics. Its Visualization Engine provides a user interface for "deep dive" diagnostics information. The user can "click through" or "launch in context" to the Visualization Engine from the Tivoli Enterprise Portal when detailed information is required. The Visualization Engine can also be used as a stand alone user interface; this user interface is a good solution for software developers and performance analysts.

Most information provided by ITCAM Agent for WebSphere Applications and available through the Tivoli Enterprise Portal can also be viewed through the Visualization Engine. The Visualization Engine also provides additional diagnostic information, including:

- Method entry/exit and stack tracing,
- Lock analysis,
- Heap object analysis for memory leak diagnosis,
- Thread information,
- "In-flight" request analysis to detect malfunctioning applications.

For details on the capabilities of ITCAM for Application Diagnostics Managing Server, and information on deploying it, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

The diagram on Figure 2 on page 5 shows how ITCAM Agent for WebSphere Applications interacts with the components of the Managing Server. (The Data Collector is a component of the Agent).

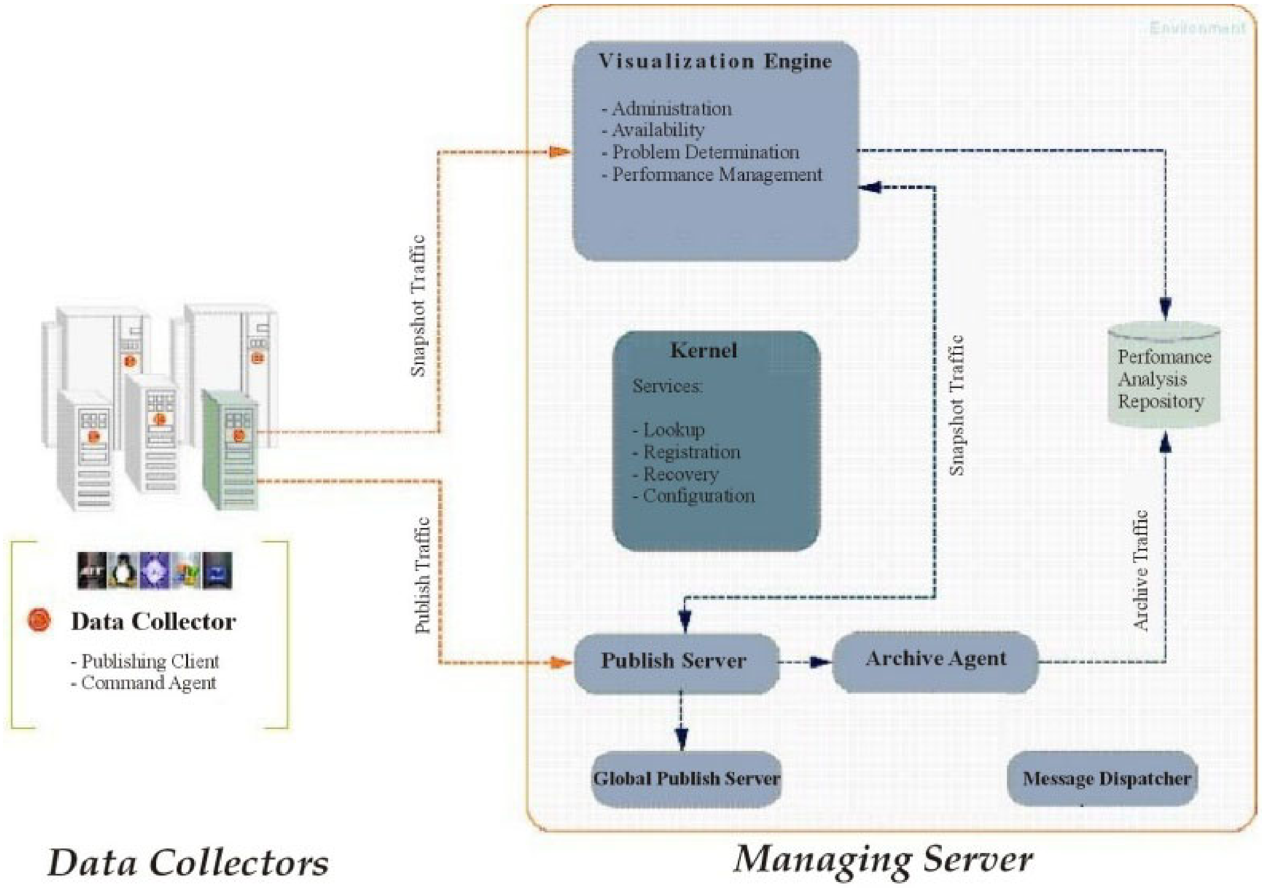


Figure 2. Agent interaction with ITCAM for Application Diagnostics Managing Server

Components of the Agent

ITCAM Agent for WebSphere Applications consists of two components: the *Data Collector* and the *Monitoring Agent*. These components are deployed on every monitored host (except the Deployment Manager in WebSphere Network Deployment or Extended Deployment) by a single installer. For interaction with IBM Tivoli Monitoring, the Agent provides *application support files* that are to be installed on servers and clients in the IBM Tivoli Monitoring infrastructure.

Data Collector

The Data Collector collects monitoring and diagnostics information from the application server using the following methods:

- In *Byte Code Instrumentation (BCI)* the Data Collector injects monitoring calls (probes) into the Java™ code that processes application requests. Data is collected on request processing time and on different types of nested requests within the process. The use of BCI creates a performance overhead; the amount of collected information, and thus the overhead, is determined by the *monitoring level*, which can be set for every monitored application server. With IBM Tivoli Monitoring, levels L1 and L2 are supported; with ITCAM for Application Diagnostics Managing Server, the additional level L3 is available.

- *Performance Monitoring Interface (PMI)* is an API provided by IBM WebSphere Application Server, supplying a number of performance metrics.
- *Garbage Collection logs* are written by IBM WebSphere Application Server, and contain detailed information about the garbage collection process. Such information can be useful for application monitoring and enhancement.

The Data Collector sends the information to the monitoring agent. It also communicates directly with the Managing Server (if the Managing Server infrastructure is used).

You must configure the Data Collector for every instance of the application server that you need to monitor.

Monitoring Agent

The Monitoring Agent collects information from the Data Collector, and processes and aggregates it for presentation to the user. It also parses application server logs.

In WebSphere Extended Deployment, if cell monitoring is configured, the monitoring agent communicates to the Deployment Manager over the network to retrieve configuration and performance information for the cell.

The Monitoring Agent sends monitoring information to the Tivoli Enterprise Monitoring Server. It also receives Take Action commands from the Tivoli Enterprise Monitoring Server. When these commands involve server management actions (starting, stopping, or restarting the application server), the monitoring agent performs these actions.

Application support files

To enable ITCAM Agent for WebSphere Applications interaction with IBM Tivoli Monitoring, the application support files shipped with the Agent **must** be installed on all hub Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and Tivoli Enterprise Portal clients except browser-based clients.

On the Tivoli Enterprise Monitoring Server, support files provide the ITCAM for Application Diagnostics data tables and situations.

On the Tivoli Enterprise Portal Server, support files provide the ITCAM for Application Diagnostics workspaces that display the monitoring information and include code that processes situation information for the Summary workspaces.

On the Tivoli Enterprise Portal client, support files provide the ITCAM for Application Diagnostics Helps and Language Packs.

Prerequisites to installation

The instructions in the subsequent chapters assume the following:

- If ITCAM Agent for WebSphere Applications will communicate with the IBM Tivoli Monitoring infrastructure, you are familiar with basic usage of the Tivoli Enterprise Portal and have installed the base components of this infrastructure, including:
  - A Tivoli Enterprise Monitoring Server (monitoring server)
  - A Tivoli Enterprise Portal (portal) server
  - Tivoli Enterprise Portal clients

- If ITCAM Agent for WebSphere Applications will communicate with ITCAM for Application Diagnostics Managing Server, you are familiar with basic usage of the Visualization Engine and have deployed the Managing Server.

To obtain the most recent installation updates, review the Release Note information for this product. You can find this information online by viewing IBM Technotes. To access the Technotes, see the *IBM Tivoli Composite Application Manager for Application Diagnostics: Troubleshooting Guide*.

System and software prerequisites

The software and hardware requirements for installing ITCAM Agent for WebSphere Applications are listed at https://www.ibm.com/developerworks/wikis/display/tivolimonitoring/Prerequisites+for+ITCAM+for+Application+Diagnostics+7.1.0.1.

Part 2. Installing and Configuring ITCAM Agent for WebSphere Applications on Windows

Chapter 2. Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Windows

This chapter includes tasks that you need to perform before installing the ITCAM Agent for WebSphere Applications on Windows.

System and software prerequisites

The software and hardware requirements before installing ITCAM for Application Diagnostics are listed at the following Web site:

https://www.ibm.com/developerworks/wikis/display/tivolimonitoring/Prerequisites+for+ITCAM+for+Application+Diagnostics+7.1.0.1

Required tasks before installation

Perform the tasks in each of the following sections before you start installing the ITCAM Agent for WebSphere Applications.

Permissions

The user who installs ITCAM Agent for WebSphere Applications on Windows must have Administrator privileges.

If you will be configuring the Data Collector to monitor instances of the application server, this user must also have privileges (read, write and execute) for the application server directory.

If you are performing an upgrade of the Data Collector, this installation user must have read/write privileges to the home directory for the previous version of the Data Collector.

Adjusting for ports being blocked by your firewall or being used by other applications

At various times during the installation you will need to specify or accept the defaults for port numbers used by ITCAM Agent for WebSphere Applications.

By default, ITCAM Agent for WebSphere Applications will communicate in the following ways:

- If the IBM Tivoli Monitoring infrastructure is used, the Agent will make outbound connections to the Tivoli Enterprise Monitoring Server host.
- If the ITCAM for Application Diagnostics Managing Server is used, and the Data Collector is configured for one or more application server instances, it will need to open ports in the 8200 to 8399 range for inbound communication.
- With WebSphere Network Deployment or Extended Deployment, the Agent will make outbound connections to the Deployment Manager host. The port number is available in the Deployment Manager administrative console.

You need to ensure that these connections are not blocked by a firewall. If they are blocked, you must either modify the communication settings during installation and configuration of the Agent, or change the settings of the firewall. To determine the connections that your firewall may block, see the documentation supplied with the firewall.

If you are using ITCAM for Application Diagnostics Managing Server, you also need to make sure that ports used for inbound communication are not used by other applications. If they are used by other applications, you will need to change the ports for Data Collector inbound communication when configuring the Data Collector (see Step 6 on page 36). To list the ports used by other applications, run the command `netstat -a`; in its output, look for lines that include `LISTENING`.

WebSphere Global Security: setting the user name and password in client properties files

The Data Collector needs to communicate with WebSphere Administrative Services using the Remote Method Invocation (RMI) or SOAP protocol. If WebSphere Global Security is enabled, this communication requires a user name and password. You can set them when configuring the Data Collector to monitor an application server instance. For security reasons, you may also prefer to encrypt the username and password and store them in client properties files before Data Collector configuration.

Use the `sas.client.properties` file for an RMI connection, or the `soap.client.properties` file for a SOAP connection.

Note: if you choose to perform this operation, you will need to do it separately for each monitored application server profile.

Enabling user ID and password input from sas.client.props for RMI connector types

The Configuration Tool and the silent configuration provide means for you to retrieve the user ID and password (instead of entering them in the panel or silent configuration option) from the `sas.client.props` file when using a Remote Method Invocation (RMI) connection to WebSphere and WebSphere Global Security is enabled. In order for this function to work, you must set properties in the `sas.client.props` file. Perform the following procedure:

1. Set the following properties in *AppServer_home*\profiles\profile_name\properties\sas.client.props:

   ```
   com.ibm.CORBA.loginSource=properties
   com.ibm.CORBA.securityEnabled=true
   com.ibm.CORBA.loginUserid=user_ID
   com.ibm.CORBA.loginPassword=password
   ```

2. Run the following command to encrypt the password:

   ```
   PropFilePasswordEncoder.bat
     AppServer_home\profiles\profile_name\properties\sas.client.props
     com.ibm.CORBA.loginPassword
   ```

   Run it from the *AppServer_home*\profiles\profile_name\bin directory.

Enabling user ID and password input from soap.client.props for SOAP connector types

The Configuration Tool and the silent configuration provide means for you to retrieve the user ID and password (instead of entering them in the panel or silent configuration option) from the `soap.client.props` file when using a SOAP connection to WebSphere and WebSphere Global Security is enabled. In order for this function to work, you must set properties in the soap.client.props file. Perform the following procedure:

1. Set the following properties in *AppServer_home*\profiles*profile_name*\properties\soap.client.props:

   ```
   com.ibm.SOAP.securityEnabled=true
   com.ibm.SOAP.loginUserid=user_ID
   com.ibm.SOAP.loginPassword=password
   ```

2. Run the following command to encrypt the password:

   ```
   PropFilePasswordEncoder.bat
     AppServer_home\profiles\profile_name\properties\soap.client.props
     com.ibm.SOAP.loginPassword
   ```

   Run it from the *AppServer_home*\profiles*profile_name*\bin directory.

What to do next

1. Close all other applications.
2. See "Installing ITCAM Agent for WebSphere Applications on Windows" on page 15.

Chapter 3. Installing and configuring ITCAM Agent for WebSphere Applications on Windows

This chapter provides complete instructions for installing ITCAM Agent for WebSphere Applications on Microsoft® Windows platforms.

Both components of the Agent, the Data Collector and the Monitoring Agent (see "Components of the Agent" on page 5), will be installed.

The Agent supports a deep dive diagnostics only install, where the IBM Tivoli Monitoring Infrastructure is not used; the Agent communicates with the Managing Server only. In this case, you need to configure the monitoring agent not to communicate to a Tivoli Enterprise Monitoring Server, and ensure that the monitoring agent is not started automatically.

If the IBM Tivoli Monitoring Infrastructure is used, you need to ensure that the monitoring agent is started automatically when the system boots up.

If you are upgrading from ITCAM for WebSphere 6.1, ITCAM for WebResources 6.2, or ITCAM for WebSphere 7.0, you need to install the Agent on all hosts where the Data Collector or the Tivoli Enterprise Monitoring Agent was installed. The Tivoli Enterprise Monitoring Agent will be upgraded automatically. For the Data Collector, you will need to upgrade monitoring of application server instances to the new version using the configuration tool; see "Upgrading monitoring to Data Collector 7.1" on page 60.

Installing ITCAM Agent for WebSphere Applications on Windows

Perform the following steps to install ITCAM Agent for WebSphere Applications on Windows.

If the ITCAM for WebSphere Tivoli Enterprise Monitoring Agent or ITCAM for Web Resources WebSphere Tivoli Enterprise Monitoring Agent is installed on the host, use the same process to upgrade it.

Attention: you must install ITCAM Agent for WebSphere Applications version 7.1 before installing version 7.1.0.1.

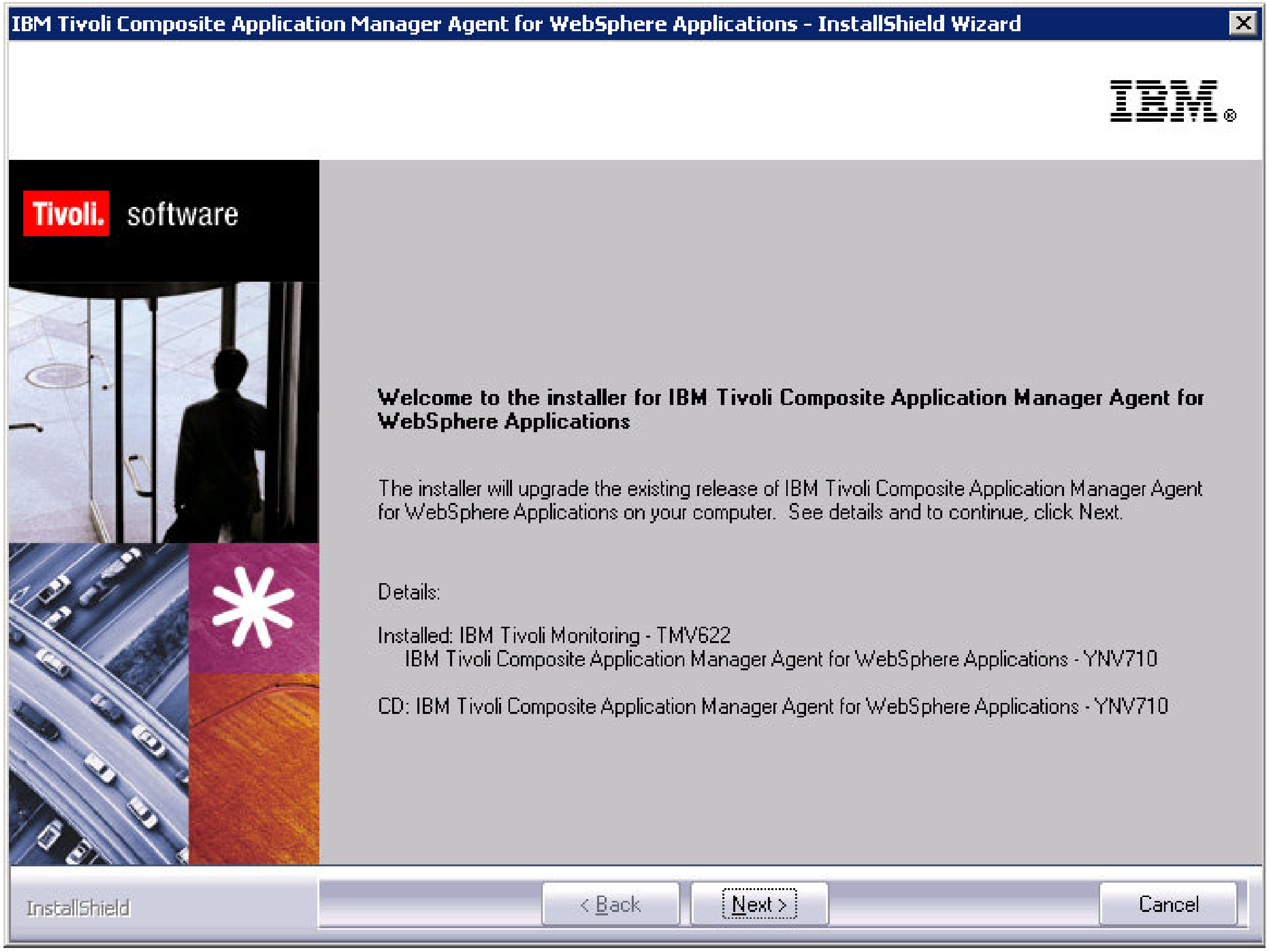
Attention: if any Data Collectors of a version lower than 6.1 Fix Pack 4 connects to this Tivoli Enterprise Monitoring Agent, monitoring for these Data Collectors will cease after the upgrade. Once you upgrade the monitoring of the application server instances to the new version of the Data Collector (see "Upgrading monitoring to Data Collector 7.1" on page 60), monitoring will start again.

If the current version of ITCAM Agent for WebSphere Applications is already installed on the host, you can use this process to reinstall it. Windows for selecting the installation directory, encryption key, and program folder will not be displayed; the reinstallation uses the same settings as the existing installation.

Before starting the process, make sure the Manage Tivoli Enterprise Monitoring Services (MTMS) utility is not running. If it is running, stop it. An upgrade installation can fail if the utility is running.

Step 1: Invoke setup.exe

After loading the ITCAM Agent for WebSphere Applications Winfows DVD, locate and double-click the setup.exe file within the `WINDOWS` directory. The initial InstallShield window opens:



IBM Tivoli Composite Application Manager Agent for WebSphere Applications - InstallShield Wizard

Welcome to the installer for IBM Tivoli Composite Application Manager Agent for WebSphere Applications

The installer will upgrade the existing release of IBM Tivoli Composite Application Manager Agent for WebSphere Applications on your computer. See details and to continue, click Next.

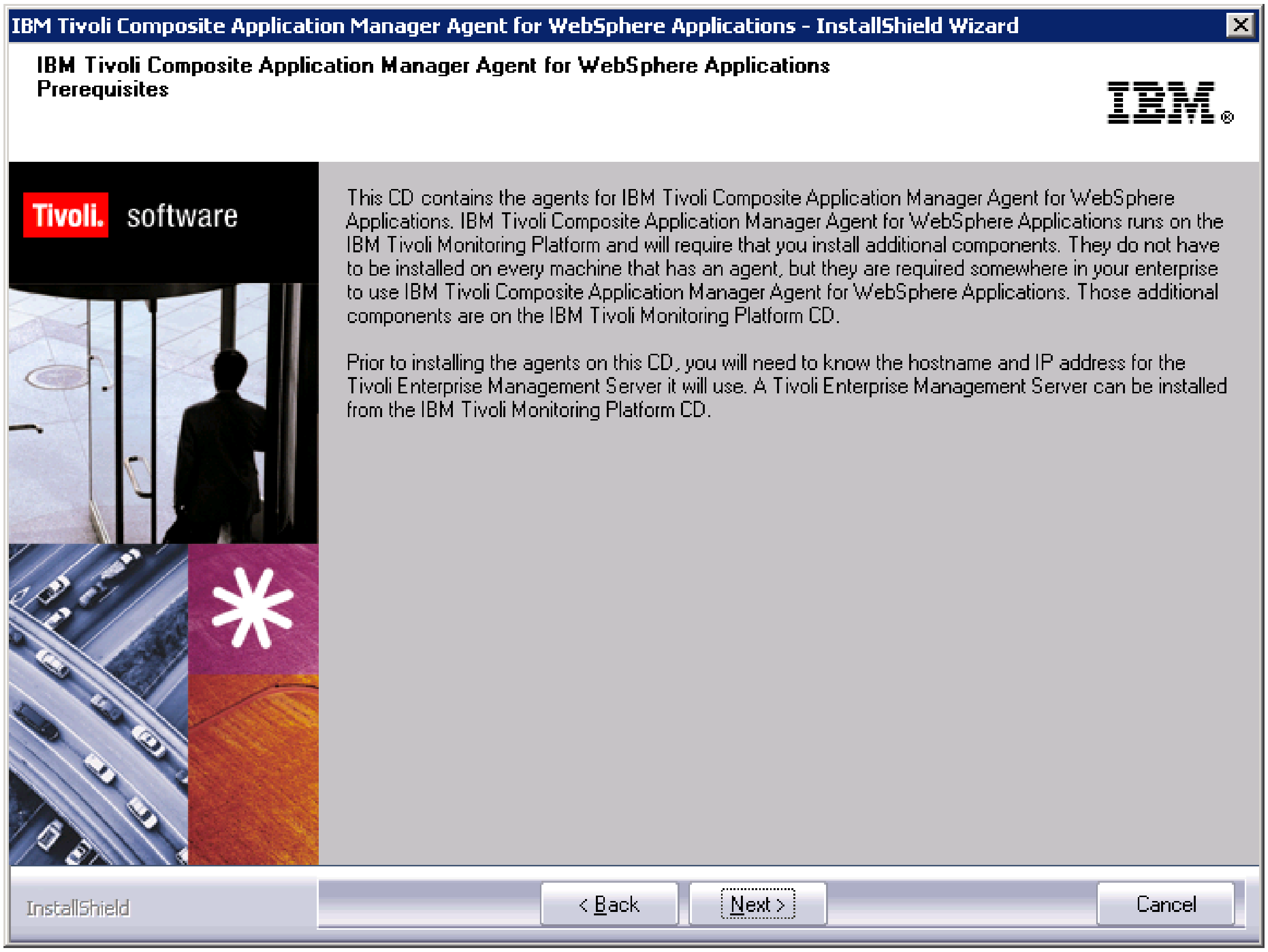
Details:

Installed: IBM Tivoli Monitoring - TMV622
IBM Tivoli Composite Application Manager Agent for WebSphere Applications - YNV710

CD: IBM Tivoli Composite Application Manager Agent for WebSphere Applications - YNV710

Figure 3. Installation Welcome window

Click **Next**. The product prerequisites window opens:



IBM Tivoli Composite Application Manager Agent for WebSphere Applications - InstallShield Wizard
IBM Tivoli Composite Application Manager Agent for WebSphere Applications
Prerequisites
IBM
Tivoli. software
InstallShield
< Back
Next >
Cancel

This CD contains the agents for IBM Tivoli Composite Application Manager Agent for WebSphere Applications. IBM Tivoli Composite Application Manager Agent for WebSphere Applications runs on the IBM Tivoli Monitoring Platform and will require that you install additional components. They do not have to be installed on every machine that has an agent, but they are required somewhere in your enterprise to use IBM Tivoli Composite Application Manager Agent for WebSphere Applications. Those additional components are on the IBM Tivoli Monitoring Platform CD.

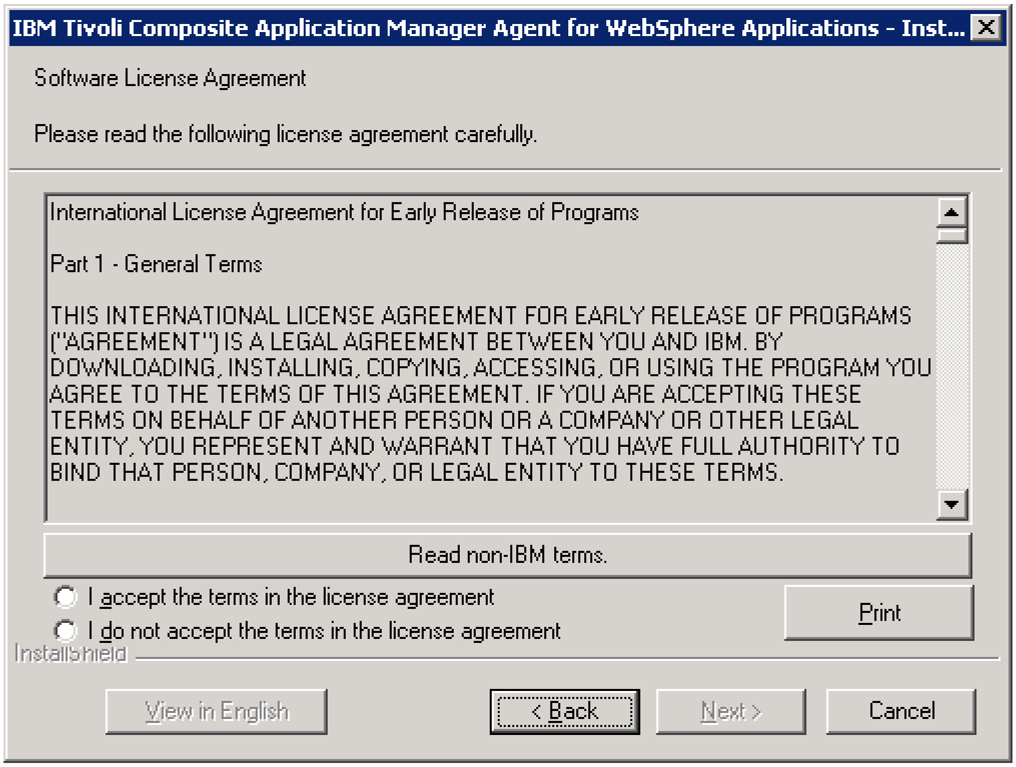
Prior to installing the agents on this CD, you will need to know the hostname and IP address for the Tivoli Enterprise Management Server it will use. A Tivoli Enterprise Management Server can be installed from the IBM Tivoli Monitoring Platform CD.

Figure 4. Prerequisites window

If the environment meets the prerequisites, click **Next**. Before installing the Agent, you need to know the hostname and IP address for the Tivoli Enterprise Monitoring Server it will use.

Step 2: Accept the product license

The Software License Agreement window is displayed.



IBM Tivoli Composite Application Manager Agent for WebSphere Applications - Inst...

Software License Agreement

Please read the following license agreement carefully.

International License Agreement for Early Release of Programs

Part 1 - General Terms

THIS INTERNATIONAL LICENSE AGREEMENT FOR EARLY RELEASE OF PROGRAMS ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU AND IBM. BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS.

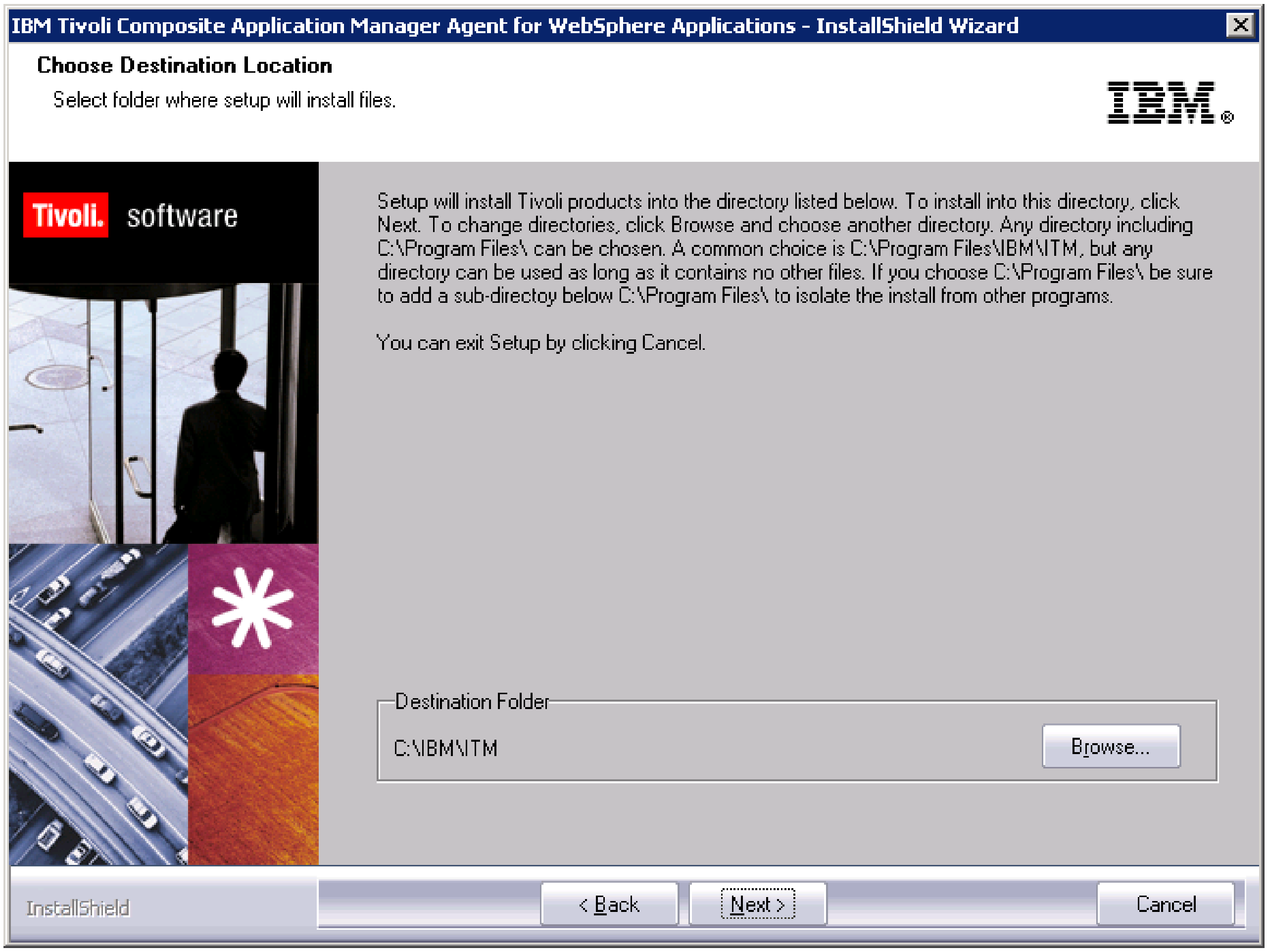
Read non-IBM terms.
○ I accept the terms in the license agreement
○ I do not accept the terms in the license agreement
Print
InstallShield
View in English
< Back
Next >
Cancel

Figure 5. Software License Agreement window

Select **I accept the terms in the license agreement** and click **Next**.

Step 3: Choose the destination folder for the installation files

In an upgrade or update installation, the destination directory is determined automatically, and this step is skipped. On a new installation, the **Choose destination location** window opens.



IBM Tivoli Composite Application Manager Agent for WebSphere Applications - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

Setup will install Tivoli products into the directory listed below. To install into this directory, click Next. To change directories, click Browse and choose another directory. Any directory including C:\Program Files\ can be chosen. A common choice is C:\Program Files\IBM\ITM, but any directory can be used as long as it contains no other files. If you choose C:\Program Files\ be sure to add a sub-directoy below C:\Program Files\ to isolate the install from other programs.

You can exit Setup by clicking Cancel.

Destination Folder

C:\IBM\ITM

Figure 6. Choose Destination Location window

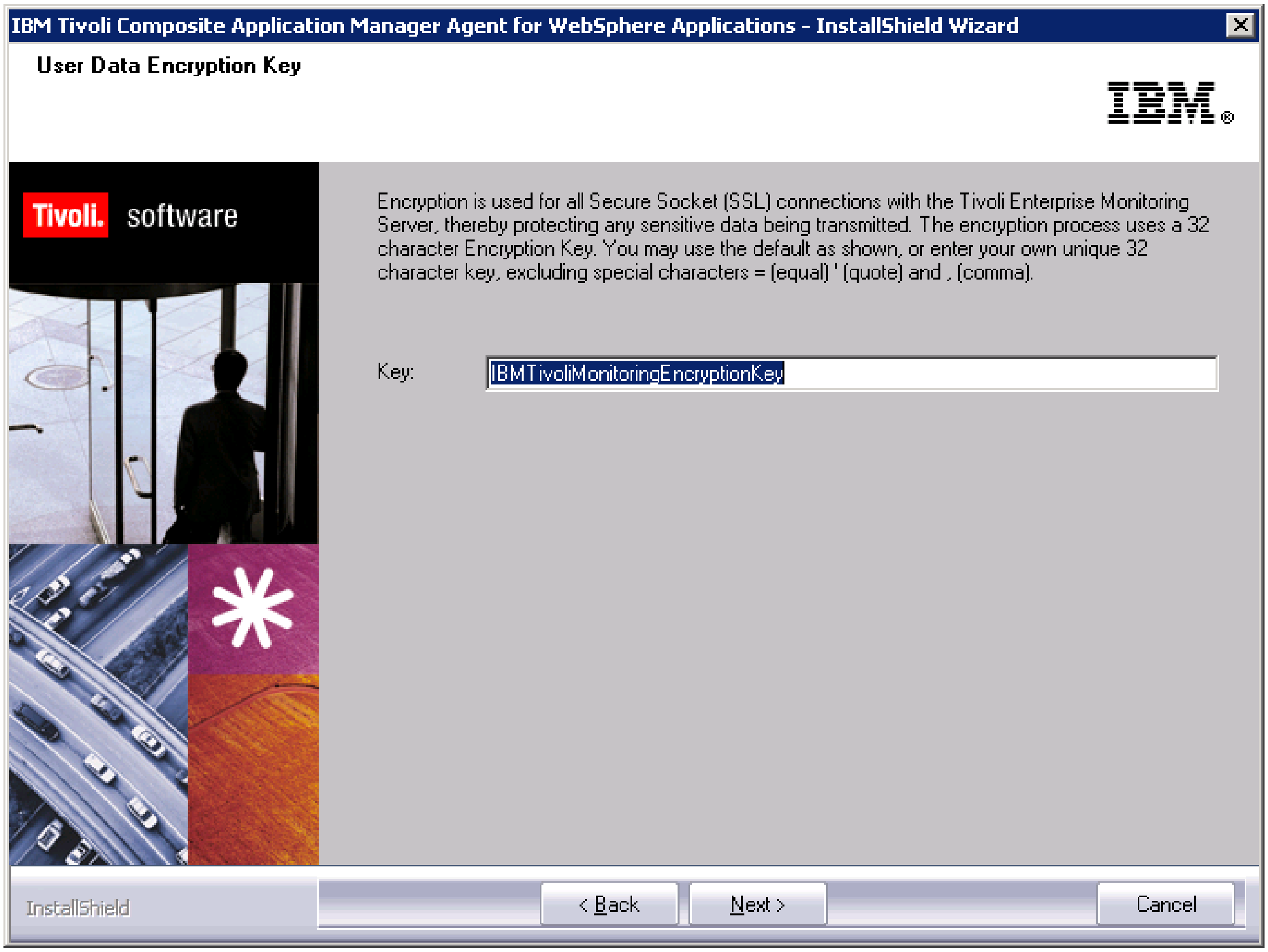
This window shows the folder (*ITM_home*) where the Agent is to be installed. The destination folder can be shared with other IBM Tivoli Monitoring products. If you want to use a location other than the default (`C:\IBM\ITM`), click **Browse**, and select the folder that you want to use.

When the correct folder is specified, click **Next**.

Attention: If the current version of ITCAM Agent for WebSphere Applications is already installed on the host, this window will not be displayed. The reinstallation will use the same directory as the existing installation. Proceed to the next step.

Step 4: Enter the IBM Tivoli Monitoring encryption key

In an upgrade or update installation, or when some IBM Tivoli Monitoring components are already installed, the data encryption key is already set, and this step is skipped. On a new installation, the **User Data Encryption Key** window opens. It prompts you for the 32-character encryption key used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment:



IBM Tivoli Composite Application Manager Agent for WebSphere Applications - InstallShield Wizard

User Data Encryption Key

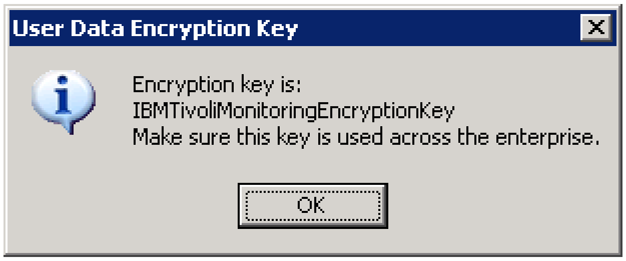
Encryption is used for all Secure Socket (SSL) connections with the Tivoli Enterprise Monitoring Server, thereby protecting any sensitive data being transmitted. The encryption process uses a 32 character Encryption Key. You may use the default as shown, or enter your own unique 32 character key, excluding special characters = (equal) ' (quote) and , (comma).

Key: IBMTivoliMonitoringEncryptionKey

Figure 7. User Data Encryption Key window

See IBM Tivoli Monitoring: Installation and Setup Guide for details about the encryption key. Click **Next** when you have specified the key.

A confirmation window opens.



User Data Encryption Key

Encryption key is:
IBMTivoliMonitoringEncryptionKey
Make sure this key is used across the enterprise.

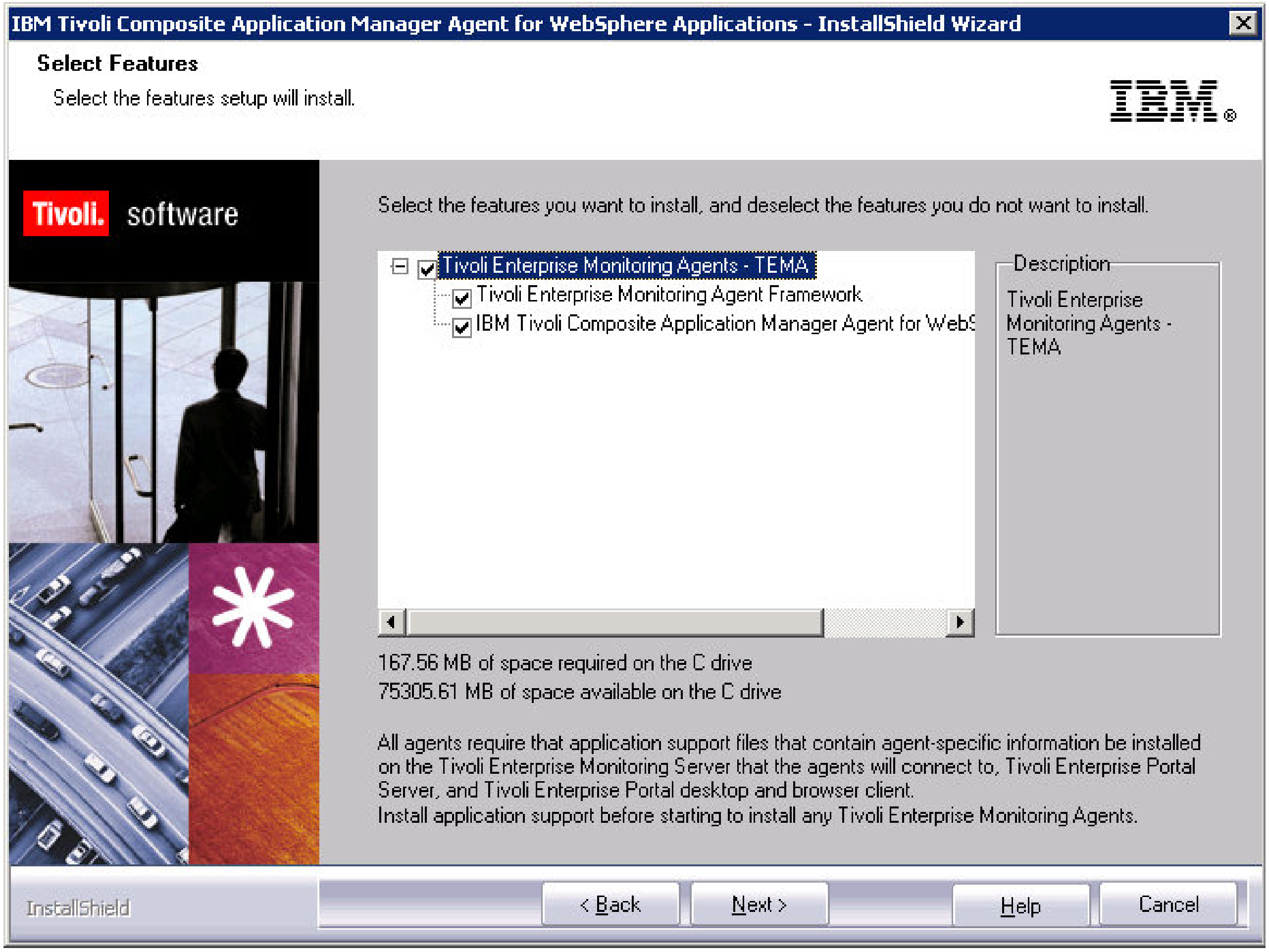
Figure 8. Encryption Key confirmation window

Click **OK** to confirm the encryption key.

Attention: If the current version of ITCAM Agent for WebSphere Applications is already installed on the host, this window will not be displayed. The reinstallation will use the same key as the existing installation. Proceed to the next step.

Step 5: Select the product components you want to install

The **Select Features** window is displayed.



IBM Tivoli Composite Application Manager Agent for WebSphere Applications - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- ☑ Tivoli Enterprise Monitoring Agents - TEMA
  - ☑ Tivoli Enterprise Monitoring Agent Framework
  - ☑ IBM Tivoli Composite Application Manager Agent for WebS

Description

Tivoli Enterprise Monitoring Agents - TEMA

167.56 MB of space required on the C drive

75305.61 MB of space available on the C drive

All agents require that application support files that contain agent-specific information be installed on the Tivoli Enterprise Monitoring Server that the agents will connect to, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop and browser client.
Install application support before starting to install any Tivoli Enterprise Monitoring Agents.

Figure 9. Select Features window

When you are performing an update from an earlier maintenance level, the installed components are selected automatically.

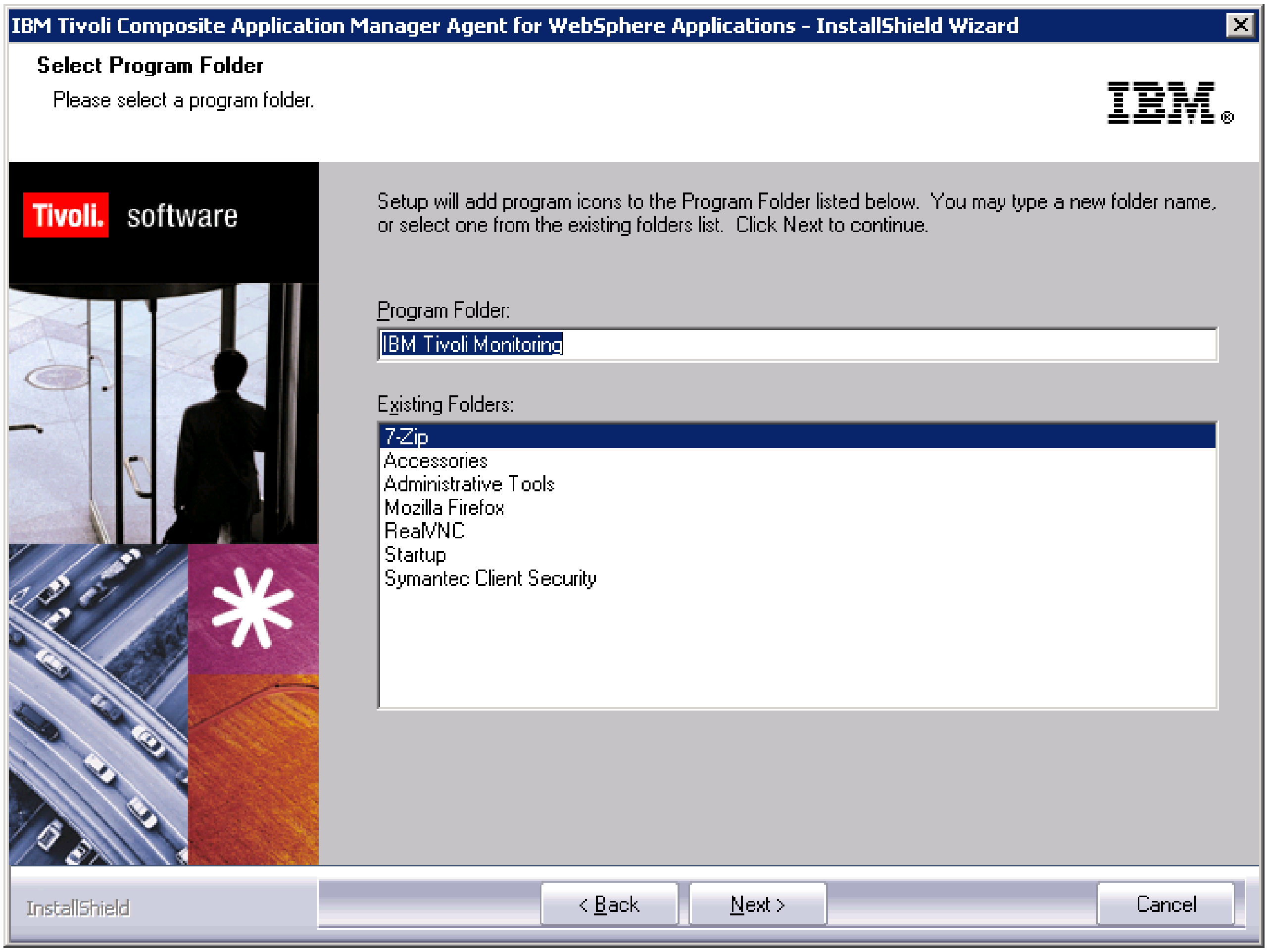
Select **Tivoli Enterprise Monitoring Agents - TEMA**. This window might vary if the IBM Tivoli Monitoring framework is already installed on this host.

Important: If any IBM Tivoli Monitoring Agent is already installed on this host, make sure to expand the tree in this window and explicitly check **IBM Tivoli Composite Application Manager Agent for WebSphere Applications**. By default, if an IBM Tivoli Monitoring Agent is found, it will not be checked even if you check the top level box.

Click **Next**.

Step 6: Select Windows program folder

The **Select Program Folder** window opens. It displays the Windows program folder for IBM Tivoli Monitoring programs:



IBM Tivoli Composite Application Manager Agent for WebSphere Applications - InstallShield Wizard

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folder:

IBM Tivoli Monitoring

Existing Folders:

7-Zip
Accessories
Administrative Tools
Mozilla Firefox
RealVNC
Startup
Symantec Client Security

Figure 10. Select Program Folder window

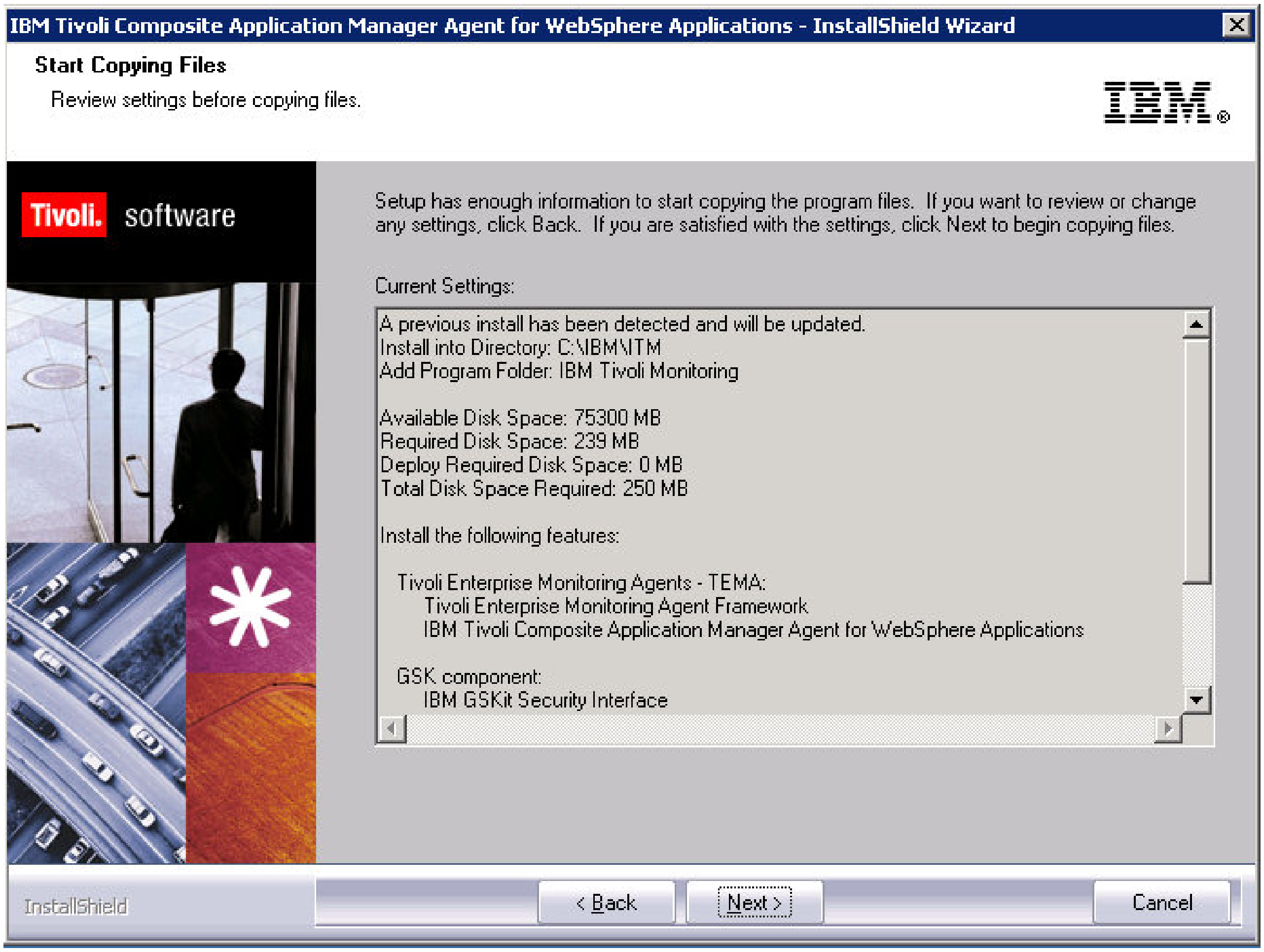
You can modify the name of the folder (under the **Programs** menu) where IBM Tivoli Monitoring programs will be listed.

Then, click **Next**.

Attention: If the current version of ITCAM Agent for WebSphere Applications is already installed on the host, this window will not be displayed. The reinstallation will use the same program folder as the existing installation. Proceed to the next step.

Step 7: Verify selected features

The **Start Copying Files** window opens, showing the features that you have selected, the disk space requirements for the installation, and the available disk space.


IBM Tivoli Composite Application Manager Agent for WebSphere Applications - InstallShield Wizard
Start Copying Files
Review settings before copying files.
IBM
Tivoli. software
InstallShield
< Back
Next >
Cancel

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
A previous install has been detected and will be updated.
Install into Directory: C:\IBM\ITM
Add Program Folder: IBM Tivoli Monitoring

Available Disk Space: 75300 MB
Required Disk Space: 239 MB
Deploy Required Disk Space: 0 MB
Total Disk Space Required: 250 MB

Install the following features:

  Tivoli Enterprise Monitoring Agents - TEMA:
      Tivoli Enterprise Monitoring Agent Framework
      IBM Tivoli Composite Application Manager Agent for WebSphere Applications

  GSK component:
      IBM GSKit Security Interface
```

Figure 11. Selected features verification window

Verify that the features that you want to install, including **Monitoring Agent for WebSphere**, are in the list. If you need to make changes, click **Back**.

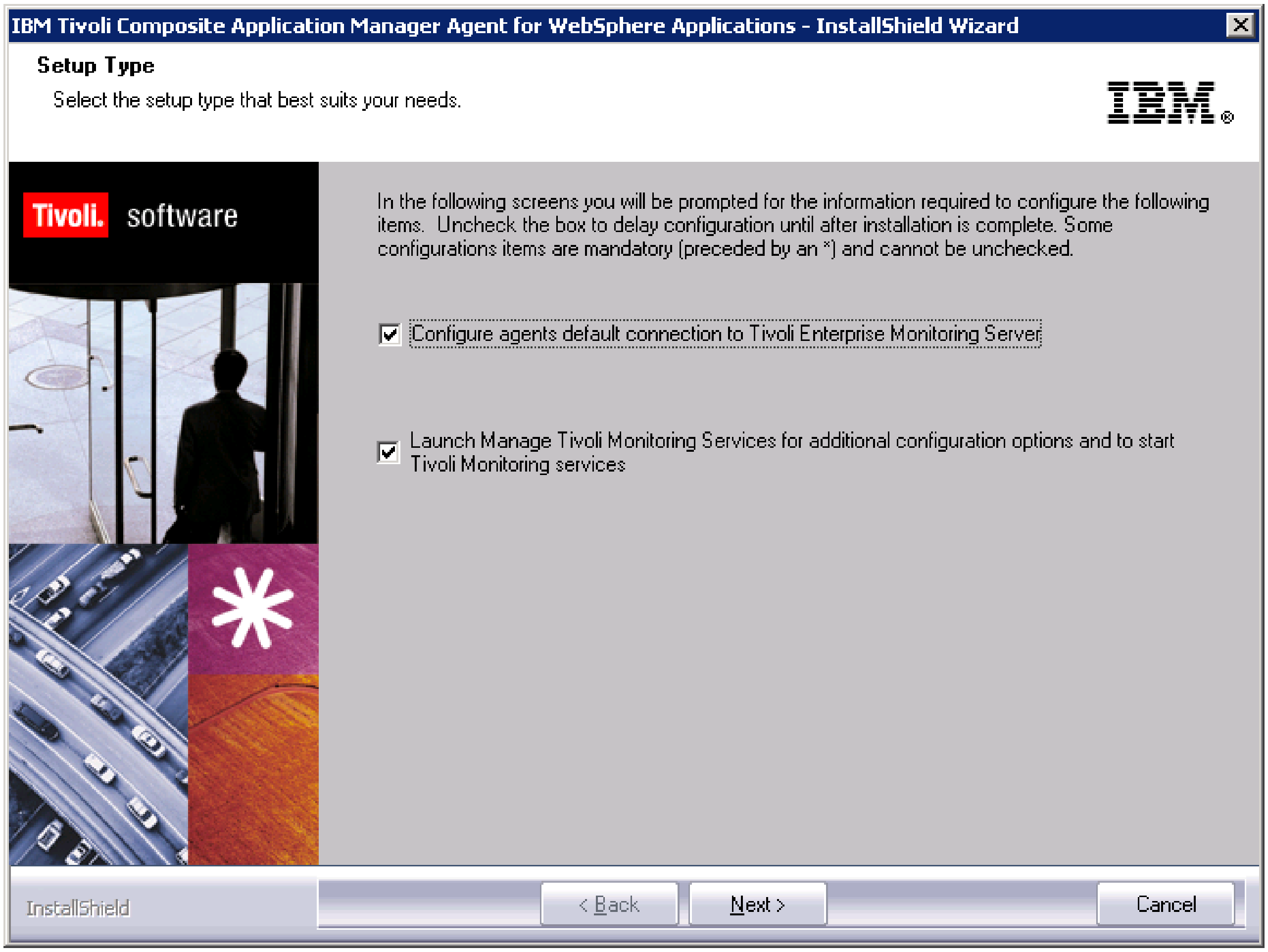
If the list is correct, click **Next**.

The system displays a warning that you will not be able to cancel the installation after this point. Click **Yes** to start the installation.

The installer copies the necessary files to the destination directory.

Step 8: Select the items to configure

When the copying of filese is complete, you may select whether to configure the Agent in the **Setup Type** window.


IBM Tivoli Composite Application Manager Agent for WebSphere Applications - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

In the following screens you will be prompted for the information required to configure the following items. Uncheck the box to delay configuration until after installation is complete. Some configurations items are mandatory (preceded by an *) and cannot be unchecked.

☑ Configure agents default connection to Tivoli Enterprise Monitoring Server

☑ Launch Manage Tivoli Monitoring Services for additional configuration options and to start Tivoli Monitoring services

Figure 12. Setup Type window

By default, all the checkboxes are selected. This means that you will be prompted to configure the Agent.

If you are *not* using the IBM Tivoli Monitoring infrastructure (in a deep dive diagnostics only install), uncheck both checkboxes. You will still be presented with the Agent configuration screen in order to configure the Data Collector to monitor application server instances.

If you are using IBM Tivoli Monitoring infrastructure, keep the first checkbox checked, as you will need to configure the monitoring agent before configuring the Data Collector. If you keep the second checkbox checked, the Managing Tivoli Monitoring Services utility will be started after the configuration; you can use it to configure automatic starting of the monitoring agent and any other IBM Tivoli Monitoring settings.

When the selections are correct, click **Next** to finish the installation. If one or both of the configuration options are selected, configuration windows are displayed next; see "Configuring ITCAM Agent for WebSphere Applications on Windows" on page 25.

Configuring ITCAM Agent for WebSphere Applications on Windows

This section provides instructions on configuring ITCAM Agent for WebSphere Applications.

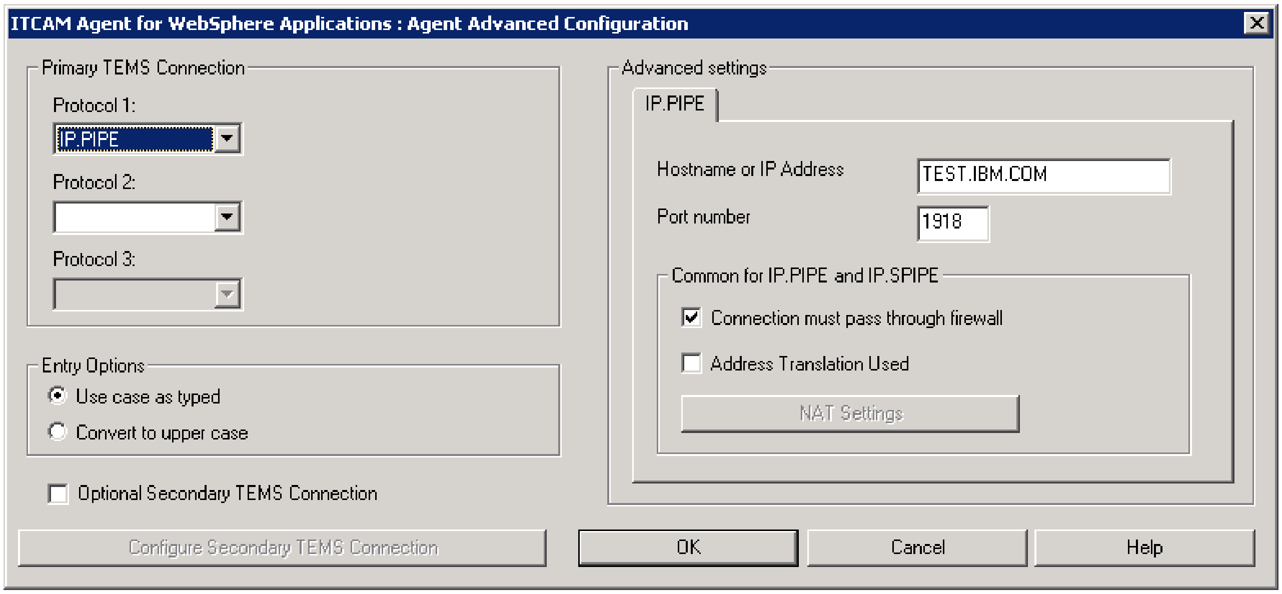
Entering the Agent Configuration window

You may skip this section if you are configuring the Agent immediately after installing it, as the installer starts the Tivoli Enterprise Monitoring Server (TEMS) connection configuration window (if required) and the Agent configuration window automatically.

To perform most of the configuration procedures described in this section, you need to start from the **Agent Configuration** window. To enter this window, enter the Windows Start Menu and click **Programs** → **IBM Tivoli** → **Monitoring** → **Manage Tivoli Monitoring Services**. The **Manage Tivoli Monitoring Services** window is displayed. For details on the Manage Tivoli Monitoring Services application, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Right-click **ITCAM Agent for WebSphere Applications** and select **Reconfigure...**.

A window for configuring the TEMS connection will be displayed.



ITCAM Agent for WebSphere Applications : Agent Advanced Configuration

Primary TEMS Connection

Protocol 1: IP.PIPE

Protocol 2:

Protocol 3:

Entry Options

● Use case as typed

○ Convert to upper case

□ Optional Secondary TEMS Connection

Advanced settings

IP.PIPE

Hostname or IP Address: TEST.IBM.COM

Port number: 1918

Common for IP.PIPE and IP.SPIPE

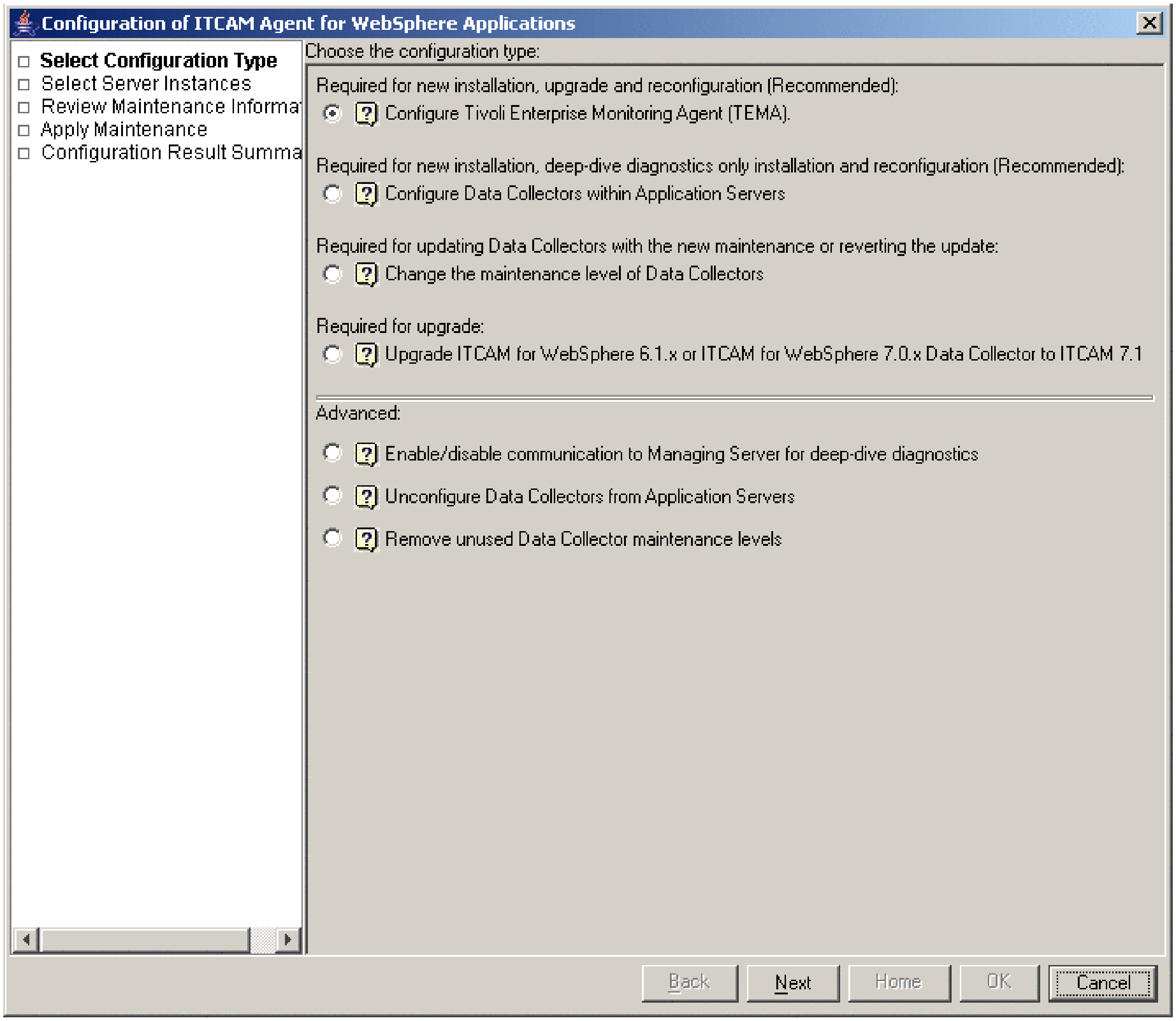
☑ Connection must pass through firewall

□ Address Translation Used

Figure 13. TEMS connection configuration window

If IBM Tivoli Monitoring infrastructure is not used (in a deep dive diagnostics only installation), ignore this window and click **OK**. If the TEMS connection is already configured, you do not need to make any changes; click **OK**. Otherwise, see "Configure the monitoring agent connection to the monitoring server" on page 26.

After this window, the Agent Configuration window is displayed.



Configuration of ITCAM Agent for WebSphere Applications

□ **Select Configuration Type**
□ Select Server Instances
□ Review Maintenance Informa
□ Apply Maintenance
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):
● Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):
○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:
○ Change the maintenance level of Data Collectors

Required for upgrade:
○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:
○ Enable/disable communication to Managing Server for deep-dive diagnostics
○ Unconfigure Data Collectors from Application Servers
○ Remove unused Data Collector maintenance levels

Figure 14. The Agent Configuration window

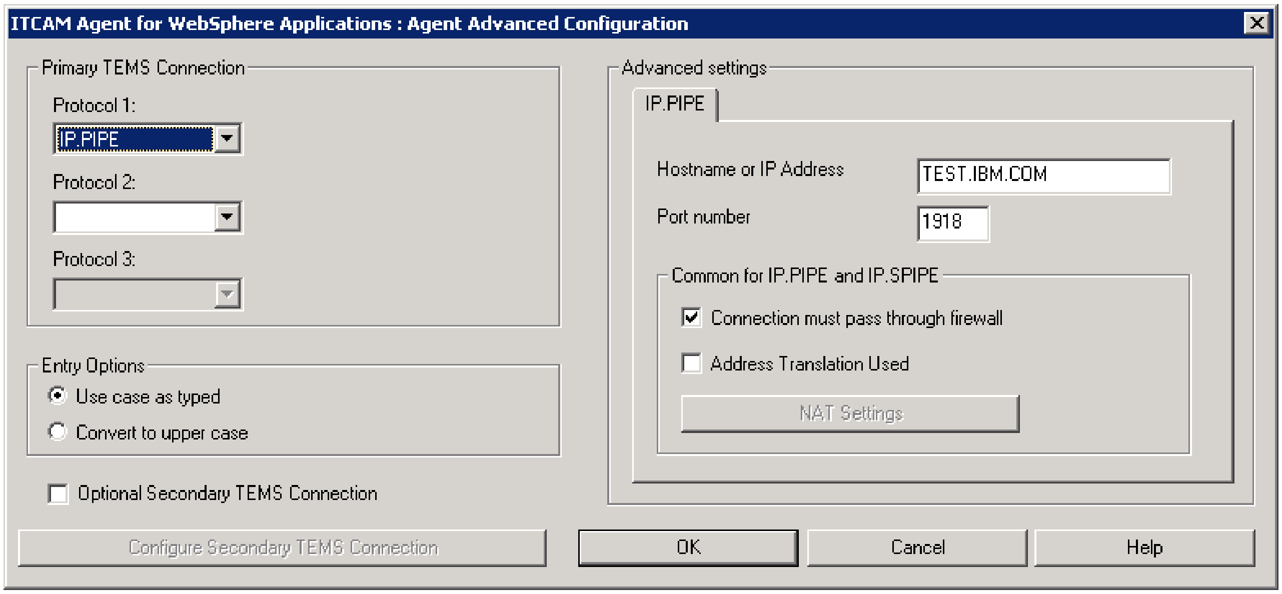
Note: On Windows, the window for configuring Monitoring Agent configuration to the Tivoli Enterprise Monitoring Server is always displayed at the beginning of the configuration process. This is different from Linux and UNIX systems, where this window is displayed at the end of the configuration process.

Configure the monitoring agent connection to the monitoring server

After installation of the agent, if you have selected **Configure agents default connection to Tivoli Enterprise Monitoring Server** in the Figure 12 on page 24, the **Configuration defaults for connecting to a TEMS** window opens. Use this window to configure the connection of the Monitoring Agent to a Tivoli Enterprise Monitoring Server.

If you need to change this information later, use the **Manage Tivoli Monitoring Services** window; to do this, right-click **ITCAM Agent for WebSphere Applications** and select **Reconfigure...**.

Tip: To open the the **Manage Tivoli Monitoring Services** window, you can enter the Windows Start Menu and click **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**. For details on the Manage Tivoli Monitoring Services application, see IBM Tivoli Monitoring: Installation and Setup Guide.



ITCAM Agent for WebSphere Applications : Agent Advanced Configuration

Primary TEMS Connection

Protocol 1: IP.PIPE

Protocol 2:

Protocol 3:

Entry Options

● Use case as typed

○ Convert to upper case

□ Optional Secondary TEMS Connection

Advanced settings

IP.PIPE

Hostname or IP Address: TEST.IBM.COM

Port number: 1918

Common for IP.PIPE and IP.SPIPE

☑ Connection must pass through firewall

□ Address Translation Used

Figure 15. Configuring the monitoring agent connection to the monitoring server

If IBM Tivoli Monitoring infrastructure is not used (in a deep dive diagnostics only installation), ignore this window and click **OK**. (Do not click **Cancel**).

Specify these parameters as explained in *IBM Tivoli Monitoring: Installation and Setup Guide*.

- If the monitoring agent must access the monitoring server across a firewall, select **Connection must pass through firewall**.
- Identify the protocol that the monitoring agent will use to communicate with the hub monitoring server. You have five choices: IP.UDP, IP.PIPE, IP.SPIPE, SNA or No TEMS. The value that you specify here must match the value specified when installing the monitoring server. You can also set a secondary protocol if required.
- If your site has set up failover support for its Tivoli monitoring agents, select **Optional Secondary TEMS Connection**, and specify the same communication protocols you chose when installing this monitoring server.

Click **OK**.

For the protocol or protocols that you have selected in the previous window, specify these fields as explained in Table 2.

Table 2. Communications protocol settings

Field	**Description**
IP.UDP Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port # and/or Port Pools	The listening port for the hub monitoring server.

Table 2. Communications protocol settings (continued)

Field	Description
IP.PIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port Number	The listening port for the monitoring server. The default value is 1918.
IP.SPIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port number	The listening port for the hub monitoring server. The default value is 3660.
SNA Settings	
Network Name	The SNA network identifier for your location.
LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
LU 6.2 LOGMODE	The name of the LU6.2 LOGMODE. The default value is CANCTDCS.
TP Name	The transaction program name for the monitoring server.
Local LU Alias	The LU alias.

Click **OK**.

Configure Monitoring Agent settings

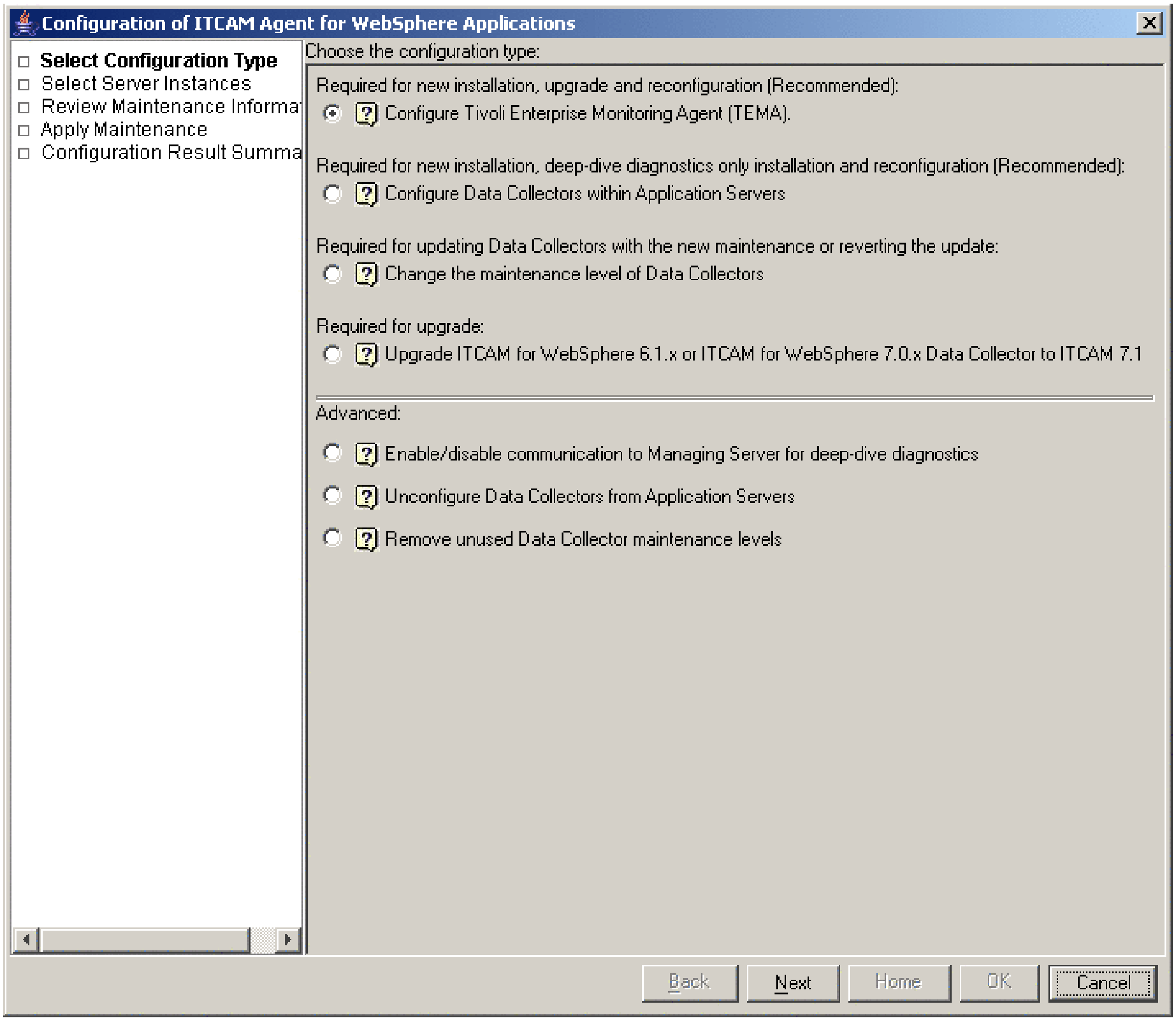
If the IBM Tivoli Monitoring infrastructure is used, you **must** configure Monitoring Agent settings before configuring the Data Collector to monitor any application server instances. Do not perform this configuration in a deep dive diagnostics only installation, where IBM Tivoli Monitoring is not used.

You may change the port that is used for communication between the Data Collector and the monitoring agent (this communication is on the local host, except if the monitoring agent is used for IBM i Data Collectors); the default port is 63335. You may also set an alternate node name that determines how the agent will be displayed in the Tivoli Enterprise Portal navigation tree.

While you can change these at a later time, it is normally most convenient to set them when initially configuring the communication. In this case no manual changes to configuration files is required to change the port number, and no customization of the Tivoli Enterprise Portal view could have been performed by any user. So, if you need to make such changes, make them at installation time if possible.

To configure Monitoring Agent settings, perform the following procedure:

1. Enter the Agent Configuration window. After installation of the Agent, this window opens automatically. Otherwise, see "Entering the Agent Configuration window" on page 25.


Configuration of ITCAM Agent for WebSphere Applications
□ Select Configuration Type
□ Select Server Instances
□ Review Maintenance Informa
□ Apply Maintenance
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

● Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

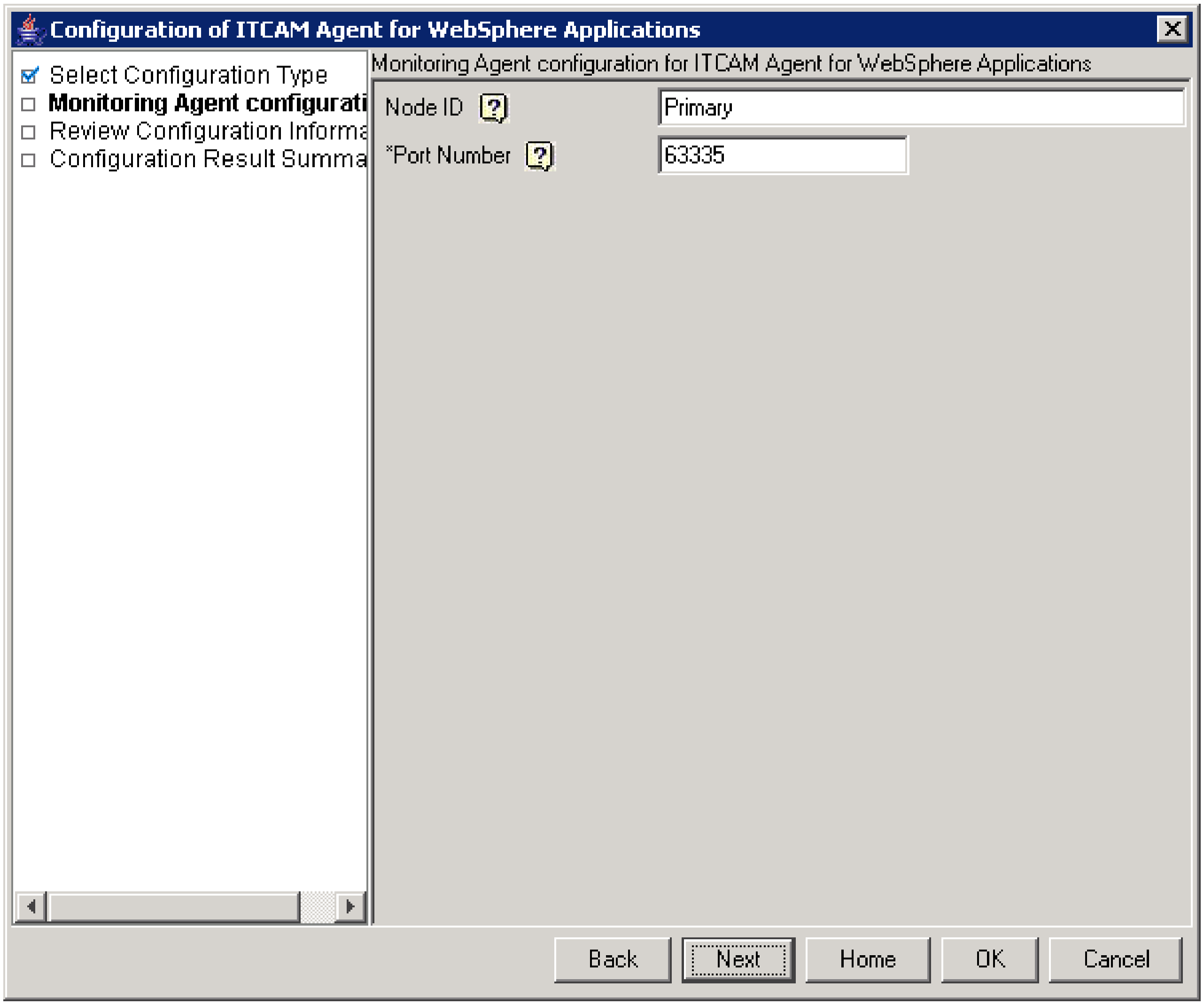
○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 16. Configuring Communication to the monitoring agent, window 1

2. Select **Configure Tivoli Enterprise Monitoring Agent (TEMA)** and click **Next**.
3. In the Agent Configuration page you can set an alternative Node ID for identifying the agent. This is the identifier that will determine how the agent will be displayed in the Tivoli Enterprise Portal navigation tree. The default is `Primary`, used in conjunction with the host name of the computer where the Agent is installed. In the **Port** field you can specify a TCP socket port that the monitoring agent will use to listen for connection requests from the Data Collectors. Normally, do not change this value. The port will only be used for local communication on the host (except if you use the monitoring agent to support Data Collectors on IBM i hosts, see *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Data Collector Installation and Configuration Guide for IBM i*. Click **Next**.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
□ **Monitoring Agent configurati**
□ Review Configuration Informa
□ Configuration Result Summa

Monitoring Agent configuration for ITCAM Agent for WebSphere Applications

Node ID: Primary

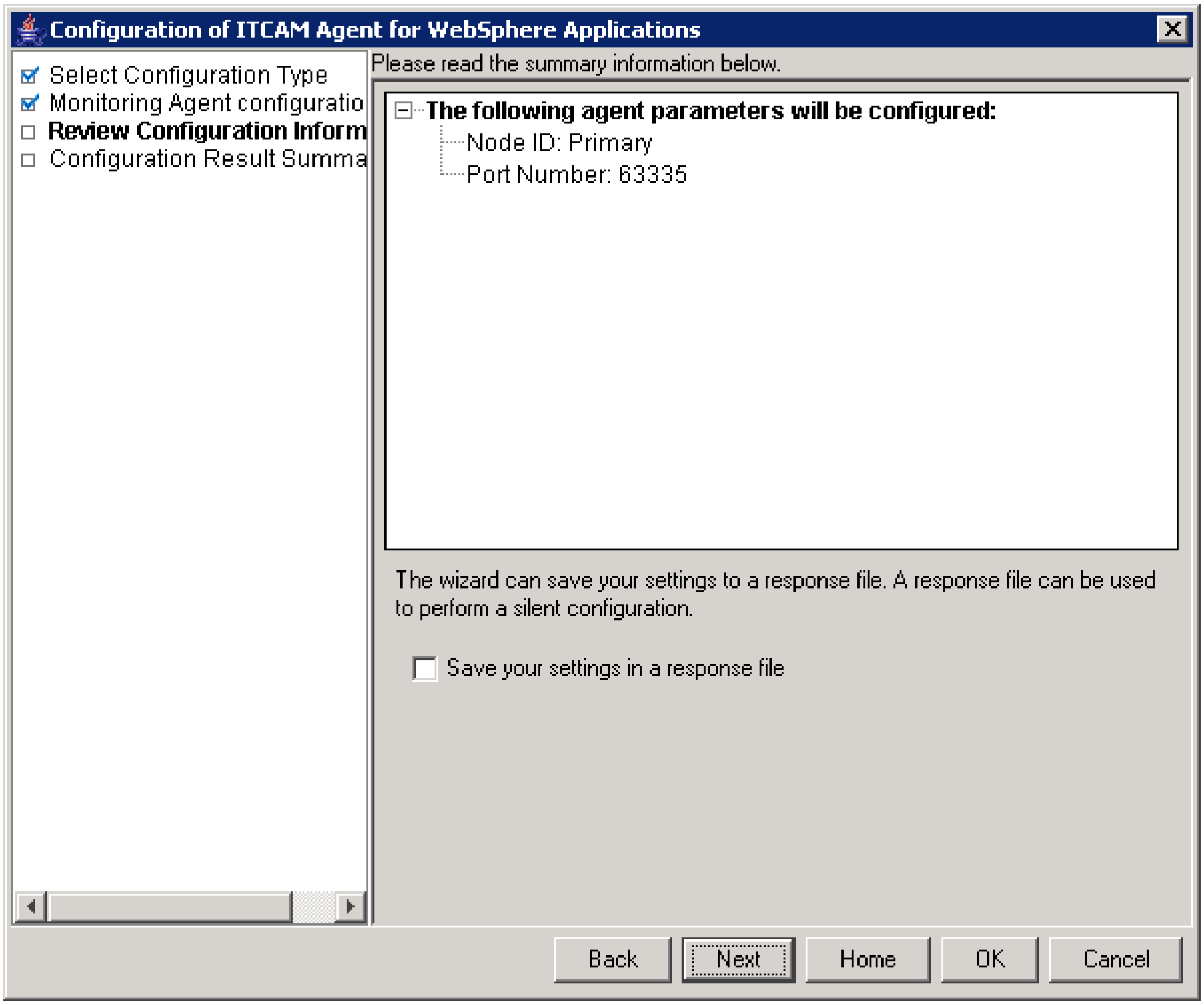
*Port Number: 63335

Figure 17. Configuring Communication to the Monitoring Agent, window 2

Enter the Node ID if necessary; change the port number if necessary. Click **Next**.

Attention: Valid characters for the node ID include A-z, a-z, 0-9, underbar (_), dash (-), and period (.); do not use other characters.

4. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Monitoring Agent configuratio
□ Review Configuration Inform
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Please read the summary information below.

The following agent parameters will be configured:

- Node ID: Primary
- Port Number: 63335

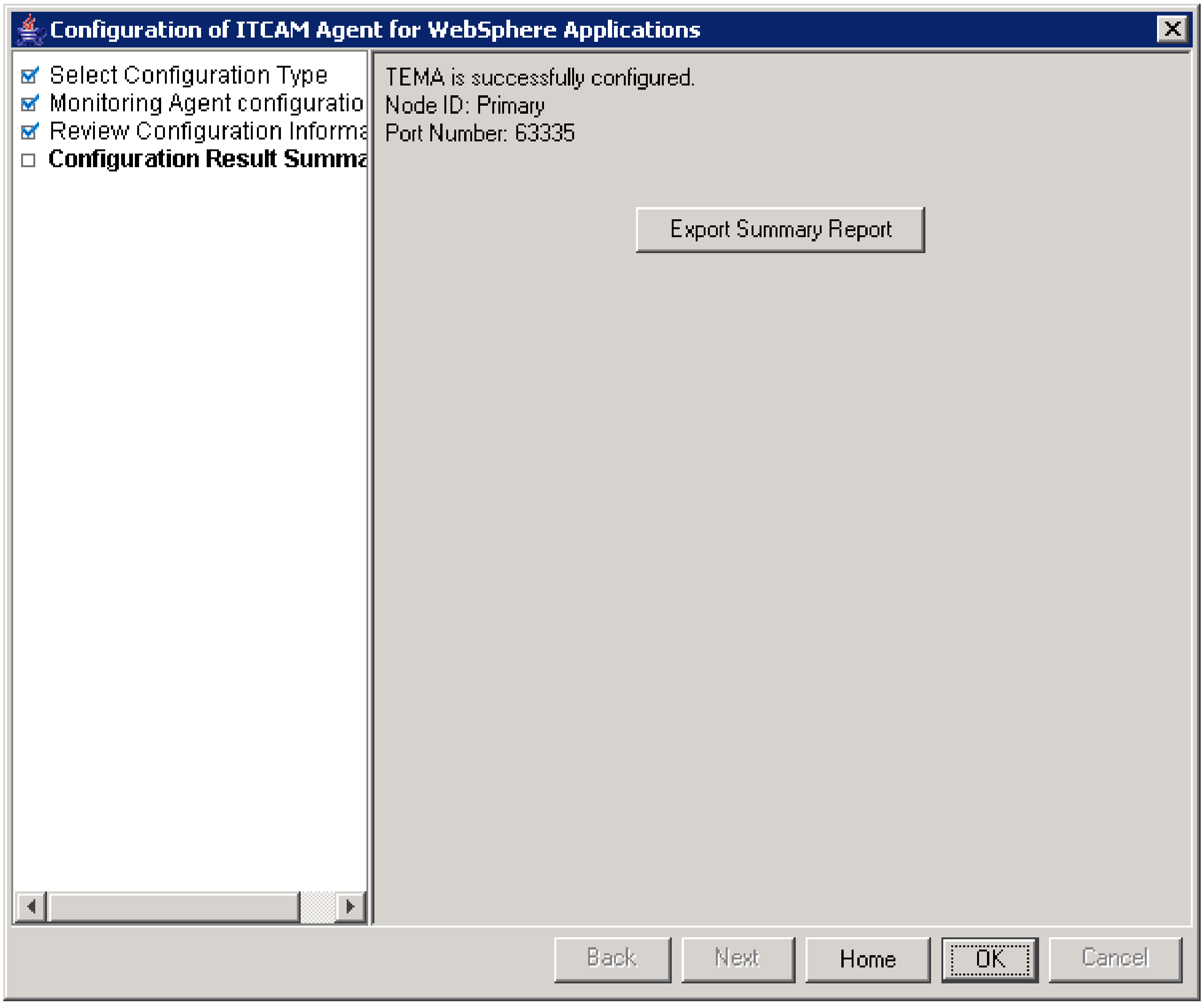
The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

□ Save your settings in a response file

Figure 18. Configuring Communication to the monitoring agent, window 3

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location, then click **Next**. Otherwise, leave the box unchecked and click **Next**.

5. The monitoring agent is successfully configured.



Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Monitoring Agent configuratio
☑ Review Configuration Informa
□ Configuration Result Summa
Export Summary Report
Back
Next
Home
OK
Cancel

TEMA is successfully configured.
Node ID: Primary
Port Number: 63335

Figure 19. Configuring Communication to the monitoring agent, window 4

Click **Home** to return to the **Agent Configuration** window, or click **OK** to complete the configuration process.

Configure the Data Collector to monitor application server instances

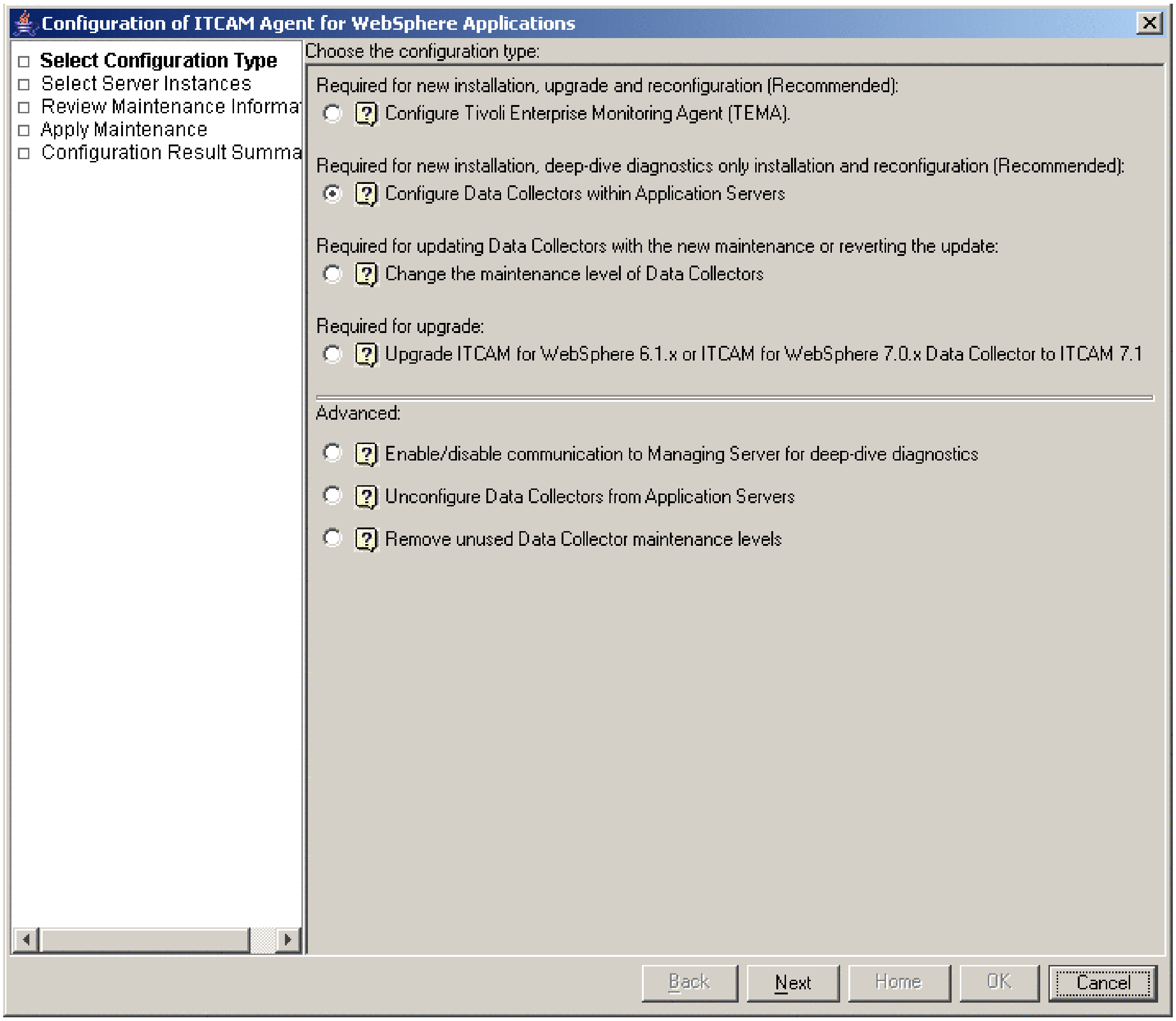
You must configure the Data Collector for each application server instance that you need to monitor.

Important: Do not configure the Data Collector to monitor an instance of WebSphere Application Server that hosts the Managing Server Visualization Engine. You may, however, use the Data Collector for monitoring any other WebSphere Application Server instances on the same node.

To configure the Data Collector to monitor a server instance, perform the following procedure:

1. Enter the Agent Configuration window. After installation of the Agent, if you have selected **Launch Manage Tivoli Monitoring Services for additional configuration options and to start Tivoli Monitoring services** in the Figure 12 on page 24, this window opens automatically. Otherwise, see “Entering the

Agent Configuration window" on page 25.



Configuration of ITCAM Agent for WebSphere Applications

- □ **Select Configuration Type**
- □ Select Server Instances
- □ Review Maintenance Informa
- □ Apply Maintenance
- □ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

● Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

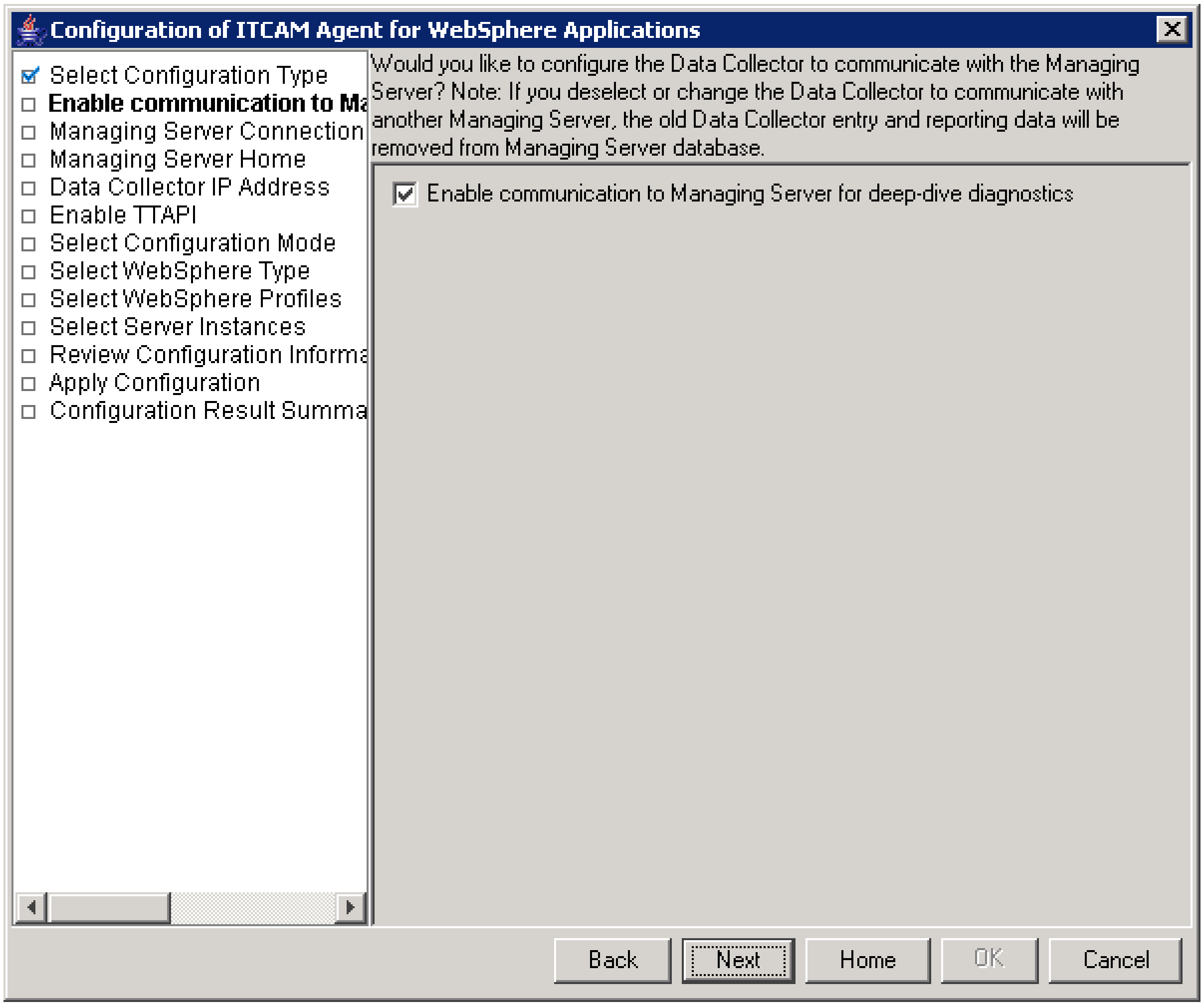
○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 20. Configuring the Data Collector to monitor application server instances, window 1

2. Select **Configure Data Collectors within Application Servers** and click **Next**.
3. You can choose to configure the Data Collector to communicate with ITCAM for Application Diagnostics Managing Server. Otherwise, this application server instance will not be monitored by the Managing Server infrastructure. (IBM Tivoli Monitoring is not affected by this setting).


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ Enable communication to Ma
□ Managing Server Connection
□ Managing Server Home
□ Data Collector IP Address
□ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Would you like to configure the Data Collector to communicate with the Managing Server? Note: If you deselect or change the Data Collector to communicate with another Managing Server, the old Data Collector entry and reporting data will be removed from Managing Server database.

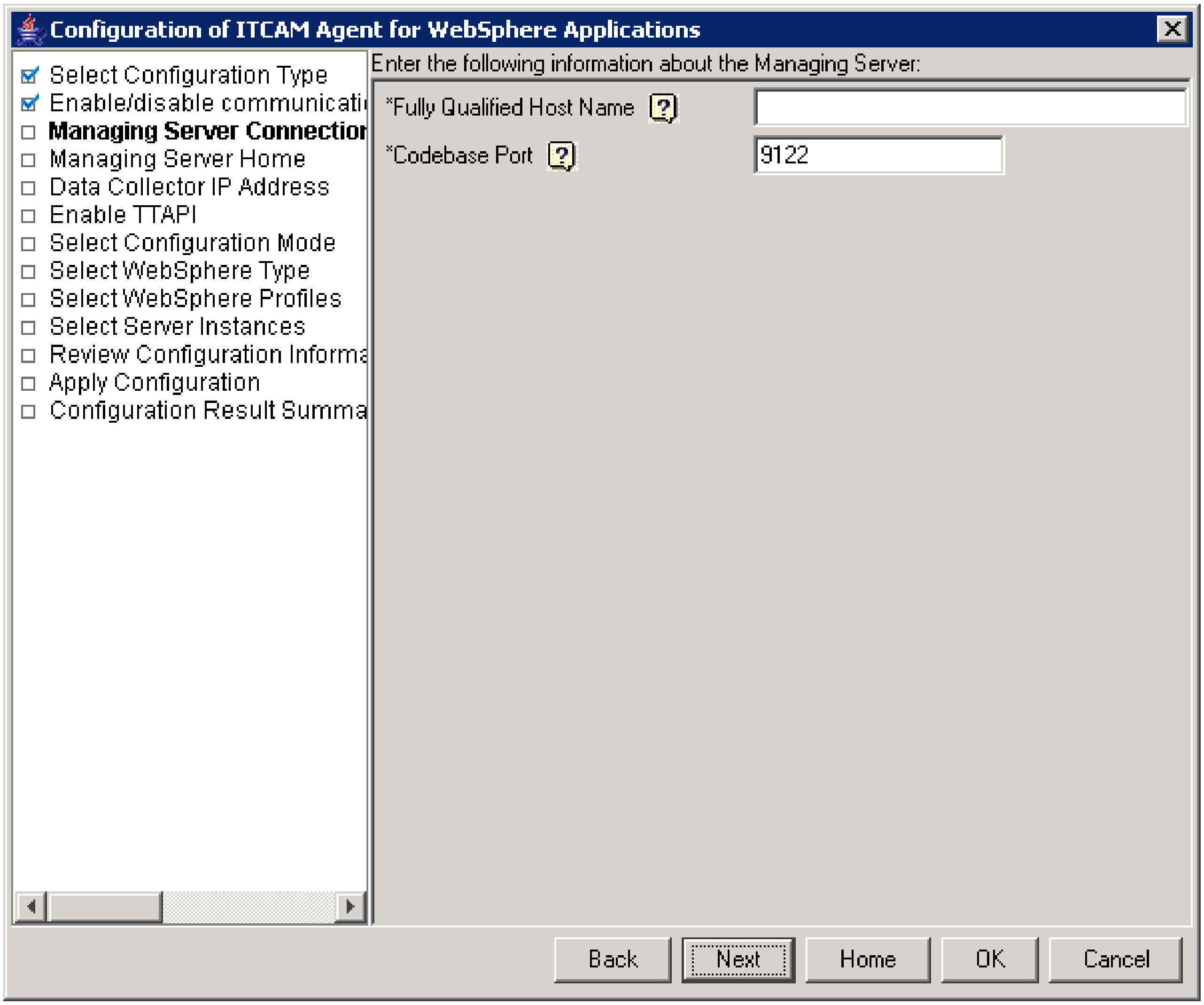
☑ Enable communication to Managing Server for deep-dive diagnostics

Figure 21. Configuring the Data Collector to monitor application server instances, window 2

If you want to configure the Data Collector to communicate with the Managing Server, check the **Enable communication to Managing Server for deep-dive diagnostics** box. Then, Click **Next**. If you left the box unchecked, go to step 7 on page 37.

Note: If you leave the box unchecked, you can still configure the Data Collector to communicate with the Managing Server later. See “Configure Data Collector communication with the Managing Server” on page 53.

4. Enter the fully qualified host name of the Managing Server. If a split Managing Server installation is used, this must be the host where the Kernel is located.



Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- ☑ Enable/disable communicati
- □ **Managing Server Connectior**
- □ Managing Server Home
- □ Data Collector IP Address
- □ Enable TTAPI
- □ Select Configuration Mode
- □ Select WebSphere Type
- □ Select WebSphere Profiles
- □ Select Server Instances
- □ Review Configuration Informa
- □ Apply Configuration
- □ Configuration Result Summa

Enter the following information about the Managing Server:

*Fully Qualified Host Name	
*Codebase Port	9122

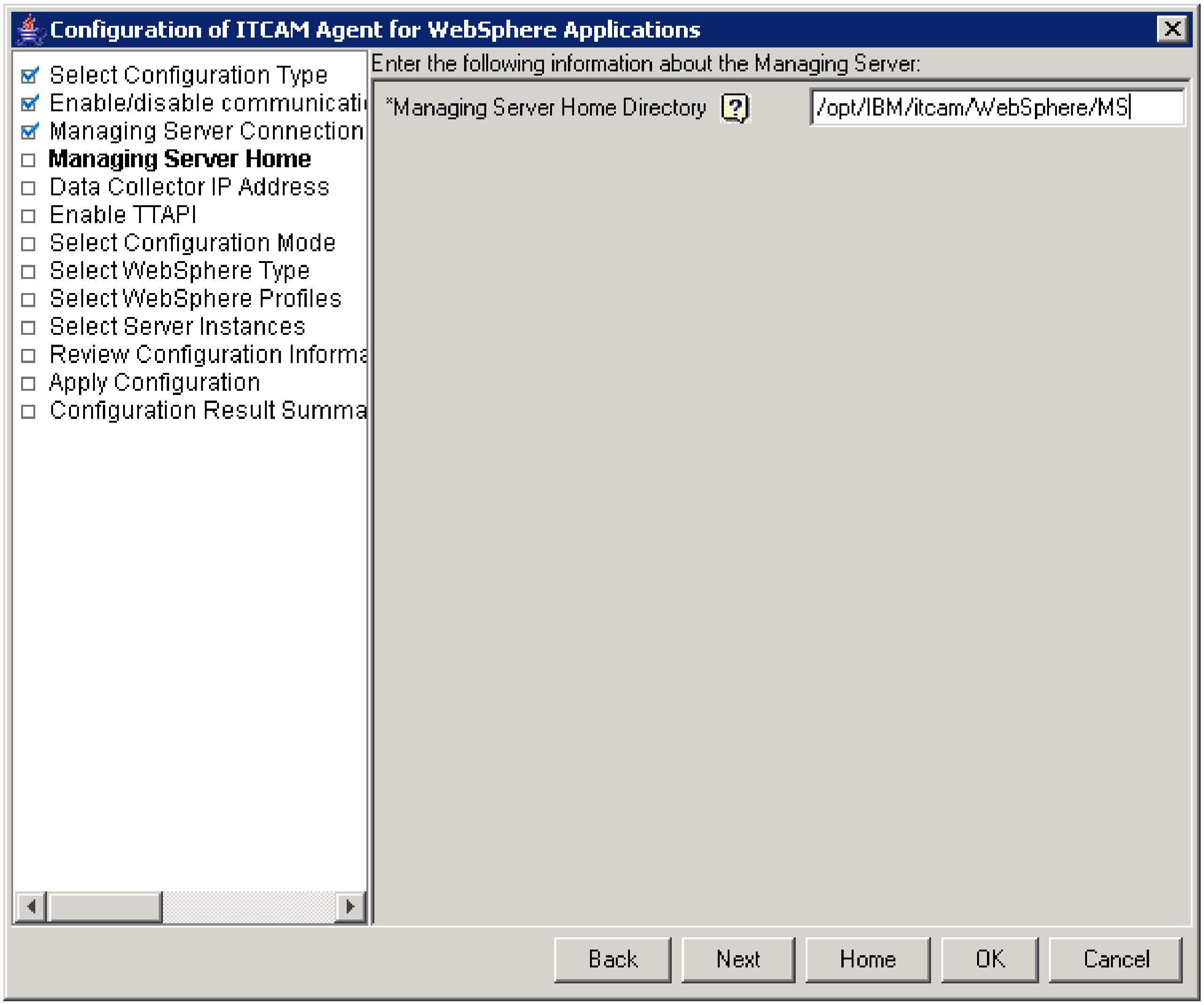
Figure 22. Configuring the Data Collector to monitor application server instances, window 3

If the Managing Server is installed on the same host as the Agent, the address and port for this Managing Server will be displayed by default, but you can change them.

After entering the host name, you may also change the port number on which the Managing Server Kernel is listening. Then, click **Next**.

Note: This port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the .ITCAM61_MS_CONTEXT.properties file located under the Managing Server Home directory. See IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide.

5. Set the Managing Server home directory, which is the destination directory chosen during the installation of the Managing Server.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
☑ Managing Server Connection
□ Managing Server Home
□ Data Collector IP Address
□ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Enter the following information about the Managing Server:

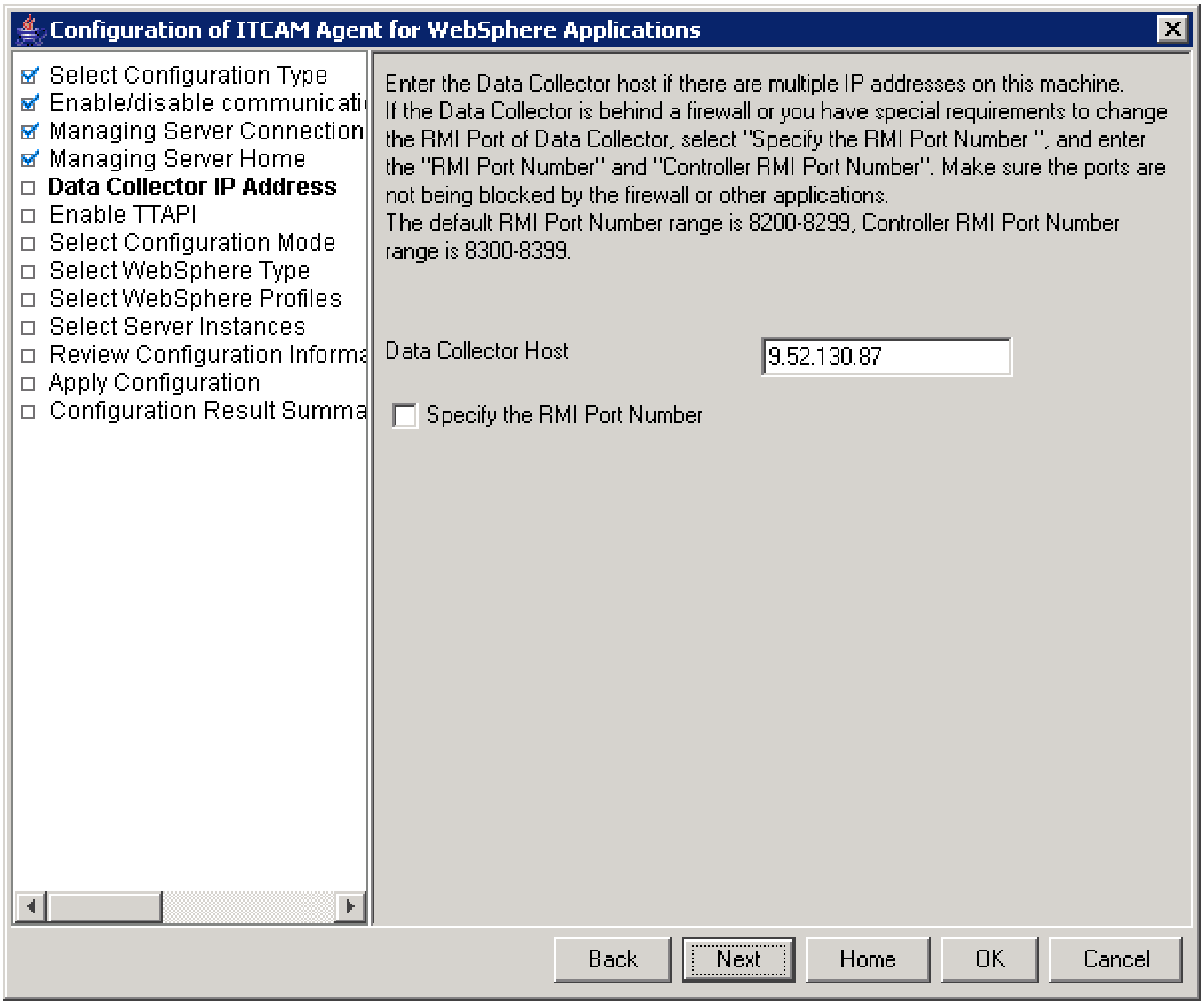
*Managing Server Home Directory ? /opt/IBM/itcam/WebSphere/MS

Figure 23. Configuring the Data Collector to monitor application server instances, window 4

If the Managing Server is running and the configuration utility has been able to communicate to it, its home directory will be displayed by default. If the Managing Server is not available at the time of communication, you need to enter the home directory.

If the Managing Server home directory is not displayed, input it. Click **Next**.

6. If there are multiple IP address on this host, select the address that the Data Collector needs to use for communication with the Managing Server. Also, if you need to change the ports that the Data Collector uses to accept incoming connections from the Managing Server (in case of split Managing Server installation, the Publish Server), select "Specify the RMI Port Number", and enter the "RMI Port Number" and "Controller RMI Port Number". Make sure the ports are not being blocked by the firewall or other applications. The default RMI port Number range is 8200-8299; the Controller RMI Port Number range is 8300-8399.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
☑ Managing Server Connection
☑ Managing Server Home
□ Data Collector IP Address
□ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Enter the Data Collector host if there are multiple IP addresses on this machine.
If the Data Collector is behind a firewall or you have special requirements to change the RMI Port of Data Collector, select "Specify the RMI Port Number ", and enter the "RMI Port Number" and "Controller RMI Port Number". Make sure the ports are not being blocked by the firewall or other applications.
The default RMI Port Number range is 8200-8299, Controller RMI Port Number range is 8300-8399.

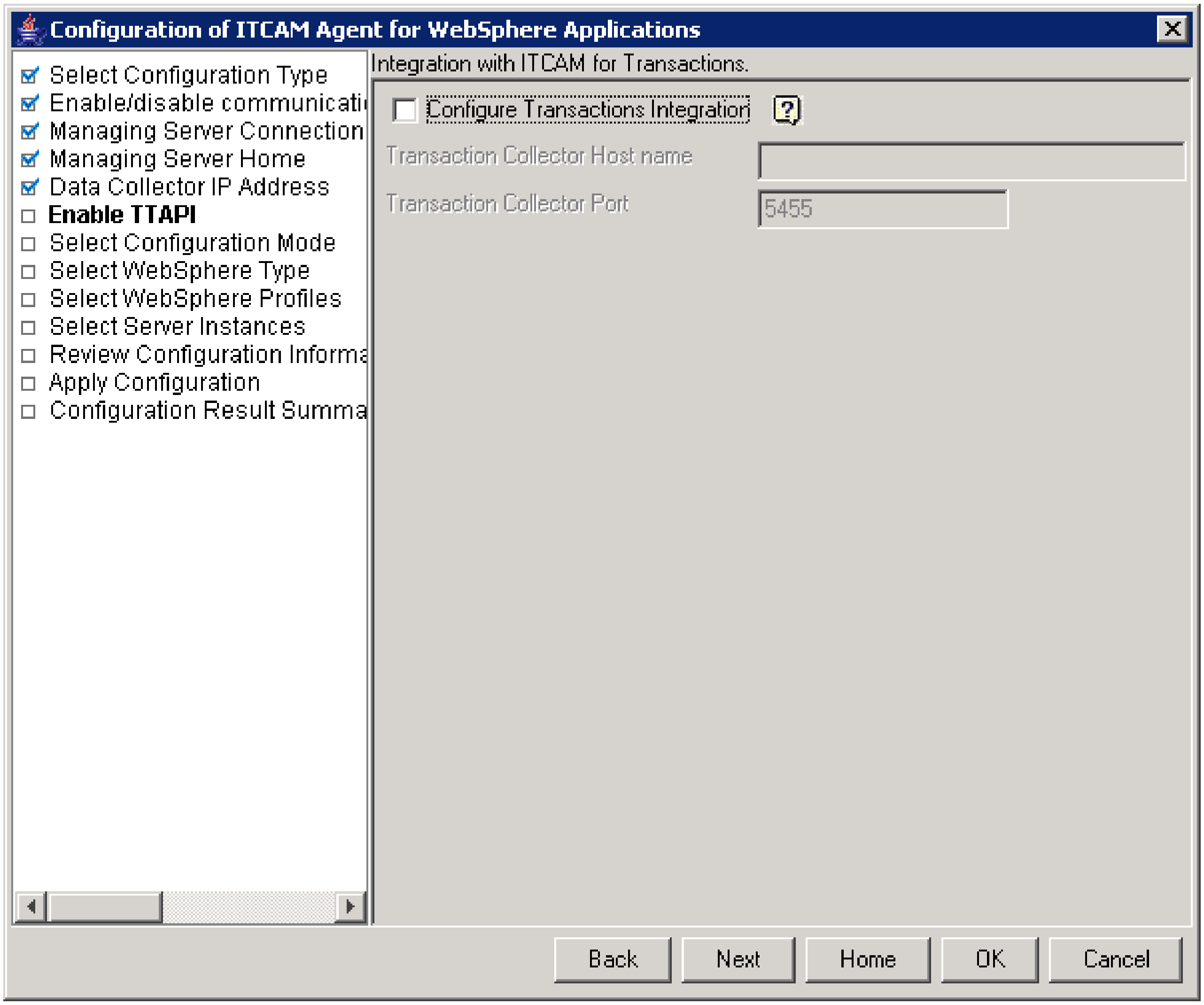
Data Collector Host: 9.52.130.87

□ Specify the RMI Port Number

Figure 24. Configuring the Data Collector to monitor application server instances, window 5

After making any necessary changes, click **Next**.

7. You can enable the Transaction Tracking API function in the following window. Transaction Tracking Application Programming Interface (TTAPI) enables the integration of ITCAM Agent for WebSphere Applications and ITCAM for Transactions. With TTAPI, the Data Collector can send transaction information to ITCAM for Transactions; also, if ITCAM for Application Diagnostics Managing Server is used, transaction specific information is available in the Visualization Engine. TTAPI also enables integration of the Data Collector with the Robotic Response Time component (or T6 agent).


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
☑ Managing Server Connection
☑ Managing Server Home
☑ Data Collector IP Address
□ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Integration with ITCAM for Transactions.

□ Configure Transactions Integration

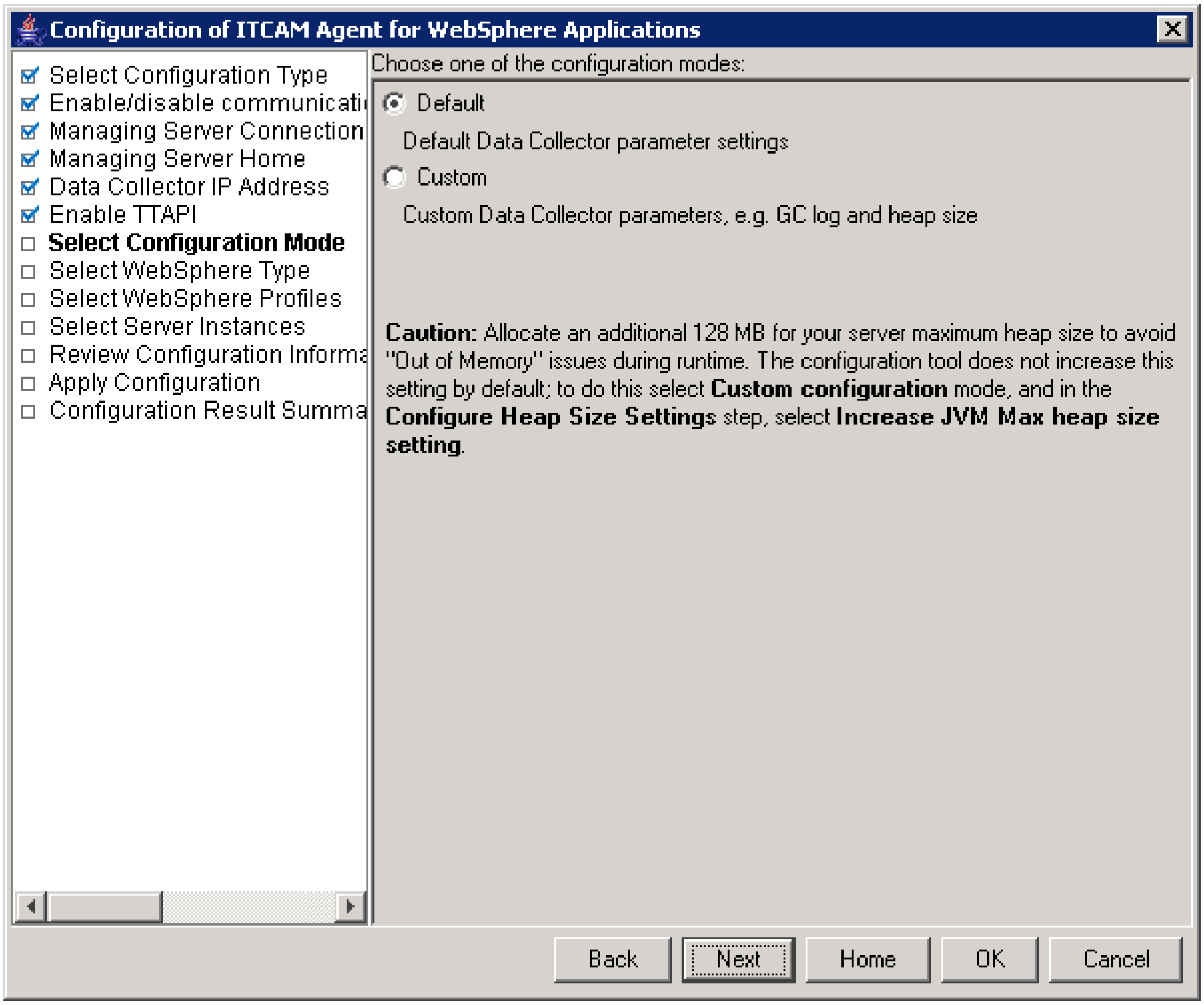
Transaction Collector Host name

Transaction Collector Port 5455

Figure 25. Configuring the Data Collector to monitor application server instances, window 6

To enable TTAPI, check the **Configure Transactions Integration** box, and enter the fully qualified host name or IP address for ITCAM for Transaction Tracking agent and the port number that the Data Collector uses to connect to it. Then, click **Next**. If you do not need to enable the Transaction Tracking API function, leave the box unchecked and click **Next**.

8. A window for selecting the configuration mode is displayed.



Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
☑ Managing Server Connection
☑ Managing Server Home
☑ Data Collector IP Address
☑ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose one of the configuration modes:

● Default

Default Data Collector parameter settings

○ Custom

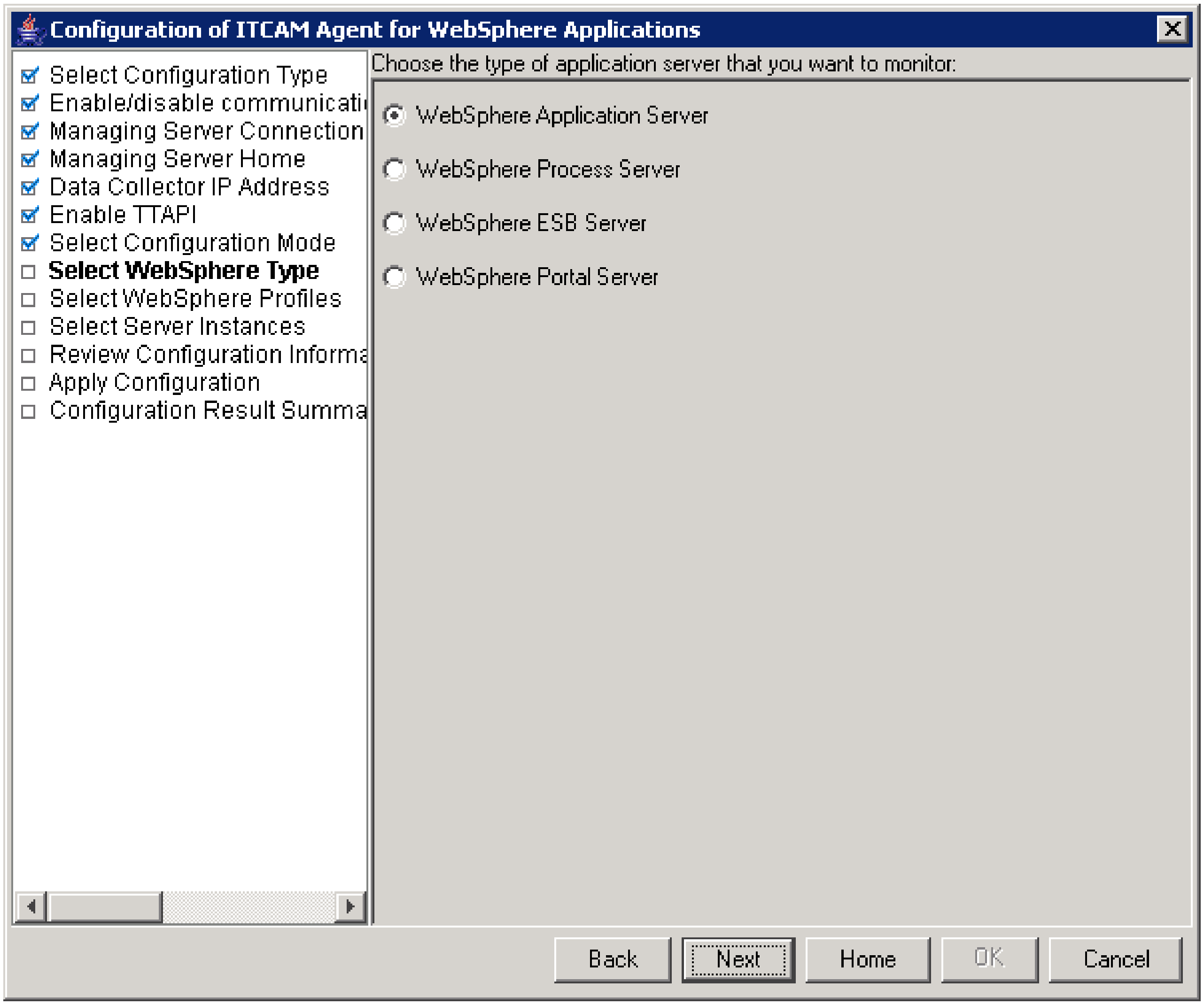
Custom Data Collector parameters, e.g. GC log and heap size

Caution: Allocate an additional 128 MB for your server maximum heap size to avoid "Out of Memory" issues during runtime. The configuration tool does not increase this setting by default; to do this select **Custom configuration** mode, and in the **Configure Heap Size Settings** step, select **Increase JVM Max heap size setting**.

Figure 26. Configuring the Data Collector to monitor application server instances, window 7

If you need to modify Garbage Collection logging settings, increase the Maximum Heap size, or disable backing up the application server configuration, select **Custom**. (In this case, the configuration utility will display additional windows for these settings). Otherwise, choose **Default**. Click **Next**.

9. A window for choosing the type of application server that the Data Collector monitors is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
☑ Managing Server Connection
☑ Managing Server Home
☑ Data Collector IP Address
☑ Enable TTAPI
☑ Select Configuration Mode
□ **Select WebSphere Type**
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the type of application server that you want to monitor:

● WebSphere Application Server

○ WebSphere Process Server

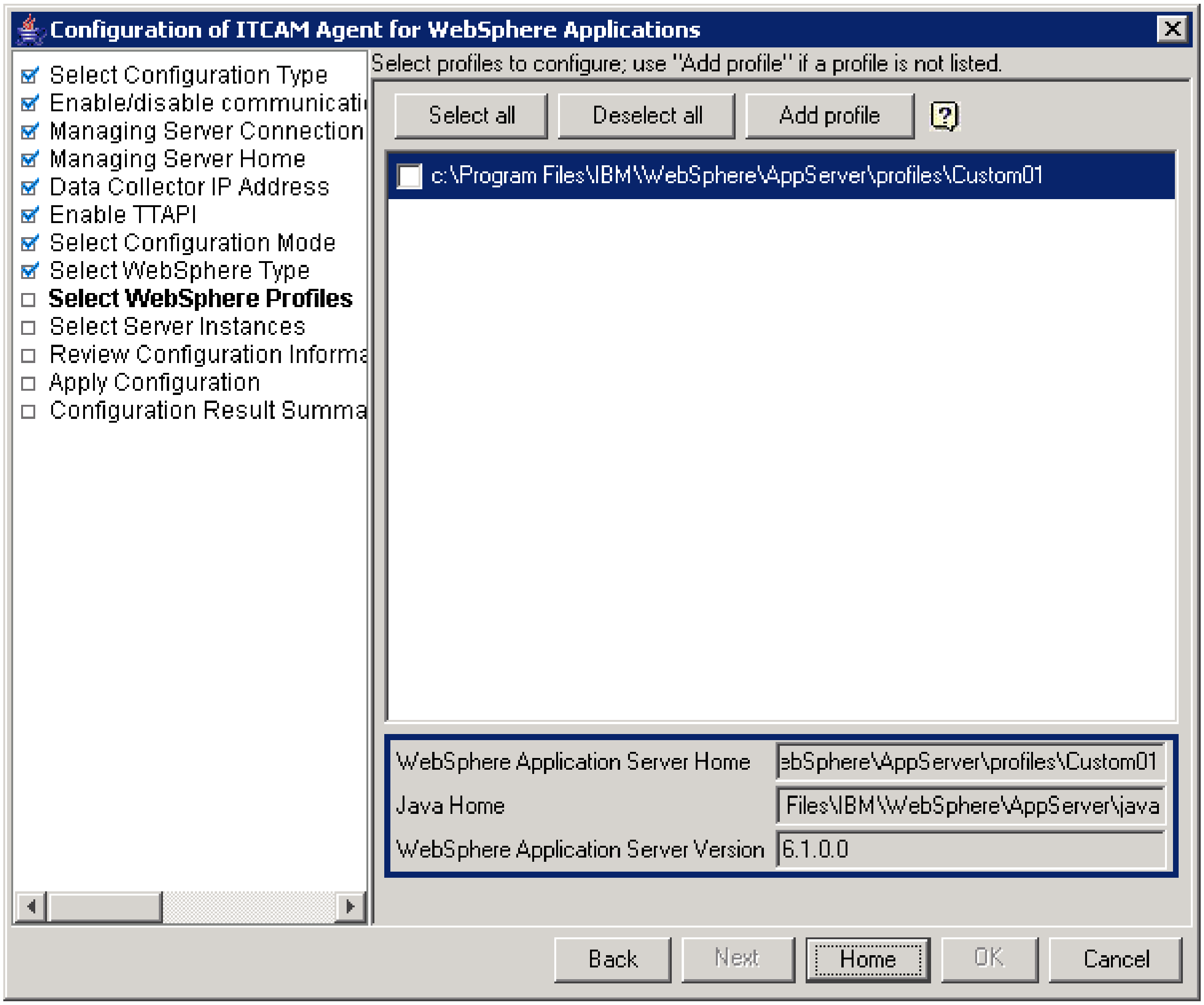
○ WebSphere ESB Server

○ WebSphere Portal Server

Figure 27. Configuring the Data Collector to monitor application server instances, window 8

Select the application server type, and click **Next**.

10. Discovered application server profiles are listed in the following window.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Enable/disable communicati
☑ Managing Server Connection
☑ Managing Server Home
☑ Data Collector IP Address
☑ Enable TTAPI
☑ Select Configuration Mode
☑ Select WebSphere Type
□ **Select WebSphere Profiles**
□ Select Server Instances
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa

Select profiles to configure; use "Add profile" if a profile is not listed.

□ c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01

WebSphere Application Server Home	ebSphere\AppServer\profiles\Custom01
Java Home	Files\IBM\WebSphere\AppServer\java
WebSphere Application Server Version	6.1.0.0

Figure 28. Configuring the Data Collector to monitor application server instances, window 9

Check the box for the profile for which you want to configure the Data Collector. You can select multiple profiles from the list; the Data Collector will be configured for each of the selected server profiles. If the application server profile you want to use does not show up in the list, specify the application server profile's installation directory by click **Add profile**. If multiple installations are found, make sure the one selected is running. The selected profile information is displayed below the selection box. Select the application server that the Data Collector will monitor and click **Next**.

11. Select the server instance(s) you want to configure. For a stand-alone (not Network Deployment and not Extended Deployment) environment, enter the application server's host name or IP address and the SOAP/RMI port of the application server instance you are configuring. For a Network Deployment or Extended Deployment environment, you must specify the Deployment Manager host name or IP address and SOAP/RMI port.

Important:

- If the application server has more than one instance and the Data Collector is already configured for some of them, only the instances for which it is not configured are initially listed in this window. To display configured instances, select the **Include configured server instances** check box. If you select a configured instance, it will be reconfigured.

- For a stand-alone environment, instances must be running during the configuration.
- For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running.

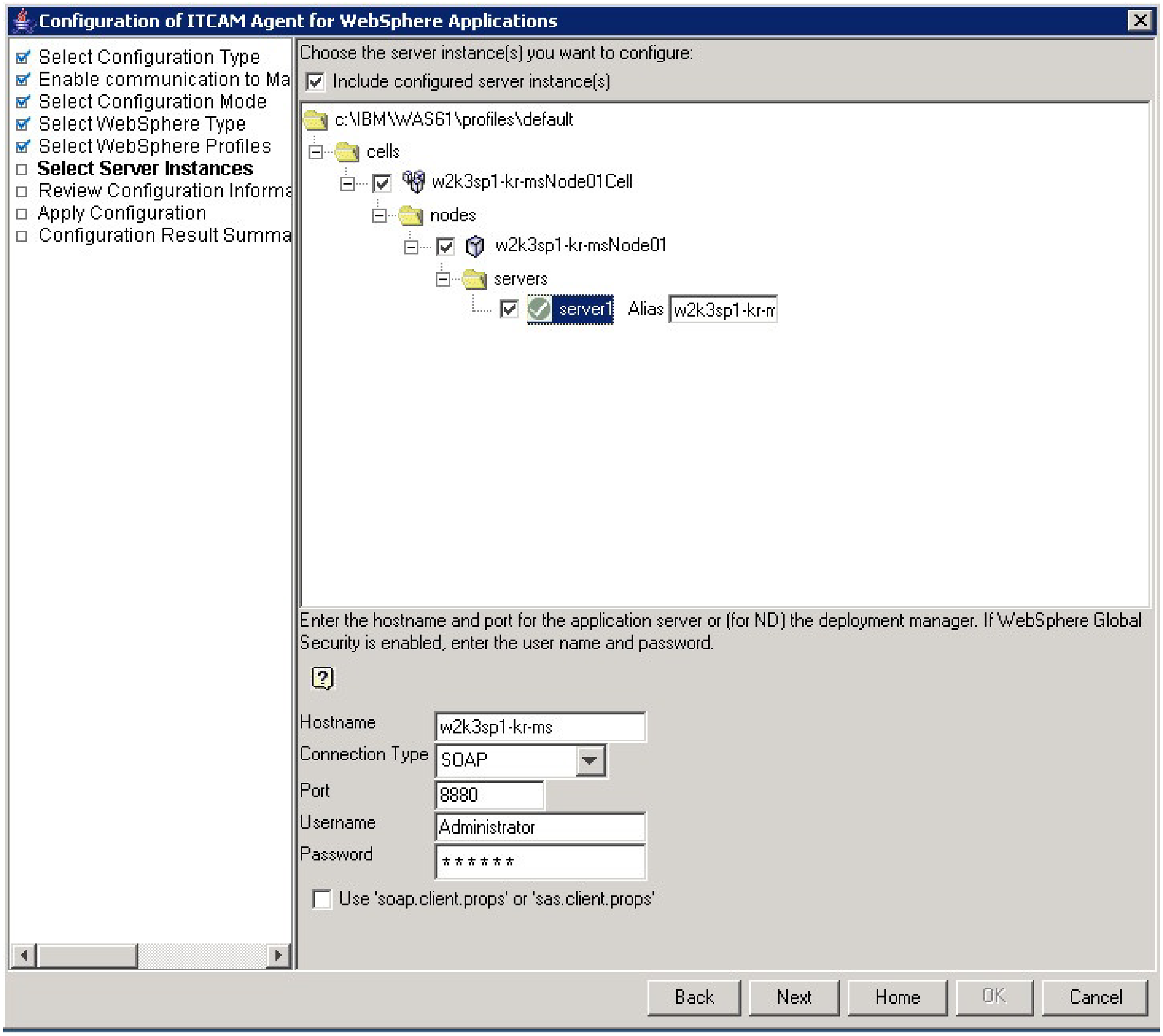
You can refer to the following table to establish Data Collector and application server communication:

Table 3. Fields for establishing Data Collector and application server communication

Field	**What to do**
Host Name	Type the fully qualified host name or IP address of the application server instance that the Data Collector monitors. Do not include a protocol in the host name. For example, type myserver.ibm.tivoli.com, not https://myserver.ibm.tivoli.com. Note: If using a Network Deployment environment, provide the host name of the Deployment Manager instead.
Connector Type	Select the type of connection the Data Collector and application server will use for communication.
Port	If you selected SOAP as the connector type, enter the connector port used by the application server instance to send commands using the Simple Object Access Protocol (SOAP). The SOAP port is identified in the `SOAP_CONNECTOR_ADDRESS` end point definition within the `AppServer_home/profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml` file for the application server instance. **Note:** If using Network Deployment, provide the SOAP port of the Deployment Manager instead. If you selected RMI as the connector type, enter the connector port used by the application server instance to send commands using RMI.
Username (only for Global Security enabled)	Type the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server. If, instead of typing the user ID, you want to retrieve the user ID from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.

Table 3. Fields for establishing Data Collector and application server communication (continued)

Field	What to do
Password (only for Global Security enabled)	Type the password that corresponds to the user specified in the **Username** field. If, instead of typing the password, you want to retrieve the password from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.


Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- ☑ Enable communication to Ma
- ☑ Select Configuration Mode
- ☑ Select WebSphere Type
- ☑ Select WebSphere Profiles
- □ **Select Server Instances**
- □ Review Configuration Informa
- □ Apply Configuration
- □ Configuration Result Summa

Choose the server instance(s) you want to configure:

☑ Include configured server instance(s)

```
c:\IBM\WAS61\profiles\default
  cells
    ☑ w2k3sp1-kr-msNode01Cell
      nodes
        ☑ w2k3sp1-kr-msNode01
          servers
            ☑ server1  Alias w2k3sp1-kr-m
```

Enter the hostname and port for the application server or (for ND) the deployment manager. If WebSphere Global Security is enabled, enter the user name and password.

Hostname: w2k3sp1-kr-ms

Connection Type: SOAP

Port: 8880

Username: Administrator

Password: ******

□ Use 'soap.client.props' or 'sas.client.props'

Figure 29. Configuring the Data Collector to monitor application server instances, window 10

Next to every selected instance, you can enter a server alias. This alias determines the name of the Tivoli Enterprise Portal node for this instance. Valid characters for the alias include A-z, a-z, 0-9, underbar (_), dash (-), and period (.); do not use other characters.

Important: if you have selected several application server profiles, the connection information (host name, port, connection type, and username/password) may be different for every profile. Select an instance in each profile and enter the information for the profile. Make sure that information is correct for every profile.

Check the boxes next to the instances that must be monitored by the Data Collector, complete the fields, and click **Next**.

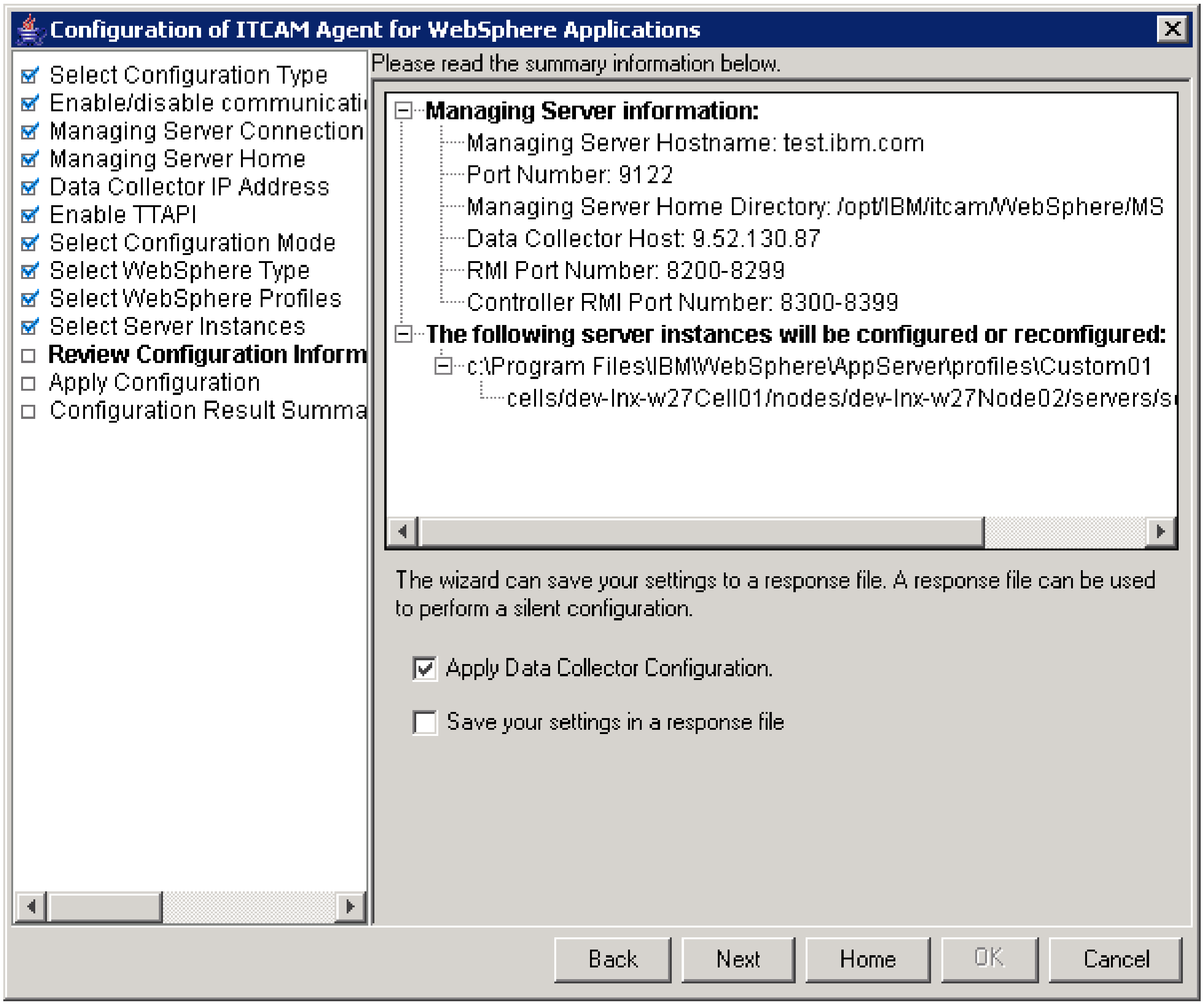
If the configuration utility is not able to communicate with any of the server instances, the selection window is displayed again, and the instances are highlighted in red. Select an instance highlighted in red to see the error message for it.

Important: If you have selected Custom configuration in Step 8 on page 38, the following additional windows will be displayed at this point:

- **Configure GC Log settings**: in this window, you can change the path and cycle settings for the Garbage Collection log for each application server instance. To change the log path, double click the **GC Log Path** table cell. To change the log cycle settings, double click the **GC Cycles** table cell.

  The **GC Cycles** setting is only supported if IBM Developer Kit for Java is used. The format of this setting is `x, y`; `x` and `y` are numbers. The logging will be performed to `x` files in rotation; information for `y` garbage collection cycles will be sent to one file before switching to the next file.
- **Configure Heap Size settings**: in this window, you can increase the maximum heap size for the application server instances. For best performance, increase the heap size for all instances; to do this, select the **Select All** box. You can increase the heap size for individual instances by selecting the **Increase JVM Max heap size setting** box in table rows.

12. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.



Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
☑ Managing Server Connection
☑ Managing Server Home
☑ Data Collector IP Address
☑ Enable TTAPI
☑ Select Configuration Mode
☑ Select WebSphere Type
☑ Select WebSphere Profiles
☑ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Please read the summary information below.

Managing Server information:

Managing Server Hostname: test.ibm.com

Port Number: 9122

Managing Server Home Directory: /opt/IBM/itcam/WebSphere/MS

Data Collector Host: 9.52.130.87

RMI Port Number: 8200-8299

Controller RMI Port Number: 8300-8399

The following server instances will be configured or reconfigured:

c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01

cells/dev-lnx-w27Cell01/nodes/dev-lnx-w27Node02/servers/s

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

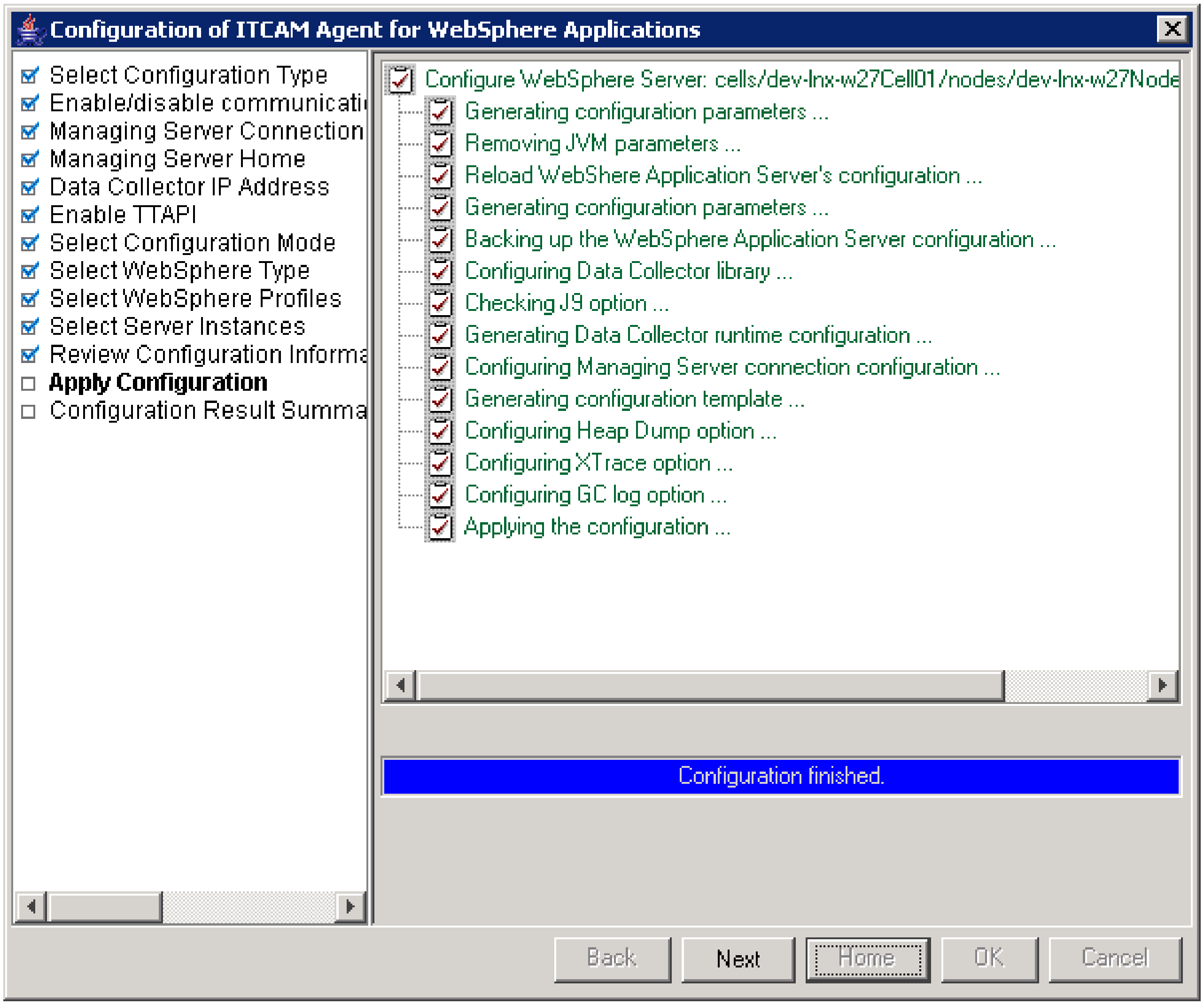
☑ Apply Data Collector Configuration.

□ Save your settings in a response file

Figure 30. Configuring Communication to the monitoring agent, window 11

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Data Collector Configuration**, the configuration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

13. The configuration utility validates the application server connection and applies the configuration.



Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- ☑ Enable/disable communicati
- ☑ Managing Server Connection
- ☑ Managing Server Home
- ☑ Data Collector IP Address
- ☑ Enable TTAPI
- ☑ Select Configuration Mode
- ☑ Select WebSphere Type
- ☑ Select WebSphere Profiles
- ☑ Select Server Instances
- ☑ Review Configuration Informa
- □ **Apply Configuration**
- □ Configuration Result Summa

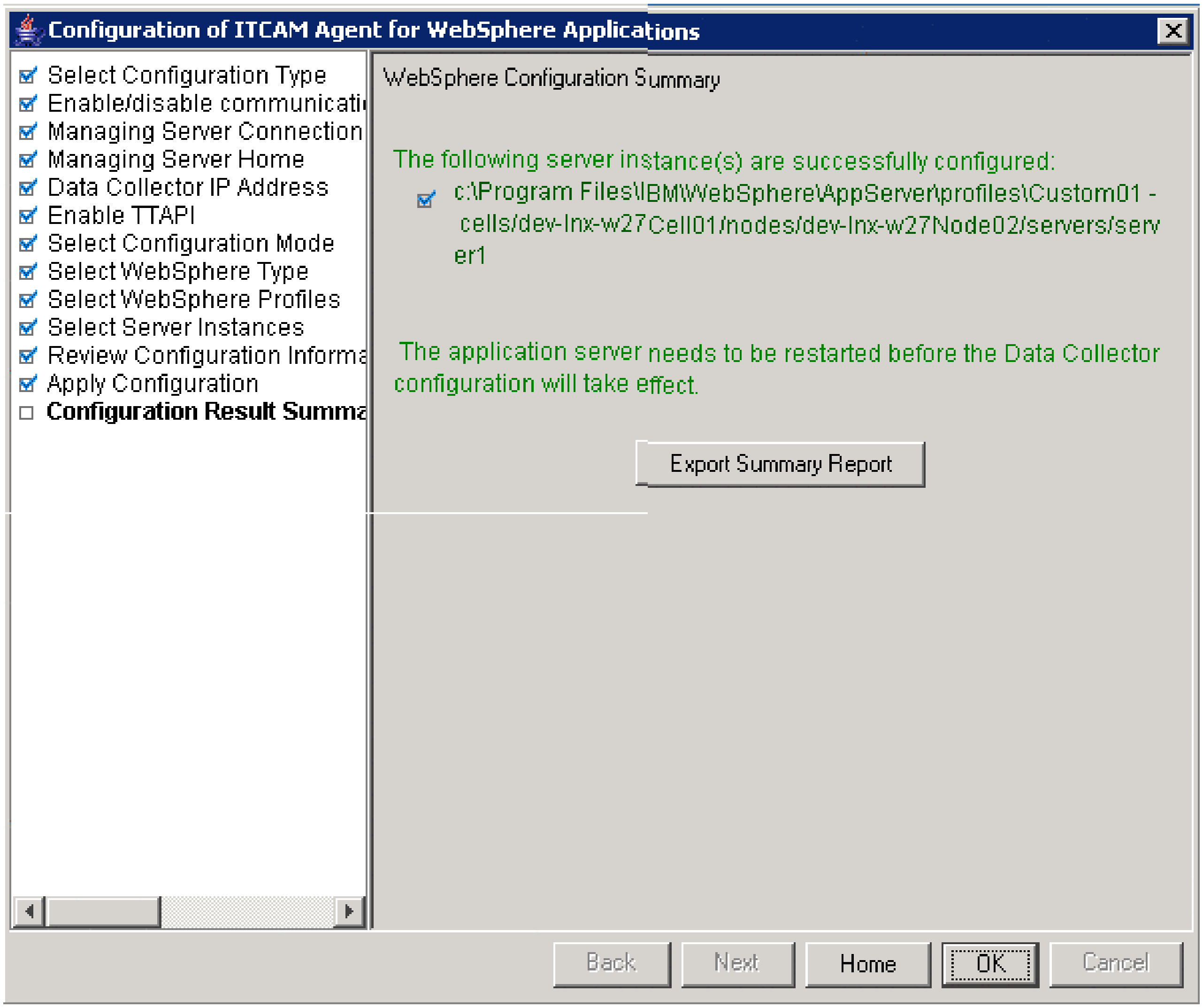
☑ Configure WebSphere Server: cells/dev-lnx-w27Cell01/nodes/dev-lnx-w27Node
- ☑ Generating configuration parameters ...
- ☑ Removing JVM parameters ...
- ☑ Reload WebShere Application Server's configuration ...
- ☑ Generating configuration parameters ...
- ☑ Backing up the WebSphere Application Server configuration ...
- ☑ Configuring Data Collector library ...
- ☑ Checking J9 option ...
- ☑ Generating Data Collector runtime configuration ...
- ☑ Configuring Managing Server connection configuration ...
- ☑ Generating configuration template ...
- ☑ Configuring Heap Dump option ...
- ☑ Configuring XTrace option ...
- ☑ Configuring GC log option ...
- ☑ Applying the configuration ...

Configuration finished.

Figure 31. Configuring the Data Collector to monitor application server instances, window 12

Click **Next**

14. WebSphere configuration summary information is displayed.


Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- ☑ Enable/disable communicati
- ☑ Managing Server Connection
- ☑ Managing Server Home
- ☑ Data Collector IP Address
- ☑ Enable TTAPI
- ☑ Select Configuration Mode
- ☑ Select WebSphere Type
- ☑ Select WebSphere Profiles
- ☑ Select Server Instances
- ☑ Review Configuration Informa
- ☑ Apply Configuration
- □ **Configuration Result Summa**

WebSphere Configuration Summary

The following server instance(s) are successfully configured:

☑ c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01 - cells/dev-lnx-w27Cell01/nodes/dev-lnx-w27Node02/servers/server1

The application server needs to be restarted before the Data Collector configuration will take effect.

Figure 32. Configuring the Data Collector to monitor application server instances, window 13

To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window, or click **OK** to complete the configuration process.

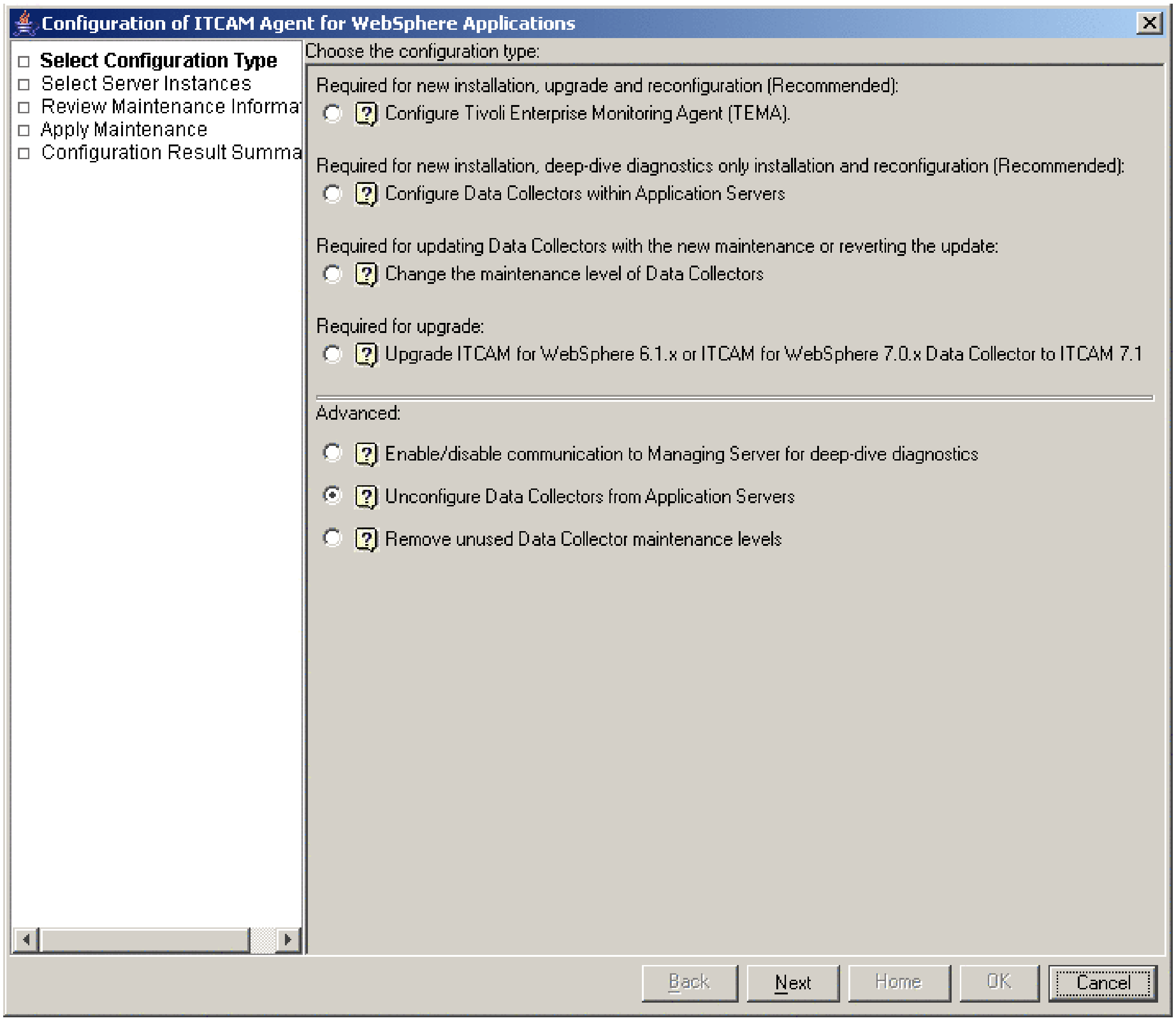
Important: After configuring the Data Collector to monitor an application server instance, perform the applicable steps in "Additional steps for configuring the Data Collector on Windows" on page 91, including a restart of the application server. The Data Collector configuration will take effect after the server is restarted.

Unconfigure the Data Collector for application server instances

If you no longer want the Data Collector to monitor an application server instance, you can unconfigure the Data Collector from it.

To do this, perform the following steps:

1. Enter the Agent Configuration window. After installation of the Agent, if you have selected **Launch Manage Tivoli Monitoring Services for additional configuration options and to start Tivoli Monitoring services** in the Figure 12 on page 24, this window opens automatically. Otherwise, see “Entering the Agent Configuration window” on page 25.


Configuration of ITCAM Agent for WebSphere Applications
□ Select Configuration Type
□ Select Server Instances
□ Review Maintenance Informa
□ Apply Maintenance
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

○ Enable/disable communication to Managing Server for deep-dive diagnostics

● Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 33. Unconfiguring the Data Collector for application server instances, window 1

2. Select **Unconfigure Data Collectors from Application Servers** and click **Next**.
3. Select the server instance(s) you want to unconfigure. All the instances monitored by this installation of the Agent are listed.

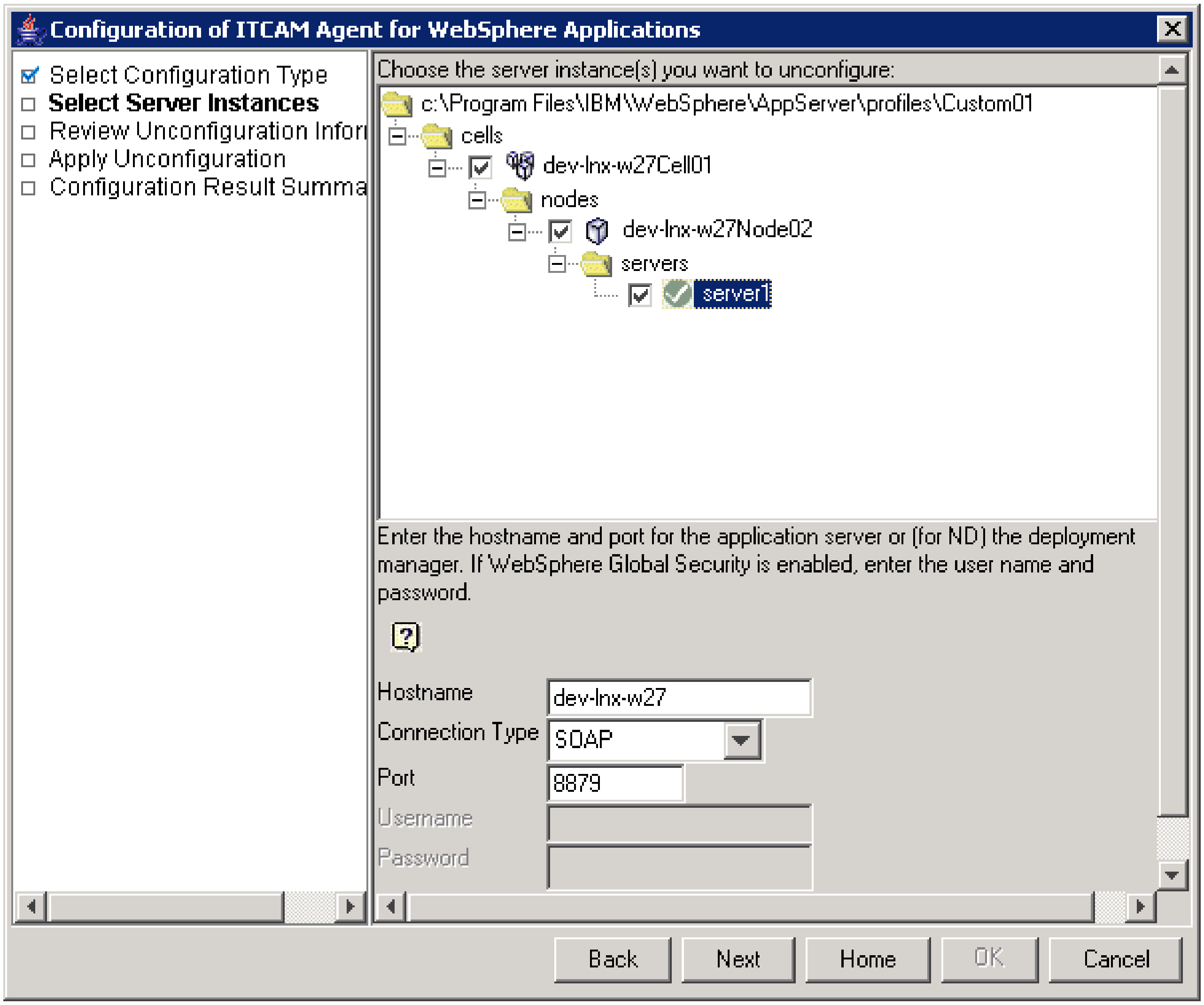
   Note:

   - Instance(s) must be running during the configuration.
   - For Network Deployment environment the Node Agent and Deployment Manager must also be running.

   You also need to set the connection parameters for the application server instances. By default, the information that was set during initial Data Collector configuration for each instance will be displayed (except username and password). The following table lists the fields:

Table 4. Fields for establishing Data Collector and application server communication

Field	What to do
Host Name	Type the fully qualified host name or IP address of the application server instance that the Data Collector monitors. Do not include a protocol in the host name. For example, type myserver.ibm.tivoli.com, not https://myserver.ibm.tivoli.com. Note: If using a Network Deployment environment, provide the host name of the Deployment Manager instead.
Connector Type	Select the type of connection the Data Collector and application server will use for communication.
Port	If you selected SOAP as the connector type, enter the connector port used by the application server instance to send commands using the Simple Object Access Protocol (SOAP). The SOAP port is identified in the `AppServer_home/profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml` file for the instance of application server that the Data Collector will monitor. **Note:** If using Network Deployment, provide the SOAP port of the Deployment Manager instead. If you selected RMI as the connector type, enter the connector port used by the application server instance to send commands using RMI.
Username (only for Global Security enabled)	Type the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server. If, instead of typing the user ID, you want to retrieve the user ID from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.
Password (only for Global Security enabled)	Type the password that corresponds to the user specified in the **Username** field. If, instead of typing the password, you want to retrieve the password from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
□ **Select Server Instances**
□ Review Unconfiguration Infor
□ Apply Unconfiguration
□ Configuration Result Summa

Choose the server instance(s) you want to unconfigure:

```
c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
  cells
    ☑ dev-lnx-w27Cell01
      nodes
        ☑ dev-lnx-w27Node02
          servers
            ☑ server1
```

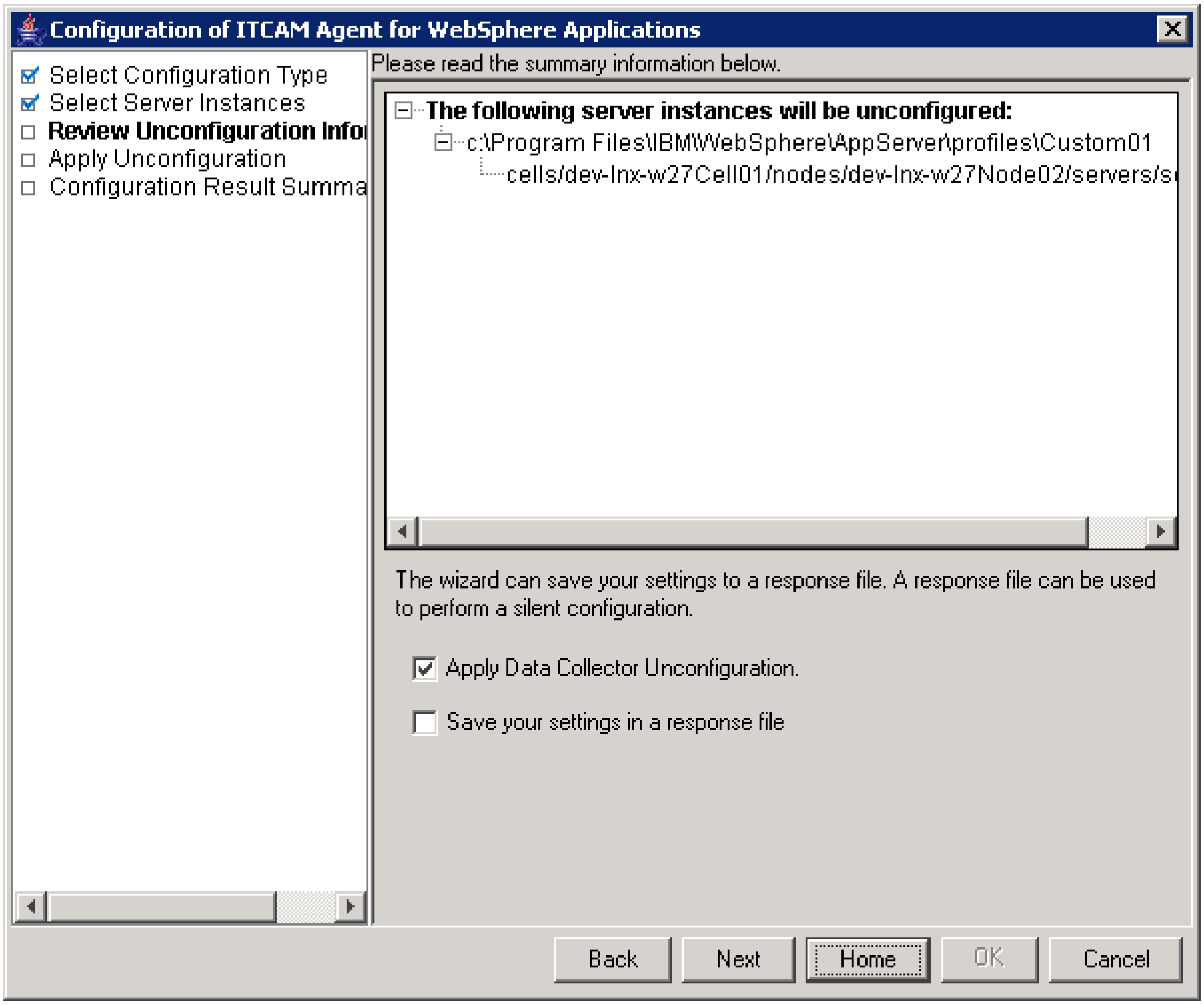
Enter the hostname and port for the application server or (for ND) the deployment manager. If WebSphere Global Security is enabled, enter the user name and password.

Hostname: dev-lnx-w27
Connection Type: SOAP
Port: 8879
Username:
Password:

Figure 34. Unconfiguring the Data Collector for application server instances, window 2

Check the boxes next to any instances you no longer want to monitor. Then, click **Next**.

4. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Server Instances
□ Review Unconfiguration Infor
□ Apply Unconfiguration
□ Configuration Result Summa

Please read the summary information below.

The following server instances will be unconfigured:
c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
cells/dev-lnx-w27Cell01/nodes/dev-lnx-w27Node02/servers/s

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

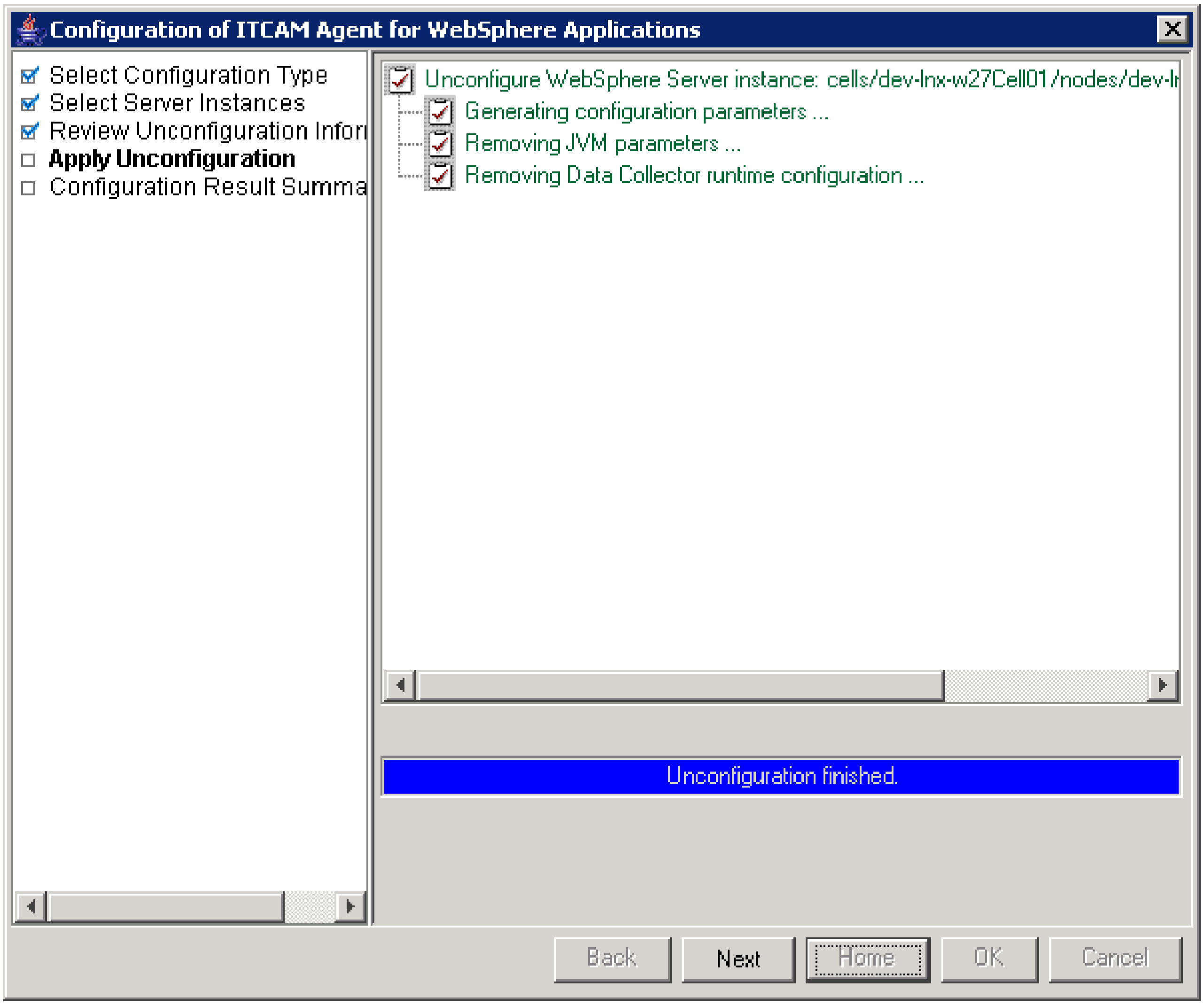
☑ Apply Data Collector Unconfiguration.

□ Save your settings in a response file

Figure 35. Unconfiguring the Data Collector for application server instances, window 3

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Data Collector Unconfiguration**, the unconfiguration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

5. The configuration utility will validate the applications server connection and apply the unconfiguration.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Select Server Instances
☑ Review Unconfiguration Infor
□ **Apply Unconfiguration**
□ Configuration Result Summa

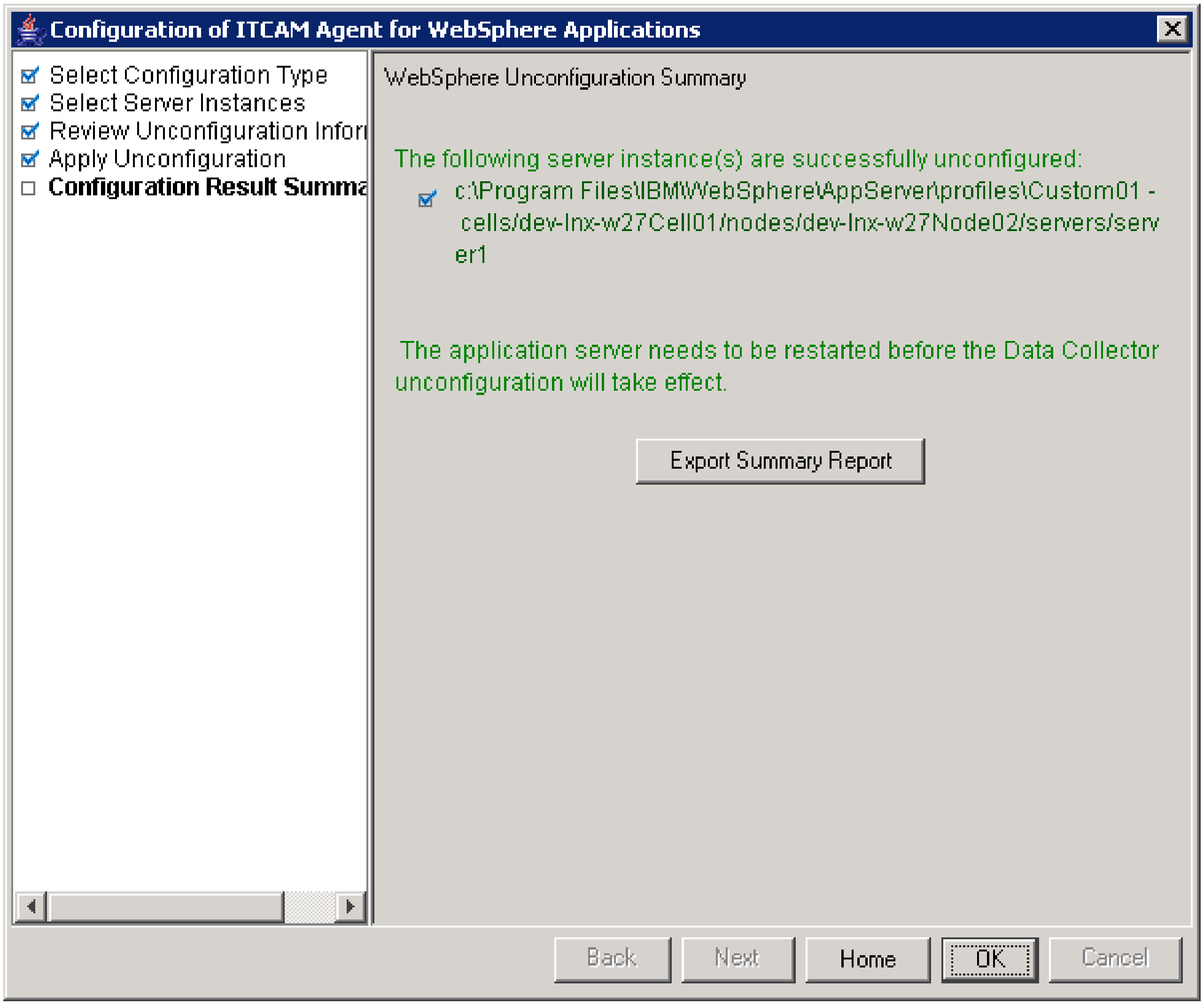
☑ Unconfigure WebSphere Server instance: cells/dev-lnx-w27Cell01/nodes/dev-l
- ☑ Generating configuration parameters ...
- ☑ Removing JVM parameters ...
- ☑ Removing Data Collector runtime configuration ...

Unconfiguration finished.

Figure 36. Unconfiguring the Data Collector for application server instances, window 4

Click **Next**.

6. WebSphere unconfiguration summary information is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Server Instances
☑ Review Unconfiguration Infor
☑ Apply Unconfiguration
□ Configuration Result Summa
WebSphere Unconfiguration Summary
Export Summary Report
Back
Next
Home
OK
Cancel

The following server instance(s) are successfully unconfigured:

☑ c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01 - cells/dev-lnx-w27Cell01/nodes/dev-lnx-w27Node02/servers/server1

The application server needs to be restarted before the Data Collector unconfiguration will take effect.

Figure 37. Unconfiguring the Data Collector for application server instances, window 5

To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window, or click **OK** to complete the configuration process.

Configure Data Collector communication with the Managing Server

If you have configured the Data Collector to monitor an application server instance, you may later change its configuration for communication with the ITCAM for Application Diagnostics Managing Server for this instance. You may also change Transaction Tracking integration configuration.

In this way, you may:

- If you have previously not configured it to communicate to the Managing Server, enable such communication.
- If it was already configured to communicate to the Managing Server, change the address or port number for the Managing Server kernel, or disable such communication.

You may perform such configuration on many configured application server instances at the same time.

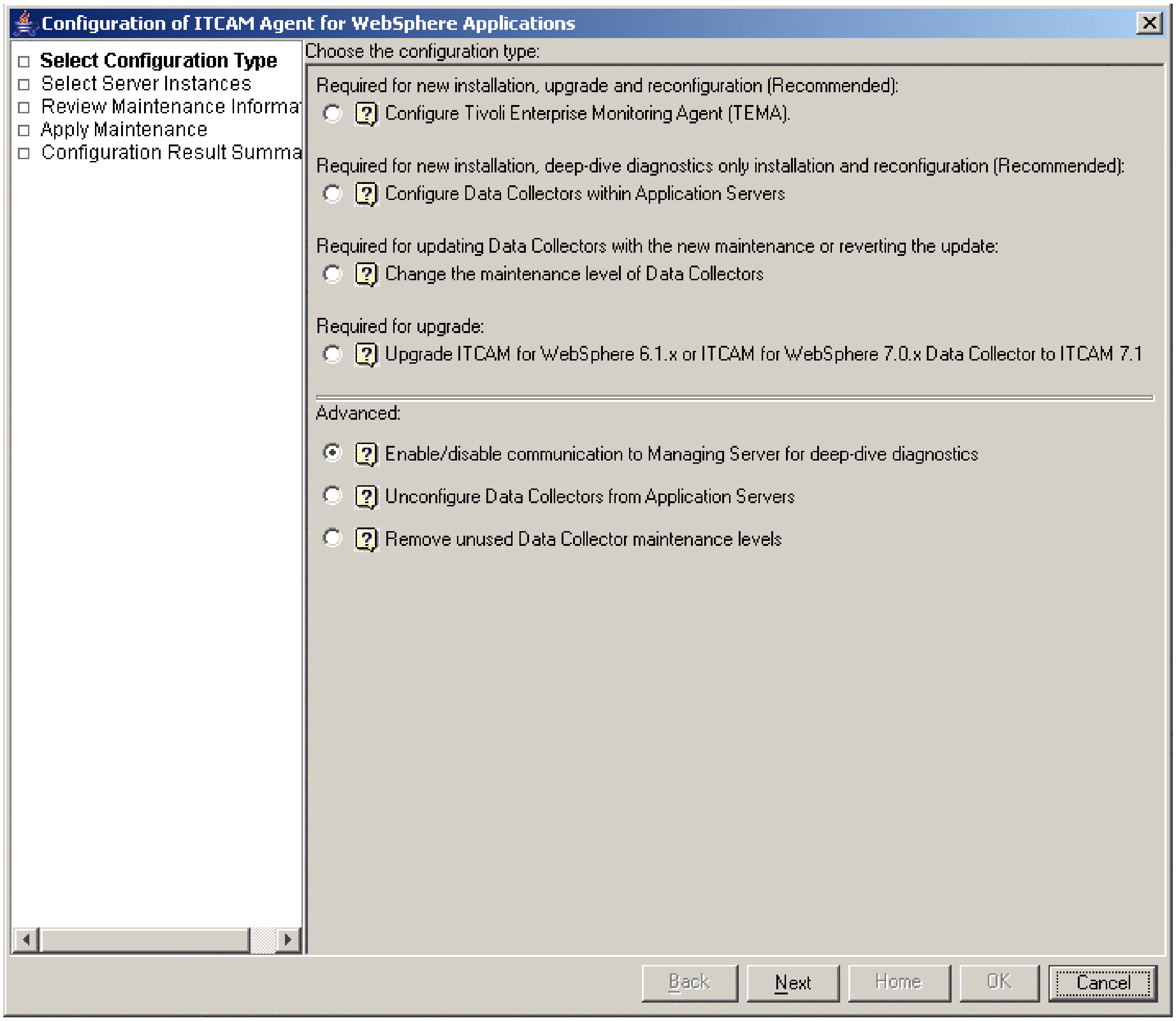
Note: If the Data Collector communicates to the Managing Server, you can also use the Visualization Engine to disable such communication (**Administration** > **Server Management** > **Data Collector Configuration**). See Table 5 for a comparison between these two ways of disabling Data Collector communication to the Managing Server:

Table 5. Comparison of ways to disable Data Collector communication to the Managing Server.

Disable Data Collector communication to the Managing Server using Data Collector configuration	Disable Data Collector communication to the Managing Server using the Visualization Engine
The application server instance is not listed in the Visualization Engine.	The application server instance remains listed in the Visualization Engine.
The Visualization Engine shows no information on the application server instance.	The Visualization Engine shows whether the application server instance is up or down; monitoring information is not available.
No system or network resources are used for Managing Server communication.	Some system and network resources are used to maintain Managing Server communication.
You do not need to apply maintenance fixes for the Agent that only impact Managing Server communication.	You need to apply maintenance fixes for the Agent that only impact Managing Server communication.
In order to re-enable communication, you need to perform Data Collector configuration again, and restart the application server.	In order to re-enable communication using the Visualization Engine, you do not need to restart the application server.

Complete the following steps to enable, disable, or configure Data Collector communication with the Managing Server:

1. Enter the Agent Configuration window. After installation of the Agent, if you have selected **Launch Manage Tivoli Monitoring Services for additional configuration options and to start Tivoli Monitoring services** in the Figure 12 on page 24, this window opens automatically. Otherwise, see "Entering the Agent Configuration window" on page 25.



Configuration of ITCAM Agent for WebSphere Applications

□ Select Configuration Type
□ Select Server Instances
□ Review Maintenance Informa
□ Apply Maintenance
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

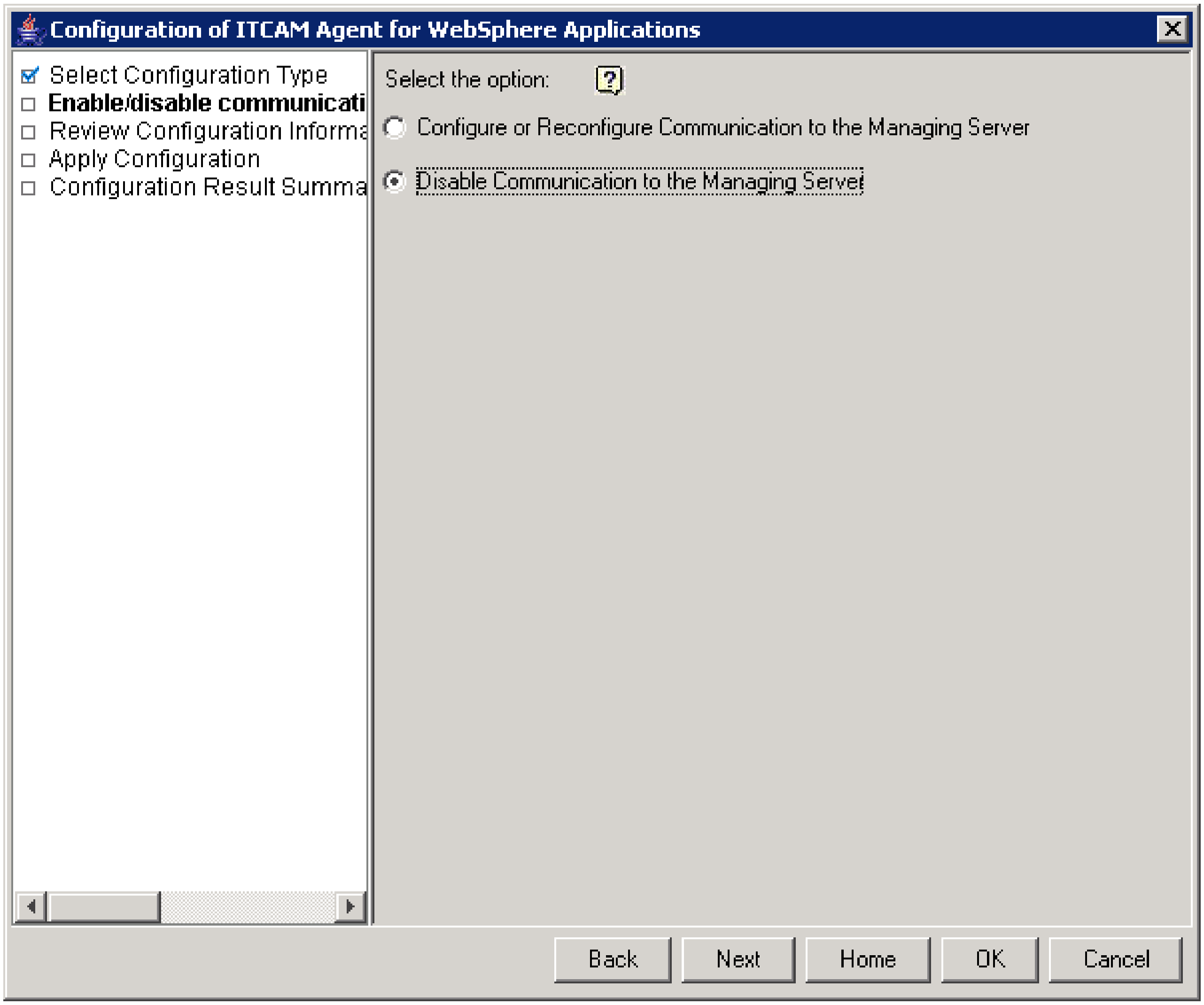
● Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 38. Configuring Data Collector communication with the Managing Server, window 1

2. Select **Enable/disable communication to Managing Server for deep-dive diagnostics** and click **Next**.
3. In the following window you must choose whether to enable or modify the Managing Server connection settings, or to disable communication with the Managing Server.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ Enable/disable communicati
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Select the option: ?

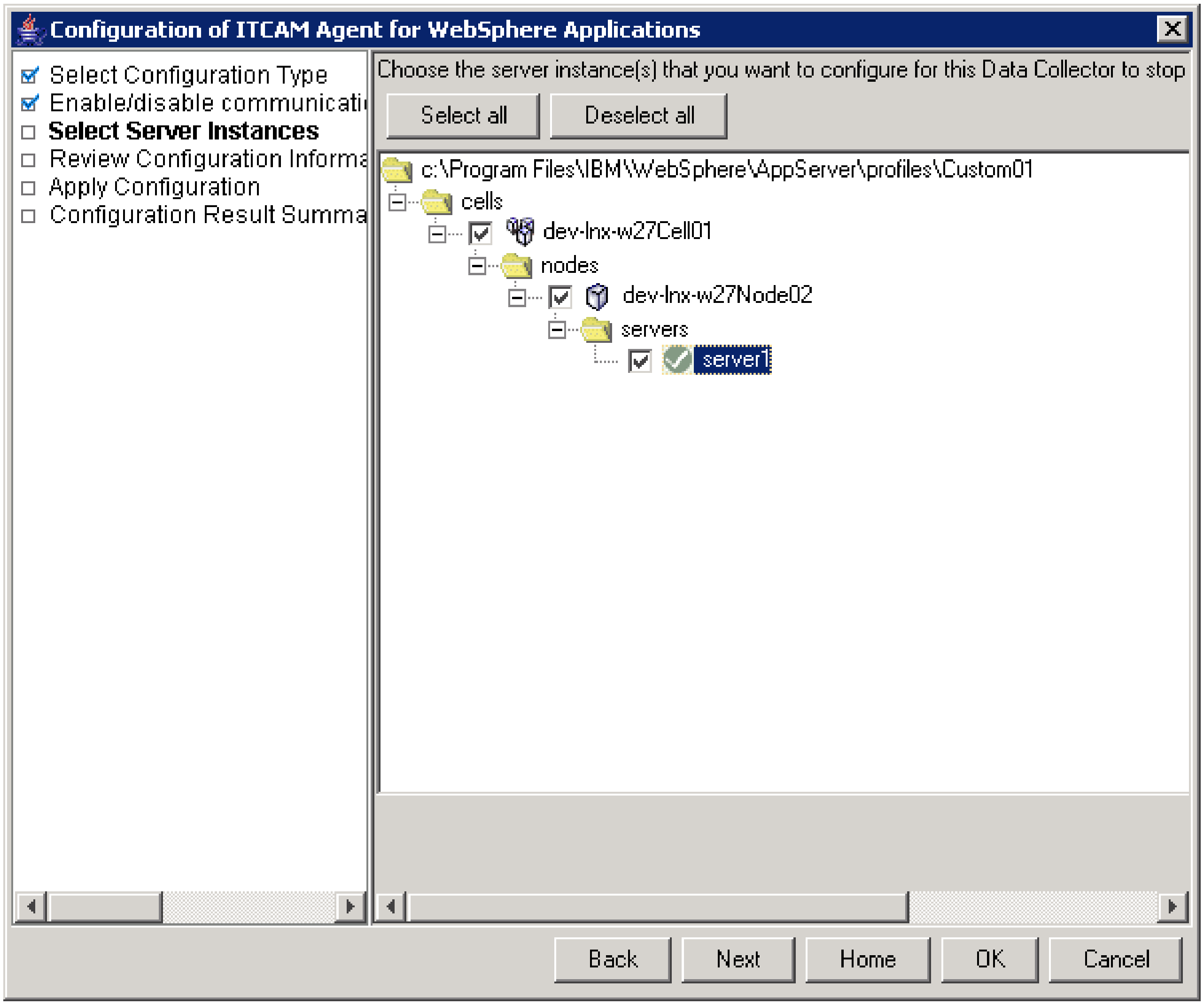
○ Configure or Reconfigure Communication to the Managing Server

● Disable Communication to the Managing Server

Figure 39. Configuring Data Collector communication with the Managing Server, window 2

If you wish to enable Managing Server communication that was previously not configured, or to change the address or port of the Managing Server, or to change Transaction Tracking integration configuration, select **Configure or Reconfigure communication to the Managing Server**. Click **Next**. Then, follow the procedure described in Steps 4 on page 34 to7 on page 37 to set up the Managing Server and Transaction Tracking integration configuration details. Then, go to Step 7 on page 59.If you wish to disable communication with the Managing Server, select **Disable the Managing Server connection settings.** and click **Next**.

4. Select the server instances for which you want to disable Managing Server communication. All the instances monitored by this installation of the Agent are listed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
□ Select Server Instances
□ Review Configuration Informa
□ Apply Configuration
□ Configuration Result Summa
Select all
Deselect all
Back
Next
Home
OK
Cancel

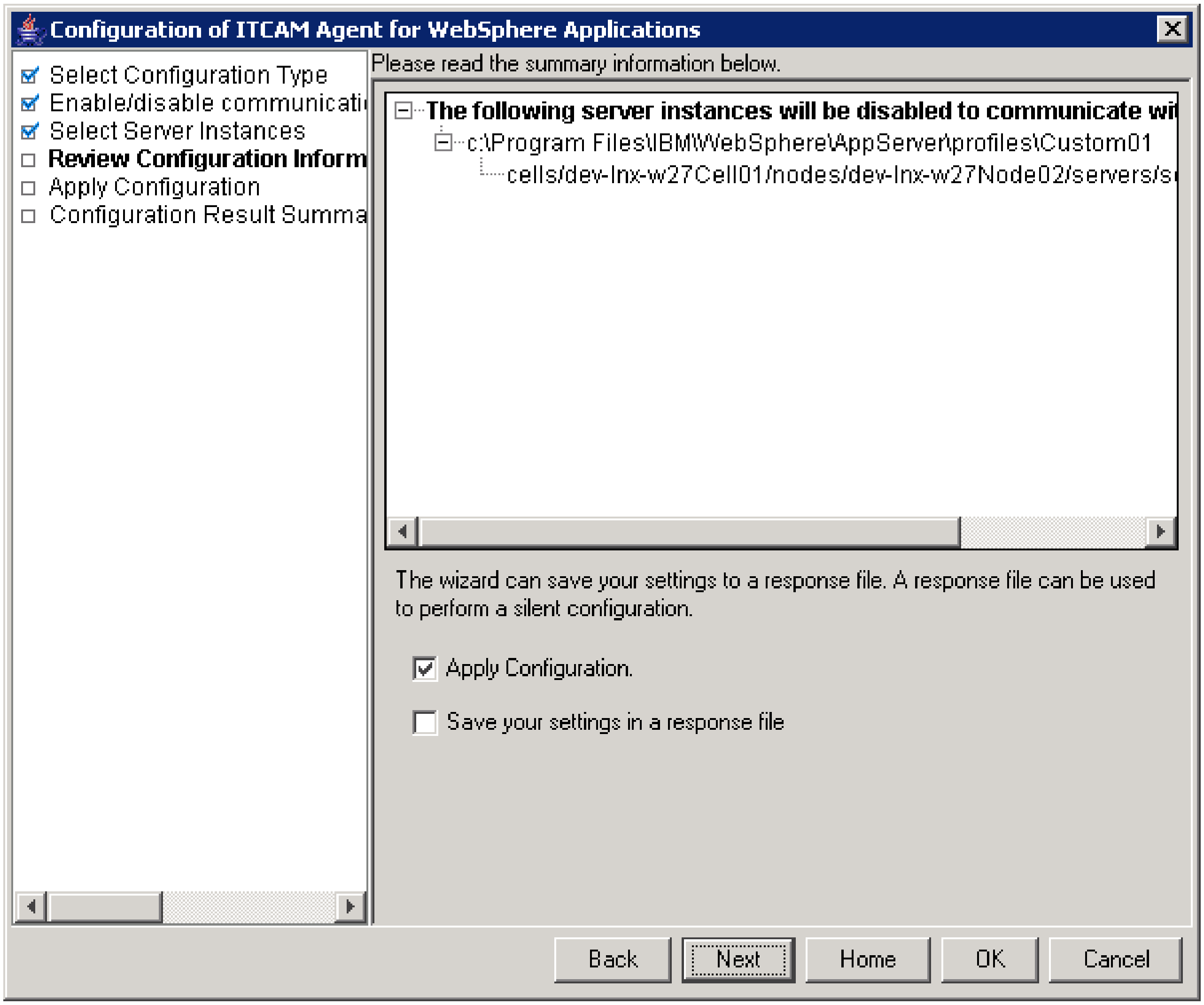
Choose the server instance(s) that you want to configure for this Data Collector to stop

c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
- cells
  - ☑ dev-lnx-w27Cell01
    - nodes
      - ☑ dev-lnx-w27Node02
        - servers
          - ☑ server1

Figure 40. Configuring Data Collector communication with the Managing Server, window 3

Check the boxes next to the instances that must no longer be monitored with the Managing Server, and click **Next**.

5. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
☑ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Please read the summary information below.

The following server instances will be disabled to communicate wi
c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
cells/dev-lnx-w27Cell01/nodes/dev-lnx-w27Node02/servers/s

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

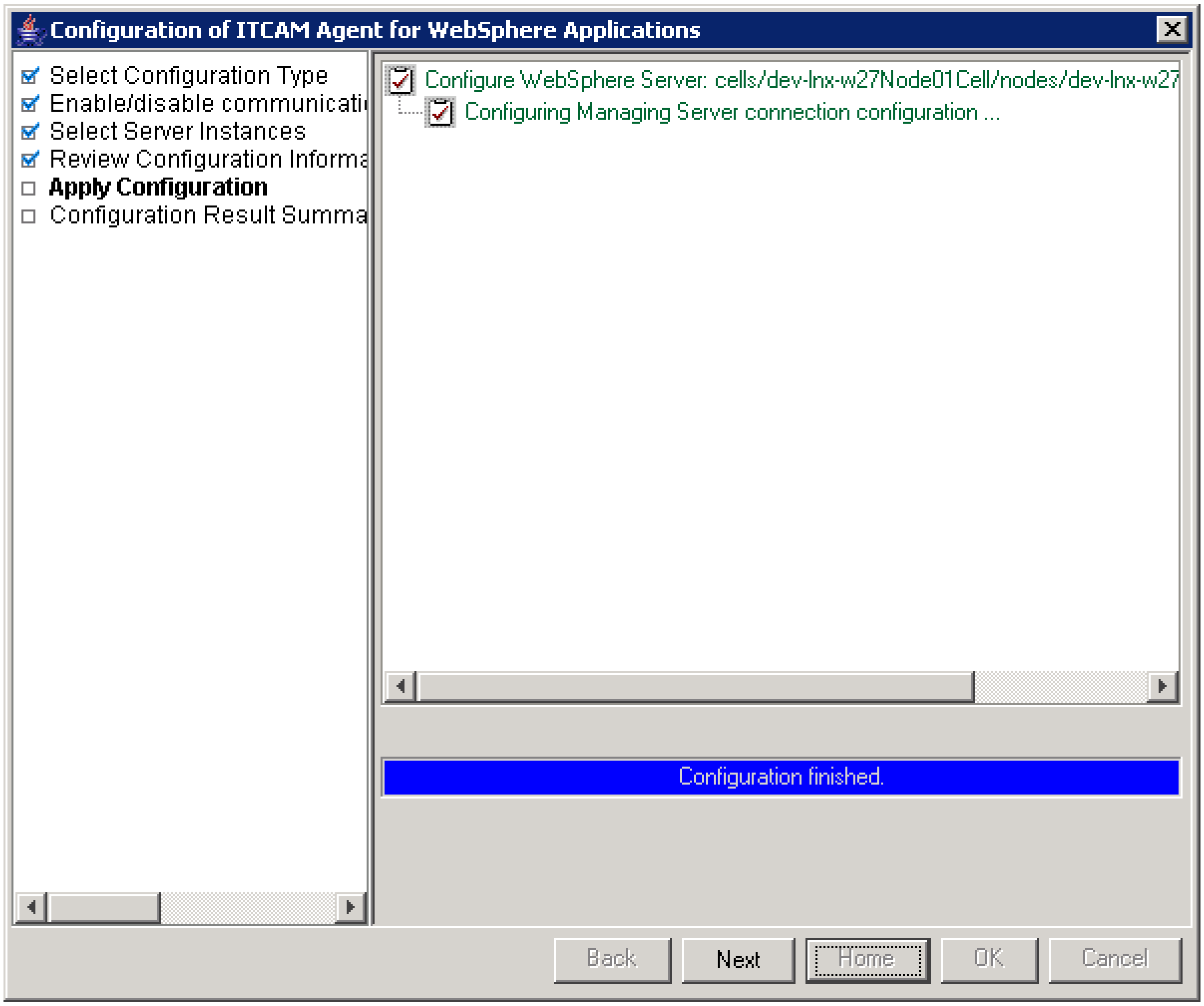
☑ Apply Configuration.

□ Save your settings in a response file

Figure 41. Configuring Data Collector communication with the Managing Server, window 4

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Configuration**, the new configuration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

6. The configuration utility applies the changes.



Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- ☑ Enable/disable communicati
- ☑ Select Server Instances
- ☑ Review Configuration Informa
- □ **Apply Configuration**
- □ Configuration Result Summa

☑ Configure WebSphere Server: cells/dev-lnx-w27Node01Cell/nodes/dev-lnx-w27

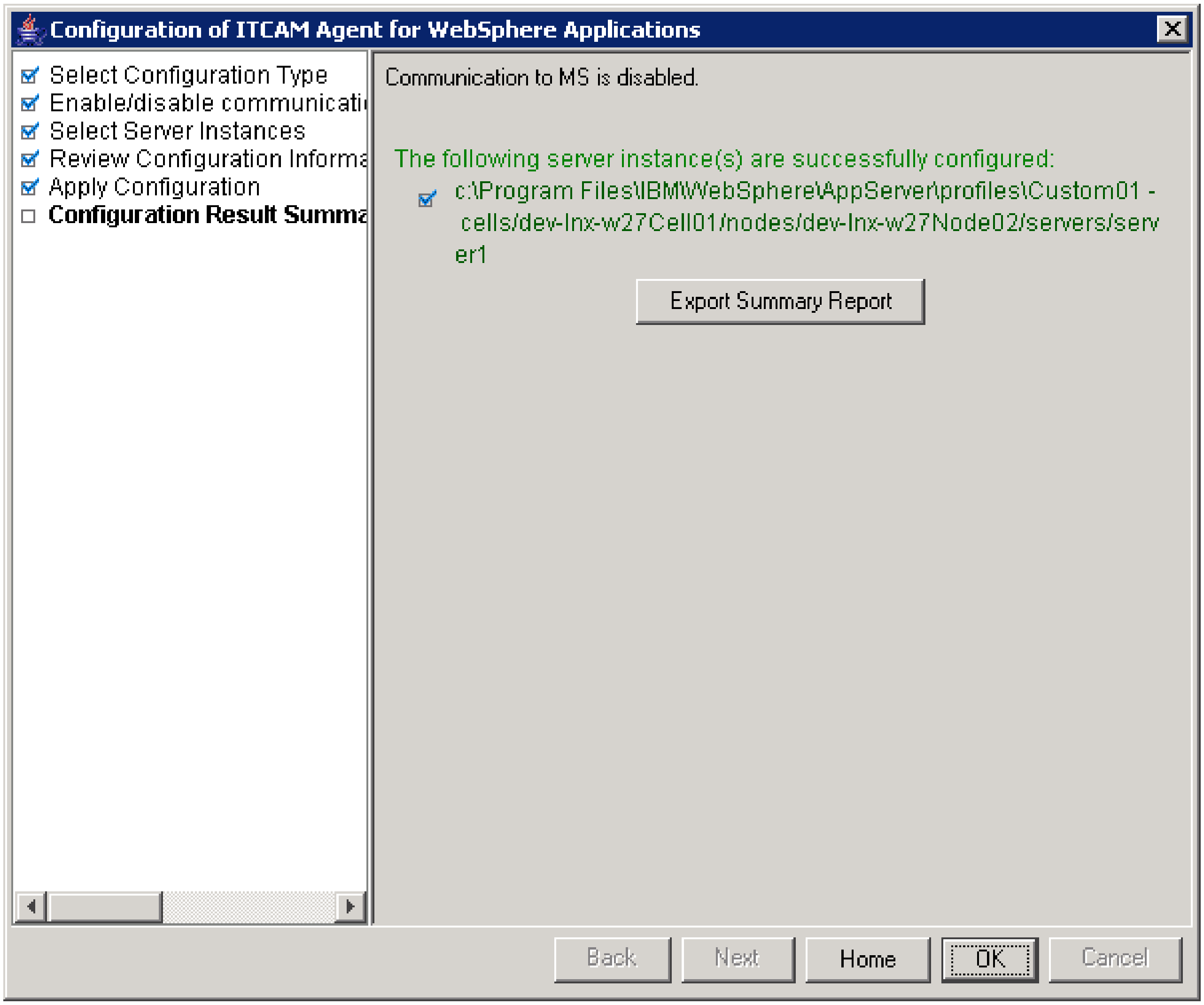
☑ Configuring Managing Server connection configuration ...

Configuration finished.

Figure 42. Configuring Data Collector communication with the Managing Server, window 5

Click **Next**.

7. A summary is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicati
☑ Select Server Instances
☑ Review Configuration Informa
☑ Apply Configuration
□ Configuration Result Summa
Export Summary Report
Back
Next
Home
OK
Cancel

Communication to MS is disabled.

The following server instance(s) are successfully configured:

☑ c:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01 - cells/dev-lnx-w27Cell01/nodes/dev-lnx-w27Node02/servers/server1

Figure 43. Configuring Data Collector communication with the Managing Server, window 5

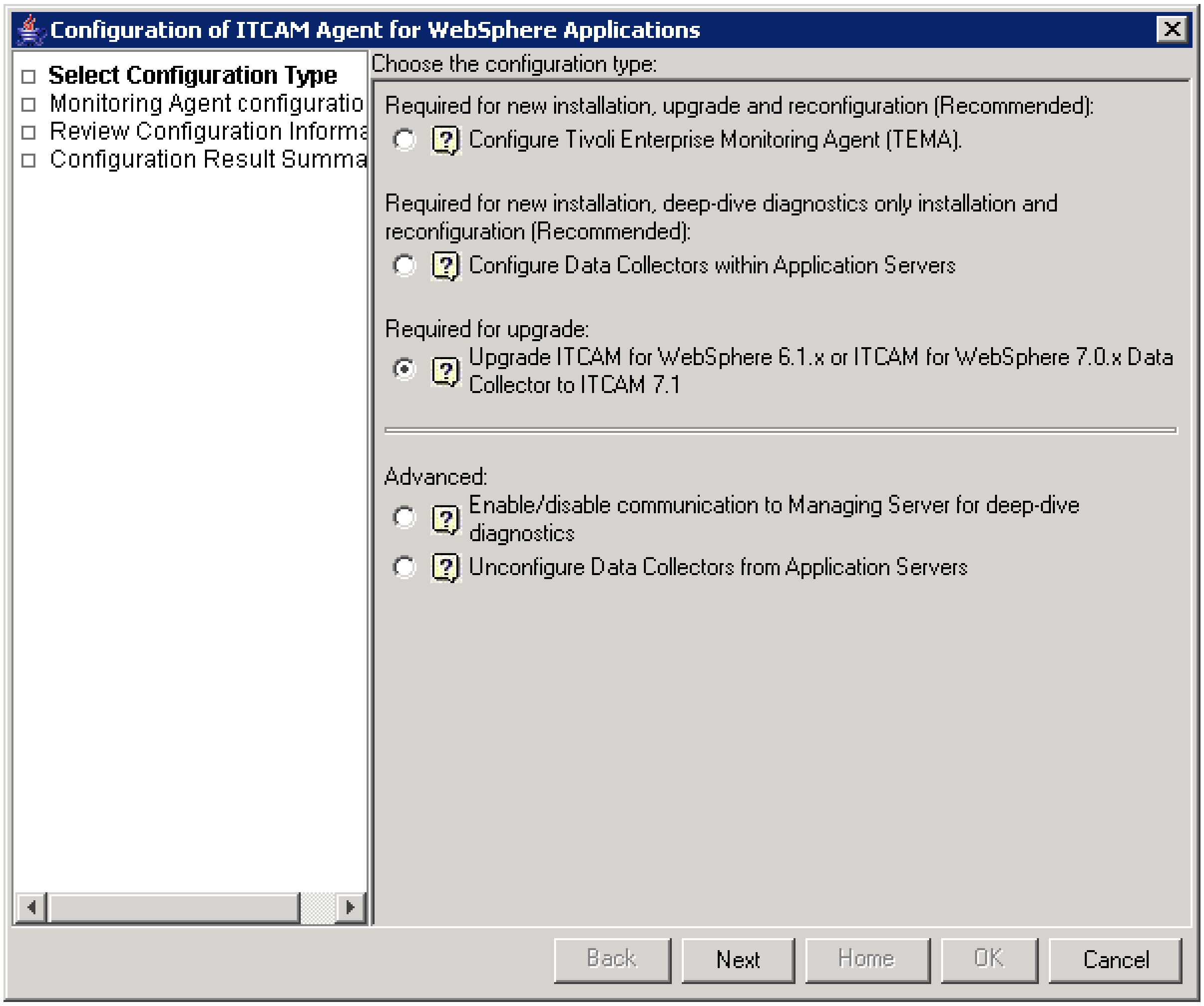
To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window, or click **OK** to complete the configuration process.

Upgrading monitoring to Data Collector 7.1

If an application server instance is monitored by a previous version of the Data Collector (from ITCAM for WebSphere 6.1, ITCAM for Web Resources 6.2, or ITCAM for WebSphere 7.0), you can upgrade monitoring to version 7.1.

To upgrade monitoring of server instances to Data Collector version 7.1, perform the following procedure:

1. Enter the Agent Configuration window. After installation of the Agent, this window opens automatically. Otherwise, see "Entering the Agent Configuration window" on page 25.



Configuration of ITCAM Agent for WebSphere Applications

□ Select Configuration Type
□ Monitoring Agent configuratio
□ Review Configuration Informa
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for upgrade:

● Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

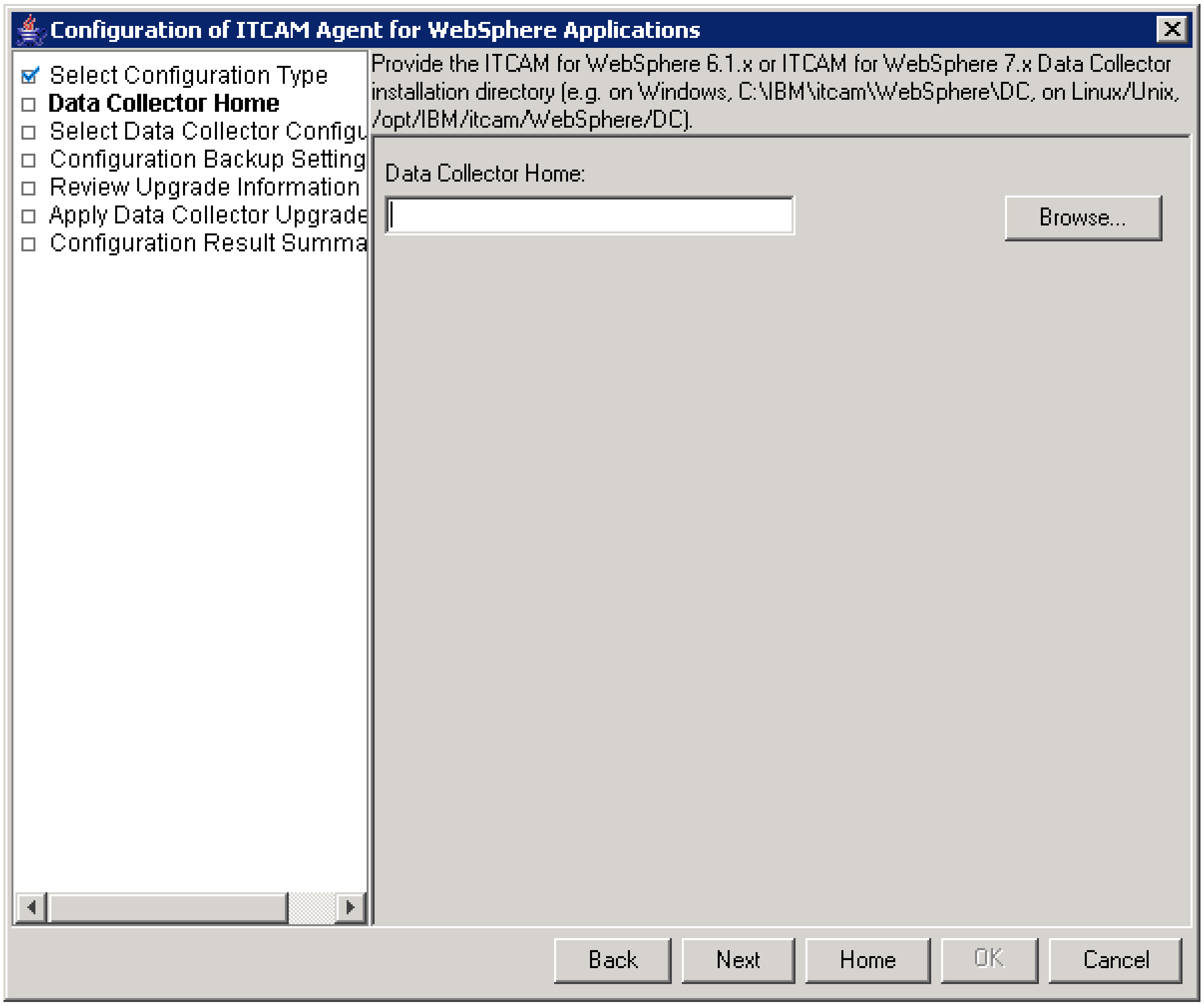
Advanced:

○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

Figure 44. Upgrading monitoring to Data Collector 7.1, window 1

2. Select **Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1** and click **Next**.
3. Set the home directory of the previous version of the Data Collector.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ Data Collector Home
□ Select Data Collector Configu
□ Configuration Backup Setting
□ Review Upgrade Information
□ Apply Data Collector Upgrade
□ Configuration Result Summa
Browse...
Back
Next
Home
OK
Cancel

Provide the ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.x Data Collector installation directory (e.g. on Windows, C:\IBM\itcam\WebSphere\DC, on Linux/Unix, /opt/IBM/itcam/WebSphere/DC).

Data Collector Home:

Figure 45. Upgrading monitoring to Data Collector 7.1, window 2

Enter the full path to the directory in which the older version of the Data Collector as installed. If it was configured with the default options, the path is `C:\IBM\itcam\WebSphere\DC`. Then, click **Next**.

4. Select the server instances you want to upgrade. All the instances monitored by this installation of the older Data Collector are listed.

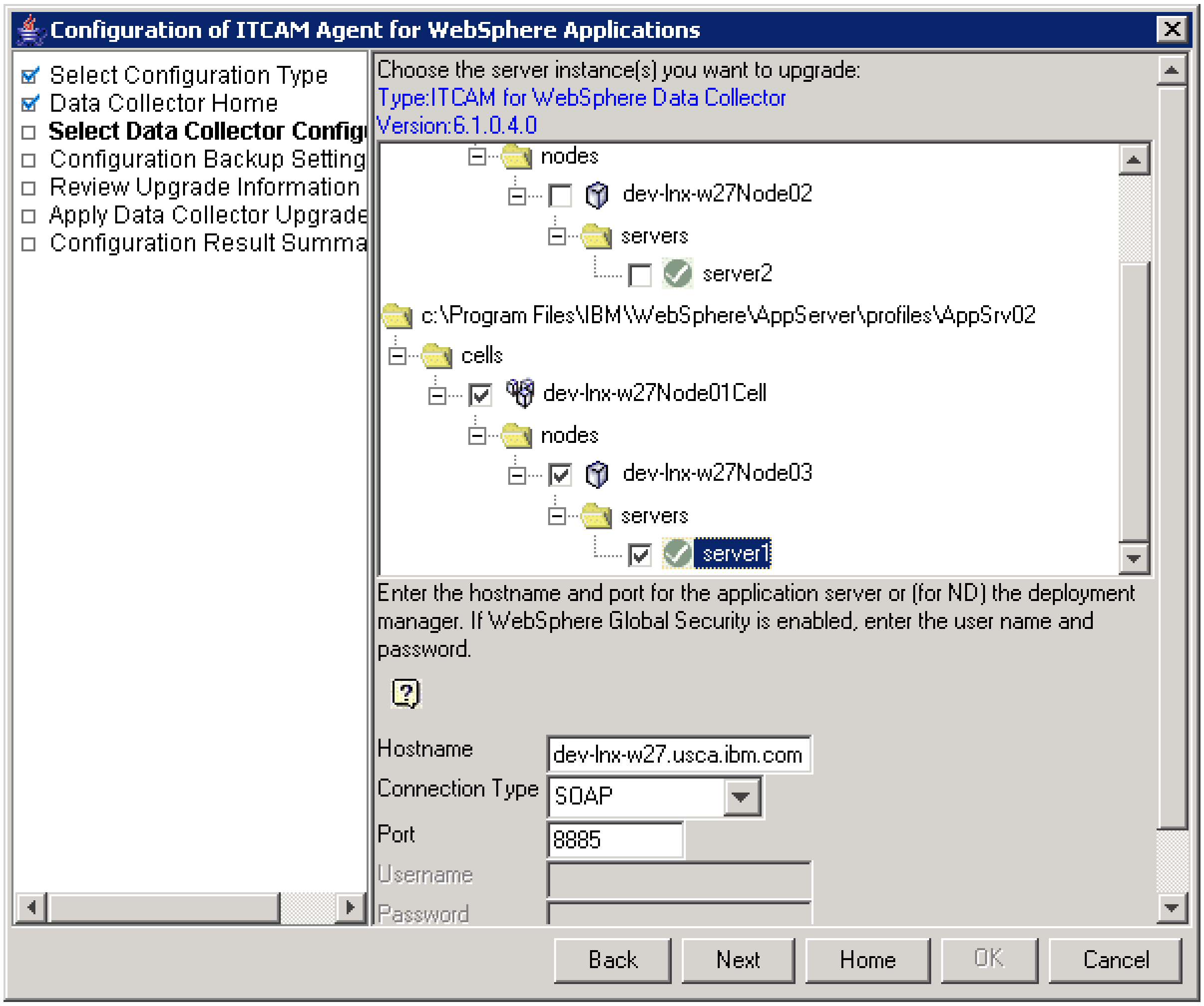
   Note:

   - For a stand alone environment, instances must be running during the configuration.
   - For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running.

   You also need to set the connection parameters for the application server instances. By default, the information that was set during initial Data Collector configuration for each instance will be displayed (except username and password). The following table lists the fields:

Table 6. Fields for establishing Data Collector and application server communication

Field	**What to do**
Host Name	Type the fully qualified host name or IP address of the application server instance that the Data Collector monitors. Do not include a protocol in the host name. For example, type myserver.ibm.tivoli.com, not https://myserver.ibm.tivoli.com. Note: If using a Network Deployment environment, provide the host name of the Deployment Manager instead.
Connector Type	Select the type of connection the Data Collector and application server will use for communication.
Port	If you selected SOAP as the connector type, enter the connector port used by the application server instance to send commands using the Simple Object Access Protocol (SOAP). The SOAP port is identified in the `AppServer_home/profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml` file for the instance of application server that the Data Collector will monitor. **Note:** If using Network Deployment, provide the SOAP port of the Deployment Manager instead. If you selected RMI as the connector type, enter the connector port used by the application server instance to send commands using RMI.
Username (only for Global Security enabled)	Type the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server. If, instead of typing the user ID, you want to retrieve the user ID from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.
Password (only for Global Security enabled)	Type the password that corresponds to the user specified in the **Username** field. If, instead of typing the password, you want to retrieve the password from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
□ Select Data Collector Config
□ Configuration Backup Setting
□ Review Upgrade Information
□ Apply Data Collector Upgrade
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the server instance(s) you want to upgrade:

Type:ITCAM for WebSphere Data Collector

Version:6.1.0.4.0

```
      nodes
        □ dev-lnx-w27Node02
            servers
              □ server2
c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02
  cells
    ☑ dev-lnx-w27Node01Cell
      nodes
        ☑ dev-lnx-w27Node03
            servers
              ☑ server1
```

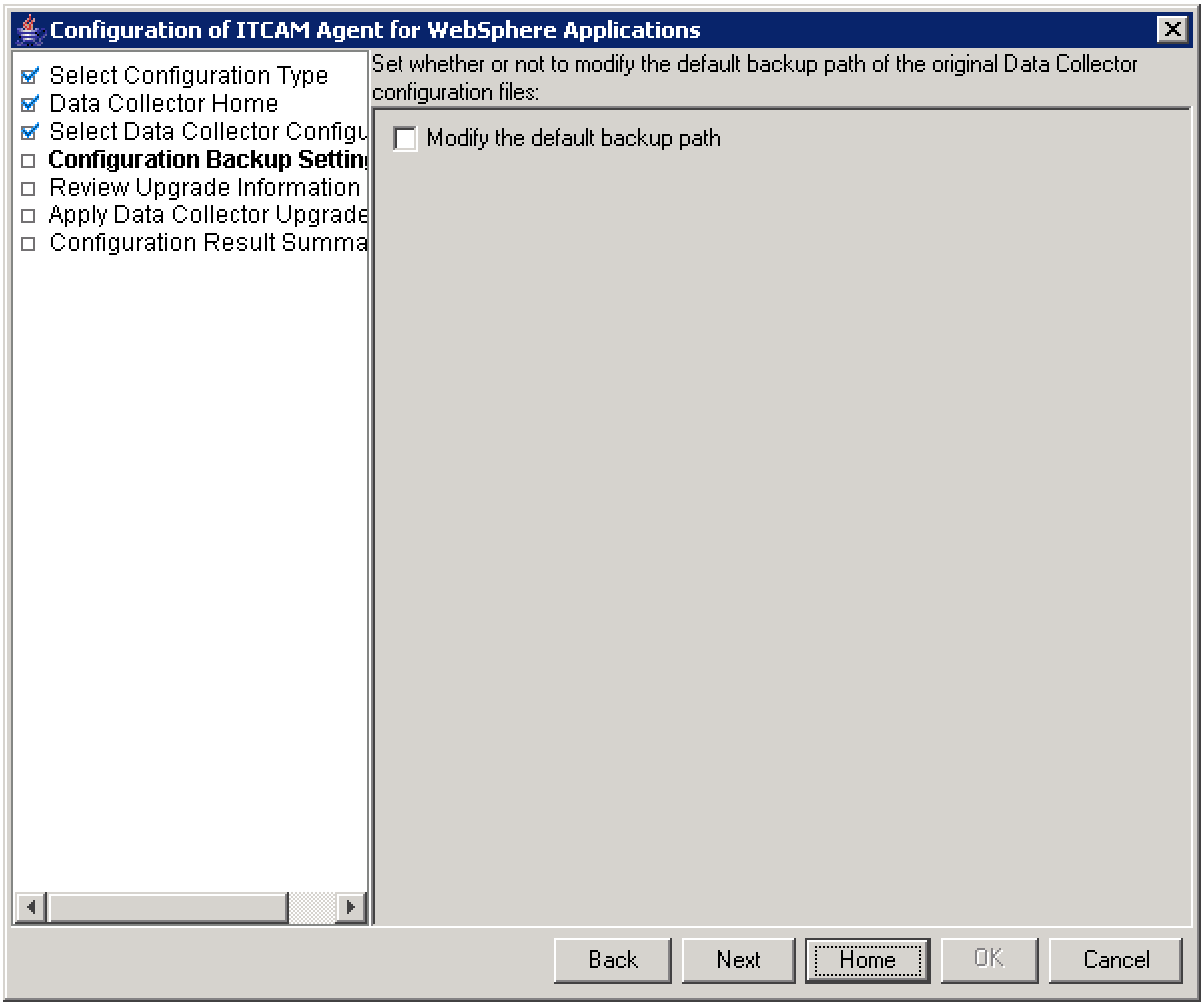
Enter the hostname and port for the application server or (for ND) the deployment manager. If WebSphere Global Security is enabled, enter the user name and password.

Hostname	dev-lnx-w27.usca.ibm.com
Connection Type	SOAP
Port	8885
Username	
Password	

Figure 46. Upgrading monitoring to Data Collector 7.1, window 3

Check the boxes next to the instances you want to configure. Then, click **Next**.

5. In the following window, choose whether you want to modify the path for backing up application server configuration files. Normally you do not need to change it.



Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Configu
□ Configuration Backup Settin
□ Review Upgrade Information
□ Apply Data Collector Upgrade
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

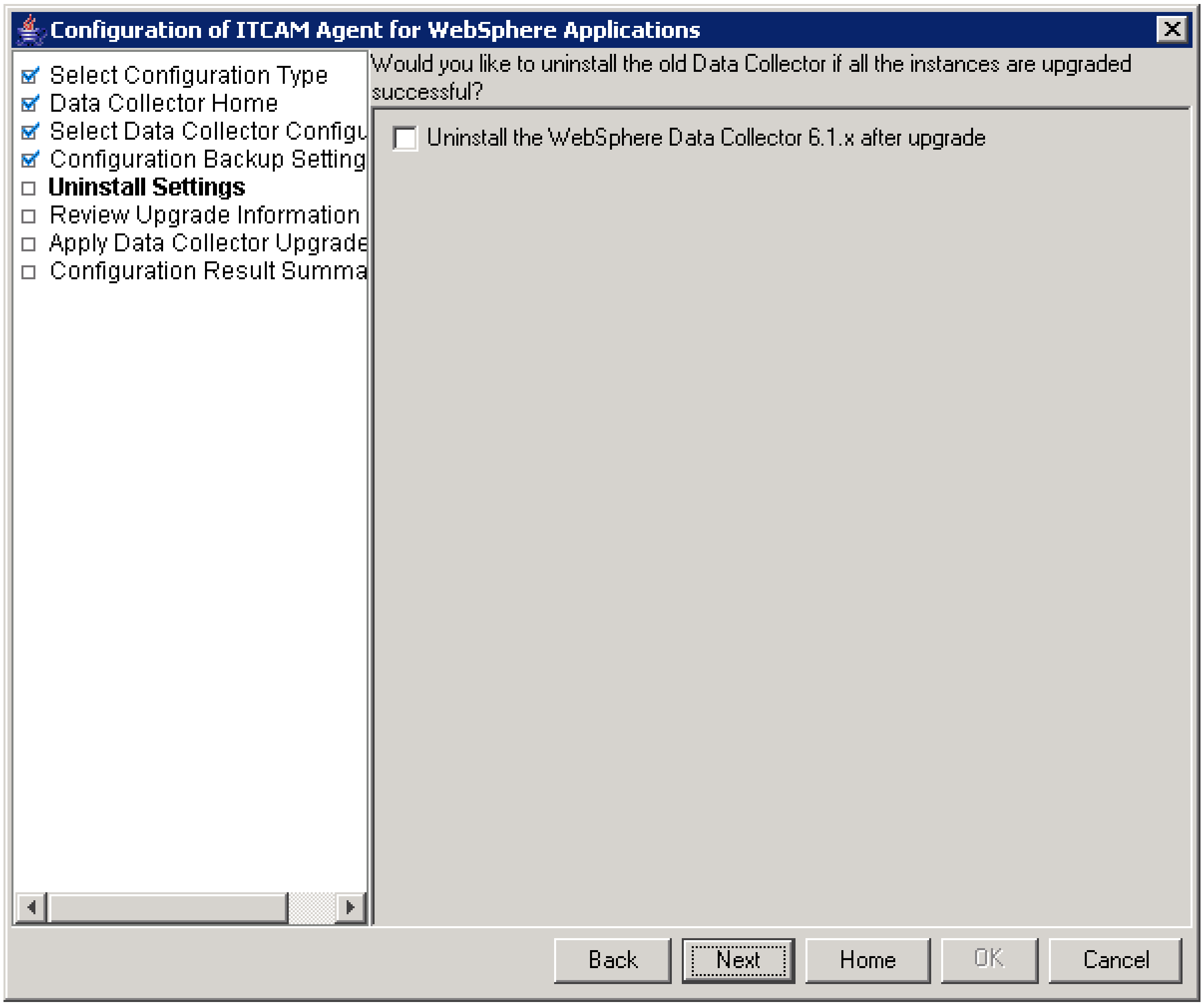
Set whether or not to modify the default backup path of the original Data Collector configuration files:

□ Modify the default backup path

Figure 47. Upgrading monitoring to Data Collector 7.1, window 4

If you wish to change the backup path, check the box and click **Browse** to set the new path.Click **Next**.

6. If the following window is displayed, choose whether you want to uninstall the old Data Collector after upgrading the instances. (If the window is not displayed, proceed to the next step).


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Configu
☑ Configuration Backup Setting
□ **Uninstall Settings**
□ Review Upgrade Information
□ Apply Data Collector Upgrade
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Would you like to uninstall the old Data Collector if all the instances are upgraded successful?

□ Uninstall the WebSphere Data Collector 6.1.x after upgrade

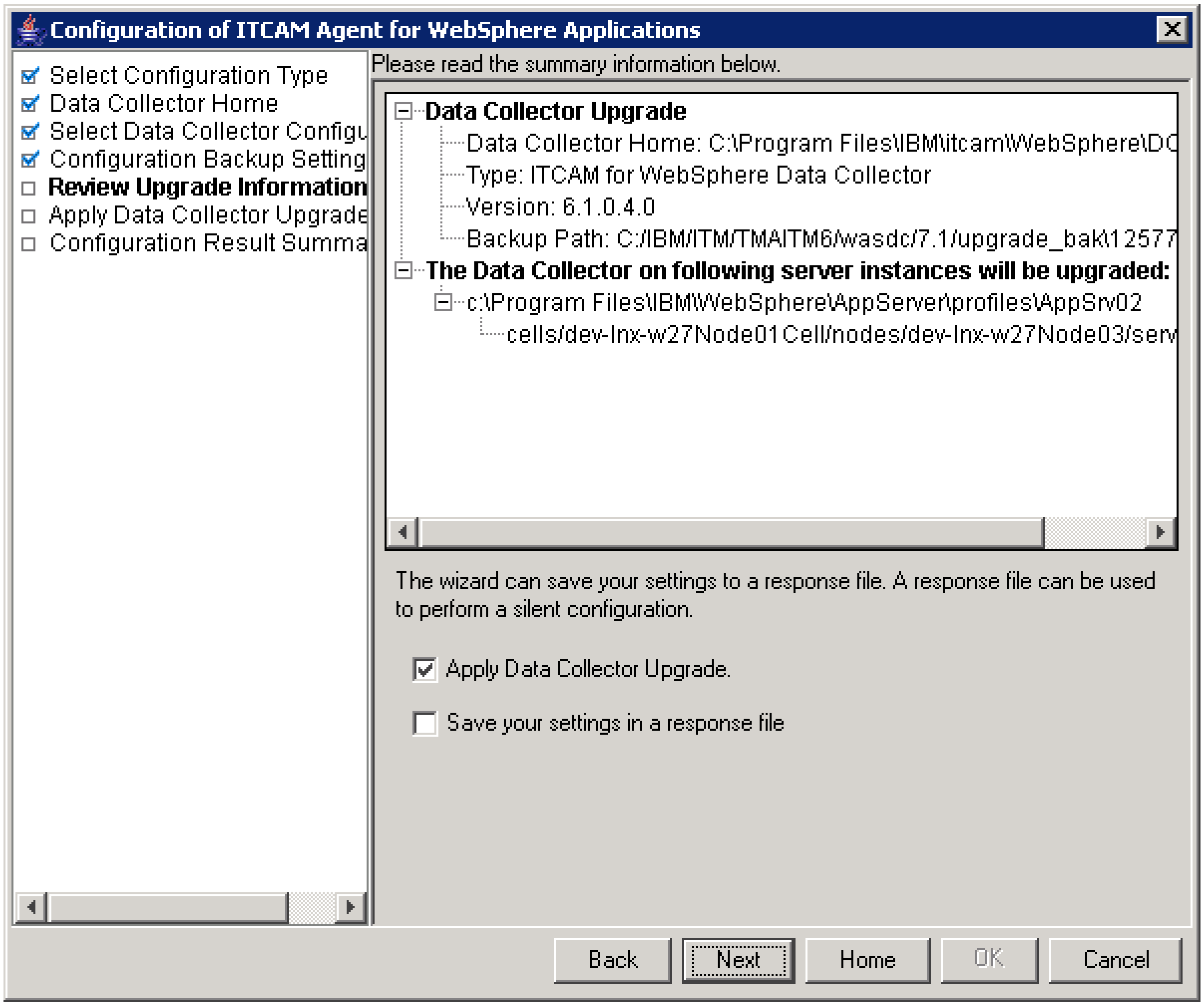
Figure 48. Upgrading monitoring to Data Collector 7.1, window 5

If you are upgrading all application server instances monitored by the older Data Collector on this host, you may choose to perform the uninstallation. If there are instances you are not upgrading, unconfigure the old Data Collector for them using its own configuration utility before uninstalling it. There is no requirement to uninstall the old Data Collector.

If you wish to uninstall the old Data Collector, check the box.

Click **Next**.

7. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Configu
☑ Configuration Backup Setting
□ Review Upgrade Information
□ Apply Data Collector Upgrade
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Please read the summary information below.

- **Data Collector Upgrade**
  - Data Collector Home: C:\Program Files\IBM\itcam\WebSphere\DC
  - Type: ITCAM for WebSphere Data Collector
  - Version: 6.1.0.4.0
  - Backup Path: C:/IBM/ITM/TMAITM6/wasdc/7.1/upgrade_bak\12577
- **The Data Collector on following server instances will be upgraded:**
  - c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02
    - cells/dev-lnx-w27Node01Cell/nodes/dev-lnx-w27Node03/serv

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

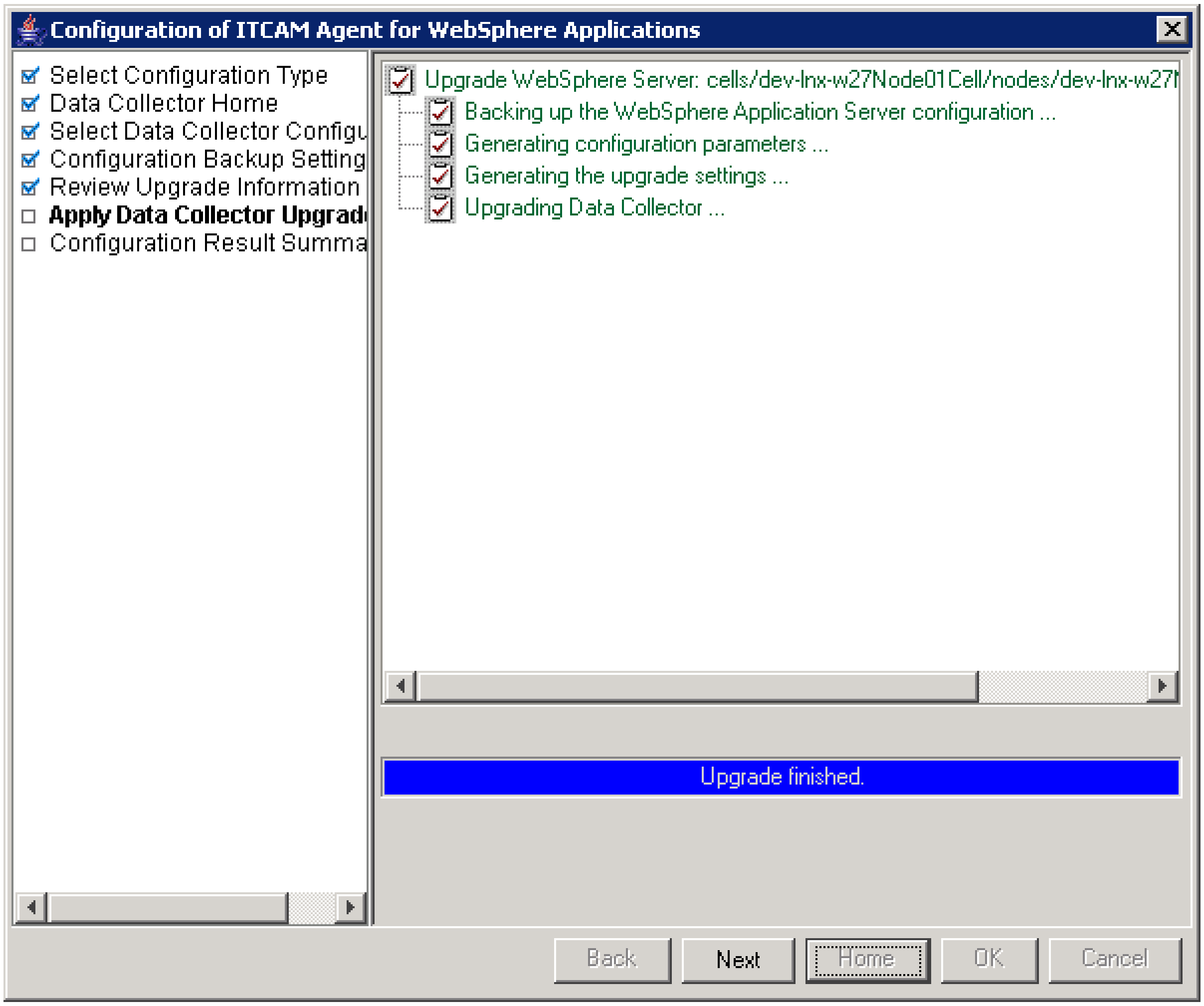
☑ Apply Data Collector Upgrade.

□ Save your settings in a response file

Figure 49. Upgrading monitoring to Data Collector 7.1, window 6

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Data Collector Upgrade**, the upgrade will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

8. The configuration utility will validate the applications server connection and apply the upgrade.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Configu
☑ Configuration Backup Setting
☑ Review Upgrade Information
□ Apply Data Collector Upgrad
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

☑ Upgrade WebSphere Server: cells/dev-lnx-w27Node01Cell/nodes/dev-lnx-w27N

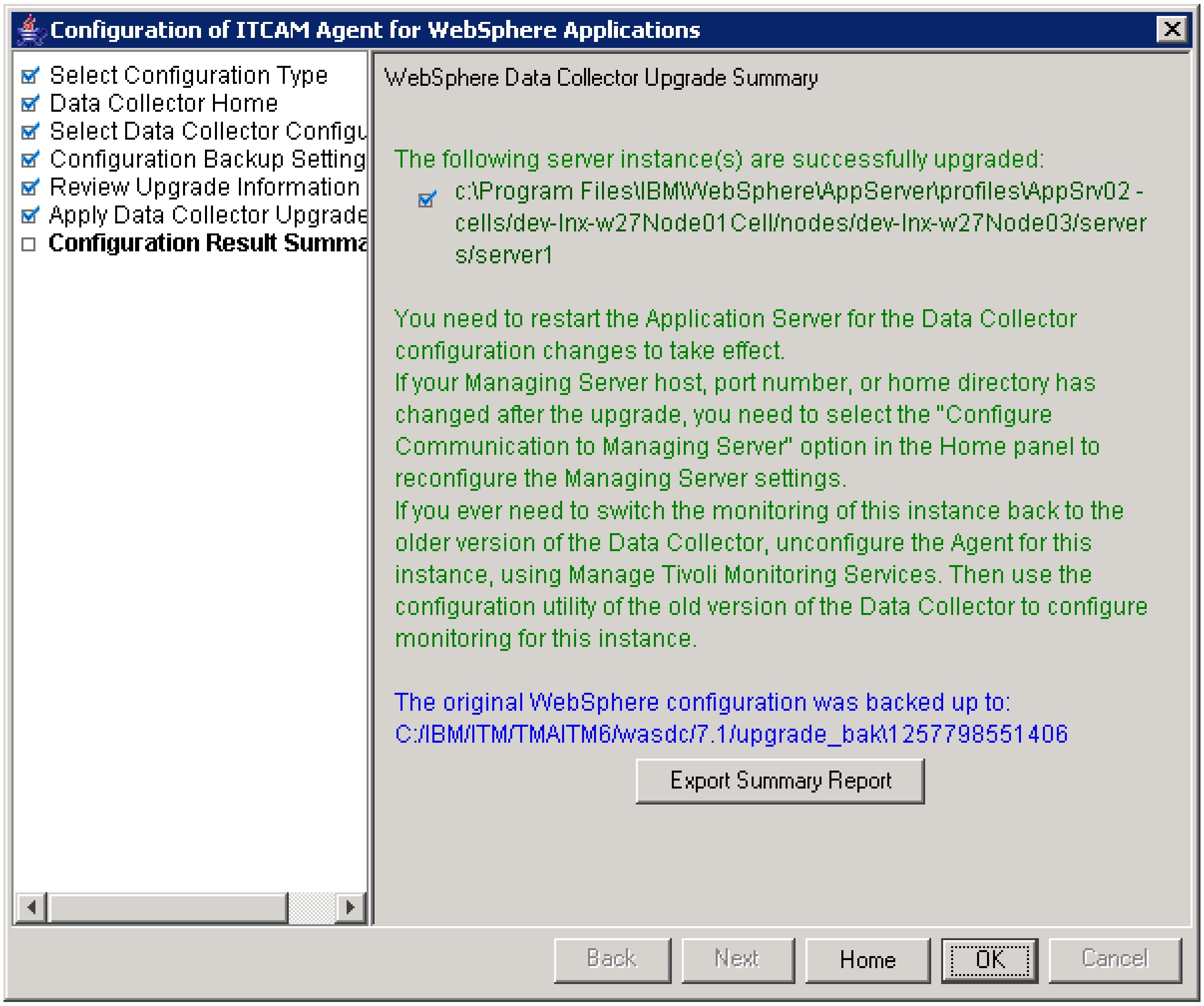
- ☑ Backing up the WebSphere Application Server configuration ...
- ☑ Generating configuration parameters ...
- ☑ Generating the upgrade settings ...
- ☑ Upgrading Data Collector ...

Upgrade finished.

Figure 50. Upgrading monitoring to Data Collector 7.1, window 7

Click **Next**.

9. WebSphere unconfiguration summary information is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Configu
☑ Configuration Backup Setting
☑ Review Upgrade Information
☑ Apply Data Collector Upgrade
□ Configuration Result Summa
Export Summary Report
Back
Next
Home
OK
Cancel

WebSphere Data Collector Upgrade Summary

The following server instance(s) are successfully upgraded:

☑ c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02 - cells/dev-lnx-w27Node01Cell/nodes/dev-lnx-w27Node03/servers/server1

You need to restart the Application Server for the Data Collector configuration changes to take effect.
If your Managing Server host, port number, or home directory has changed after the upgrade, you need to select the "Configure Communication to Managing Server" option in the Home panel to reconfigure the Managing Server settings.
If you ever need to switch the monitoring of this instance back to the older version of the Data Collector, unconfigure the Agent for this instance, using Manage Tivoli Monitoring Services. Then use the configuration utility of the old version of the Data Collector to configure monitoring for this instance.

The original WebSphere configuration was backed up to:
C:/IBM/ITM/TMAITM6/wasdc/7.1/upgrade_bak\1257798551406

Figure 51. Upgrading monitoring to Data Collector 7.1, window 8

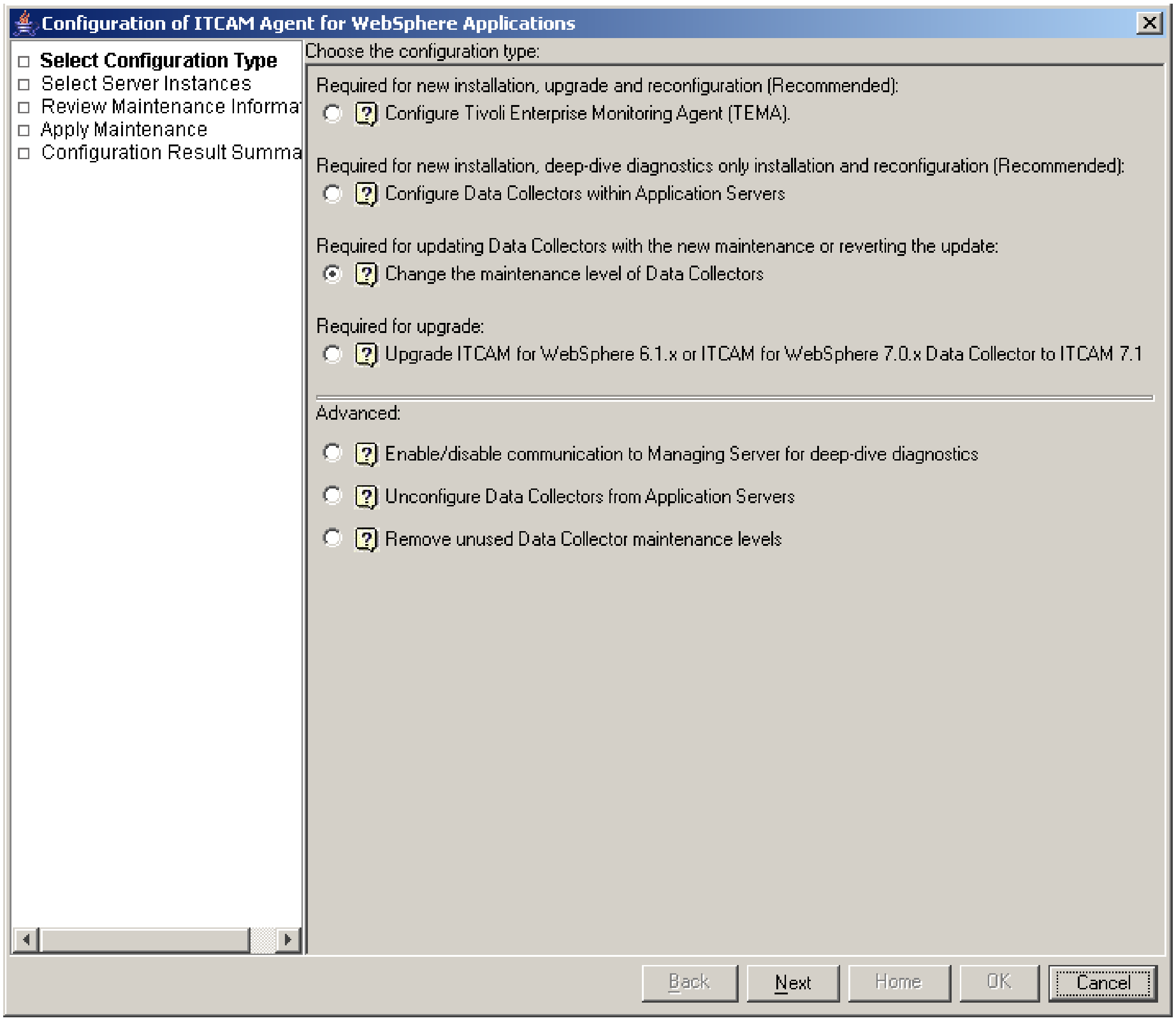
To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window.

Changing Data Collector maintenance level

If an application server instance is monitored by the Data Collector version 7.1, and more than one maintenance level for this version is installed by the host (for example, 7.1.0 and 7.1.0.1), you can change the maintenance level. After installing a new maintenance level, you must perform this change to update the monitoring of application server instances. You can not remove an old maintenance level until all monitored server instances are moved to another level.

To change the Data Collector maintenance level for monitored application server instances, perform the following procedure:

1. Enter the Agent Configuration window. After installation of the Agent, this window opens automatically. Otherwise, see “Entering the Agent Configuration window” on page 25.


Configuration of ITCAM Agent for WebSphere Applications

- □ **Select Configuration Type**
- □ Select Server Instances
- □ Review Maintenance Informa
- □ Apply Maintenance
- □ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

● Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

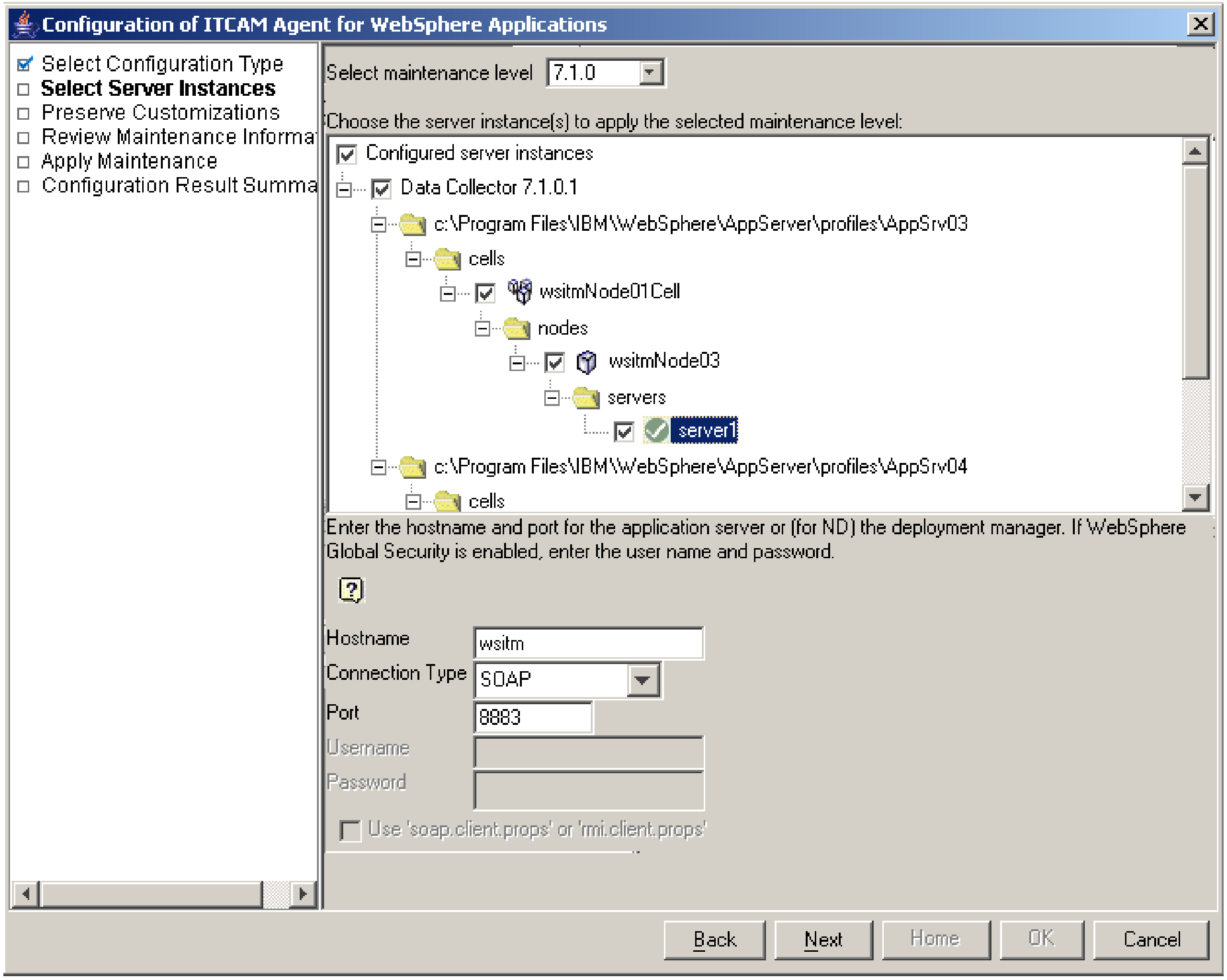
○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 52. Changing Data Collector maintenance level, window 1

2. Select **Change the maintenance level of Data Collectors** and click **Next**.
3. Select the required maintenance level, and the server instances you want to upgrade. All the instances monitored by this installation of the Agent are listed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ Select Server Instances
□ Preserve Customizations
□ Review Maintenance Informa
□ Apply Maintenance
□ Configuration Result Summa
☑ Configured server instances
☑ Data Collector 7.1.0.1
c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv03
cells
☑ wsitmNode01Cell
nodes
☑ wsitmNode03
servers
☑ server1
c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv04
cells
Back
Next
Home
OK
Cancel

Select maintenance level 7.1.0

Choose the server instance(s) to apply the selected maintenance level:

Enter the hostname and port for the application server or (for ND) the deployment manager. If WebSphere Global Security is enabled, enter the user name and password.

Hostname wsitm

Connection Type SOAP

Port 8883

Username

Password

□ Use 'soap.client.props' or 'rmi.client.props'

Figure 53. Changing Data Collector maintenance level, window 2

Note:

- For a stand alone environment, instances must be running during the configuration.
- For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running.

You also need to set the connection parameters for the application server instances. By default, the information that was set during initial Data Collector configuration for each instance will be displayed (except username and password). The following table lists the fields:

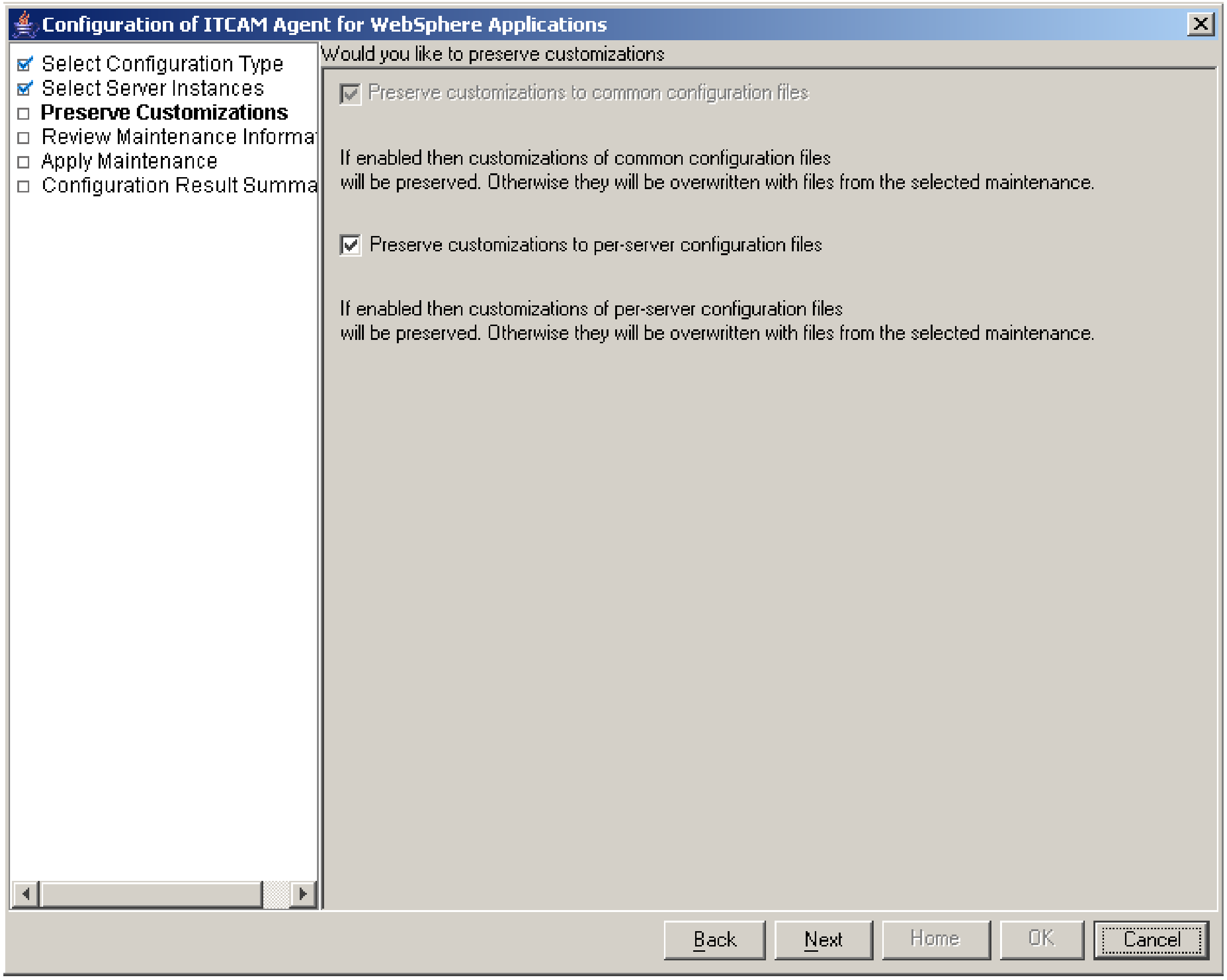
Table 7. Fields for establishing Data Collector and application server communication

Field	**What to do**
Host Name	Type the fully qualified host name or IP address of the application server instance that the Data Collector monitors. Do not include a protocol in the host name. For example, type myserver.ibm.tivoli.com, not https://myserver.ibm.tivoli.com. Note: If using a Network Deployment environment, provide the host name of the Deployment Manager instead.
Connector Type	Select the type of connection the Data Collector and application server will use for communication.
Port	If you selected SOAP as the connector type, enter the connector port used by the application server instance to send commands using the Simple Object Access Protocol (SOAP). The SOAP port is identified in the `AppServer_home/profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml` file for the instance of application server that the Data Collector will monitor. **Note:** If using Network Deployment, provide the SOAP port of the Deployment Manager instead. If you selected RMI as the connector type, enter the connector port used by the application server instance to send commands using RMI.
Username (only for Global Security enabled)	Type the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server. If, instead of typing the user ID, you want to retrieve the user ID from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.
Password (only for Global Security enabled)	Type the password that corresponds to the user specified in the **Username** field. If, instead of typing the password, you want to retrieve the password from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.

Check the boxes next to the instances you want to configure. Then, click **Next**.

4. In the following window, choose whether the update is to preserve modifications that were made to custom Data Collector configuration files (see “Properties files for the Data Collector” on page 217). Unless you have special requirements, preserve the customizations; ensure that both checkboxes are selected.

Attention: You can only choose whether to preserve common configuration files if this is the first time you are changing instances on this host to this maintenance level. At this time the common files will be processed. If you have already changed any instances to the level, this checkbox is unavailable.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Select Server Instances
□ **Preserve Customizations**
□ Review Maintenance Informa
□ Apply Maintenance
□ Configuration Result Summa

Would you like to preserve customizations

☑ Preserve customizations to common configuration files

If enabled then customizations of common configuration files
will be preserved. Otherwise they will be overwritten with files from the selected maintenance.

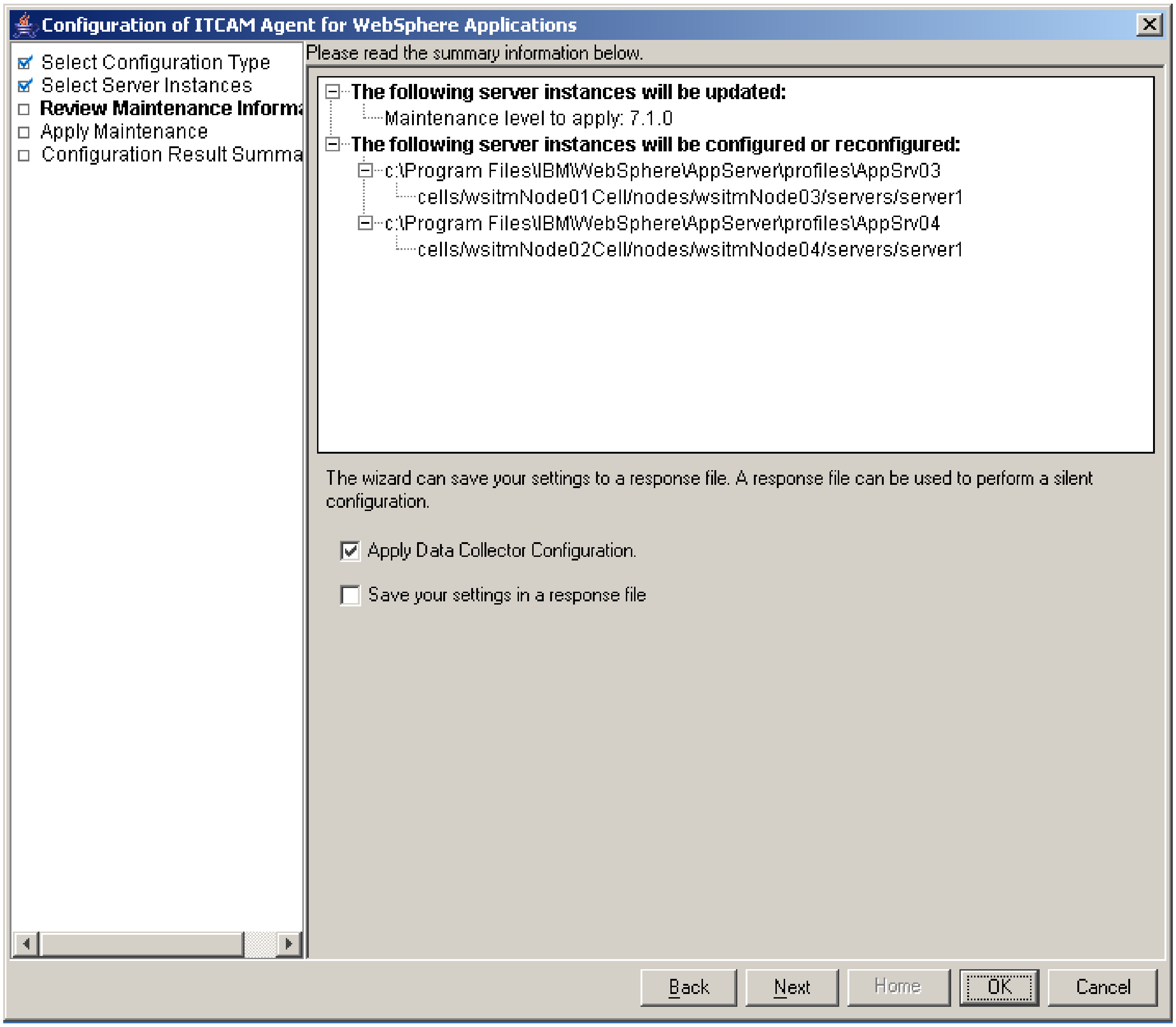
☑ Preserve customizations to per-server configuration files

If enabled then customizations of per-server configuration files
will be preserved. Otherwise they will be overwritten with files from the selected maintenance.

Figure 54. Changing Data Collector maintenance level, window 3

Click **Next**.

5. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Select Server Instances
□ **Review Maintenance Informa**
□ Apply Maintenance
□ Configuration Result Summa

Please read the summary information below.

```
⊟ The following server instances will be updated:
   └ Maintenance level to apply: 7.1.0
⊟ The following server instances will be configured or reconfigured:
   ⊟ c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv03
      └ cells/wsitmNode01Cell/nodes/wsitmNode03/servers/server1
   ⊟ c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv04
      └ cells/wsitmNode02Cell/nodes/wsitmNode04/servers/server1
```

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

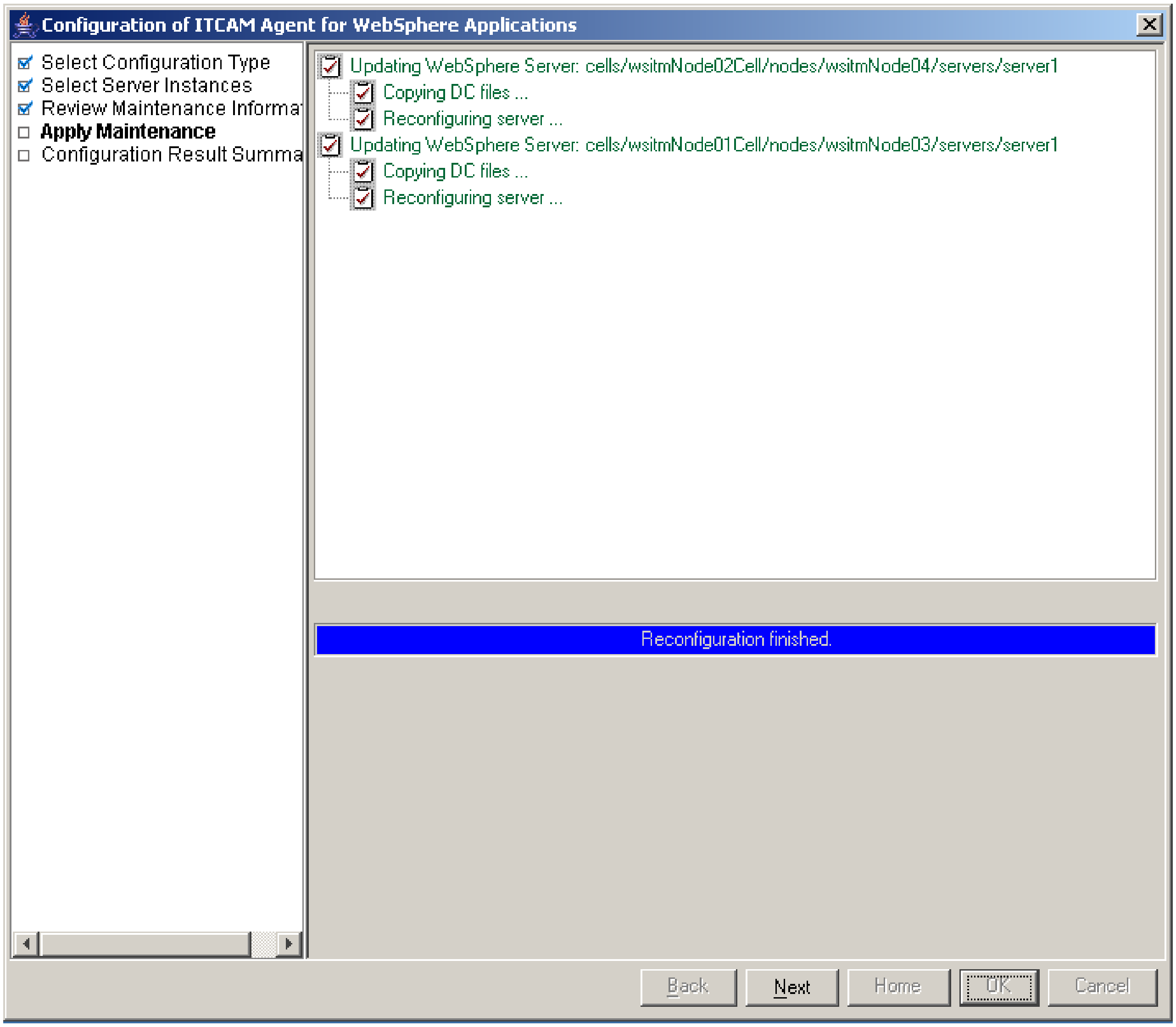
☑ Apply Data Collector Configuration.

□ Save your settings in a response file

Figure 55. Changing Data Collector maintenance level, window 4

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Configuration**, the new configuration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

6. The configuration utility will validate the applications server connection and apply the change.



Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Server Instances
☑ Review Maintenance Informat
□ **Apply Maintenance**
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

☑ Updating WebSphere Server: cells/wsitmNode02Cell/nodes/wsitmNode04/servers/server1
- ☑ Copying DC files ...
- ☑ Reconfiguring server ...

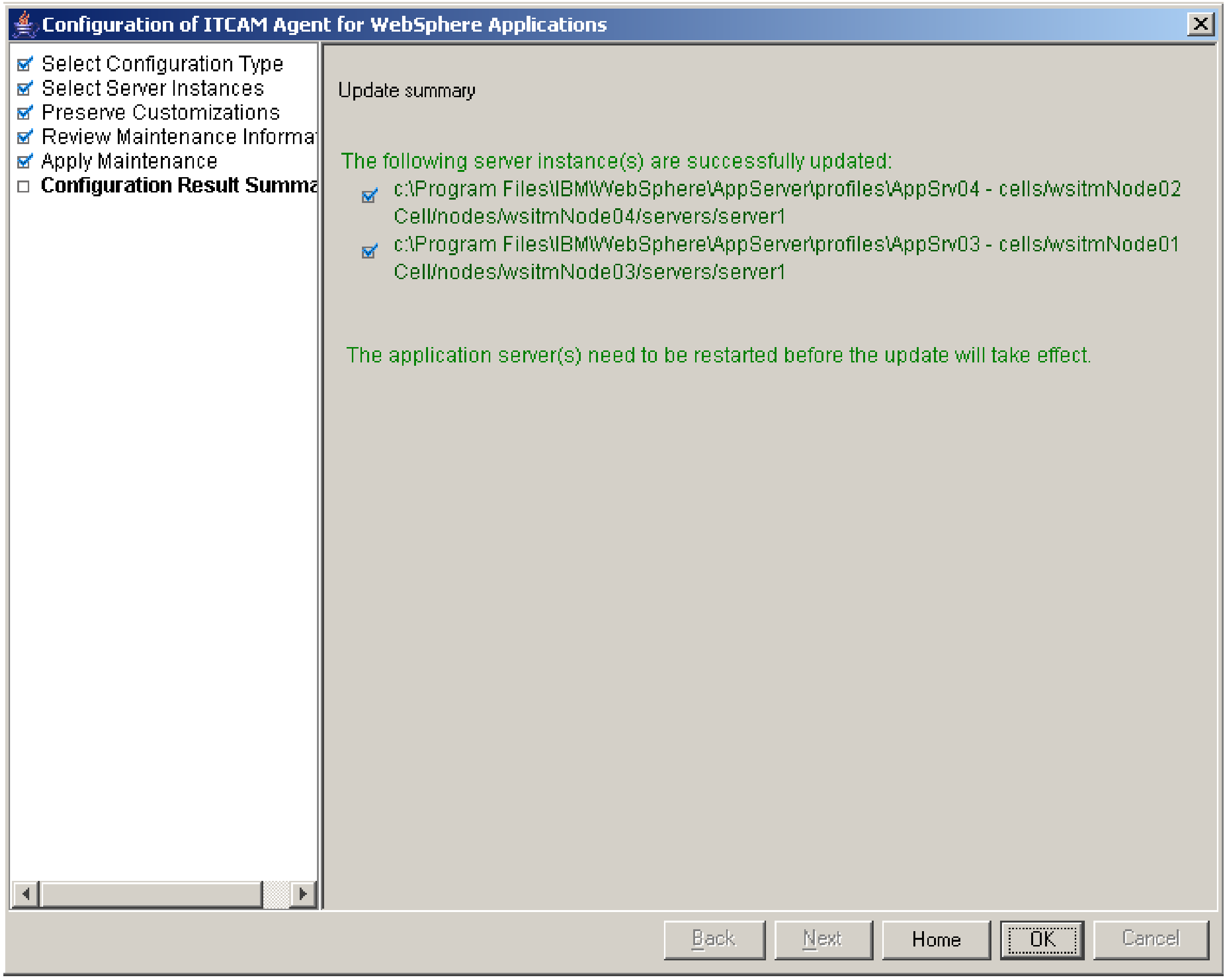
☑ Updating WebSphere Server: cells/wsitmNode01Cell/nodes/wsitmNode03/servers/server1
- ☑ Copying DC files ...
- ☑ Reconfiguring server ...

Reconfiguration finished.

Figure 56. Changing Data Collector maintenance level, window 5

Click **Next**.

7. Summary information is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Server Instances
☑ Preserve Customizations
☑ Review Maintenance Informa
☑ Apply Maintenance
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Update summary

The following server instance(s) are successfully updated:

☑ c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv04 - cells/wsitmNode02Cell/nodes/wsitmNode04/servers/server1

☑ c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv03 - cells/wsitmNode01Cell/nodes/wsitmNode03/servers/server1

The application server(s) need to be restarted before the update will take effect.

Figure 57. Changing Data Collector maintenance level, window 6

To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window.

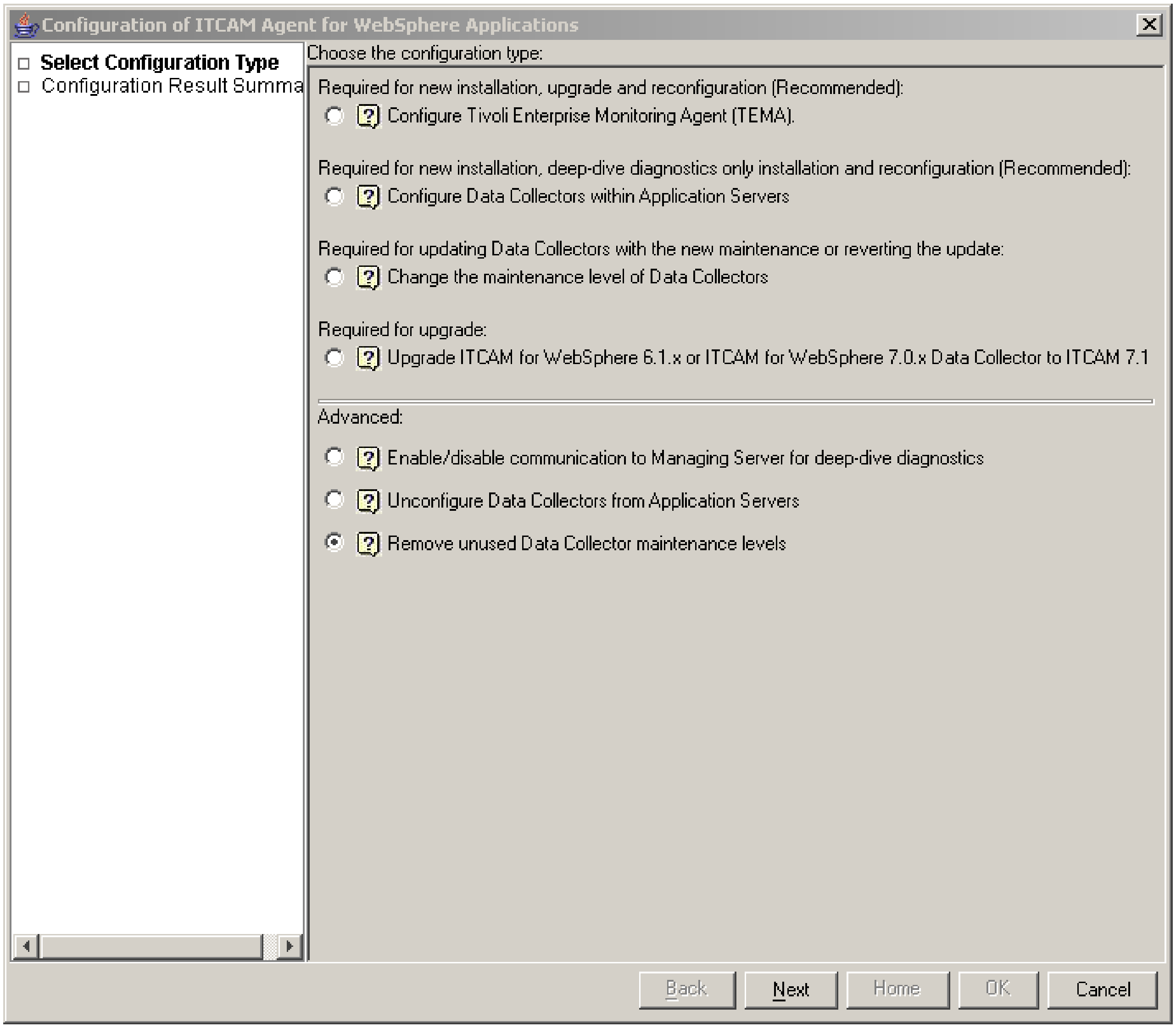
Tip: If an older maintenance level is no longer used, you can remove it. See "Removing a Data Collector maintenance level."

Removing a Data Collector maintenance level

If an older maintenance level of the Data Collector version 7.1 is installed, and all the monitored applications server instances were updated to the new maintenance level, you can remove the older maintenance level.

To remove an unused maintenance level Data Collector version 7.1, perform the following procedure:

1. Enter the Agent Configuration window. After installation of the Agent, this window opens automatically. Otherwise, see "Entering the Agent Configuration window" on page 25.



Configuration of ITCAM Agent for WebSphere Applications

□ **Select Configuration Type**
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):
○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):
○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:
○ Change the maintenance level of Data Collectors

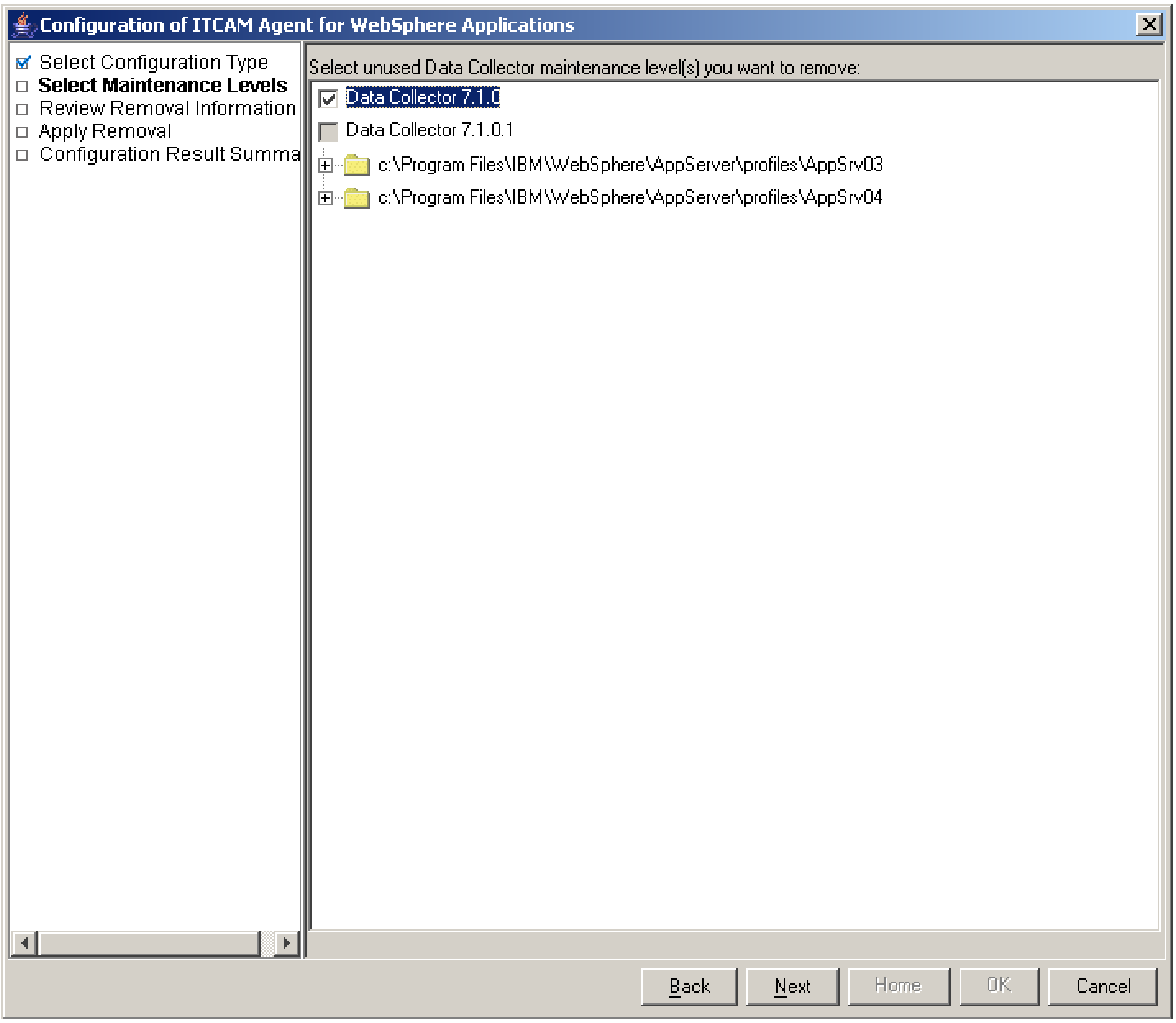
Required for upgrade:
○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:
○ Enable/disable communication to Managing Server for deep-dive diagnostics
○ Unconfigure Data Collectors from Application Servers
● Remove unused Data Collector maintenance levels

Figure 58. Uninstalling a Data Collector maintenance level, window 1

2. Select **Remove unused Data Collector maintenance levels** and click **Next**.
3. Select the maintenance levels to remove. Only the levels that are not used for any application server instances are available for selection. For other available maintenance level, this window shows a list of application server instances monitored by them.

   Tip: If you want to remove a Data Collector maintenance level, but this window shows it as used for application server instances, change the maintenance level for the instances. See "Changing Data Collector maintenance level" on page 69.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ **Select Maintenance Levels**
□ Review Removal Information
□ Apply Removal
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Select unused Data Collector maintenance level(s) you want to remove:

☑ Data Collector 7.1.0

□ Data Collector 7.1.0.1

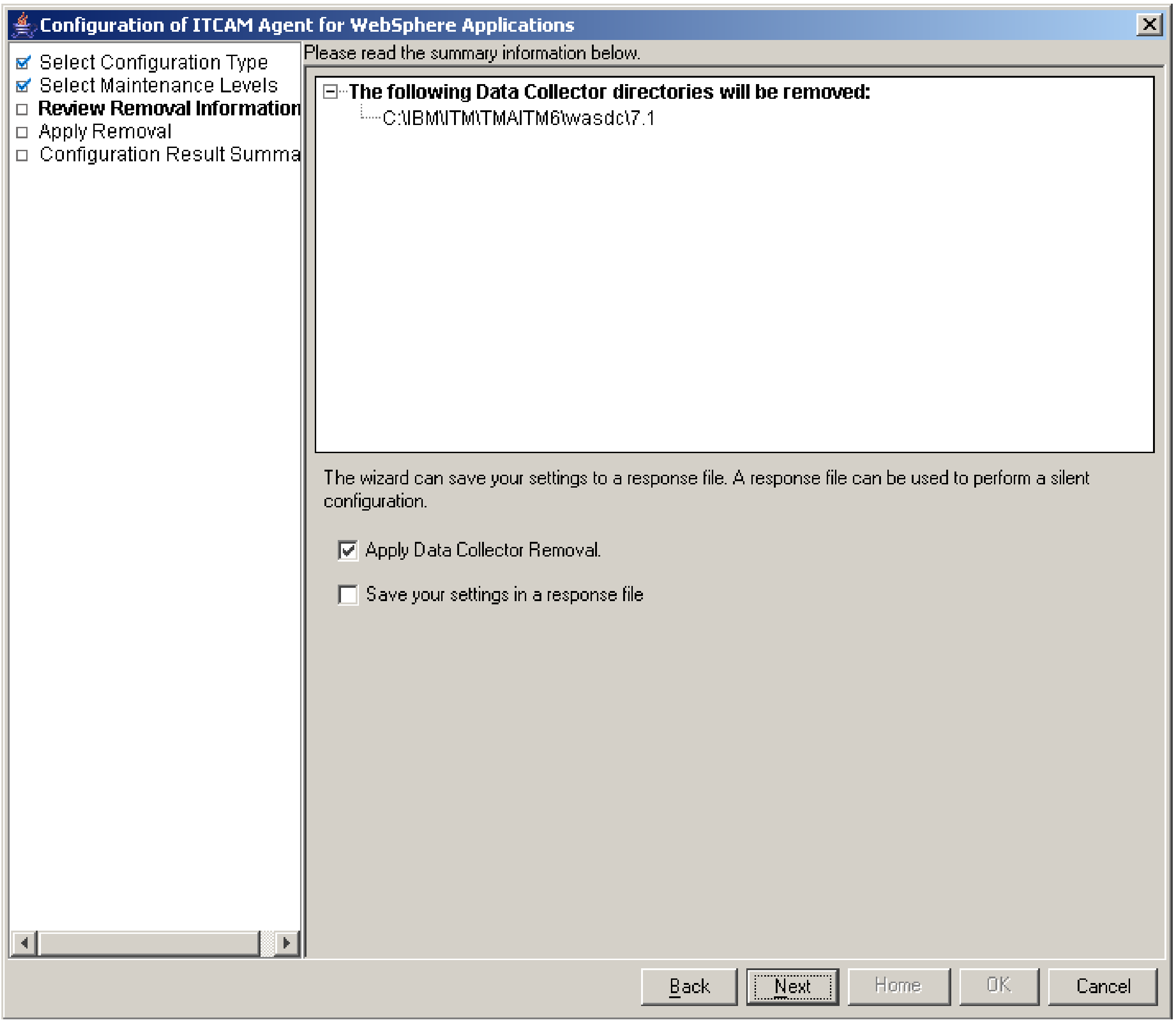
c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv03

c:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv04

Figure 59. Uninstalling a Data Collector maintenance level, window 2

Check the boxes next to the levels you want to uninstall. Then, click **Next**.

4. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- ☑ Select Maintenance Levels
- □ **Review Removal Information**
- □ Apply Removal
- □ Configuration Result Summa

Please read the summary information below.

The following Data Collector directories will be removed:

C:\IBM\ITM\TMAITM6\wasdc\7.1

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

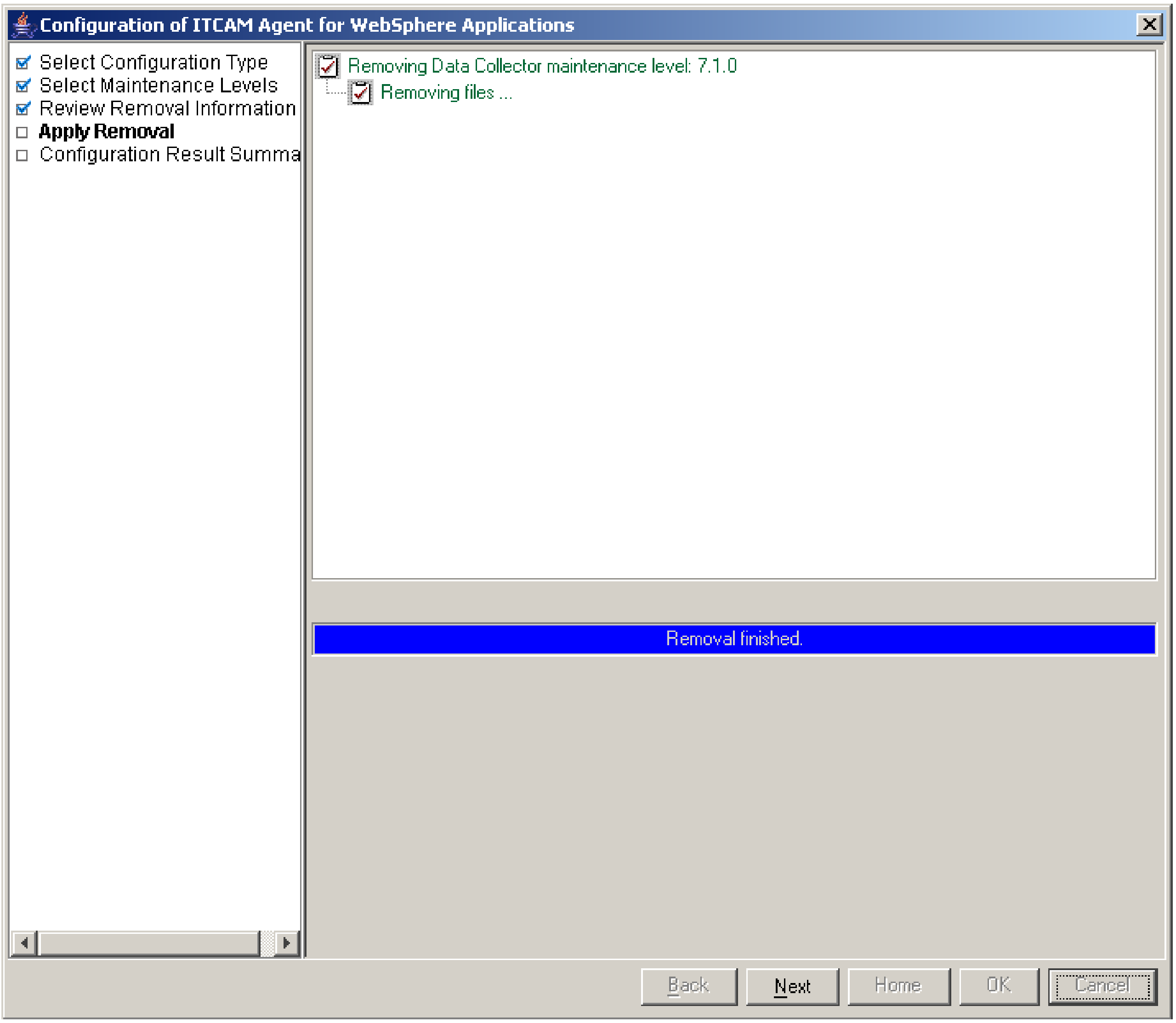
☑ Apply Data Collector Removal.

□ Save your settings in a response file

Figure 60. Uninstalling a Data Collector maintenance level, window 3

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Configuration**, the new configuration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

5. The configuration utility will apply the changes.



Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Maintenance Levels
☑ Review Removal Information
□ Apply Removal
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Removing Data Collector maintenance level: 7.1.0

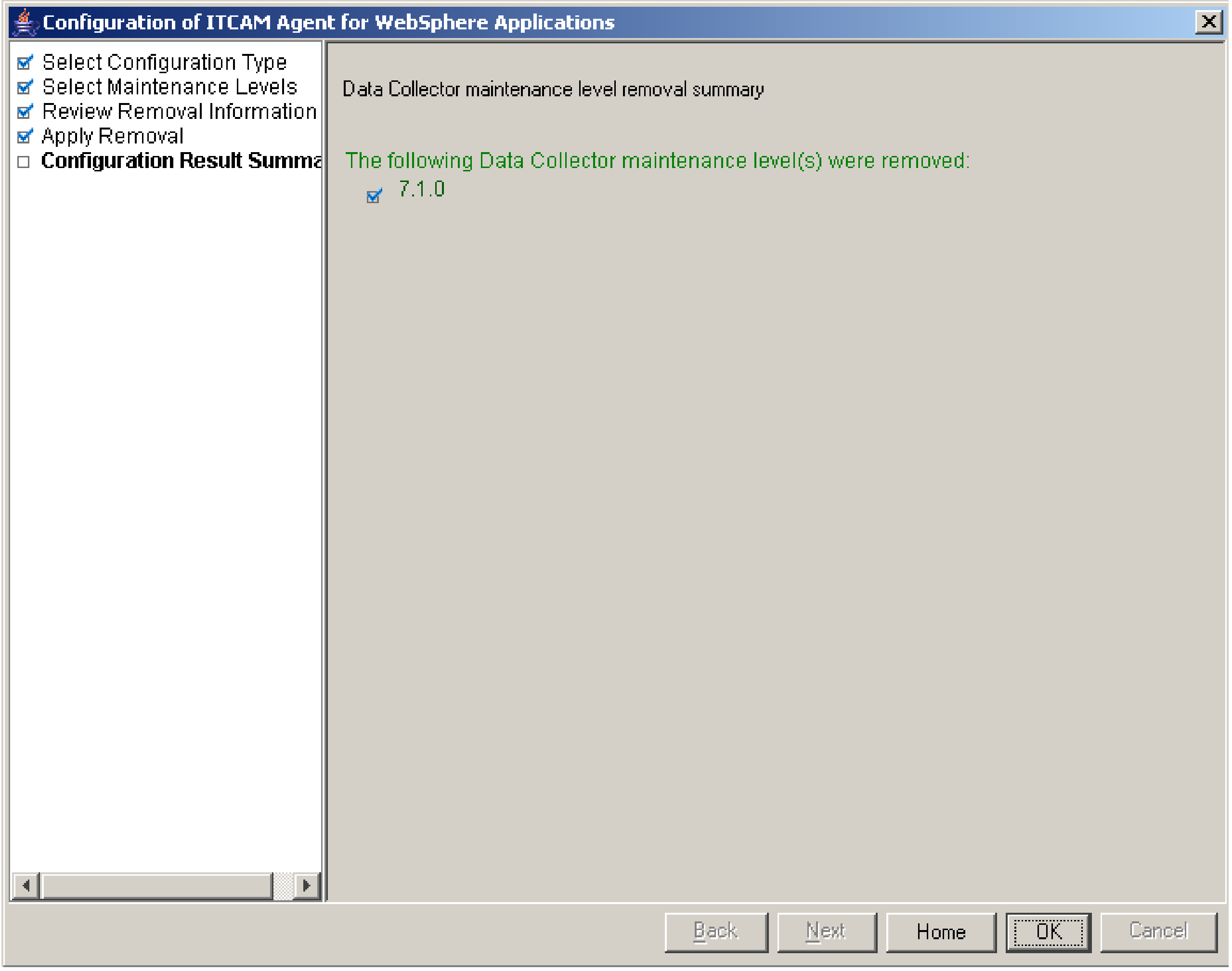
Removing files ...

Removal finished.

Figure 61. Uninstalling a Data Collector maintenance level, window 4

Click **Next**.

6. Summary information is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Maintenance Levels
☑ Review Removal Information
☑ Apply Removal
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Data Collector maintenance level removal summary

The following Data Collector maintenance level(s) were removed:

☑ 7.1.0

Figure 62. Uninstalling a Data Collector maintenance level, window 5

To export the summary report to a file, click the **Export Summary Report** button. Click **Home** to return to the **Agent Configuration** window.

Installing application support on Windows

To ensure that ITCAM Agent for WebSphere Applications works within your IBM Tivoli Monitoring infrastructure, you need to install application support files for it on every hub monitoring server, portal server, and portal client. After configuring the Agent on the monitored host, you also need to enable Tivoli monitoring history collection. You do not need to install application support files if IBM Tivoli Monitoring is not used (in a deep dive diagnostics only installation).

Important: You will need to stop the monitoring server, portal server, or portal client when installing the support files.

Attention: you must install support files for ITCAM Agent for WebSphere Applications version 7.1 before installing them for version 7.1.0.1.

Installing application support on the Tivoli Enterprise Monitoring Server

1. Stop the Tivoli Enterprise Monitoring Server. The installer automatically stops the Tivoli Enterprise Monitoring Server; you can also choose to stop the server manually before starting the installer. Perform the following steps to stop the Tivoli Enterprise Monitoring Server manually:
   a. Click **Start** → **Programs** → **IBM Tivoli Monitoring** → **Manage Tivoli Monitoring Services**.
   b. Right-click Tivoli Enterprise Monitoring Server.
   c. In the pop-up menu, select **Stop**.
2. Access the `\WINDOWS` subdirectory on the agent installation media.
3. Double-click **`setup.exe`**.
4. Click **Next** on the Welcome window.
5. The Software License Agreement window is displayed. Select **I accept the terms in the license agreement** and click **Next**.
6. Select **Tivoli Enterprise Monitoring Server - TEMS** and click **Next**.

   Note: If you have other components installed on the same computer, such as the desktop client, also select those components to install the component-specific application support.
7. If you need to install the Agent remotely, select the agent to add it to the remote deployment depot, and click **Next**. Otherwise, click **Next** without selecting any agents.
8. Review the installation summary details. Click **Next** to start the installation.
9. Select the setup type that best suits your needs.

   In the following steps you will be promoted for the information required to configure the items that are listed in the **Setup Type** window. You can uncheck the box to delay the configuration until the installation is complete. Some configuration items are mandatory (preceded by an *) and cannot be unchecked.
10. Specify the location of the monitoring server. Choose **On this computer** to install application support on the host you are running the setup file on, and **On a different computer** otherwise. Then click **OK**.
11. Select the application support to add to the monitoring server and click **OK**. By default, application supports which are not yet installed on this server are selected.
12. Review the application support addition details and click **Next**.
13. Specify the default values for the agent to use when it communicates with the monitoring server and click **OK**.

    Note:
    - You can specify three methods for communication to set up backup communication methods. If the method you have identified as Protocol 1 fails, Protocol 2 is used.
    - You can specify the default values for a backup communication between the agent and the monitoring server by selecting **Option Secondary TEMS Connection**.

    a. If the agent must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.

   b. Identify the type of protocol that the agent uses to communicate with the monitoring server. You have five choices: `IP.UDP`, `IP.PIPE`, `IP.SPIPE`, `SNA`, `No TEMS`.

14. Define the communications between agents and the monitoring server and click **OK**. For details of the information, see Table 2 on page 27.
15. Click **Finish**.

Installing application support on the Tivoli Enterprise Portal Server

1. Open **Manage Tivoli Enterprise Monitoring Services.**
2. Stop the portal server by right-clicking it and clicking **Stop**.
3. Access the `\WINDOWS` subdirectory on the agent installation media.
4. Double-click **`setup.exe`**.
5. Click **Next** on the Welcome window.
6. The Software License Agreement window is displayed. Select **I accept the terms in the license agreement** and click **Next**.
7. Select **Tivoli Enterprise Portal Server - TEPS** and click **Next**.

   Note: If you have other components installed on the same computer, such as the desktop client, also select those components to install the component-specific application support.
8. If you need remote configuration in the future, select the agent to add it to the remote deployment depot, and click **Next**. Otherwise, click **Next** without selecting any agents.
9. Review the installation summary details. Click **Next** to start the installation.
10. Select the setup type that best suits your needs.

    In the following steps you will be promoted for the information required to configure the items that list in the **Setup Type** window. You can uncheck the box to delay the configuration until the installation is complete. Some configuration items are mandatory (preceded by an *) and cannot be unchecked.
11. Type the host name for the portal server and click **Next**.
12. Click **Finish**.
13. Restart the portal server.

Important: If the Tivoli Enterprise Portal Server provides the browser client, check that the Eclipse help server has been configured. See "Ensuring that the Eclipse server has been configured" on page 84.

Installing application support on the Tivoli Enterprise Portal desktop client

1. Stop the desktop client before performing this procedure.
2. Access the `\WINDOWS` subdirectory on the agent installation media.
3. Double-click **`setup.exe`**.
4. Click **Next** on the Welcome window.
5. The Software License Agreement window is displayed. Select **I accept the terms in the license agreement** and click **Next**.
6. Select **TEP Desktop Client - TEPD** and click **Next**.

7. If you need remote configuration in the future, select the agent to add it to the remote deployment depot, and click **Next**. Otherwise, click **Next** without selecting any agents.
8. Review the installation summary details. Click **Next** to start the installation.
9. Select the setup type that best suits your needs.

   In the following steps you will be promoted for the information required to configure the items that list in the **Setup Type** window. You can uncheck the box to delay the configuration until the installation is complete. Some configuration items are mandatory (preceded by an *) and cannot be unchecked.
10. Type the host name for the portal server and click **Next**.
11. Click **Finish** to complete the installation.

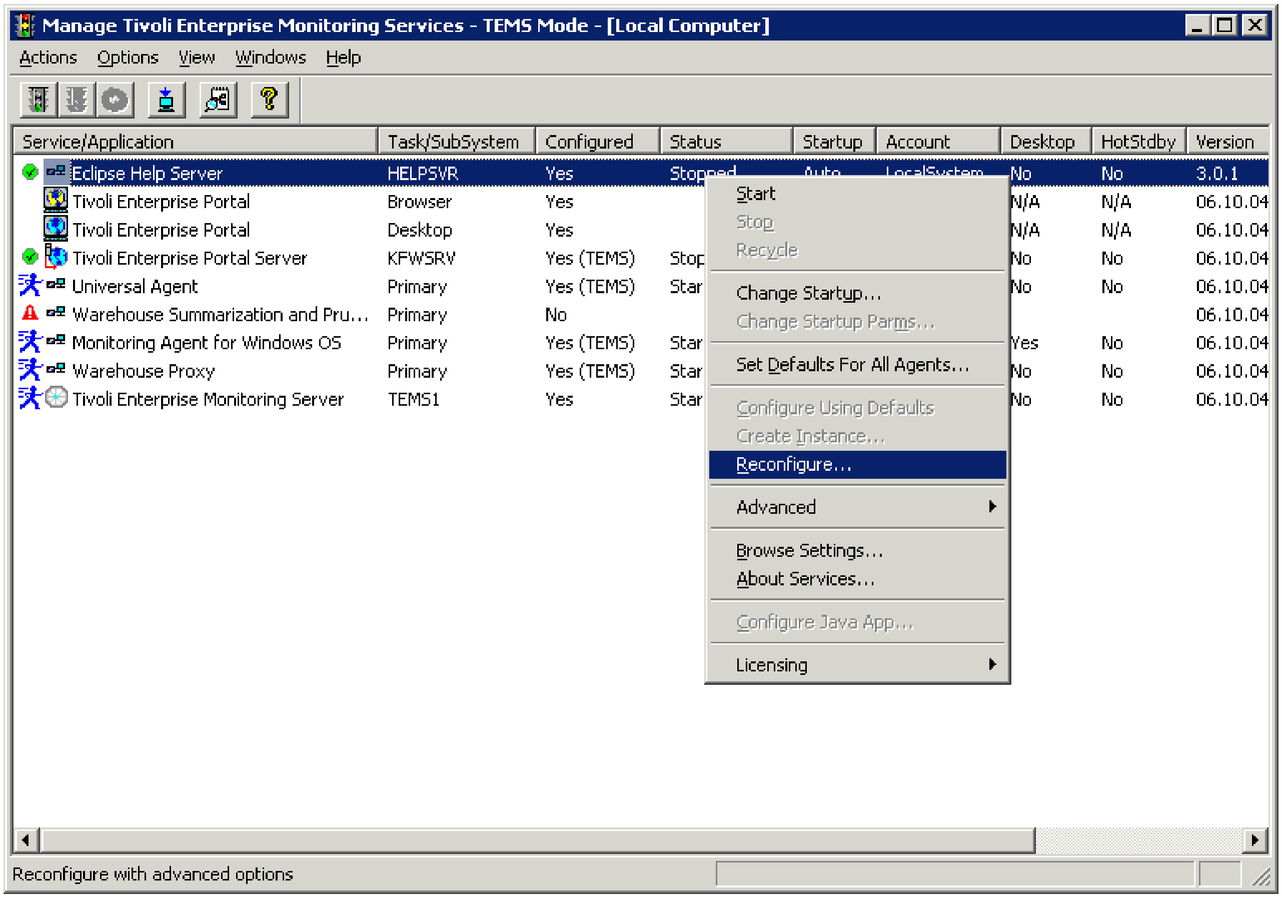
Important: Check that the Eclipse help server has been configured for the client. See "Ensuring that the Eclipse server has been configured."

Ensuring that the Eclipse server has been configured

After installing application support files on a Tivoli Enterprise Portal Server that provides the browser client or on a Tivoli Enterprise Portal desktop client, you must check the Eclipse help server for the portal client to ensure that it has been configured.

Start Manage Tivoli Enterprise Monitoring Services (**Start** > **All Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**), and ensure that the **Eclipse Help Server** entry indicates **Yes** in the Configured column.

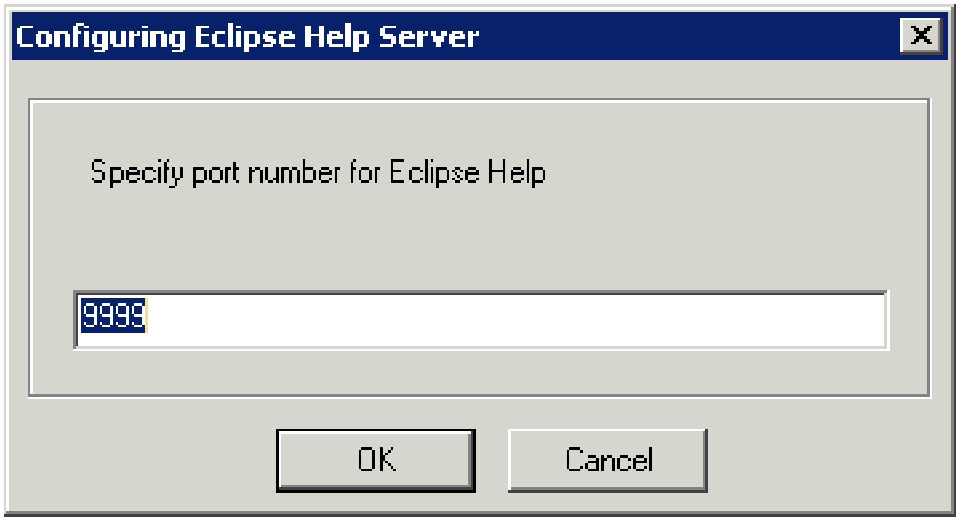
If indicates **No**, you must configure the Eclipse server. To do this, right-click the entry, and select **Configure Using Defaults** from the pop-up menu:



Service/Application	Task/SubSystem	Configured	Status	Startup	Account	Desktop	HotStdby	Version
Eclipse Help Server	HELPSVR	Yes	Stopped	Auto	LocalSystem	No	No	3.0.1
Tivoli Enterprise Portal	Browser	Yes				N/A	N/A	06.10.04
Tivoli Enterprise Portal	Desktop	Yes				N/A	N/A	06.10.04
Tivoli Enterprise Portal Server	KFWSRV	Yes (TEMS)	Stop			No	No	06.10.04
Universal Agent	Primary	Yes (TEMS)	Star			No	No	06.10.04
Warehouse Summarization and Pru...	Primary	No						06.10.04
Monitoring Agent for Windows OS	Primary	Yes (TEMS)	Star			Yes	No	06.10.04
Warehouse Proxy	Primary	Yes (TEMS)	Star			No	No	06.10.04
Tivoli Enterprise Monitoring Server	TEMS1	Yes	Star			No	No	06.10.04

Figure 63. Configuring the Eclipse server

You are prompted for the port number that the Eclipse Help Server will use:



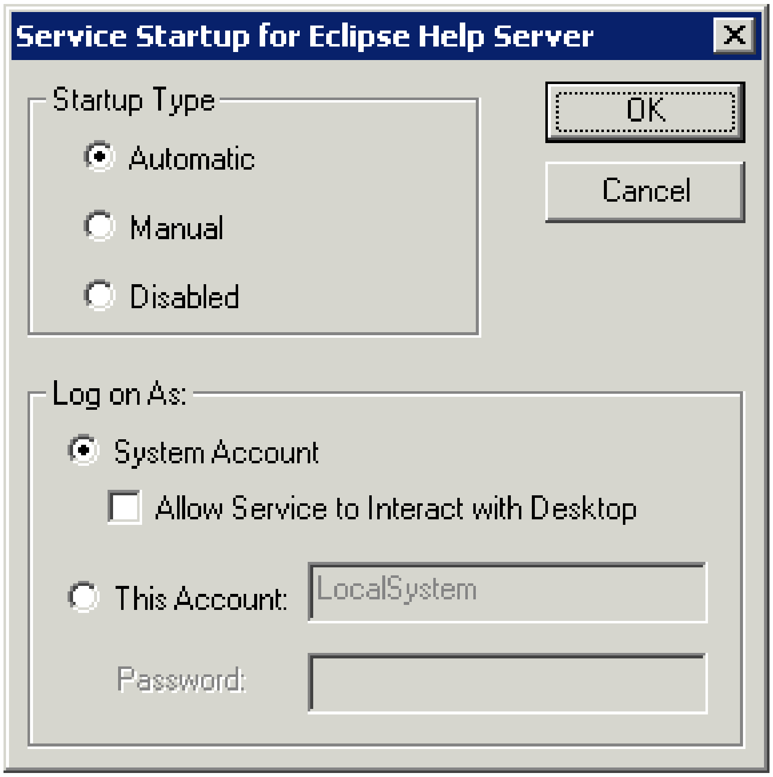
Specify port number for Eclipse Help

9999

Figure 64. Defining the port number for the Eclipse Help Server

Ensure that this value is set to the same port number that you specified when installing IBM Tivoli Monitoring, and click **OK**.

If you want the Eclipse help server to start automatically whenever this node is started, right-click the **Eclipse Help Server** entry, and select **Change Startup** from the pop-up menu. The Eclipse server's startup parameters are displayed:



Service Startup for Eclipse Help Server

Startup Type

● Automatic

○ Manual

○ Disabled

Log on As:

● System Account

□ Allow Service to Interact with Desktop

○ This Account: LocalSystem

Password:

Figure 65. Specifying Eclipse help server startup type

Select **Automatic** in the **startup type** field, and click **OK**.

Enabling history collection

If you require collection of history data, you need to enable it by using a script on the Tivoli Enterprise Portal Server.

The `kynHistoryConfigure.bat` script is installed with the Agent support files. It requires the IBM Tivoli Monitoring user interface component (`tacmd` command).

You need to run the script every time a node of one or more new affinity types is connected to the IBM Tivoli Monitoring infrastructure. A node represents an application server instance, and the following affinity types are available:

- WebSphere Application Server (AFF_CAM_WAS_SERVER)
- WebSphere Portal Server (AFF_CAM_WAS_PORTAL_SERVER)
- WebSphere ESB Server (AFF_CAM_WAS_ESB_SERVER)
- WebSphere Process Server (AFF_CAM_WAS_PROCESS_SERVER)
- WebSphere Workplace Server (AFF_CAM_WAS_WORKPLACE_SERVER)

At least one server instance of the new affinity type must be running and connected to the IBM Tivoli Monitoring infrastructure when the script is started.

It is best practice to run this script when the Agents on the monitored servers are already configured and connected to the Tivoli Enterprise Monitoring Server. In this way, history will be enabled for all the affinity types used in the environment. If a new affinity type is added to the environment, run the script again.

To run the script, you need to know the name of the Tivoli Enterprise Monitoring Server, as configured on the Tivoli Enterprise Portal Server. If there is more than one hub Tivoli Enterprise Monitoring Server, you need to run the script for each of the Tivoli Enterprise Monitoring Servers.

The script is located in the *ITM_HOME*\bin directory. Run it with the following command:

```
kynHistoryConfigure.bat username password TEMS_name
```

username is the name of a Tivoli Enterprise Portal user with administrative privileges (for example, SYSADMIN). *password* is the password for this user. *TEMS_name* is the name of the Tivoli Enterprise Monitoring Server, as configured on the Tivoli Enterprise Portal Server.

Silent installation and configuration on Windows

The installer and the configuration utility support a *silent* mode. In this mode, no user interaction is required for an installation or configuration. Instead, the parameters are taken from a *response file*. You may install and uninstall the Agent and support files; also, all the tasks that you can perform in the configuration utility are also available in silent mode.

Response files have a text format. You can create a response file based on one of the samples provided on the installation DVD.

You may also create a response file during configuration (see “Configuring ITCAM Agent for WebSphere Applications on Windows” on page 25), modify it if necessary, and then use it for a silent configuration. In this way, you can quickly reproduce similar configuration many times, for example, on different hosts.

Performing a silent installation or uninstallation on Windows

You can use the Installer to install or uninstall ITCAM Agent for WebSphere Applications in silent mode. You can also install or uninstall support files for the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal client on Windows in silent mode. To do this, modify the sample files provided on the installation DVD, and then run the installer from the command line.

To perform a silent installation or uninstallation, first you need to prepare the response file. Then, run the installer, supplying the name of the response file.

Attention: you must install ITCAM Agent for WebSphere Applications version 7.1 before installing version 7.1.0.1.

Preparing the response file for Agent installation

To prepare a response file for installing the Agent, perform the following procedure:

1. On the product installation DVD, in the `WINDOWS\Deploy` directory, locate the `YN_Silent_Install.txt` file.
2. Make a copy of this file, and open it in a text editor.

3. Modify any of the following properties, if necessary. Do not modify any other properties.

Table 8. Agent installation response file properties

Response file property	**Meaning**
Install Directory	The directory (*ITM_home*) where the Agent is to be installed. The destination directory can be shared with other IBM Tivoli Monitoring products. If you want to use a location other than the default (`C:\IBM\ITM`), click **Browse**, and select the folder that you want to use. **Note:** You can have multiple installations of the Agent on the same host. In this case, specify a different destination folder for each installation.
Install Folder	The Windows program folder (under the **Programs** menu) where IBM Tivoli Monitoring programs will be listed.
EncryptionKey	The 32-character encryption key used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment. See IBM Tivoli Monitoring: Installation and Setup Guide for details about the encryption key.

4. Save the edited copy in a work directory, for example, as `C:\TEMP\SILENT.TXT`.

Preparing the response file for Agent uninstallation

To prepare a response file for uninstalling the Agent, perform the following procedure:

1. On the product installation DVD, in the `WINDOWS` directory, locate the `silent.txt` file.
2. Copy the file to a work directory, for example, as `C:\TEMP\SILENT.TXT`. Do not modify the copy.

Preparing the response file for Support Files installation

To prepare a response file for installing the support files on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal client, perform the following procedure:

1. On the product installation DVD, in the `WINDOWS\Deploy` directory, locate the `YN_Support_Install.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Find the following lines, and comment out (by adding **;** as the first character) those that do not apply to the host you are installing on:

```
KYNWICMS=ITCAM Agent for WebSphere Applications Support ( TEMS )
KYNWIXEW=ITCAM Agent for WebSphere Applications Support ( TEP Workstation )
KYNWICNS=ITCAM Agent for WebSphere Applications Support ( TEP Server )
```

4. Save the edited copy in a work directory, for example, as `C:\TEMP\SILENT.TXT`.

Preparing the response file for Support Files uninstallation

To prepare a response file for uninstalling the support files on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal client, perform the following procedure:

1. On the product installation DVD, in the `WINDOWS\Deploy` directory, locate the `YN_Support_Unnstall.txt` file.

2. Make a copy of this file, and open it in a text editor.
3. Find the following lines, and comment out (by adding **;** as the first character) those that do not apply to the host you are installing on:

   ```
   KYNWICMS=ITCAM Agent for WebSphere Applications Support ( TEMS )
   KYNWIXEW=ITCAM Agent for WebSphere Applications Support ( TEP Workstation )
   KYNWICNS=ITCAM Agent for WebSphere Applications Support ( TEP Server )
   ```
4. Save the edited copy in a work directory, for example, as `C:\TEMP\SILENT.TXT`.

Attention: You do not need to install application support files if IBM Tivoli Monitoring is not used (in a deep dive diagnostics only installation).

Running the Installer in silent mode

After preparing the response file for your installation and uninstallation, run the installer, specifying the path and name for the response file. Perform the following procedure:

1. Open a Windows command prompt window, and change to the WINDOWS directory on the installation DVD.
2. Invoke setup as follows. Specify the parameters in the exact order shown:

   ```
   start /wait setup /z"/sfresponse_file_name" /s /f2"log_file_name"
   ```

   where *response_file_name* is the name of the response file you have prepared (with full path), and *log_file_name* is the name of the log file that the Installer will write (with full path). For example:

   ```
   start /wait setup /z"/sfC:\TEMP\SILENT.TXT" /s /f2"C:\TEMP\INSTALL.LOG"
   ```

Attention: if you are performing an upgrade or maintenance level update, and the Monitoring Agent is currently running, silent installation will be aborted.

You can find complete information about silent IBM Tivoli Monitoring installation in "Appendix B. Performing a silent installation of IBM Tivoli Monitoring" of the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Performing a silent configuration on Windows

You can use the Configuration utility in Silent mode to perform all configuration tasks for ITCAM Agent for WebSphere Applications. To do this, prepare the response file by modifying a sample provided with the Anent, or use a response file saved during interactive configuration.

All configuration tasks (see "Configuring ITCAM Agent for WebSphere Applications on Windows" on page 25) for the Agent can also be performed in Silent mode, without user interaction. This may be especially useful for large-scale deployments.

To perform a configuration task, you need to prepare a response file, and then start the configuration utility.

Preparing a response file

To perform a configuration task using silent mode, you can prepare a response file for configuration in any one of two ways:

- Create a copy of a sample response file for the task. Modify this copy, and save it in a work directory, for example, as `C:\TEMP\SILENT`Sample response files are located in the *`ITM_home`*`\TMAITM6` directory. For file names and instructions, see "Modifying sample response files for configuration tasks" on page 90.

- Perform the configuration procedure using the GUI (see “Configuring ITCAM Agent for WebSphere Applications on Windows” on page 25). In this procedure, check the **Save Configuration Setting in a Response File** box, and select the name for the response file. Modify the file if necessary, and use it for similar silent configuration on different instances and/or hosts. (Saving a response file is not available for configuring Monitoring Agent connection to the Monitoring Server).

  Attention: if you need to modify any paths in the response file, make sure to modify the `\` characters to `\\`, `:` characters to `\:`, and prefix spaces with `\` (for example, `C\:\\Program\ Files\\IBM\\WebSphere`). If you need to modify the profile home path for Data Collector Configuration, or the instance name in Data Collector unconfiguration or upgrade, make sure to replace all occurrences. For more detail on the information in the file, see “Modifying sample response files for configuration tasks” and the comments in the sample response files.

Running the Configuration utility in silent mode

After preparing the response file for a configuration task, run the configuration utility, specifying the path and name for the response file. Perform the following procedure:

1. Open a Windows command prompt window, and change to the *ITM_home*`\installITM` directory.
2. Invoke the configuration utility as follows. Specify the parameters in the exact order shown:

   ```
   kinconfg -nresponse_file_name -ckyn
   ```

   where *response_file_name* is the name of the response file you have prepared (with full path). For example:

   ```
   kinconfg -nC:\TEMP\SILENT.TXT -ckyn
   ```

Modifying sample response files for configuration tasks

For each of the configuration tasks for ITCAM Agent for WebSphere Applications, a sample response file is available in the *ITM_home*`\TMAITM6` directory. Make a copy of the file and edit it as required, using the information provided in the comments within the file. For more information on specific configuration options, see “Configuring ITCAM Agent for WebSphere Applications on Windows” on page 25.

- **Configuring Monitoring Agent connection to the Monitoring Server and Data Collector connection to the monitoring agent**, while two separate tasks in the GUI configuration (see “Configure the monitoring agent connection to the monitoring server” on page 26 and “Configure Monitoring Agent settings” on page 28), are performed with one response file. If the Agent is to communicate with the IBM Tivoli Monitoring infrastructure, you must perform this configuration task before configuring the Data Collector to monitor any application server instances. Do not perform this task if Tivoli Monitoring is not used (in a deep dive diagnostics only installation). The sample file name is `ynv_silent_config_agent.txt`.
- **Configuring the Data Collector to monitor an application server instance**: the sample file name is `ynv_silent_config_wasdc.txt`.
- **Unconfiguring the Data Collector from an application server instance**: the sample file name is `ynv_silent_unconfig_wasdc.txt`.
- **Configure the Data Collector communication with the Managing Server**: the sample file name is `ynv_silent_config_ms.txt`.

- **Upgrade an application server instance from an older version of the Data Collector**: the sample file name is `ynv_silent_upgrade_wasdc.txt`.
- **Change the Data Collector maintenance level for monitoring an application server instance**: the sample file name is `ynv_silent_reconfig_wasdc.txt`
- **Remove unused Data Collector maintenance levels**: the sample file name is `ynv_silent_remove_unused_wasdc.txt`

The response file is a text file, containing parameter names and values in the format *parameter*=*value*, for example:

```
KERNEL_HOST01=servername.domain.com
```

Comment lines begin with a number sign (#). Do not use blank lines.

Any \ character must be escaped as \\, : as \:, and spaces must be prefixed with \, for example:

```
MS_AM_HOME=C\:\\Program\ Files\\ITCAM\\MS
```

In the file sections marked as "repeatable", parameters are specific to a profile path or an application server instance name. For these parameters, use the path or name as a key, in the format *parameter*.*key*=*value*. For example:

```
KYN_WAS_HOME.C\:\\Program\ Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01=
   C\:\\Program Files\\IBM\\WebSphere\\AppServer
KYN_WAS_SERVERS.C\:\\Program\ Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01=
   cells/ITCAMCell/nodes/ITCAMNode/servers/server1,
   cells/ITCAMCell/nodes/ITCAMNode/servers/server2

KYN_WAS_HOME.C\:\\Program\ Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv02=
   C\:\\Program Files\\IBM\\WebSphere\\AppServer
KYN_WAS_SERVERS.C\:\\Program\ Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01=
   cells/ITCAMCell/nodes/ITCAMNode/servers/server3
```

Additional steps for configuring the Data Collector on Windows

For every application server instance where the Data Collector was configured, perform the following steps, as applicable.

Setting up a secure connection to the Managing Server

If the Data Collector will communicate with ITCAM for Application Diagnostics Managing Server, you may need to set up a secure connection.

See Appendix A, “Setting up security,” on page 251 for more information on setting up a secure (SSL) connection between the Data Collector and the Managing Server.

JDK 1.4.2 J9: enabling Java core dumps and heap dumps

If you have JDK 1.4.2 J9, you need to perform the procedure in this section to enable Java core dumps and heap dumps. On all other JDK versions, Java core dumps and heap dumps are enabled by default.

J9 is typically used on the following platforms:

- 1.4.2 JDK, 64-bit AMD64 on **Windows** and **Linux**
- 1.4.2 JDK, 32-bit i386. (J9 JVM is used only if the -Xj9 JVM option is specified.)

One way to check whether you have J9 is to check the system out log (typically SystemOut.log) for a line that contains `J2RE 1.4.2 IBM J9`.

If you have IBM JDK 1.4.2 J9, to enable Java core dumps and heap dumps perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server being monitored by the Data Collector.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
4. In the **Generic JVM arguments** field, add the following string of text:

   ```
   -Xtrace
   ```
5. Click **Apply**.
6. In the Messages dialog box, click **Save**.
7. In the Save to Master Configuration dialog box:
   - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.

Note: if you find the following message in the application server native_stderr.log file:

```
The JVM option is invalid: -Xtrace Could not create the Java virtual machine.
```

Or,

```
[ Unrecognized option: -Xtrace ] [ JVMCI123: Unable to parse 1.2 format supplied
options - rc=-6 ] Could not create JVM.
```

this means you do not have IBM JDK 1.4.2 J9. In this case, you need to remove the `-Xtrace` JVM argument.

IBM JDK 1.4.2: removing the -Xnoclassgc argument

If an older version of the Data Collector (prior to 6.1 fix pack 1 6.1.0-TIV-ITCAMfWAS_MP-FP0001) was earlier configured for this application server instance, the `-Xnoclassgc` JVM parameter may be present, as that version required it. Remove this argument, as its presence may lead to a slowdown in performance.

Perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server being monitored by the Data Collector.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
4. If `-Xnoclassgc` is still specified in the **Generic JVM arguments**, remove the setting.
5. Click **Apply**.
6. In the Messages dialog box, click **Save**.
7. In the Save to Master Configuration dialog box:
   - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.

Completing and verifying Data Collector configuration

To finish and verify configuration of the Data Collector for an application server instance, complete the following steps:

1. Restart the instance of the application server that will be monitored by the Data Collector. See "Restarting the application server" on page 263.
2. You know the Data Collector configuration has failed if any of the following problems occur:
   - After the configuration, the application server fails to restart.
   - During a GUI configuration, the summary panel for the Configuration Tool indicates the configuration has failed.
   - During a silent configuration, the command line indicates a message that the configuration has failed.
   - After the configuration, there are messages in the Tivoli common log file that indicates configuration has failed.

   If the Data Collector configuration has failed:
   - Restore the application server configuration that you had before attempting the failed configuration. See "Restoring the application server configuration after a failed Data Collector configuration" on page 271.
   - Run the GUI or silent configuration again.
   - If the configuration fails repeatedly, contact IBM Support. If directed by IBM Support, configure the application server instance manually; see "Manually configuring the Data Collector to monitor an application server instance" on page 272.
3. If Terminal Services are enabled on **Windows 2000** or **Windows 2003 Server**, run the following command:
   ```
   change user /execute
   ```
4. If you are using the IBM Tivoli Monitoring infrastructure, start a Tivoli Enterprise Portal client and verify that you can see monitored data for the application server instance.
5. If you are using the ITCAM for Application Diagnostics Managing Server infrastructure, access the Visualization Engine and verify that you can see monitored data for the application server instance.

Uninstalling ITCAM Agent for WebSphere Applications on Windows

To remove ITCAM Agent for WebSphere Applications on Windows, first unconfigure the Data Collector from all application server instances. See "Unconfigure the Data Collector for application server instances" on page 47.

After this, perform the following procedure:

1. From the desktop, click **Start** → **Settings** → **Control Panel** (for Windows 2000) or **Start** → **Control Panel** (for Windows 2003).
2. Click **Add or Remove Programs**.
3. Select **IBM Tivoli Monitoring**.
4. Click **Change**.
5. Perform one of the following procedures:
   - If you want to remove all IBM Tivoli Monitoring components, including the Agent, select **Remove** and click **Next**. Click **OK** to confirm the uninstallation.

- If you want to remove the Agent but not other IBM Tivoli Monitoring components, select **Modify** and click **Next**. Deselect the Agent and click**Next** several times to complete the uninstallation.

6. Click **Finish**.

Note: If you have uninstalled the Agent without unconfiguring the Data Collector for any application server instance, see “Manually removing Data Collector configuration from an application server instance” on page 275.

Installing and uninstalling a Language Pack on Windows

A Language Pack enables user interaction with the agent in a language other than English. For example, when a Spanish language pack is installed, the Tivoli Enterprise Portal workspaces and the internal messages of the Agent are displayed in Spanish.

To enable full support for a language, you must install the Language Pack on the agent host and all hosts where the Tivoli monitoring support files for the agent are installed (hub Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and all Tivoli Enterprise Portal desktop clients).

If you no longer want to use a language, uninstall the language pack for it.

Before installing or uninstalling a Language Pack, ensure that:

- The agent and the Tivoli Enterprise Portal Support Files are installed.
- The Java runtime environment (JRE) is available on every host where you are planning to install the Language Pack. (The JRE is required by IBM Tivoli Monitoring).

Installing a Language Pack on Windows

To install a Language Pack on Windows you need to use the installer on the Language Pack DVD. The procedure is the same on the Agent host, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client.

Perform the following procedure:

1. Start `lpinstaller.exe` from the Language Pack DVD.
2. Select the language of the installer and click OK.

   Note: In this step, you select the language for the installer user interface, not the language pack that will be installed.
3. Click **Next** on the Introduction window.
4. Select **Add/Update** and click **Next**.
5. Select the folder where the National Language Support package (NLSPackage) files are located. This is the `nlspackage` folder on the Language Pack DVD.
6. Select **ITCAM Agent for WebSphere Applications**.
7. Select the languages to install and click **Next**.

   Note: You can hold down the **Ctrl** key for multiple selections.
8. Examine the installation summary page and click **Next** to begin installation.
9. Click **Next**.
10. Click **Finish** to exit the installer.

11. If you are installing the Language Pack on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart the server or client. If the Eclipse Help Server is running, restart it as well.

Uninstalling a Language Pack on Windows

To uninstall a Language Pack on Windows you need to use the installer on the Language Pack DVD. The procedure is the same on the Agent host, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client.

Perform the following procedure:

1. Start `lpinstaller.exe` from the Language Pack DVD.
2. Select the language of the installer and click OK.

   Note: In this step, you select the language for the installer user interface, not the language pack that will be installed.
3. Click **Next** on the Introduction window.
4. Select **Remove** and click **Next**.
5. Select **ITCAM Agent for WebSphere Applications**.
6. Select the languages to uninstall and click **Next**.

   Note: You can hold down the **Ctrl** key for multiple selections.
7. Examine the installation summary page and click **Next** to begin installation.
8. Click **Next**.
9. Click **Finish** to exit the installer.
10. If you are installing the Language Pack on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart the server or client. If the Eclipse Help Server is running, restart it as well.

Part 3. Installing and Configuring ITCAM Agent for WebSphere Applications on UNIX and Linux

Chapter 4. Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Linux and UNIX systems

This chapter includes tasks that you need to perform before installing ITCAM Agent for WebSphere Applications on UNIX and Linux systems.

System and software prerequisites

The software and hardware requirements before installing ITCAM for Application Diagnostics are listed at the following Web site:

https://www.ibm.com/developerworks/wikis/display/tivolimonitoring/Prerequisites+for+ITCAM+for+Application+Diagnostics+7.1.0.1

What to do next

See "Required tasks before installation."

Required tasks before installation

Perform the tasks in each of the following sections before you attempt to install the Data Collector.

Permissions

If the IBM Tivoli Monitoring framework is being installed on the host for the first time, root privileges are required for installation. Otherwise, a non-root user account can be used, but it must meet certain requirements.

The Agent requires the IBM Tivoli Framework; the Agent installer will, by default, install this framework. The framework includes Global Security Kit (GSKit); installation of GSKit requires root permissions. Therefore, if the IBM Tivoli Monitoring framework was not installed on the host, you must use a root account to install the Agent.

However, if the IBM Tivoli Framework is already installed on the host, you may use a non-root account for installation. This must be the account that owns all the application server profiles that will be monitored by the Data Collector. The account must meet the following requirements for every application server profile to be monitored:

- The user must be able to start and stop WebSphere Application Server using the standard `startServer.sh` and `stopServer.sh` scripts.
- The user must have privileges (read, write and execute) for accessing the application server directory tree.
- The files in the *AppServer_home* directory must be owned by this user.
- The user must have read/write permission for the IBM Tivoli Monitoring home directory (by default, `/opt/IBM/ITM`) and the `logs` subdirectory in it.
- The user must have read and write privileges to the application server log directory: *`AppServer_home`*`/profiles/`*`profile_name`*`/logs`; if the files `wsadmin.traceout` and `wsadmin.valout` exist in this directory, the user must have read/write permission for these files.

- If you are performing an upgrade of the Agent, this installation user must have read/write permission for the home directory for the previous versions of the monitoring agent and Data Collector.
- The user must have read and write privileges to one of the following system temporary directories. These directories will be used by the InstallShield portion of the installation program:

Table 9. Default temporary directories for the InstallShield portion of the installation program

Operating system	Directory
Solaris or **HP-UX**	It is one of the following paths: • If it exists: `/var/tmp/ibm_am_installer_dc` • If the `/var/tmp/ibm_am_installer_dc` directory does not exist, `/var/tmp`
Linux and **all other UNIX platforms**	It is one of the following paths: • If it exists: `/tmp/ibm_am_installer_dc` • If the `/tmp/ibm_am_installer_dc` directory does not exist, `/tmp`

Important: If IBM WebSphere Application Server was installed by root, but all the instances to be monitored are owned by a non-root account, you need to perform the following procedure before using this non-root account to install the Agent:

1. As the root user, run the following commands:
   ```
   chown -R wasuser:wasgroup AppServer_home/properties/version/history
   chown wasuser:wasgroup AppServer_home/properties/version
   ```
   The *wasuser* and the *wasgroup* are the user and group of the application server instance.
2. As your non-root user, run the following command:
   ```
   ./versioninfo.sh
   ```

   If the application server version (not an error message) is displayed, you have performed the change successfully, and may use the non-root account to install the Agent.

Adjusting for ports being blocked by your firewall or being used by other applications

At various times during the installation you will need to specify or accept the defaults for port numbers used by ITCAM Agent for WebSphere Applications.

By default, ITCAM Agent for WebSphere Applications will communicate in the following ways:

- If the IBM Tivoli Monitoring infrastructure is used, the Agent will make outbound connections to the Tivoli Enterprise Monitoring Server host.
- If the ITCAM for Application Diagnostics Managing Server is used, and the Data Collector is configured for one or more application server instances, it will need to open ports in the 8200 to 8399 range for inbound communication.
- With WebSphere Network Deployment or Extended Deployment, the Agent will make outbound connections to the Deployment Manager host. The port number is available in the Deployment Manager administrative console.

You need to ensure that these connections are not blocked by a firewall. If they are blocked, you must either modify the communication settings during installation and configuration of the Agent, or change the settings of the firewall. To determine the connections that your firewall may block, see the documentation supplied with the firewall.

If you are using ITCAM for Application Diagnostics Managing Server, you also need to make sure that ports used for inbound communication are not used by other applications. If they are used by other applications, you will need to change the ports for Data Collector inbound communication when configuring the Data Collector (see Step 6 on page 36). To list the ports used by other applications, run the command `netstat -a`; in its output, look for lines that include `LISTENING`.

HP-UX: tuning HotSpot JVM garbage collection

For HotSpot JVM, the default NewSize and MaxNewSize might be too small for some applications if these applications allocate large numbers of short living objects. Some tuning is recommended for an application that allocates many short living objects:

```
-XX:+DisableExplicitGC -XX:NewSize=128m -XX:MaxNewSize=256m
```

Also, the default MaxPermSize might be small for some applications too. It is recommended to use `-XX:MaxPermSize=128m` or `-XX:MaxPermSize=256m`

Note: Change NewSize, MaxNewSize, and MaxPermSize based on the Maximum (-Xmx) and Minimum (-Xms) heap settings of the JVM. Before you modify these parameters, consult the HotSpot JVM documentation for details, at the following Web site:

http://www.hp.com/products1/unix/java/infolibrary/prog_guide/hotspot.html#tools

Making sure there are no invalid mounted file systems

There might be file systems that are specified as mounted in the `/etc/`*`file_systems`* FILEfile, which are not actually mounted or have lost connection with the computer on which the Agent is being installed. In this case, the installation may hang without producing any error messages.

To prevent this, complete the following steps:

1. Either mount all file systems listed in the `/etc/`*`file_systems`* file, or comment out all files systems listed in the `/etc/`*`file_systems`* file that are not mounted.

   `file_systems_file` is the file that lists the mounted file systems. For example, on **AIX**® it is called `filesystems`, and on **Linux** it is called `fstab`.
2. Verify that the following commands can be run successfully and without error messages:

   ```
   df -a
   df -k
   ```

WebSphere Global Security: setting the user name and password in client properties files

The Data Collector needs to communicate with WebSphere Administrative Services using the Remote Method Invocation (RMI) or SOAP protocol. If WebSphere Global Security is enabled, this communication requires a user name and password. You can set them when configuring the Data Collector to monitor an application server instance. For security reasons, you may also prefer to encrypt the username and password and store them in client properties files before Data Collector configuration.

Use the `sas.client.properties` file for an RMI connection, or the `soap.client.properties` file for a SOAP connection.

Note: if you choose to perform this operation, you will need to do it separately for each monitored application server profile.

Enabling user ID and password input from sas.client.props for RMI connector types

The Configuration Tool and the silent configuration provide means for you to retrieve the user ID and password (instead of entering them in the panel or silent configuration option) from the `sas.client.props` file when using a Remote Method Invocation (RMI) connection to WebSphere and WebSphere Global Security is enabled. In order for this function to work, you must set properties in the `sas.client.props` file. Perform the following procedure:

1. Set the following properties in *AppServer_home*/profiles/*profile_name*/properties/sas.client.props:

   ```
   com.ibm.CORBA.loginSource=properties
   com.ibm.CORBA.securityEnabled=true
   com.ibm.CORBA.loginUserid=user_ID
   com.ibm.CORBA.loginPassword=password
   ```

2. Run the following command to encrypt the password:

   ```
   ./PropFilePasswordEncoder.sh
     AppServer_home/profiles/profile_name/properties/sas.client.props
     com.ibm.CORBA.loginPassword
   ```

   Run it from the *AppServer_home*/profiles/*profile_name*/bin directory.

Enabling user ID and password input from soap.client.props for SOAP connector types

The Configuration Tool and the silent configuration provide means for you to retrieve the user ID and password (instead of entering them in the panel or silent configuration option) from the `soap.client.props` file when using a SOAP connection to WebSphere and WebSphere Global Security is enabled. In order for this function to work, you must set properties in the `soap.client.props` file. Perform the following procedure:

1. Set the following properties in *AppServer_home*/profiles/*profile_name*/properties/soap.client.props:

   ```
   com.ibm.SOAP.securityEnabled=true
   com.ibm.SOAP.loginUserid=user_ID
   com.ibm.SOAP.loginPassword=password
   ```

2. Run the following command to encrypt the password:

   ```
   ./PropFilePasswordEncoder.sh
     AppServer_home/profiles/profile_name/properties/soap.client.props
     com.ibm.SOAP.loginPassword
   ```

   Run it from the *AppServer_home*/profiles/*profile_name*/bin directory.

AIX 5.3: Prerequisite APAR

If your WebSphere environment is running with AIX Version 5.3, you must install APAR IY65196 before installing the monitoring agent; for more information, go to http://www.ibm.com/support/docview.wss?uid=isg1IY65196.

Linux: timezone setting for historical data collection

If your site uses Linux as its WebSphere Application Server operating environment, you need to synchronize historical data collection at the agent with the timezone of the Tivoli Enterprise Portal client. To do this, set a time zone variable in the Linux `/etc/profile` file. For example, to set the Linux time zone to the U.S. Pacific time zone, perform the following steps:

1. Perform one of the following actions:
   - For Red Hat Linux, set:
     ```
     ZONE="US/Pacific"
     export ZONE
     ```
   - For SuSE and Novell Linux, set:
     ```
     TIMEZONE="US/Pacific"
     export TIMEZONE
     ```
2. Reboot your Linux computer.

HP-UX: Mounting the Agent installation DVD

If you plan on using the DVD to install the Agent on HP-UX, run this command when mounting the DVD:

```
mount -F cdfs -o ro,cdcase,rr /dev/dsk/dvd_device /mnt/cdrom
```

Make sure the value for *dvd_device* corresponds to your particular DVD device.

What to do next

See Chapter 5, "Installing and configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems," on page 105

Chapter 5. Installing and configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems

This chapter provides instructions for installing and configuring ITCAM Agent for WebSphere Applications on any supported UNIX or Linux environment, including:

- Linux running on Intel®
- Linux running on pSeries®
- Linux running on zSeries®
- AIX
- HP-UX
- Solaris

The Agent supports a deep dive diagnostics only installation, where the IBM Tivoli Monitoring Infrastructure is not used; the Agent communicates with the Managing Server only. In this case, you need to configure the monitoring agent not to communicate to a Tivoli Enterprise Monitoring Server, and ensure that the monitoring agent is not started automatically.

If the IBM Tivoli Monitoring Infrastructure is used, you need to ensure that the monitoring agent is started automatically when the system boots up.

If you are upgrading from ITCAM for WebSphere 6.1, ITCAM for Web Resources 6.2, or ITCAM for WebSphere 7.0, you need to install the Agent on all hosts where the Data Collector or the Tivoli Enterprise Monitoring Agent was installed. If you use the same installation directory, The Tivoli Enterprise Monitoring Agent will be upgraded automatically. For the Data Collector, you will need to upgrade monitoring of application server instances to the new version using the configuration tool; see "Upgrading monitoring to Data Collector 7.1 using command line" on page 125 and "Upgrading monitoring to Data Collector 7.1 using GUI" on page 168.

Installing ITCAM Agent for WebSphere Applications on Linux and UNIX systems

Perform the following steps to install ITCAM Agent for WebSphere Applications on UNIX and Linux systems.

If the ITCAM for WebSphere Tivoli Enterprise Monitoring Agent or ITCAM for Web Resources WebSphere Tivoli Enterprise Monitoring Agent is installed on the host, use the same process to upgrade it.

Attention: you must install ITCAM Agent for WebSphere Applications version 7.1 before installing version 7.1.0.1.

Attention: if any Data Collector of a version lower than 6.1 Fix Pack 4 connects to this Tivoli Enterprise Monitoring Agent, monitoring for this Data Collector will cease after the upgrade. Once you upgrade the monitoring of the application server instances to the new version of the Data Collector (see "Upgrading monitoring to Data Collector 7.1 using command line” on page 125 and “Upgrading monitoring to Data Collector 7.1 using GUI” on page 168), monitoring will start again.

Before starting the process, make sure the Manage Tivoli Enterprise Monitoring Services (MTMS) utility is not running. If it is running, stop it.

Step 1: Invoke the installer

After loading the ITCAM Agent for WebSphere Applications for Linux and UNIX and changing to its root directory, locate the installation script, install.sh, and invoke it:

```
./install.sh
```

Step 2: Supply the name of the installation directory

The install script prompts you for the name of the installation directory where the ITCAM Agent for WebSphere Applications will be installed. The directory (*ITM_HOME*) can be shared with other IBM Tivoli Monitoring products. When installing ITCAM Agent for Application Diagnostics version 7.1, if the Tivoli Enterprise Monitoring Agent component of ITCAM for WebSphere 6.1 or of ITCAM for WebResources 6.2 was installed on this computer, use the same installation directory; when installing version 7.1.0.1, enter the installation directory of version 7.1. In both cases, the monitoring agent will be upgraded automatically.

```
Enter the name of the IBM Tivoli Monitoring directory
[ default = /opt/IBM/ITM ]:
```

Specify the absolute or relative directory name, or press **Enter** to accept the default. The installer looks for the directory name you specified and, if it does not exist, prompts you with the following message:

```
"/opt/IBM/ITM" does not exist
Try to create it [ y or n; "y" is default ]?
```

Press **Enter**.

If the Monitoring Agent is running, the installer warns that it will be restarted during the installation. Press **Enter** to continue.

Step 3: Select installation options

The installer displays background information about installation requirements, searches the DVD for the components available for installation, and prompts you about the available installation options:

```
Select one of the following:

1) Install products to the local host.
2) Install products to depot for remote deployment (requires TEMS).
3) Install TEMS support for remote seeding.
4) Exit install.

Please enter a valid number:  1
```

Important: Option 2 will only work if the version of Tivoli Enterprise Monitoring Server is 6.2.2.2 or higher.

Enter 1. The installer starts initializing.

Note:

- Option 2 applies to remote agent deployment. If you want to add installation files for this agent to your site deployment depot, run `install.sh` on the hub Tivoli Enterprise Monitoring Server (TEMS) host, and invoke this option.
- Option 3 applies to the installation of TEMS support files. See "Installing application support on Linux and UNIX systems" on page 190.

Step 4: Accept the product license agreement

After the initialization, the installer displays the product license agreement:

```
International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING
THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF
YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON
OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND
WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON,
COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT
AGREE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE
PROGRAM; AND

Press Enter to continue viewing the license agreement, or
enter "1" to accept the agreement, "2" to decline it, "3"
to print it, "4" to read non-IBM terms, or "99" to go back
to the previous screen.
```

If you accept the license agreement, enter 1.

Step 5: Enter the IBM Tivoli Monitoring encryption key

You might be prompted for the 32-character encryption key used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment:

```
Enter a 32-character encryption key, or just press Enter to use the default
        Default = IBMTivoliMonitoringEncryptionKey
....+....1....+....2....+....3..
```

See IBM Tivoli Monitoring: Installation and Setup Guide for details about the encryption key. This prompt is not displayed when the key is already set in this installation of Tivoli Monitoring, for example, during an upgrade installation.

Supply the 32-character key, or accept the default. The key information is displayed:

```
GSkit encryption key has been set.
Key File directory: /opt/IBM/ITM/keyfiles
```

Step 6: Install prerequisites and specify the component to install

The installer displays the installed components of IBM Tivoli Monitoring, and if any prerequisites for the Agent are not installed, prompts you to install them, for example:

```
The following products are currently installed in "/opt/IBM/TEMA:"

  IBM GSKit Security Interface V07.40.27.00 @ Linux Intel R2.4 (32 bit)/Intel
 R2.6 (32 bit)/x86_64 R2.6 (32 bit)
  IBM Tivoli Composite Application Manager Agent for WebSphere Applications
 V07.10.00.01 @ Linux Intel R2.6 (32 bit)/Intel R2.6 GCC 2.9.5 (64 bit)/Intel
 R2.6 (64 bit)
  Monitoring Agent for Linux OS V06.22.01.00 @ Linux Intel R2.6 (32 bit)/Intel
 R2.6 (64 bit)
  Tivoli Enterprise Services User Interface V06.10.07.04 @ Linux Intel R2.4
 (32 bit)
  Tivoli Enterprise Services User Interface V06.22.01.00 @ Linux Intel R2.6
 (32 bit)/Intel R2.6 GCC 2.9.5 (64 bit)/Intel R2.6 (64 bit)



The following prerequisites should be installed now:

  IBM Tivoli Monitoring Shared Libraries V622R100 @ Linux Intel R2.6 (32 bit)
  Tivoli Enterprise Services User Interface V622R100 @ Linux Intel R2.6 (32 bit)

Do you want to install these prerequisites [ 1=Yes, 2=No ; default is "1" ] ?
```

If you need to install any prerequisites, press **Enter** to install them. If you are prompted to install prerequisistes but choose not to install them, the installer will not continue.

Then, the installer displays the components available for the version of the operating system (Linux, AIX, HP-UX, or Solaris) you are installing on, for example:

```
Product packages are available for this operating system and component support
categories:

 1) IBM Tivoli Monitoring components for this operating system
 2) Tivoli Enterprise Portal Browser Client support
 3) Tivoli Enterprise Portal Desktop Client support
 4) Tivoli Enterprise Portal Server support
 5) Tivoli Enterprise Monitoring Server support
 6) Other operating systems

Type the number or type "q" to quit selection
[ number "1" or "IBM Tivoli Monitoring components for this operating system" is
default]:
```

Enter 1. The installer prompts you with the following message:

```
The following products are available for installation:

 1) IBM Tivoli Composite Application Manager Agent for WebSphere
 Applications  V07.10.00.01
 2) all of the above

Type the numbers for the products you want to install, type "b" to
 change operating system, or type "q" to quit selection.
If you enter more than one number, separate the numbers by a comma
 or a space.

Type your selections here:
```

Enter 1. The installer displays a confirmation prompt:

```
The following products will be installed:

  IBM Tivoli Composite Application Manager Agent for WebSphere Applications
  V07.10.01.00

Are your selections correct [ 1=Yes, 2=No ; default is "1" ] ?
```

Enter 1 (or press **Enter** to accept the default).

Step 7: Install the product software

The installer displays several status messages as the product files are installed. When that installation completes, you are prompted to specify whether you want to install additional packages:

```
Do you want to install additional products or product support packages [ 1=Yes,
2=No; default is "2" ]?
```

Enter 1 or 2, as appropriate. The installer completes the installation processing and displays the command for starting the configuration:

```
You may now congifure any locally installed IBM Tivoli Monitoring product
via the "/opt/IBM/ITM/bin/itmcmd config" command.
```

Deep dive diagnostics only installation: disabling Monitoring Agent autostart

If you are performing a deep dive diagnostics only installation, where IBM Tivoli Monitoring is not used, disable Monitoring Agent autostart. Do not disable it if Tivoli Monitoring is used.

To disable Monitoring Agent autostart, perform the following procedure:

1. Check the contents of the file *ITM_home*/registry/AutoStart, and get the number from that file. Use this number as *NUM* in the following step.
2. Edit the autostart file for the operating system:
   - On AIX: /etc/rc.itm*NUM*
   - On HP-UX: /sbin/init.d/ITMAgents*NUM*
   - On Linux: /etc/init.d/ITMAgents*NUM*
   - On Solaris: /etc/init.d/ITMAgents*NUM*

   In this file, find and comment out (using the # symbol) the lines with the `itmcmd agent start yn` and `itmcmd agent stop yn` commands.

   Example:

   ```
   start_all()
   {
   /bin/su - root -c " /opt/IBM/YN1024/bin/itmcmd agent start yn >/dev/null 2>&1"
   }

   stop_all()
   {
   /bin/su - root -c " /opt/IBM/YN1024/bin/itmcmd agent stop yn >/dev/null 2>&1"
   }
   ```

   In this example, you need to comment out both lines starting with `/bin/su`.

What to do next

On AIX, if the version of IBM Development Kit is lower than SR10, you need to issue a forced stop command for the Agent once after installing it:

```
ITM_home/bin/itmcmd agent -f stop yn
```

You must configure the components of the Agent. See “Configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems” on page 110

If you are using IBM Tivoli Monitoring infrastructure, you must install application support files on hub Tivoli Enterprise Monitoring Servers, and all Tivoli Enterprise

Portal Servers and Tivoli Enterprise Portal desktop clients. For a detailed procedure, see "Installing application support on Linux and UNIX systems" on page 190.

Configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems

This section instructs you how to configure ITCAM Agent for WebSphere Applications.

On UNIX and Linux platforms, the software provides two methods for configuring the Agent. You can use the command line or the GUI. The configuration results are equivalent.

Configuring the Agent using command line

To configure the Agent using the command line, use the **itmcmd** utility.

Change to the `*ITM_home*/bin` directory (by default, `/opt/IBM/ITM/bin`) and run the following command:

```
./itmcmd config -A yn
```

`yn` is the two-character IBM Tivoli Monitoring product code for ITCAM Agent for WebSphere Applications.

Important: after configuration of any type, **itmcmd** will prompt you to enter the settings for Agent communication with the Tivoli Enterprise Monitoring Server. If IBM Tivoli Monitoring infrastructure is used, you must configure these settings the first time the configuration is offered.

Configuring Monitoring Agent settings and communication with the Monitoring Server using command line

If the IBM Tivoli Monitoring infrastructure is used, you **must** configure Monitoring Agent settings before configuring the Data Collector to monitor any application server instances. You also need to configure Monitoring Agent communication to the Monitoring Server. Do not perform this configuration in a deep dive diagnostics only installation, where IBM Tivoli Monitoring is not used.

You can change the port that is used for communication between the Data Collector and the monitoring agent (this communication is on the local host, except if the monitoring agent is used for IBM i Data Collectors). The default port is 63335. You can also set an alternate node name that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree.

While you can change these values at a later time, it is normally most convenient to set them when initially configuring the communication. In this case no changes to configuration files is required to change the port number, and no customization of the Tivoli Enterprise Portal view could have been performed by any user. So, if you need to make such changes, make them at installation time if possible.

To configure Monitoring Agent settings and communication with the Monitoring Server on UNIX or Linux systems using command line, perform the following procedure:

1. Change to the `*ITM_home*/bin` directory (by default, `/opt/IBM/ITM/bin`) and run the following command:

```
./itmcmd config -A yn
```

The **itmcmd** utility prompts you whether you want to change Agent configuration:

```
Agent configuration started...
Edit "ITCAM Agent for WebSphere Applications" settings? [ 1=Yes, 2=No ]
 (default is: 1):
```

Enter 1, or press **Enter** to accept the default.

2. The utility prompts you to select the configuration type:

   ```
   Select Configuration Type :
   Choose the configuration type:

   Configuration type description:
       1.Use this option to configure the Tivoli Enterprise Monitoring Agent
   (TEMA) port number or Agent ID. If you modify the Tivoli Monitoring Agent
   port, all Application Servers with Data Collectors must be restarted to
   complete the reconfiguration.
       2.Use this option to configure the Data Collector to monitor
   application server instances. You can also use this option to configure the
   Data Collector to connect to the Managing Server. The option requires that
   either the Application Servers are running (WAS Base Edition) or the Node
   Agent and Deployment Manager are running (WAS ND or XD). The Servers must
   be restarted to complete the configuration.
       3.Use this option to unconfigure the Data Collector from Application
   Server instances. This option will remove all Data Collector configuration
   and runtime filesfor these instances. It requires that either the Application
   Servers are running (WAS Base Edition) or the Node Agent and Deployment
   Manager are running (WAS ND or XD). The Server instances must be restarted
   to complete the configuration. After the unconfiguration, your Application
   Server instances will no longer be monitored.
       4.Use this option to reconfigure your Data Collectors to use a different
   Managing Server, change Managing Server information, or disable Data Collector
   communication to the Managing Server. The Data Collector must be already
   configured to monitor at least one application server instance. You will
   need to restart the application servers monitored by the Data Collector.
       5.Use this option to upgrade ITCAM for WebSphere 6.1.x Data Collector
   to ITCAM 7.1; also to upgrade ITCAM for WAS 7.0.x Data Collector to
   ITCAM 7.1. It requires that either the Application Servers are running
   (WAS Base Edition) or the Node Agent and Deployment Manager are running
   (WAS ND or XD). The Servers must be restarted to complete the configuration.
       6.Use this option to update Data Collectors with the new maintenance or
   reverting the update.It requires that either the Application Servers are
   running (WAS Base Edition) or the Node Agent and Deployment Manager are
   running (WAS ND or XD). The Servers must be restarted to complete the
   configuration.
       7.Use this option to remove unused Data Collectors maintenance levels.
   Choose the configuration type: [ 1=Configure Tivoli Enterprise Monitoring
   Agent (TEMA), 2=Configure Data Collectors within Application Servers,
   3=Unconfigure Data Collectors from Application Servers, 4=Enable/disable
   communication to Managing Server for deep-dive diagnostics, 5=Upgrade
   ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector
   to ITCAM 7.1, 6=Change Data Collectors maintenance level, 7=Remove
   unused Data Collectors maintenance levels ] (default is: 1):
   ```

   Type **1** and press **Enter** to start configuring the Data Collector communication to the monitoring agent.

3. The configuration utility prompts you for an alternative Node ID for identifying the agent. This identifier that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is "Primary", used with the host name of the computer where the Agent is installed is used.

Attention: If you install more than one copy of the Monitoring Agent on a single host, you must set the Alternative Node ID parameter to different values for each of the copies. Otherwise, the multiple copies of the Monitoring Agent will not work correctly with Tivoli Monitoring.

```
Alternative Node ID for identifying the Agent.
This is a unique id that will determine how the agent will appear in
the Tivoli Enterprise Portal navigation tree. The max Node ID length
is 24 characters.
Node ID (default is: Primary):
```

If you want to use an alternative Node ID, enter it and press **Enter**. Otherwise, simply press **Enter**.

Attention: Valid characters for the node ID include A-z, a-z, 0-9, underbar (_), dash (-), and period (.); do not use other characters.

4. The configuration utility prompts you to specify a TCP socket port that the monitoring agent will use to listen for connection requests from the Data Collectors. Normally, accept the default. The port will only be used for local communication on the host (except if you use the monitoring agent to support Data Collectors on i5/OS® hosts, see *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Data Collector Installation and Configuration Guide for IBM i*).

   ```
   Monitoring Agent Listening Port.
    The Monitoring Agent will use this TCP socket port to listen for
   connection requests coming from the Data Collector(s).
   Port Number (default is: 63335):
   ```

   Unless you have a special requirement to change the port number, press **Enter** to accept the default value.
5. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.

   ```
   The wizard can save your settings to a response file. A response file
    can be used to perform a silent configuration.
   Save Configuration Setting in a Response File [ 1=true,
    2=false ] (default is: 2):
   ```

   If you want to create a response file, enter 1, then enter the name of the file. Otherwise, enter 2, or press Enter to accept the default.
6. The following message is displayed, confirming whether the Agent will communicate to a Tivoli Enterprise Monitoring Server (TEMS):

   ```
   Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 1):
   ```

   If the IBM Tivoli Monitoring Type is used, select **1**. If it is not used (in a deep dive diagnostics only install), select **2** (in this case the configuration process will end).
7. The configuration utility prompts you for the Tivoli Enterprise Monitoring Server host name:

   ```
   TEMS Host Name (Default is: LLVMRH5):
   ```

   Type the correct host name and press **Enter**.
8. The configuration utility prompts you to choose a network protocol that the monitoring agent will use to communicate with the hub monitoring server:

   ```
   Network Protocol [ip, sna, ip.pipe or ip.spipe] (Default is: ip.pipe):
   ```

Select the protocol that was selected when the Tivoli Enterprise Monitoring Server was installed, and press **Enter**.

9. The configuration utility prompts you to select a second (backup) protocol).

```
     Now choose the next protocol number from one of these:
     - ip
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 2 (Default is: 0):
```

   If a backup protocol was selected when the Tivoli Enterprise Monitoring Server was installed, enter that protocol and press **Enter**. Otherwise, simply press **Enter**.

10. The configuration utility prompts you for the settings for each protocol that you have selected. For example, if you have selected IP.PIPE, it prompts you for the port number:

```
IP.PIPE Port Number (Default is: 1918):
```

   Type the port number and press **Enter**, or simply press **Enter** to accept the default.

   Also, for some protocols including IP.PIPE, the configuration utility prompts you for the KDC_PARTITION name:

```
Enter name of KDC_PARTITION (Default is: null):
```

   You can specify the partition name if it is available, or press **Enter** without specifying it. You can configure the partition name at a later time.

11. The configuration utility prompts you whether you want to configure a connection for a secondary TEMS:

```
Configure connection for a secondary TEMS? [1=YES, 2=NO] (Default is:2):
```

   If your environment includes a Tivoli Enterprise Monitoring Server for a failover connection, select **1**. In this case, you will need to enter its host name and settings for communication with it (see Steps 7 on page 112 to 10). Otherwise, press **Enter**.

12. The configuration utility displays the following message:

```
Enter Optional Primary Network Name or 0 for "none" (Default is: 0):
```

   Press **Enter**.

13. The agent configuration is now complete. If the monitoring agent is already started, the following message is displayed:

```
Would you like to restart the component to allow new configuration to
take effect? [1=Yes, 2=No] (Default is: 1):
```

14. Press **Enter** to restart the component. The new configuration takes effect after the restart.

Configuring the Data Collector to monitor application server instances using command line

You must configure the Data Collector for each application server instance that you need to monitor.

Important: Do not configure the Data Collector to monitor an instance of WebSphere Application Server that hosts the Managing Server Visualization Engine. You can, however, use the Data Collector for monitoring any other WebSphere Application Server instances on the same node.

To configure the Data Collector to monitor a server instance, perform the following procedure:

1. Change to the *ITM_home*/bin directory (by default, /opt/IBM/ITM/bin) and run the following command:

   ```
   ./itmcmd config -A yn
   ```

   The **itmcmd** utility prompts you whether you want to change Agent configuration:

   ```
   Agent configuration started...
   Edit "ITCAM Agent for WebSphere Applications" settings? [ 1=Yes, 2=No ]
    (default is: 1):
   ```

   Enter 1, or press **Enter** to accept the default.
2. The utility prompts you to select the configuration type:

   ```
   Select Configuration Type :
   Choose the configuration type:

   Configuration type description:
       1.Use this option to configure the Tivoli Enterprise Monitoring Agent
   (TEMA) port number or Agent ID. If you modify the Tivoli Monitoring Agent
   port, all Application Servers with Data Collectors must be restarted to
   complete the reconfiguration.
       2.Use this option to configure the Data Collector to monitor
   application server instances. You can also use this option to configure the
   Data Collector to connect to the Managing Server. The option requires that
   either the Application Servers are running (WAS Base Edition) or the Node
   Agent and Deployment Manager are running (WAS ND or XD). The Servers must
   be restarted to complete the configuration.
       3.Use this option to unconfigure the Data Collector from Application
   Server instances. This option will remove all Data Collector configuration
   and runtime filesfor these instances. It requires that either the Application
   Servers are running (WAS Base Edition) or the Node Agent and Deployment
   Manager are running (WAS ND or XD). The Server instances must be restarted
   to complete the configuration. After the unconfiguration, your Application
   Server instances will no longer be monitored.
       4.Use this option to reconfigure your Data Collectors to use a different
   Managing Server, change Managing Server information, or disable Data Collector
   communication to the Managing Server. The Data Collector must be already
   configured to monitor at least one application server instance. You will
   need to restart the application servers monitored by the Data Collector.
       5.Use this option to upgrade ITCAM for WebSphere 6.1.x Data Collector
   to ITCAM 7.1; also to upgrade ITCAM for WAS 7.0.x Data Collector to
   ITCAM 7.1. It requires that either the Application Servers are running
   (WAS Base Edition) or the Node Agent and Deployment Manager are running
   (WAS ND or XD). The Servers must be restarted to complete the configuration.
       6.Use this option to update Data Collectors with the new maintenance or
   reverting the update.It requires that either the Application Servers are
   running (WAS Base Edition) or the Node Agent and Deployment Manager are
   running (WAS ND or XD). The Servers must be restarted to complete the
   configuration.
       7.Use this option to remove unused Data Collectors maintenance levels.
   Choose the configuration type: [ 1=Configure Tivoli Enterprise Monitoring
   Agent (TEMA), 2=Configure Data Collectors within Application Servers,
   3=Unconfigure Data Collectors from Application Servers, 4=Enable/disable
   communication to Managing Server for deep-dive diagnostics, 5=Upgrade
   ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector
   to ITCAM 7.1, 6=Change Data Collectors maintenance level, 7=Remove
   unused Data Collectors maintenance levels ] (default is: 1):
   ```

   Type **2** and press **Enter** to configure the Data Collector to monitor application server instances.
3. You can choose to configure the Data Collector to communicate with ITCAM for Application Diagnostics Managing Server. Otherwise, this application

server instance will not be monitored by the Managing Server infrastructure. (IBM Tivoli Monitoring is not affected by this setting).

```
Would you like to configure the Data Collector to communicate with
the Managing Server?
Note: If you deselect or change the Data Collector to communicate with
another Managing Server, the old Data Collector entry and reporting data
will be removed from Managing Server database.

Collect Managing Server related information to configure the Data Collector
to communicate with the Managing Server.
Enable/disable communication to Managing Server for deep-dive diagnostics
[ 1=true, 2=false ] (default is: 1): 1
```

If you want to configure the Data Collector to communicate with the Managing Server, enter **1**. Otherwise, enter **2** and go to Step 10 on page 116.

Note: If you choose not to configure communication with the Managing Server at this time, you can still configure the Data Collector to work with the Managing Server later. See “Configuring the Data Collector communication with the Managing Server using command line” on page 122.

4. The following message is displayed.

   ```
   Managing Server Connection Information :

   The Managing Server will use this Fully Qualified Host Name for
   Data Collector(s) connection requests.
   Examples: host1.usca.ibm.com, devapp.tivoli.austin.ibm.com
   Fully Qualified Host Name (default is: ):
   ```

   Enter the fully qualified host name of the Managing Server. If a split Managing Server installation is used, enter the name of the host where the Kernel is located.

5. The configuration utility prompts you for the port number on which the Managing Server Kernel is listening:

   ```
   The Managing Server will use this TCP socket port to listen
    for connection requests coming from the Data Collector(s).
   This port number is defined as the value of the key
    "PORT_KERNEL_CODEBASE01", in the .ITCAM61_MS_CONTEXT.properties
    file, located under the Managing Server Home directory.
   Input Codebase Port (default is: 9122):
   ```

   If the port number was changed when the Managing Server was installed, enter the port number. Otherwise, accept the default by pressing **Enter**.

6. The following message can be displayed:

   ```
   The Managing Server can be down or not yet installed at this time.
   Do you want to configure the Data Collector to communicate with
   the Managing Server?
   1.Yes: Configure the Data Collector without validating the Managing
   Server information. The Managing Server can be down or not yet
   installed at this time.
   2.No: Let the configuration tool validate Managing Server settings.

   Do you want to configure the Data Collector to communicate with this
   Managing Server without validating MS information? [ 1=Yes, 2=No ]
   (default is: 2):
   ```

   If the Managing Server might be offline, inaccessible on the network, or not yet installed, enter 1. Otherwise, enter 2.

7. The configuration utility prompts you for the Managing Server home directory, which is the destination directory chosen during the installation of the Managing Server.

   ```
   Managing Server Home :

   Enter the installation directory of the Managing Server.
   Examples:
   (Windows) C:\Program Files\IBM\itcam\WebSphere\MS
   (UNIX) /opt/IBM/itcam/WebSphere/MS
   Managing Server Home Directory (default is: ):
   ```

   Enter the full path to the directory.
8. If there are multiple IP address on this host, you need to select the address that the Data Collector will use for communication with the Managing Server.

   ```
   Data Collector IP Address :

   Select the IP Address for the Data Collector host if there are
   multiple IP addresses on this machine. Specify the RMI (and Controller RMI)
   Port Number if you need to control the ports used by the Data Collector.
   Make sure the ports are not blocked by a firewall or other applications.
   The default RMI Port Number range is 8200-8299, the Controller RMI Port
   Number range is 8300-8399.
   Select the IP Address for the Data Collector Host (default is: ):
   ```

   Enter the Data Collector host name or IP address (for example, `9.123.98.67`).
9. The configuration utility prompts you whether you want to change the RMI port numbers for the Data Collector.

   ```
   If the Data Collector is behind a firewall or you have special
   requirements to change the RMI port numbers for the Data Collector,
   select "Yes", otherwise select "No"
   Specify the RMI Port Numbers [ 1=Yes, 2=No ] (default is: 2):
   ```

   If you need to change the ports that the Data Collector uses to accept incoming connections from the Managing Server (in case of split Managing Server installation, the Publish Server), enter **1**; then, when prompted, enter the RMI and RMI Controller port ranges. Otherwise, press **Enter** to use the defaults. The default RMI port Number range is 8200-8299; the Controller RMI Port Number range is 8300-8399.

   Important: Make sure the RMI and RMI Controller ports are not being blocked by the firewall or other applications.
10. The configuration utility prompts you whether you want to enable the Transaction Tracking API function. Transaction Tracking Application Programming Interface (TTAPI) enables the integration of ITCAM Agent for WebSphere Applications and ITCAM for Transactions. With TTAPI, the Data Collector can send transaction information to ITCAM for Transactions; also, if ITCAM for Application Diagnostics Managing Server is used, transaction-specific information is available in the Visualization Engine. TTAPI also enables integration of the Data Collector with the Robotic Response Time component (or T6 agent).

    ```
    Enable TTAPI :
    Integration with ITCAM for Transactions.

    IBM Tivoli Composite Application Manager for Transactions (ITCAM
    for Transactions) is an IBM Tivoli Monitoring based product that
    provides a unified, end-to-end transaction tracking solution for
    the IT Operations segment. It tracks transactions within and among
    applications.
    ```

```
Through the Transaction Tracking Application Programming Interface,
ITCAM for WebSphere Application Server Data Collector (DC) can
provide request and transaction data to ITCAM for Transactions and
allow seamless integration between the ITCAM for WebSphere Application
Server and ITCAM for Transactions products.

Provide the host name and the port number of the ITCAM for Transaction
Collector.
Configure Transactions Integration [ 1=Yes, 2=No ]
(default is: 2): 1
```

To enable TTAPI, enter **1**; then, when prompted, enter the fully qualified host name or IP address for ITCAM for Transaction Tracking agent and the port number that the Data Collector uses to connect to it. If you do not need to enable the Transaction Tracking API function, enter **2**.

11. The configuration utility prompts you to select the default or advanced configuration mode:

    ```
    Choose Default or Custom configuration modes:
    Choose one of the configuration modes:  [ 1=Default, 2=Custom ]
    (default is: 1):
    ```

    If you need to modify Garbage Collection logging settings, increase the Maximum Heap size, or disable backing up the application server configuration, select 2. (In this case, the configuration utility will display additional prompts for these settings). Otherwise, Press **Enter** to use the default configuration mode.

12. Select the type of application server that you want to monitor.

    ```
    Select WebSphere Type :

    Choose the type of application server that you want to monitor:
    Choose the type of application server that you want to monitor:
     [ 1=WebSphere Application Server. 2=WebSphere Process Server.
       3=WebSphere ESB Server. 4=WebSphere Portal Server ]
       (default is: 1):
    ```

    Choose the application server type that you need to monitor; or press **Enter** to choose the default application server type, WebSphere Application Server.

13. The following message is displayed.

    ```
    WebSphere Profile Configuration :

    No 'WebSphere Profile Configuration' settings available.
    Edit 'WebSphere Profile Configuration' settings.
     [1=Add, 2=Edit, 3=Del, 4=Next,5=Exit] (default is: 5):
    ```

    Select **1** to add a WebSphere profile.

14. You are prompted for the home directory of the WebSphere profile:

    ```
    Input WebSphere Profile Home (default is: ):
    ```

    Enter the full WebSphere profile home path (for example, `/opt/IBM/itcam/WebSphere/WAS/base/profiles/test`).

15. The configuration utility prompts you for the profile name.

    ```
    Input the WebSphere profile name.
    Input WebSphere Profile Name (default is: AppSrv01):
    ```

    Enter the WebSphere profile name (for example, `test`).

16. The configuration utility prompts you for the WebSphere server home directory:

```
The full path of the WebSphere home, for example,
 on Windows, C:\Program Files\IBM\WebSphere\AppServer.
 on Linux/UNIX, /opt/IBM/WebSphere/AppServer.
Input WebSphere Server Home (default is: ):
```

Enter the full path of the WebSphere server home directory (for example, /opt/IBM/itcam/WebSphere/WAS/base).

17. The configuration utility prompts you for the full names of the WebSphere server instances that you want to configure:

    ```
    Input the full name(s) of WebSphere server instance(s) that you
    want to configure. Multiple server instances should be separated by a
    comma.
     For example: cells/ITCAMCell/nodes/ITCAMNode/servers/server1,
    cells/ITCAMCell/nodes/ITCAMNode/servers/server2
    Input Instance Name(s) (default is: ):
    ```

    Enter the full names of one or several WebSphere server instances. Separate multiple server instances with commas.

18. The configuration utility prompts you for the server instance alias. By default, the alias is the same as the server instance name.

    ```
    Aliases are used to identify server instances in the Tivoli Enterprise
    Portal. Aliases for multiple server instances should be separated by commas.
    This sequence should align with the sequence of WebSphere Server Instance
    Names.
    Input Server Instance Alias (default is: server1):
    ```

    This alias determines the name of the Tivoli Enterprise Portal node for this instance. Valid characters for the alias include A-z, a-z, 0-9, underbar (_), dash (-), and period (.); do not use other characters. Enter the alias, or press **Enter** to use the default.

19. The configuration utility prompts you for the host name or IP address of the WebSphere administrative server.

    ```
    The WebSphere administrative server fully qualified host name or IP address.
    Input Administrative Server Host name (default is: localhost):
    ```

    Enter the WebSphere administrative server fully qualified host name or IP address (for example, 9.123.98.67).

20. Select the WebSphere administrative server connection type.

    ```
    The WebSphere administrative server connection type.
    Select the Server Connection Type [ 1=SOAP, 2=RMI ] (default is: 1):
    ```

    Enter **1** for a SOAP connection, or **2** for an RMI connection.

21. The configuration utility prompts you for the server administrative port number.

    ```
    The WebSphere administrative server SOAP or RMI connect port number.
    Input Server Administrative Port (default is: 8880):
    ```

    Enter the port number, or press **Enter** to accept the default.

22. The configuration utility prompts you whether you want to use the user name and password stored in the client properties file, if WebSphere Global Security is enabled.

    ```
    Do you want to use the user name and password stored in soap.client.props
     or sas.client.props of WebSphere?
    Use the user name and password stored in client properties?
     [ 1=Yes, 2=No ] (default is: 2):
    ```

If you want to use the user name and password stored in the properties file, enter **1**. If you want to enter the user name and password, enter **2**; then, when prompted, enter the WebSphere administrative user name and password. If WebSphere Global Security is disabled, enter **2**, and press **Enter** when prompted for the user name and password.

23. The following message can be displayed.

```
If server instance is already configured, do you want to
allow the re-configuration of the same server instance?
Allow Re-configuration? [ 1=Yes, 2=No ] (default is: 2):
```

If you are re-configuring a server instance that was already configured, enter **1**. Otherwise, press **Enter**.

24. The following message is displayed.

```
'WebSphere Profile Configuration' settings: Input WebSphere Profile Home
=/opt/IBM/itcam/WebSphere/WAS/base/profiles/test
Edit 'WebSphere Profile Configuration' settings. [1=Add, 2=Edit, 3=Del, 4=Next,
5=Exit] (default is: 5):
```

If you want to configure another WebSphere profile, enter **1** and go to Step 14 on page 117. Otherwise, press **Enter**.

25. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.

```
The wizard can save your settings to a response file. A response file
 can be used to perform a silent configuration.
Save Configuration Setting in a Response File [ 1=true,
 2=false ] (default is: 2):
```

If you want to create a response file, enter 1, then enter the name of the file. Otherwise, enter 2, or press Enter to accept the default.

26. The configuration utility prompts you whether this Agent connects to a Tivoli Enterprise Monitoring Server.

```
Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 1):
```

If the IBM Tivoli Monitoring infrastructure is used, enter **1**. Otherwise (in a deep dive diagnostics only install), enter **2**; in this case the configuration process will be completed.

27. Press **Enter** repeatedly to accept the existing settings for the connection to Tivoli Enterprise Monitoring Server. Alternatively, you can change these settings; see Steps 7 on page 112 to 14 on page 113

Unconfiguring the Data Collector from application server instances using command line

If you no longer want the Data Collector to monitor an application server instance, you can unconfigure the Data Collector from it.

To unconfigure the Data Collector, perform the following steps:

1. Change to the *ITM_home*/bin directory (by default, /opt/IBM/ITM/bin) and run the following command:

```
./itmcmd config -A yn
```

The **itmcmd** utility prompts you whether you want to change Agent configuration:

```
Agent configuration started...
Edit "ITCAM Agent for WebSphere Applications" settings? [ 1=Yes, 2=No ]
 (default is: 1):
```

Enter 1, or press **Enter** to accept the default.

2. The utility prompts you to select the configuration type:

   ```
   Select Configuration Type :
   Choose the configuration type:

   Configuration type description:
       1.Use this option to configure the Tivoli Enterprise Monitoring Agent
   (TEMA) port number or Agent ID. If you modify the Tivoli Monitoring Agent
   port, all Application Servers with Data Collectors must be restarted to
   complete the reconfiguration.
       2.Use this option to configure the Data Collector to monitor
   application server instances. You can also use this option to configure the
   Data Collector to connect to the Managing Server. The option requires that
   either the Application Servers are running (WAS Base Edition) or the Node
   Agent and Deployment Manager are running (WAS ND or XD). The Servers must
   be restarted to complete the configuration.
       3.Use this option to unconfigure the Data Collector from Application
   Server instances. This option will remove all Data Collector configuration
   and runtime filesfor these instances. It requires that either the Application
   Servers are running (WAS Base Edition) or the Node Agent and Deployment
   Manager are running (WAS ND or XD). The Server instances must be restarted
   to complete the configuration. After the unconfiguration, your Application
   Server instances will no longer be monitored.
       4.Use this option to reconfigure your Data Collectors to use a different
   Managing Server, change Managing Server information, or disable Data Collector
   communication to the Managing Server. The Data Collector must be already
   configured to monitor at least one application server instance. You will
   need to restart the application servers monitored by the Data Collector.
       5.Use this option to upgrade ITCAM for WebSphere 6.1.x Data Collector
   to ITCAM 7.1; also to upgrade ITCAM for WAS 7.0.x Data Collector to
   ITCAM 7.1. It requires that either the Application Servers are running
   (WAS Base Edition) or the Node Agent and Deployment Manager are running
   (WAS ND or XD). The Servers must be restarted to complete the configuration.
       6.Use this option to update Data Collectors with the new maintenance or
   reverting the update.It requires that either the Application Servers are
   running (WAS Base Edition) or the Node Agent and Deployment Manager are
   running (WAS ND or XD). The Servers must be restarted to complete the
   configuration.
       7.Use this option to remove unused Data Collectors maintenance levels.
   Choose the configuration type: [ 1=Configure Tivoli Enterprise Monitoring
   Agent (TEMA), 2=Configure Data Collectors within Application Servers,
   3=Unconfigure Data Collectors from Application Servers, 4=Enable/disable
   communication to Managing Server for deep-dive diagnostics, 5=Upgrade
   ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector
   to ITCAM 7.1, 6=Change Data Collectors maintenance level, 7=Remove
   unused Data Collectors maintenance levels ] (default is: 1):
   ```

   Type **3** and press **Enter** to unconfigure the Data Collector from application server instances.

3. The following message is displayed.

   ```
   WebSphere Server Unconfiguration :

   No 'WebSphere Server Unconfiguration' settings available.
   Edit 'WebSphere Server Unconfiguration' settings.
    [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5):
   ```

   Enter **1**.

4. The configuration utility prompts you for the WebSphere server instance names.

   ```
   Input WebSphere Server Instance Name
   For example: cells/ITCAMCell/nodes/ITCAMNode/servers/server1
   (default is: ):
   ```

Enter the full names of one or several WebSphere server instances that you no longer want to monitor with the Data Collector. Separate multiple instances with commas (for example, `cells/tivpc045Node05Cell/nodes/tivpc045test/servers/server1, cells/tivpc045Node05Cell/nodes/tivpc045test/servers/server2`)

5. The configuration utility prompts you for the host name or IP address of the WebSphere administrative server.

   ```
   Input the WebSphere administrative server host name or IP address. (If it
   has not changed since the configuration was applied, then you can leave
   this value blank)
   Input Server Admin Host Name (default is: ):
   ```

   If the WebSphere administrative server has not changed since this instance was configured, press **Enter**. Otherwise, enter the WebSphere administrative server fully qualified host name or IP address (for example, `9.123.98.67`).

6. Select the WebSphere administrative server connection type.

   ```
   The WebSphere administrative server connection type.
   (If it has not changed since the configuration was applied,
    then you can leave this value blank)
   Select Server Connection Type [ 1=SOAP, 2=RMI ]
    (default is :1):
   ```

   If the WebSphere administrative server connection has not changed since this instance was configured, press **Enter**. Otherwise, enter **1** for a SOAP connection, or **2** for an RMI connection.

7. The configuration utility prompts you for the server administrative port number.

   ```
   The WebSphere administrative server SOAP or RMI connect port number.
   (If it has not changed since the configuration was applied,
    then you can leave this value blank)
   Input Server SOAP or RMI connect port (default is: ):
   ```

   If the WebSphere administrative server port has not changed since this instance was configured, press **Enter**. Otherwise, enter the port number.

8. The configuration utility prompts you whether you want to use the user name and password stored in the client properties file, if WebSphere Global Security is enabled.

   ```
   Do you want to use the user name and password stored in soap.client.props
    or sas.client.props of WebSphere?
   Use the user name and password stored in client properties?
    [ 1=Yes, 2=No ] (default is: 2):
   ```

   If you want to use the user name and password stored in the properties file, enter **1**. If you want to enter the user name and password, enter **2**; then, when prompted, enter the WebSphere administrative user name and password. If WebSphere Global Security is disabled, enter **2**, and press **Enter** when prompted for the user name and password.

9. The following message is displayed.

   ```
   'WebSphere Server Unconfiguration' settings:
   Please input WebSphere Server Instance
   Name= cells/tivpc045Node05Cell/nodes/tivpc045test/servers/server1
   Edit 'WebSphere Server Unconfiguration' settings.
    [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5):
   ```

   If you want to unconfigure the Data Collector for more WebSphere application server instances, enter **1** and go to Step 4 on page 120. Otherwise, press **Enter**.

10. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.

    ```
    The wizard can save your settings to a response file. A response file
     can be used to perform a silent configuration.
    Save Configuration Setting in a Response File [ 1=true,
     2=false ] (default is: 2):
    ```

    If you want to create a response file, enter 1, then enter the name of the file. Otherwise, enter 2, or press **Enter** to accept the default.
11. The configuration utility prompts you whether this Agent connects to a Tivoli Enterprise Monitoring Server.

    ```
    Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 1):
    ```

    If the IBM Tivoli Monitoring infrastructure is used, enter **1**. Otherwise (in a deep dive diagnostics only install), enter **2**; in this case the unconfiguration process will be completed
12. Press **Enter** repeatedly to accept the existing settings for the connection to Tivoli Enterprise Monitoring Server. Alternatively, you can change these settings; see Steps 7 on page 112 to 14 on page 113

Configuring the Data Collector communication with the Managing Server using command line

If you have configured the Data Collector to monitor an application server instance, you can later change its configuration for communication with the ITCAM for Application Diagnostics Managing Server for this instance.

In this way, you can:

- If you have previously not configured it to communicate to the Managing Server, enable such communication.
- If it was already configured to communicate to the Managing Server, change the address or port number for the Managing Server kernel, or disable such communication.

You can perform such configuration on many configured application server instances at the same time.

Note: If the Data Collector communicates to the Managing Server, you can also use the Visualization Engine to disable such communication (**Administration** > **Server Management** > **Data Collector Configuration**). See Table 10 for a comparison between these two ways of disabling Data Collector communication to the Managing Server:

Table 10. Comparison of ways to disable Data Collector communication to the Managing Server.

Disable Data Collector communication to the Managing Server using Data Collector configuration	Disable Data Collector communication to the Managing Server using the Visualization Engine
The application server instance is not listed in the Visualization Engine.	The application server instance remains listed in the Visualization Engine.
The Visualization Engine shows no information about the application server instance.	The Visualization Engine shows whether the application server instance is up or down; monitoring information is not available.

Table 10. Comparison of ways to disable Data Collector communication to the Managing Server. (continued)

Disable Data Collector communication to the Managing Server using Data Collector configuration	**Disable Data Collector communication to the Managing Server using the Visualization Engine**
No system or network resources are used for Managing Server communication.	Some system and network resources are used to maintain Managing Server communication.
You do not need to apply maintenance fixes for the Agent that only impact Managing Server communication.	You need to apply maintenance fixes for the Agent that only impact Managing Server communication.
In order to re-enable communication, you need to perform Data Collector configuration again, and restart the application server.	In order to re-enable communication using the Visualization Engine, you do not need to restart the application server.

Complete the following steps to enable, disable, or configure Data Collector communication with the Managing Server:

1. Change to the *ITM_home*/bin directory (by default, /opt/IBM/ITM/bin) and run the following command:

   ```
   ./itmcmd config -A yn
   ```

   The **itmcmd** utility prompts you whether you want to change Agent configuration:

   ```
   Agent configuration started...
   Edit "ITCAM Agent for WebSphere Applications" settings? [ 1=Yes, 2=No ]
    (default is: 1):
   ```

   Enter 1, or press **Enter** to accept the default.

2. The utility prompts you to select the configuration type:

   ```
   Select Configuration Type :
   Choose the configuration type:

   Configuration type description:
       1.Use this option to configure the Tivoli Enterprise Monitoring Agent
   (TEMA) port number or Agent ID. If you modify the Tivoli Monitoring Agent
   port, all Application Servers with Data Collectors must be restarted to
   complete the reconfiguration.
       2.Use this option to configure the Data Collector to monitor
   application server instances. You can also use this option to configure the
   Data Collector to connect to the Managing Server. The option requires that
   either the Application Servers are running (WAS Base Edition) or the Node
   Agent and Deployment Manager are running (WAS ND or XD). The Servers must
   be restarted to complete the configuration.
       3.Use this option to unconfigure the Data Collector from Application
   Server instances. This option will remove all Data Collector configuration
   and runtime filesfor these instances. It requires that either the Application
   Servers are running (WAS Base Edition) or the Node Agent and Deployment
   Manager are running (WAS ND or XD). The Server instances must be restarted
   to complete the configuration. After the unconfiguration, your Application
   Server instances will no longer be monitored.
       4.Use this option to reconfigure your Data Collectors to use a different
   Managing Server, change Managing Server information, or disable Data Collector
   communication to the Managing Server. The Data Collector must be already
   configured to monitor at least one application server instance. You will
   need to restart the application servers monitored by the Data Collector.
       5.Use this option to upgrade ITCAM for WebSphere 6.1.x Data Collector
   to ITCAM 7.1; also to upgrade ITCAM for WAS 7.0.x Data Collector to
   ITCAM 7.1. It requires that either the Application Servers are running
   ```

```
(WAS Base Edition) or the Node Agent and Deployment Manager are running
(WAS ND or XD). The Servers must be restarted to complete the configuration.
    6.Use this option to update Data Collectors with the new maintenance or
reverting the update.It requires that either the Application Servers are
running (WAS Base Edition) or the Node Agent and Deployment Manager are
running (WAS ND or XD). The Servers must be restarted to complete the
configuration.
    7.Use this option to remove unused Data Collectors maintenance levels.
Choose the configuration type: [ 1=Configure Tivoli Enterprise Monitoring
Agent (TEMA), 2=Configure Data Collectors within Application Servers,
3=Unconfigure Data Collectors from Application Servers, 4=Enable/disable
communication to Managing Server for deep-dive diagnostics, 5=Upgrade
ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector
to ITCAM 7.1, 6=Change Data Collectors maintenance level, 7=Remove
unused Data Collectors maintenance levels ] (default is: 1):
```

Type **4** and press **Enter** to configure the Data Collector communication with the Managing Server.

3. The following message is displayed.

```
Enable/disable communication to Managing Server for deep-dive diagnostics:


Description:
    1. Configure or Reconfigure Communication to Managing Server is used
to configure Data Collectors to communicate with Managing Server (requires
server restart)
    2. Disable Data Collectors communication to Managing Server is used to
temporary disable communication between the DC and the MS. Disable does not
unconfigure the MS connection settings from Data Collector properties files.
It only modifies the property dc.operation.mode (and omit "ms") in
dc.java.properties file. (requires server restart).
Select the option:      [ 1=Configure or Reconfigure Communication to the
Managing Server, 2=Disable Communication to the Managing Server ]
(default is: 1): 2
```

If you want to enable Managing Server communication that was previously not configured, or to change the address or port of the Managing Server, enter **1**. Then, follow Steps 4 on page 115 to 10 on page 116. Then go to Step 5.

If you want to disable communication with the Managing Server, enter **2** and go to the next step.

4. The configuration utility prompts you for the WebSphere server instance names.

```
Input the full name(s) of the WebSphere server instance(s) that you want
to configure. Multiple server instances should be separated by a comma.
 For example: cells/ITCAMCell/nodes/ITCAMNode/servers/server1,
cells/ITCAMCell/nodes/ITCAMNode/servers/server2
Input the full WebSphere Server Instance Name(s) (default is: ):
```

Enter the full names of one or several WebSphere server instances for which you want to disable Managing Server communication, separate multiple instance names with commas.

5. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.

```
The wizard can save your settings to a response file. A response file
 can be used to perform a silent configuration.
Save Configuration Setting in a Response File [ 1=true,
 2=false ] (default is: 2):
```

If you want to create a response file, enter 1, then enter the name of the file. Otherwise, enter 2, or press **Enter** to accept the default.

6. The configuration utility prompts you whether this Agent connects to a Tivoli Enterprise Monitoring Server.

   ```
   Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 1):
   ```

   If the IBM Tivoli Monitoring infrastructure is used, enter **1**. Otherwise (in a deep dive diagnostics only install), enter **2**; in this case the unconfiguration process will be completed
7. Press **Enter** repeatedly to accept the existing settings for the connection to Tivoli Enterprise Monitoring Server. Alternatively, you can change these settings; see Steps 7 on page 112 to 14 on page 113

Upgrading monitoring to Data Collector 7.1 using command line

If an application server instance is monitored by a previous version of the Data Collector (from ITCAM for WebSphere 6.1, ITCAM for Web Resources 6.2, or ITCAM for WebSphere 7.0), you can upgrade monitoring to version 7.1.

To upgrade monitoring of server instances to Data Collector version 7.1, perform the following procedure:

1. Change to the *ITM_home*/bin directory (by default, /opt/IBM/ITM/bin) and run the following command:

   ```
   ./itmcmd config -A yn
   ```

   The **itmcmd** utility prompts you whether you want to change Agent configuration:

   ```
   Agent configuration started...
   Edit "ITCAM Agent for WebSphere Applications" settings? [ 1=Yes, 2=No ]
    (default is: 1):
   ```

   Enter 1, or press **Enter** to accept the default.
2. The utility prompts you to select the configuration type:

   ```
   Select Configuration Type :
   Choose the configuration type:

   Configuration type description:
       1.Use this option to configure the Tivoli Enterprise Monitoring Agent
   (TEMA) port number or Agent ID. If you modify the Tivoli Monitoring Agent
   port, all Application Servers with Data Collectors must be restarted to
   complete the reconfiguration.
       2.Use this option to configure the Data Collector to monitor
   application server instances. You can also use this option to configure the
   Data Collector to connect to the Managing Server. The option requires that
   either the Application Servers are running (WAS Base Edition) or the Node
   Agent and Deployment Manager are running (WAS ND or XD). The Servers must
   be restarted to complete the configuration.
       3.Use this option to unconfigure the Data Collector from Application
   Server instances. This option will remove all Data Collector configuration
   and runtime filesfor these instances. It requires that either the Application
   Servers are running (WAS Base Edition) or the Node Agent and Deployment
   Manager are running (WAS ND or XD). The Server instances must be restarted
   to complete the configuration. After the unconfiguration, your Application
   Server instances will no longer be monitored.
       4.Use this option to reconfigure your Data Collectors to use a different
   Managing Server, change Managing Server information, or disable Data Collector
   communication to the Managing Server. The Data Collector must be already
   configured to monitor at least one application server instance. You will
   need to restart the application servers monitored by the Data Collector.
       5.Use this option to upgrade ITCAM for WebSphere 6.1.x Data Collector
   to ITCAM 7.1; also to upgrade ITCAM for WAS 7.0.x Data Collector to
   ```

```
ITCAM 7.1. It requires that either the Application Servers are running
(WAS Base Edition) or the Node Agent and Deployment Manager are running
(WAS ND or XD). The Servers must be restarted to complete the configuration.
    6.Use this option to update Data Collectors with the new maintenance or
reverting the update.It requires that either the Application Servers are
running (WAS Base Edition) or the Node Agent and Deployment Manager are
running (WAS ND or XD). The Servers must be restarted to complete the
configuration.
    7.Use this option to remove unused Data Collectors maintenance levels.
Choose the configuration type: [ 1=Configure Tivoli Enterprise Monitoring
Agent (TEMA), 2=Configure Data Collectors within Application Servers,
3=Unconfigure Data Collectors from Application Servers, 4=Enable/disable
communication to Managing Server for deep-dive diagnostics, 5=Upgrade
ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector
to ITCAM 7.1, 6=Change Data Collectors maintenance level, 7=Remove
unused Data Collectors maintenance levels ] (default is: 1):
```

Type **5** and press **Enter** to upgrade monitoring of server instances to Data Collector version 7.1.

3. The configuration utility prompts you for the home directory of the previous version of the Data Collector.

   ```
   Data Collector Home :

   Provide the ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.x Data Collector
   installation directory (e.g. on Windows, C:\IBM\itcam\WebSphere\DC, on
   Linux/UNIX, /opt/IBM/itcam/WebSphere/DC).
   Data Collector Home (default is: ):
   ```

   Enter the full path to the directory in which the older version of the Data Collector as installed. If it was configured with the default options, the path is `/opt/IBM/itcam/WebSphere/DC`.

4. The following message is displayed.

   ```
   No 'Select Data Collector Configuration' settings available.
   Edit 'Select Data Collector Configuration' settings,
   [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5):
   ```

   Enter **1**.

5. The configuration utility prompts you for the WebSphere server instance names.

   ```
   Input WebSphere Server Instance Name
   For example: cells/ITCAMCell/nodes/ITCAMNode/servers/server1
   (default is: ):
   ```

   Enter the full names of one or several WebSphere server instances, currently monitored by the older Data Collector, that you want to upgrade. Separate multiple instances with commas (for example, `cells/tivpc045Node05Cell/nodes/tivpc045test/servers/server1, cells/tivpc045Node05Cell/nodes/tivpc045test/servers/server2`)

6. The configuration utility prompts you for the host name or IP address of the WebSphere administrative server.

   ```
   Input the WebSphere administrative server host name or IP address. (If it
   has not changed since the configuration was applied, then you can leave
   this value blank)
   Input Server Admin Host Name (default is: ):
   ```

   If the WebSphere administrative server has not changed since this instance was configured, press **Enter**. Otherwise, enter the WebSphere administrative server fully qualified host name or IP address (for example, `9.123.98.67`).

7. Select the WebSphere administrative server connection type.

```
The WebSphere administrative server connection type.
(If it has not changed since the configuration was applied,
 then you can leave this value blank)
Select Server Connection Type [ 1=SOAP, 2=RMI ]
 (default is :1):
```

If the WebSphere administrative server connection has not changed since this instance was configured, press **Enter**. Otherwise, enter **1** for a SOAP connection, or **2** for an RMI connection.

8. The configuration utility prompts you for the server administrative port number.

   ```
   The WebSphere administrative server SOAP or RMI connect port number.
   (If it has not changed since the configuration was applied,
    then you can leave this value blank)
   Input Server SOAP or RMI connect port (default is: ):
   ```

   If the WebSphere administrative server port has not changed since this instance was configured, press **Enter**. Otherwise, enter the port number.

9. The configuration utility prompts you whether you want to use the user name and password stored in the client properties file, if WebSphere Global Security is enabled.

   ```
   Do you want to use the user name and password stored in soap.client.props
    or sas.client.props of WebSphere?
   Use the user name and password stored in client properties?
    [ 1=Yes, 2=No ] (default is: 2):
   ```

   If you want to use the user name and password stored in the properties file, enter **1**. If you want to enter the user name and password, enter **2**; then, when prompted, enter the WebSphere administrative user name and password. If WebSphere Global Security is disabled, enter **2**, and press **Enter** when prompted for the user name and password.

10. The following message is displayed.

    ```
    'Select Data Collector Configuration' settings:
    Name=cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02/servers/server1
    Edit 'Select Data Collector Configuration' settings,
    [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5):
    ```

    If you want to upgrade Data Collector monitoring for more WebSphere application server instances, enter **1** and go to Step 5 on page 126. Otherwise, press **Enter**.

11. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.

    ```
    The wizard can save your settings to a response file. A response file
     can be used to perform a silent configuration.
    Save Configuration Setting in a Response File [ 1=true,
     2=false ] (default is: 2):
    ```

    If you want to create a response file, enter 1, then enter the name of the file. Otherwise, enter 2, or press **Enter** to accept the default.

12. The configuration utility prompts you whether this Agent connects to a Tivoli Enterprise Monitoring Server.

    ```
    Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 1):
    ```

    If the IBM Tivoli Monitoring infrastructure is used, enter **1**. Otherwise (in a deep dive diagnostics only install), enter **2**; in this case the unconfiguration process will be completed

13. If you have not yet configured the connection to a Monitoring Server, configure it; see “Configuring Monitoring Agent settings and communication with the Monitoring Server using command line” on page 110, starting with Step 7 on page 112. Otherwise, press **Enter** repeatedly to accept the existing settings for the connection to Tivoli Enterprise Monitoring Server. Alternatively, you can change these settings; see Steps 7 on page 112 to 14 on page 113

Changing Data Collector maintenance level using command line

If an application server instance is monitored by the Data Collector version 7.1, and more than one maintenance level for this version is installed on the host (for example, 7.1.0 and 7.1.0.1), you can change the maintenance level. You must perform this change to update the monitoring to a new maintenance level; you can not remove an old maintenance level until all monitored server instances are moved to another level.

To change the Data Collector maintenance level for server instances, perform the following procedure:

1. Change to the `ITM_home/bin` directory (by default, `/opt/IBM/ITM/bin`) and run the following command:

   ```
   ./itmcmd config -A yn
   ```

   The **itmcmd** utility prompts you whether you want to change Agent configuration:

   ```
   Agent configuration started...
   Edit "ITCAM Agent for WebSphere Applications" settings? [ 1=Yes, 2=No ]
    (default is: 1):
   ```

   Enter 1, or press **Enter** to accept the default.

2. The utility prompts you to select the configuration type:

   ```
   Select Configuration Type :
   Choose the configuration type:

   Configuration type description:
       1.Use this option to configure the Tivoli Enterprise Monitoring Agent
   (TEMA) port number or Agent ID. If you modify the Tivoli Monitoring Agent
   port, all Application Servers with Data Collectors must be restarted to
   complete the reconfiguration.
       2.Use this option to configure the Data Collector to monitor
   application server instances. You can also use this option to configure the
   Data Collector to connect to the Managing Server. The option requires that
   either the Application Servers are running (WAS Base Edition) or the Node
   Agent and Deployment Manager are running (WAS ND or XD). The Servers must
   be restarted to complete the configuration.
       3.Use this option to unconfigure the Data Collector from Application
   Server instances. This option will remove all Data Collector configuration
   and runtime filesfor these instances. It requires that either the Application
   Servers are running (WAS Base Edition) or the Node Agent and Deployment
   Manager are running (WAS ND or XD). The Server instances must be restarted
   to complete the configuration. After the unconfiguration, your Application
   Server instances will no longer be monitored.
       4.Use this option to reconfigure your Data Collectors to use a different
   Managing Server, change Managing Server information, or disable Data Collector
   communication to the Managing Server. The Data Collector must be already
   configured to monitor at least one application server instance. You will
   need to restart the application servers monitored by the Data Collector.
       5.Use this option to upgrade ITCAM for WebSphere 6.1.x Data Collector
   to ITCAM 7.1; also to upgrade ITCAM for WAS 7.0.x Data Collector to
   ITCAM 7.1. It requires that either the Application Servers are running
   (WAS Base Edition) or the Node Agent and Deployment Manager are running
   (WAS ND or XD). The Servers must be restarted to complete the configuration.
   ```

```
    6.Use this option to update Data Collectors with the new maintenance or
reverting the update.It requires that either the Application Servers are
running (WAS Base Edition) or the Node Agent and Deployment Manager are
running (WAS ND or XD). The Servers must be restarted to complete the
configuration.
    7.Use this option to remove unused Data Collectors maintenance levels.
Choose the configuration type: [ 1=Configure Tivoli Enterprise Monitoring
Agent (TEMA), 2=Configure Data Collectors within Application Servers,
3=Unconfigure Data Collectors from Application Servers, 4=Enable/disable
communication to Managing Server for deep-dive diagnostics, 5=Upgrade
ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector
to ITCAM 7.1, 6=Change Data Collectors maintenance level, 7=Remove
unused Data Collectors maintenance levels ] (default is: 1):
```

Type **6** and press **Enter** to change Data Collector maintenance level for monitoring of server instances.

3. The configuration utility prompts you for the new Data Collector maintenance level. The default is the newest maintenance level installed on the host.

   ```
   Data Collector maintenance level :

   Select Data Collector maintenance level.
   Data Collector maintenance level (default is: 7.1.0.1):
   ```

   Enter the maintenance level.

4. The following message is displayed.

   ```
   No 'Select Data Collector Configuration' settings available.
   Edit 'Select Data Collector Configuration' settings,
   [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5):
   ```

   Enter **1**.

5. The configuration utility prompts you for the WebSphere server instance names.

   ```
   Input WebSphere Server Instance Name
   For example: cells/ITCAMCell/nodes/ITCAMNode/servers/server1
   (default is: ):
   ```

   Enter the full names of one or several WebSphere server instances for which you need to change the maintenance level. Separate multiple instances with commas (for example, `cells/tivpc045Node05Cell/nodes/tivpc045test/servers/server1, cells/tivpc045Node05Cell/nodes/tivpc045test/servers/server2`)

   Important: You can enter several instance names in this step if the instances are federated to the same Deployment manager in Network Deployment. Do not enter several instances with different administrative server names.

6. The configuration utility prompts you for the host name or IP address of the WebSphere administrative server.

   ```
   The WebSphere administrative server host name or IP address.
   Please input Server Admin Host (default is: localhost):
   ```

   Enter the WebSphere administrative server fully qualified host name or IP address (for example, `9.123.98.67`).

7. Select the WebSphere administrative server connection type.

   ```
   The WebSphere administrative server connection type.
   Please select Server Connection Type [ 1=SOAP, 2=RMI ] (default is: 1):
   ```

   Enter **1** for a SOAP connection, or **2** for an RMI connection.

8. The configuration utility prompts you for the server administrative port number.

   ```
   The WebSphere administrative server port number.
   Please input Server Admin Port (default is: 8880):
   ```

   Enter the port number.
9. The configuration utility prompts you whether you want to use the user name and password stored in the client properties file, if WebSphere Global Security is enabled.

   ```
   Do you want to use the user name and password stored in soap.client.props
    or sas.client.props of WebSphere?
   Use the user name and password stored in client properties?
    [ 1=Yes, 2=No ] (default is: 2):
   ```

   If you want to use the user name and password stored in the properties file, enter **1**. If you want to enter the user name and password, enter **2**; then, when prompted, enter the WebSphere administrative user name and password. If WebSphere Global Security is disabled, enter **2**, and press **Enter** when prompted for the user name and password.
10. The following message is displayed.

    ```
    'Select Data Collector Configuration' settings:
    Name=cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02/servers/server1
    Edit 'Select Data Collector Configuration' settings,
    [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5):
    ```

    If you want to change the Data Collector maintenance level for more WebSphere application server instances, enter **1** and go to Step 5 on page 129. Otherwise, press **Enter**.
11. If this is the first time server instances are updated to this maintenance level on this host, the configuration utility prompts you whether to preserve customizations in common configuration files.

    ```
    Would you like to preserve customizations :

    If true then customizations of common configuration files
    will be preserved. Otherwise they will be overwritten with
    files from the selected maintenance.
    Preserve customizations to common configuration files
    [ 1=true, 2=false ] (default is: 1):
    ```

    Unless you have special requirements, preserve the customizations; enter **1**.
12. The configuration utility prompts you whether to preserve customizations in server instance configuration files.

    ```
    If true then customizations of per-server configuration files
    will be preserved. Otherwise they will be overwritten with
    files from the selected maintenance.
    Preserve customizations to per-server configuration files
    [ 1=true, 2=false ] (default is: 1):
    ```

    Unless you have special requirements, preserve the customizations; enter **1**.
13. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.

    ```
    The wizard can save your settings to a response file. A response file
     can be used to perform a silent configuration.
    Save Configuration Setting in a Response File [ 1=true,
     2=false ] (default is: 2):
    ```

If you want to create a response file, enter 1, then enter the name of the file. Otherwise, enter 2, or press **Enter** to accept the default.

14. The configuration utility prompts you whether this Agent connects to a Tivoli Enterprise Monitoring Server.

    ```
    Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 1):
    ```

    If the IBM Tivoli Monitoring infrastructure is used, enter **1**. Otherwise (in a deep dive diagnostics only install), enter **2**; in this case the configuration process will be completed

15. If you have not yet configured the connection to a Monitoring Server, configure it; see "Configuring Monitoring Agent settings and communication with the Monitoring Server using command line" on page 110, starting with Step 7 on page 112. Otherwise, press **Enter** repeatedly to accept the existing settings for the connection to Tivoli Enterprise Monitoring Server. Alternatively, you can change these settings; see Steps 7 on page 112 to 14 on page 113

Important: You must restart the application server instances for the new maintenance level to take effect.

Removing a Data Collector maintenance level using command line

If an older maintenance level of the Data Collector version 7.1 is installed, and all the monitored applications server instances were updated to the new maintenance level, you can remove the older maintenance level.

To remove an unused maintenance level Data Collector version 7.1, perform the following procedure:

1. Change to the *ITM_home*/bin directory (by default, /opt/IBM/ITM/bin) and run the following command:

   ```
   ./itmcmd config -A yn
   ```

   The **itmcmd** utility prompts you whether you want to change Agent configuration:

   ```
   Agent configuration started...
   Edit "ITCAM Agent for WebSphere Applications" settings? [ 1=Yes, 2=No ]
    (default is: 1):
   ```

   Enter 1, or press **Enter** to accept the default.

2. The utility prompts you to select the configuration type:

   ```
   Select Configuration Type :
   Choose the configuration type:

   Configuration type description:
       1.Use this option to configure the Tivoli Enterprise Monitoring Agent
   (TEMA) port number or Agent ID. If you modify the Tivoli Monitoring Agent
   port, all Application Servers with Data Collectors must be restarted to
   complete the reconfiguration.
       2.Use this option to configure the Data Collector to monitor
   application server instances. You can also use this option to configure the
   Data Collector to connect to the Managing Server. The option requires that
   either the Application Servers are running (WAS Base Edition) or the Node
   Agent and Deployment Manager are running (WAS ND or XD). The Servers must
   be restarted to complete the configuration.
       3.Use this option to unconfigure the Data Collector from Application
   Server instances. This option will remove all Data Collector configuration
   and runtime filesfor these instances. It requires that either the Application
   Servers are running (WAS Base Edition) or the Node Agent and Deployment
   ```

```
Manager are running (WAS ND or XD). The Server instances must be restarted
to complete the configuration. After the unconfiguration, your Application
Server instances will no longer be monitored.
    4.Use this option to reconfigure your Data Collectors to use a different
Managing Server, change Managing Server information, or disable Data Collector
communication to the Managing Server. The Data Collector must be already
configured to monitor at least one application server instance. You will
need to restart the application servers monitored by the Data Collector.
    5.Use this option to upgrade ITCAM for WebSphere 6.1.x Data Collector
to ITCAM 7.1; also to upgrade ITCAM for WAS 7.0.x Data Collector to
ITCAM 7.1. It requires that either the Application Servers are running
(WAS Base Edition) or the Node Agent and Deployment Manager are running
(WAS ND or XD). The Servers must be restarted to complete the configuration.
    6.Use this option to update Data Collectors with the new maintenance or
reverting the update.It requires that either the Application Servers are
running (WAS Base Edition) or the Node Agent and Deployment Manager are
running (WAS ND or XD). The Servers must be restarted to complete the
configuration.
    7.Use this option to remove unused Data Collectors maintenance levels.
Choose the configuration type: [ 1=Configure Tivoli Enterprise Monitoring
Agent (TEMA), 2=Configure Data Collectors within Application Servers,
3=Unconfigure Data Collectors from Application Servers, 4=Enable/disable
communication to Managing Server for deep-dive diagnostics, 5=Upgrade
ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector
to ITCAM 7.1, 6=Change Data Collectors maintenance level, 7=Remove
unused Data Collectors maintenance levels ] (default is: 1):
```

Type **7** and press **Enter** to remove a Data Collector maintenance level.

3. The configuration utility prompts you for the Data Collector maintenance level to remove.

   ```
   Data Collector maintenance levels :

   Select Data Collector maintenance levels.
   Data Collector maintenance levels (default is: 7.1.0):
   ```

   Enter the maintenance level, or press **Enter** to accept the default.

4. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.

   ```
   The wizard can save your settings to a response file. A response file
    can be used to perform a silent configuration.
   Save Configuration Setting in a Response File [ 1=true,
    2=false ] (default is: 2):
   ```

   If you want to create a response file, enter 1, then enter the name of the file. Otherwise, enter 2, or press **Enter** to accept the default.

5. The configuration utility prompts you whether this Agent connects to a Tivoli Enterprise Monitoring Server.

   ```
   Will this agent connect to a TEMS? [1=YES, 2=NO] (Default is: 1):
   ```

   If the IBM Tivoli Monitoring infrastructure is used, enter **1**. Otherwise (in a deep dive diagnostics only install), enter **2**; in this case the configuration process will be completed

6. If you have not yet configured the connection to a Monitoring Server, configure it; see “Configuring Monitoring Agent settings and communication with the Monitoring Server using command line” on page 110, starting with Step 7 on page 112. Otherwise, press **Enter** repeatedly to accept the existing settings for the connection to Tivoli Enterprise Monitoring Server. Alternatively, you can change these settings; see Steps 7 on page 112 to 14 on page 113

Configuring the Agent using GUI

To configure the Agent using the graphical user interface, use the Manage Tivoli Enterprise Monitoring Services utility.

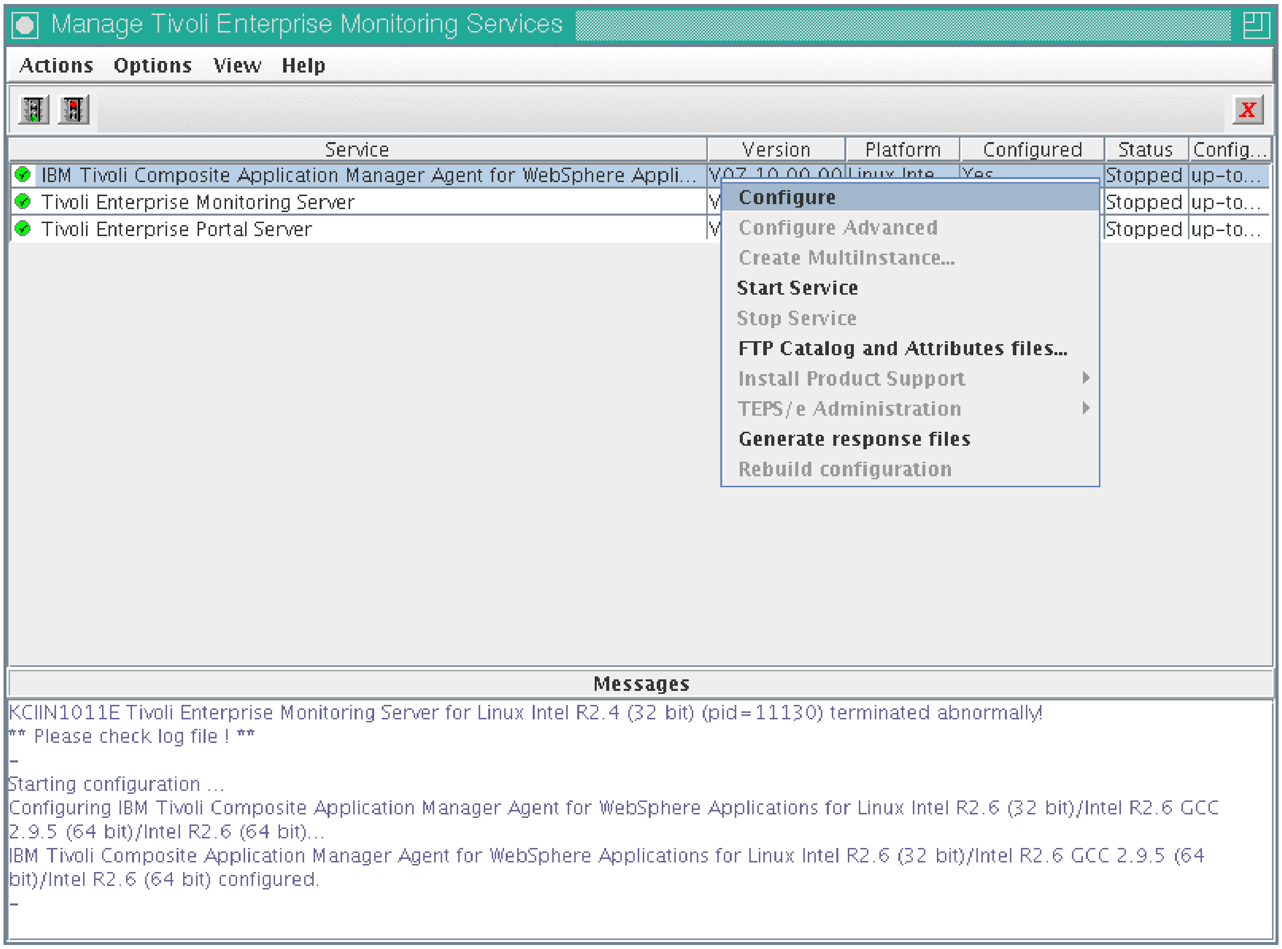
Entering the Agent Configuration window

To perform all the configuration procedures described in this section, you need to start from the **Agent Configuration** window.

Change to the *ITM_home*/bin directory (by default, /opt/IBM/ITM/bin) and run the following command:

```
./itmcmd manage
```

The Manage Tivoli Enterprise Monitoring Services utility opens.

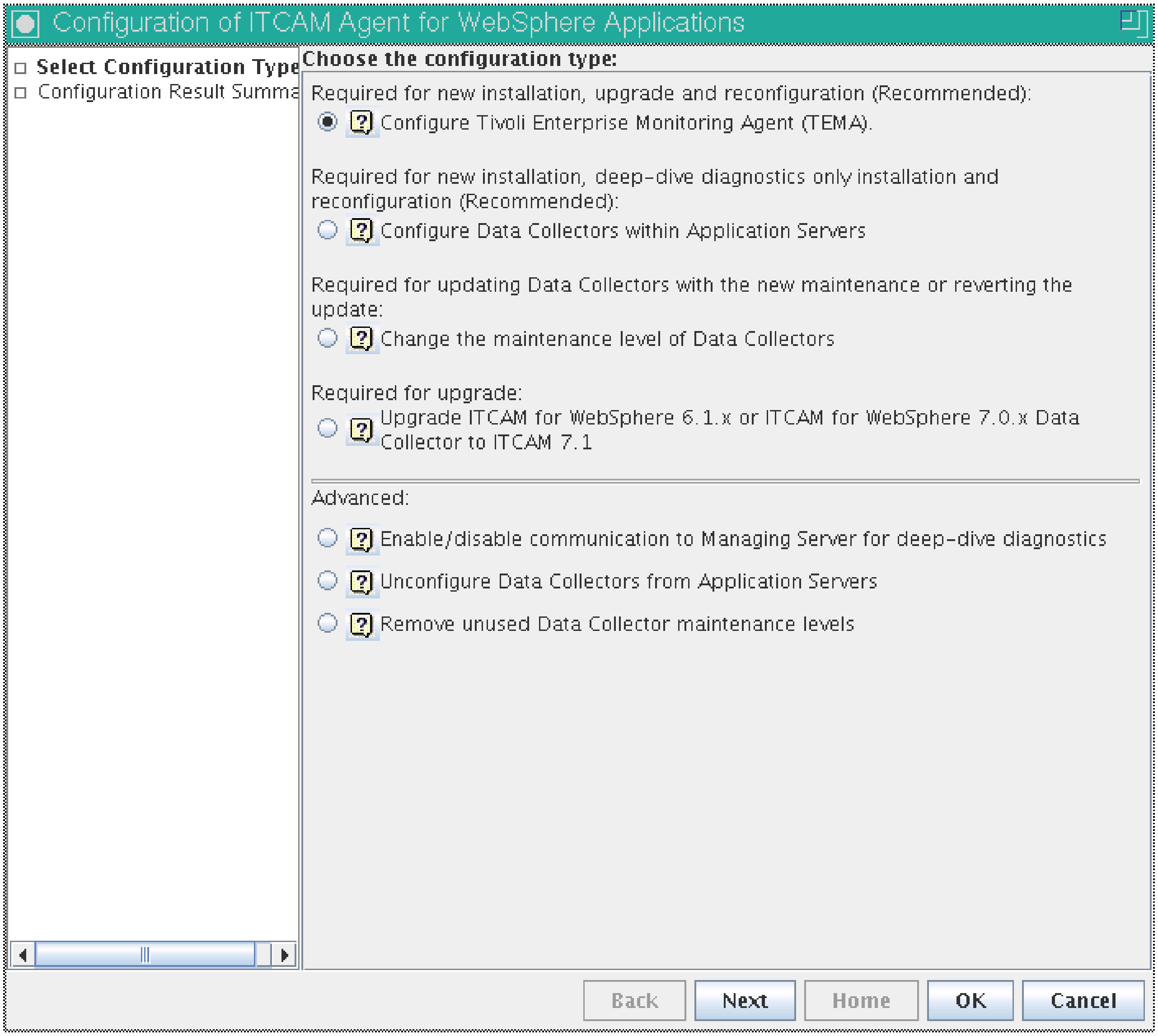


Service	Version	Platform	Configured	Status	Config...
IBM Tivoli Composite Application Manager Agent for WebSphere Appli...	V07.10.00.00	Linux Inte...	Yes	Stopped	up-to...
Tivoli Enterprise Monitoring Server	V			Stopped	up-to...
Tivoli Enterprise Portal Server	V			Stopped	up-to...

```
KCIIN1011E Tivoli Enterprise Monitoring Server for Linux Intel R2.4 (32 bit) (pid=11130) terminated abnormally!
** Please check log file ! **
-
Starting configuration ...
Configuring IBM Tivoli Composite Application Manager Agent for WebSphere Applications for Linux Intel R2.6 (32 bit)/Intel R2.6 GCC
2.9.5 (64 bit)/Intel R2.6 (64 bit)...
IBM Tivoli Composite Application Manager Agent for WebSphere Applications for Linux Intel R2.6 (32 bit)/Intel R2.6 GCC 2.9.5 (64
bit)/Intel R2.6 (64 bit) configured.
-
```

Figure 66. Manage Tivoli Enterprise Monitoring Services window on UNIX and Linux

Right-click **IBM Tivoli Composite Application Manager Agent for WebSphere Applications** and then click **Configure**. The agent configuration window opens.



Configuration of ITCAM Agent for WebSphere Applications

□ Select Configuration Type
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

● Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 67. Agent Configuration window

Note: On Linux and UNIX systems, the window for configuring Monitoring Agent configuration to the Tivoli Enterprise Monitoring Server is always displayed at the end of the configuration process. This is different from Windows, where this window is always displayed at the beginning of the configuration process.

Configuring Monitoring Agent settings and communication with the Monitoring Server using GUI

If the IBM Tivoli Monitoring infrastructure is used, you **must** configure Monitoring Agent settings before configuring the Data Collector to monitor any application server instances. You also need to configure Monitoring Agent communication to the Monitoring Server. Do not perform this configuration in a deep dive diagnostics only installation, where IBM Tivoli Monitoring is not used.

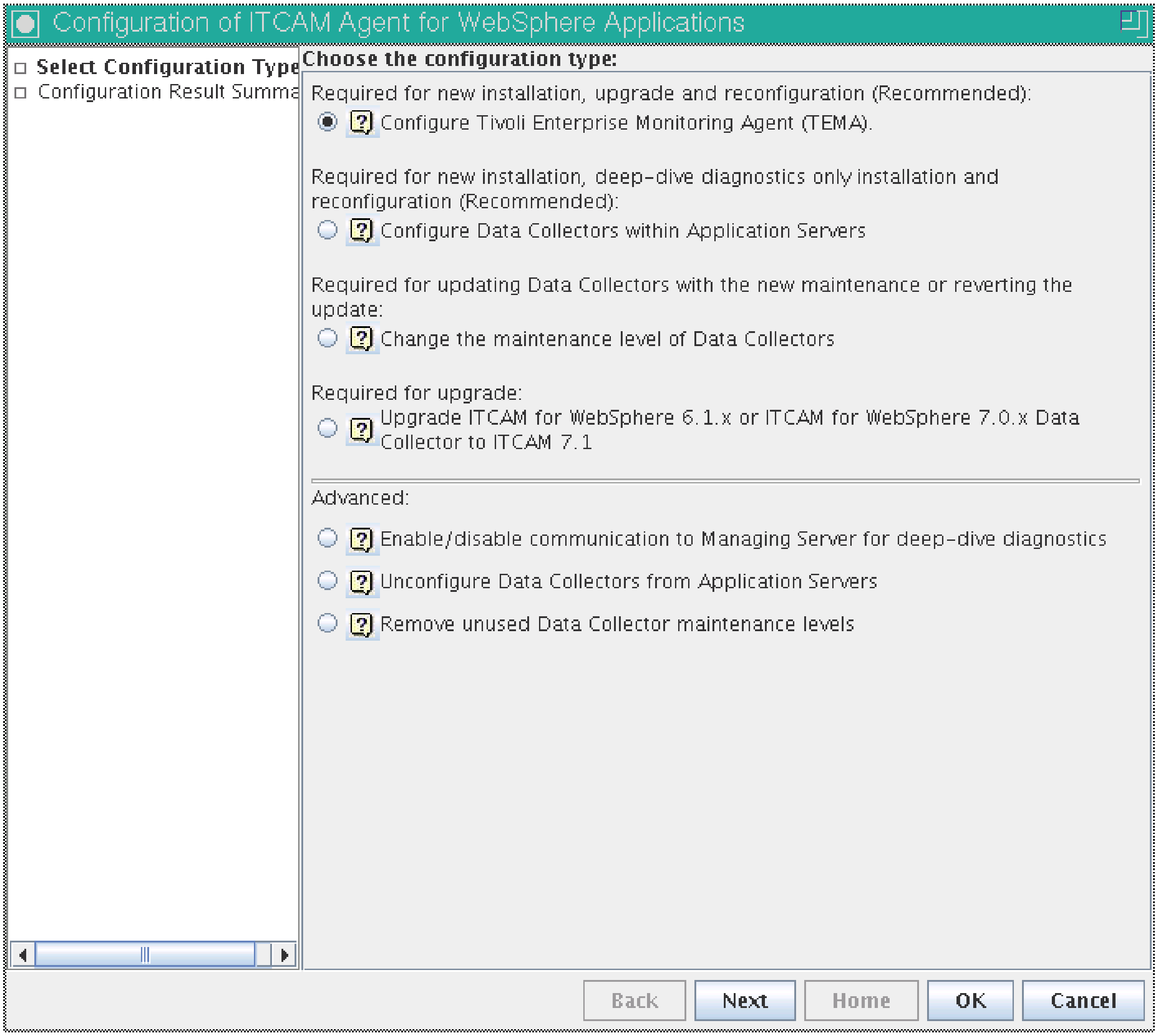
You can change the port that is used for communication between the Data Collector and the monitoring agent (this communication is on the local host, except if the monitoring agent is used for i5/OS Data Collectors); the default port is

63335. You can also set an alternate node name that determines how the agent will be displayed in the Tivoli Enterprise Portal navigation tree.

While you can change these settings at a later time, it is normally most convenient to set them when initially configuring the communication. In this case no changes to existing Data Collector configuration files is required to change the port number, and no customization of the Tivoli Enterprise Portal view could have been performed by any user. So, if you need to make such changes, make them at installation time if possible.

To configure Monitoring Agent settings and communication with the Monitoring Server, perform the following procedure:

1. Enter the Agent Configuration window. See "Entering the Agent Configuration window" on page 133.



Configuration of ITCAM Agent for WebSphere Applications

□ Select Configuration Type
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

● Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

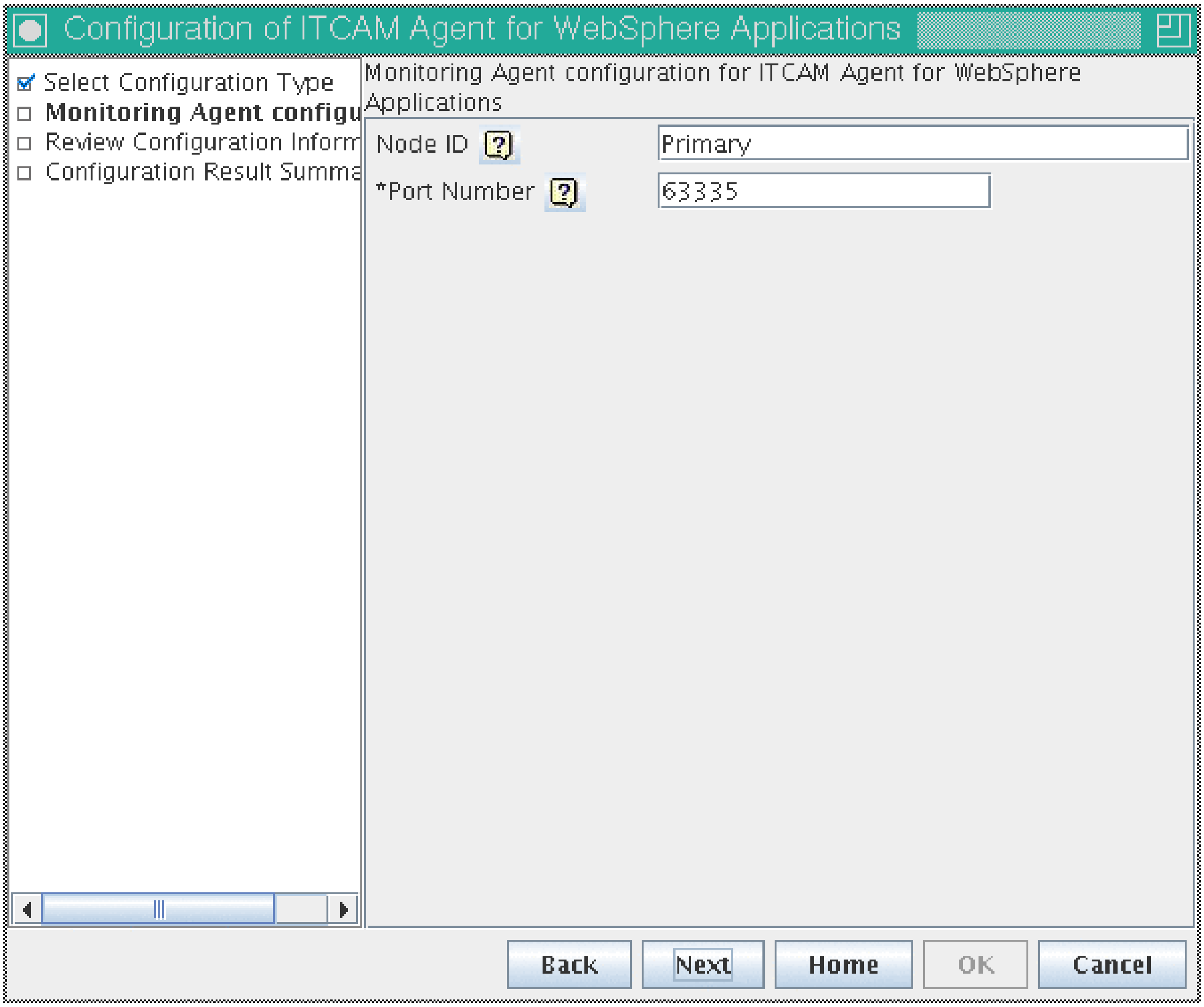
○ Remove unused Data Collector maintenance levels

Figure 68. Configuring Communication to the monitoring agent, window 1

2. Select **Configure Tivoli Enterprose Monitoring Agent (TEMA)** and click **Next**.

3. In the Agent Configuration page, you can set an alternative Node ID for identifying the agent. This is the identifier that will determine how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is `Primary`, used in conjunction with the host name of the computer where the Agent is installed. In the **Port** field, you can specify a TCP socket port that the monitoring agent will use to listen for connection requests from the Data Collectors. Normally, do not change this value. The port will only be used for local communication on the host (except if you use the monitoring agent to support Data Collectors on i5/OS hosts, see *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Data Collector Installation and Configuration Guide for IBM i*.

   Attention: If you install more than one copy of the Monitoring Agent on a single host, you must set the Alternative Node ID parameter to different values for each of the copies. Otherwise, the multiple copies of the Monitoring Agent will not work correctly with Tivoli Monitoring.


Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
□ **Monitoring Agent configu**
□ Review Configuration Inform
□ Configuration Result Summa

Monitoring Agent configuration for ITCAM Agent for WebSphere Applications

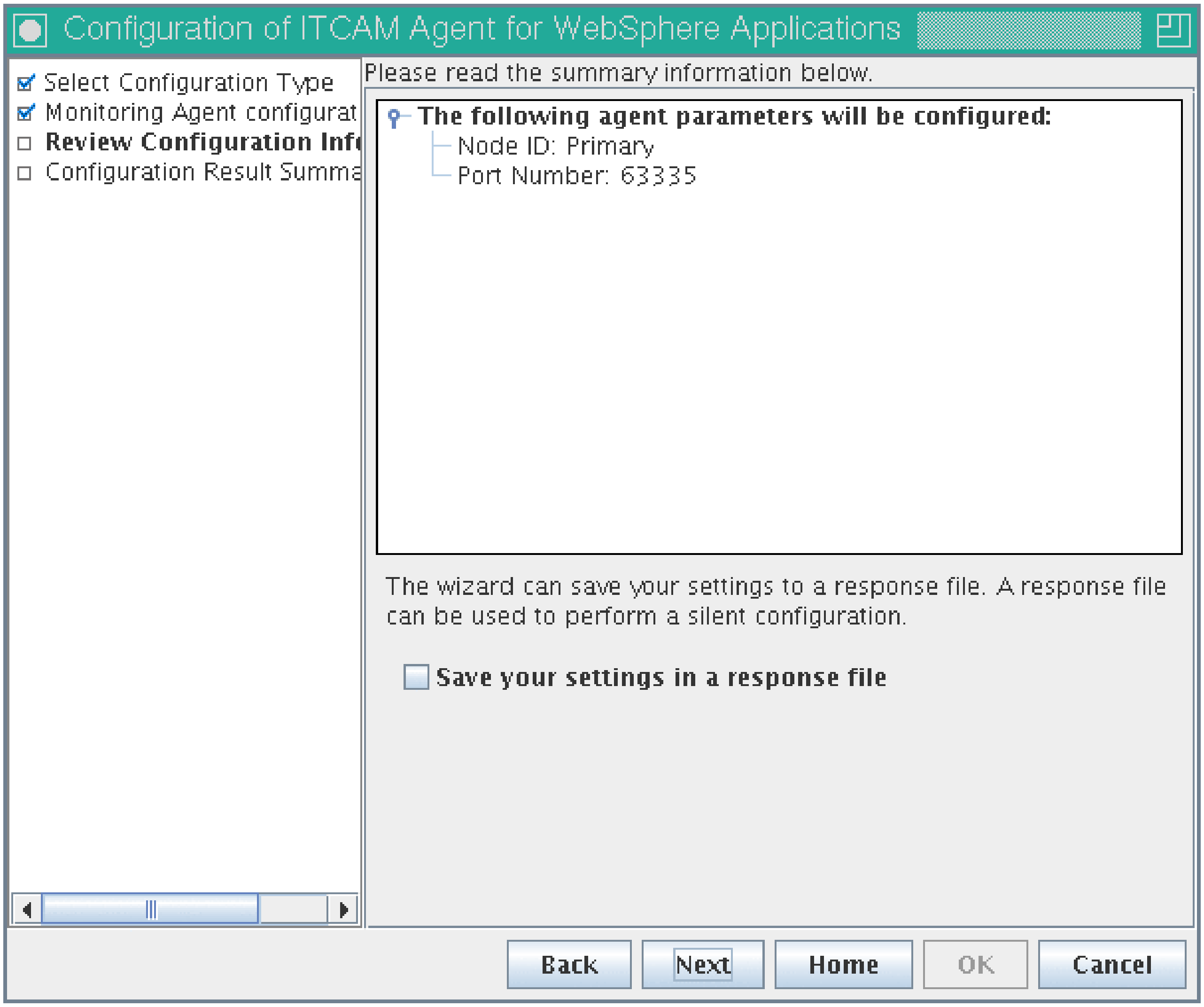
Node ID: Primary
*Port Number: 63335

Figure 69. Configuring Communication to the Monitoring Agent, window 2

Enter the Node ID if necessary; change the port number if necessary. Click **Next**.

Attention: Valid characters for the node ID include A-z, a-z, 0-9, underbar (_), dash (-), and period (.); do not use other characters.

4. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Monitoring Agent configurat
□ Review Configuration Infc
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Please read the summary information below.

The following agent parameters will be configured:
Node ID: Primary
Port Number: 63335

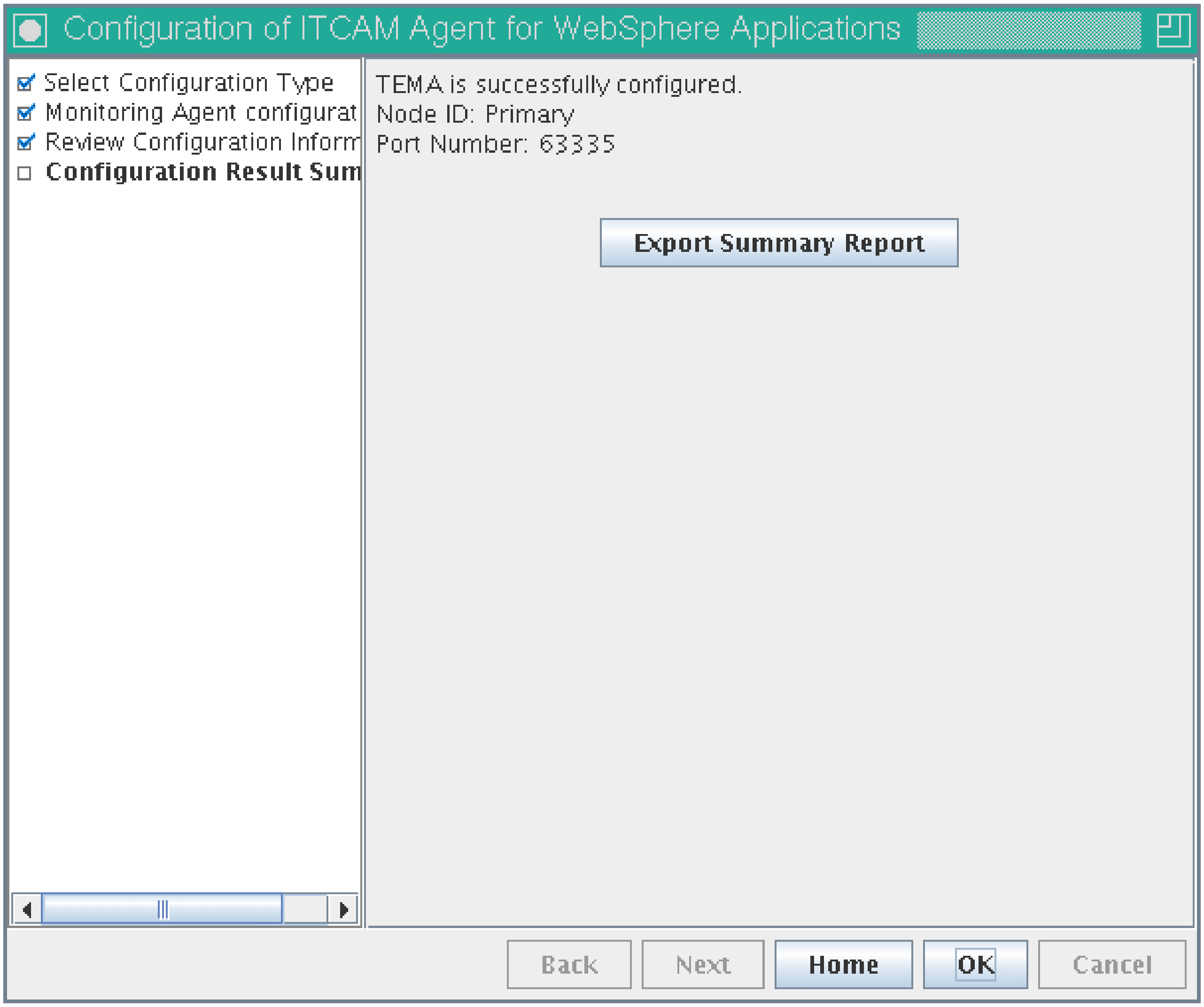
The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

□ Save your settings in a response file

Figure 70. Configuring Communication to the monitoring agent, window 3

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location, then click **Next**. Otherwise, leave the box unchecked and click **Next**.

5. The monitoring agent is successfully configured.



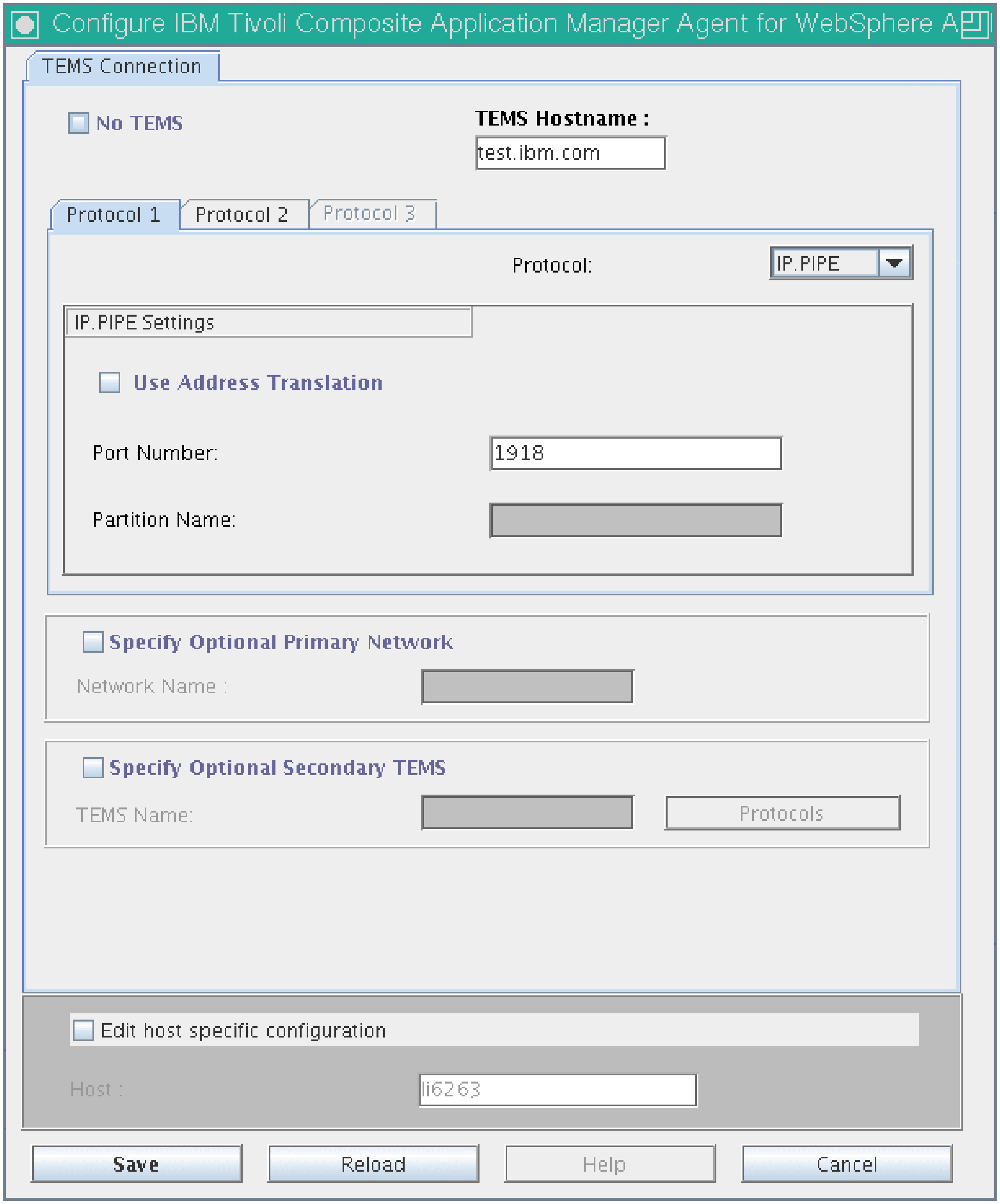
Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Monitoring Agent configurat
☑ Review Configuration Inform
□ Configuration Result Sum
Export Summary Report
Back
Next
Home
OK
Cancel

TEMA is successfully configured.
Node ID: Primary
Port Number: 63335

Figure 71. Configuring Communication to the monitoring agent, window 4

Click **OK**.

6. The **TEMS Connection** window is displayed.


Configure IBM Tivoli Composite Application Manager Agent for WebSphere A
TEMS Connection
□ No TEMS
Protocol 1
Protocol 2
Protocol 3
IP.PIPE Settings
□ Use Address Translation
Partition Name:
□ Specify Optional Primary Network
Network Name :
□ Specify Optional Secondary TEMS
TEMS Name:
Protocols
□ Edit host specific configuration
Save
Reload
Help
Cancel

TEMS Hostname : test.ibm.com

Protocol: IP.PIPE

Port Number: 1918

Host : li6263

Figure 72. Configuring Communication to the monitoring agent, window 5

7. Enter the Tivoli Enterprise Monitoring Server (TEMS) host name, and select the protocol for connection with the Tivoli Enterprise Monitoring Server. If the connection must pass through a firewall with address translation, select **IP.PIPE** and check the box **Use Address Translation**.

Specify protocol parameters and, if necessary the secondary protocols and secondary TEMS host. See *IBM Tivoli Monitoring: Installation and Setup Guide* for details.

Attention: If IBM Tivoli Monitoring is not used (in a deep dive diagnostics only installation), check **No TEMS** in this window, and click **Save**.

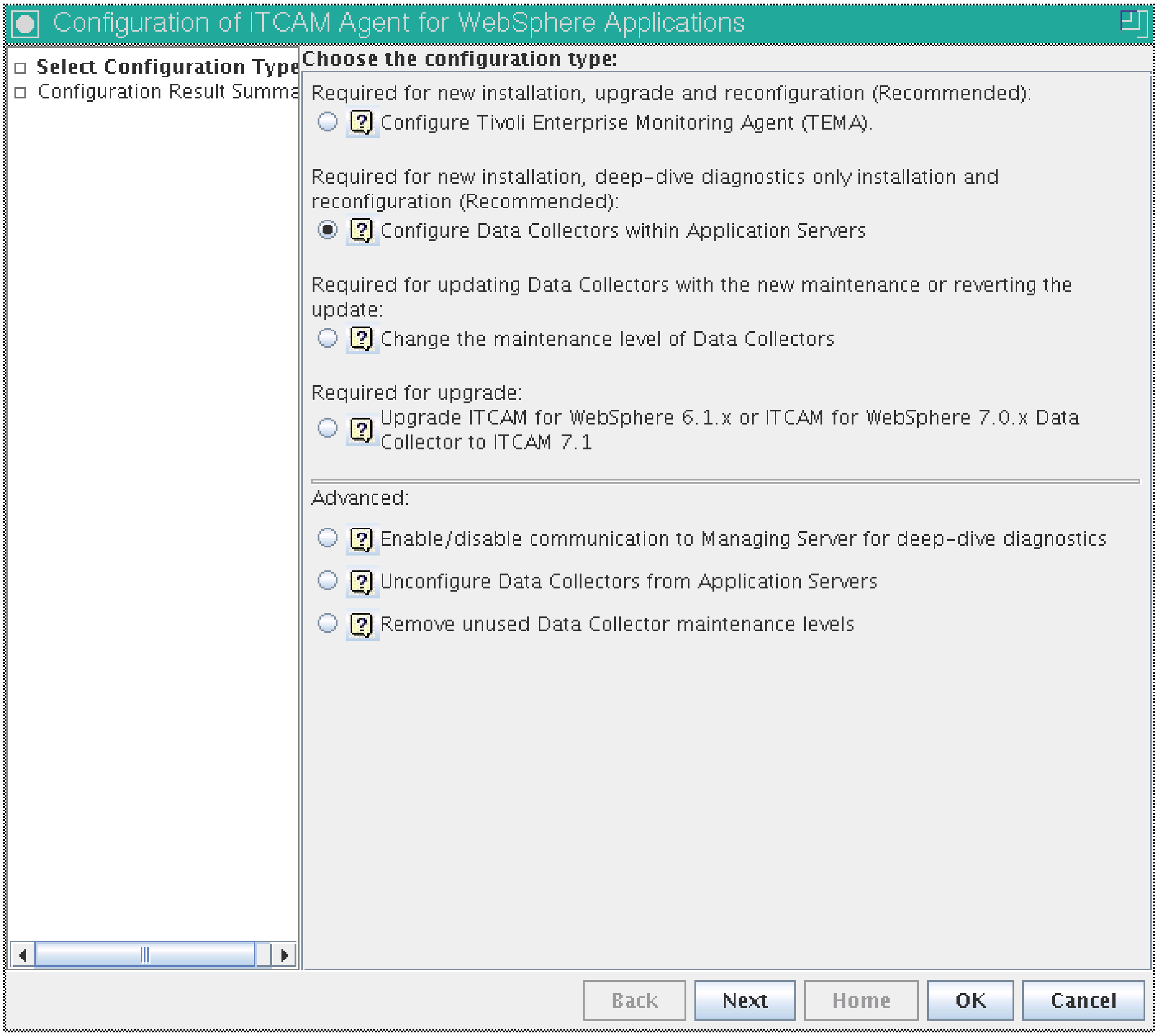
Configure the Data Collector to monitor application server instances using GUI

You must configure the Data Collector for each application server instance that you need to monitor.

Important: Do not configure the Data Collector to monitor an instance of WebSphere Application Server that hosts the Managing Server Visualization Engine. You can, however, use the Data Collector for monitoring any other WebSphere Application Server instances on the same node.

To configure the Data Collector to monitor a server instance, perform the following procedure:

1. Enter the Agent Configuration window. See "Entering the Agent Configuration window" on page 133.



Configuration of ITCAM Agent for WebSphere Applications

□ Select Configuration Type
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

● Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

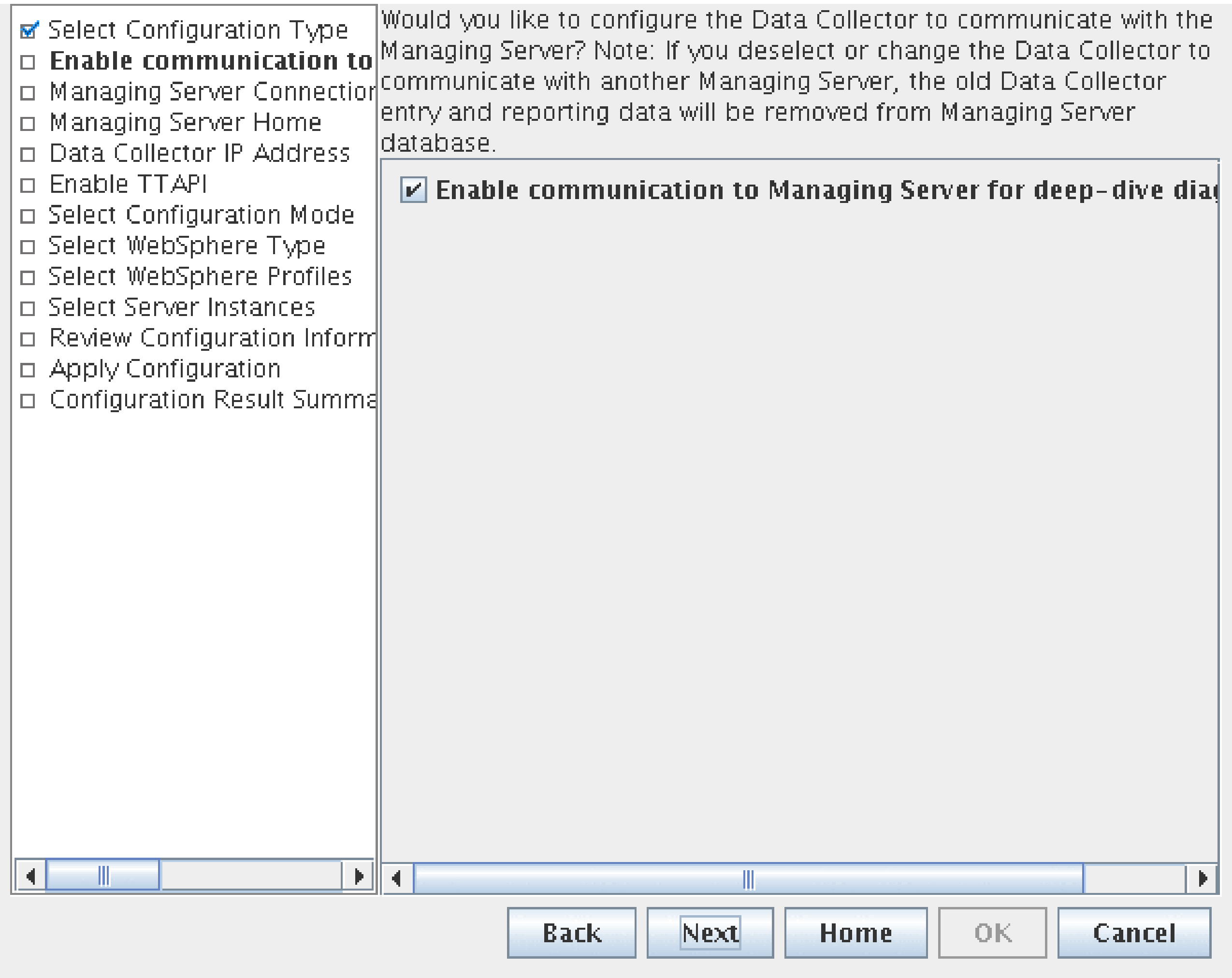
○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 73. Configuring the Data Collector to monitor application server instances, window 1

2. Select **Configure Data Collectors within Application Servers** and click **Next**.
3. You can choose to configure the Data Collector to communicate with ITCAM for Application Diagnostics Managing Server. Otherwise, this application server instance will not be monitored by the Managing Server infrastructure. (IBM Tivoli Monitoring is not affected by this setting).


☑ Select Configuration Type
□ Enable communication to
□ Managing Server Connectior
□ Managing Server Home
□ Data Collector IP Address
□ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Would you like to configure the Data Collector to communicate with the Managing Server? Note: If you deselect or change the Data Collector to communicate with another Managing Server, the old Data Collector entry and reporting data will be removed from Managing Server database.

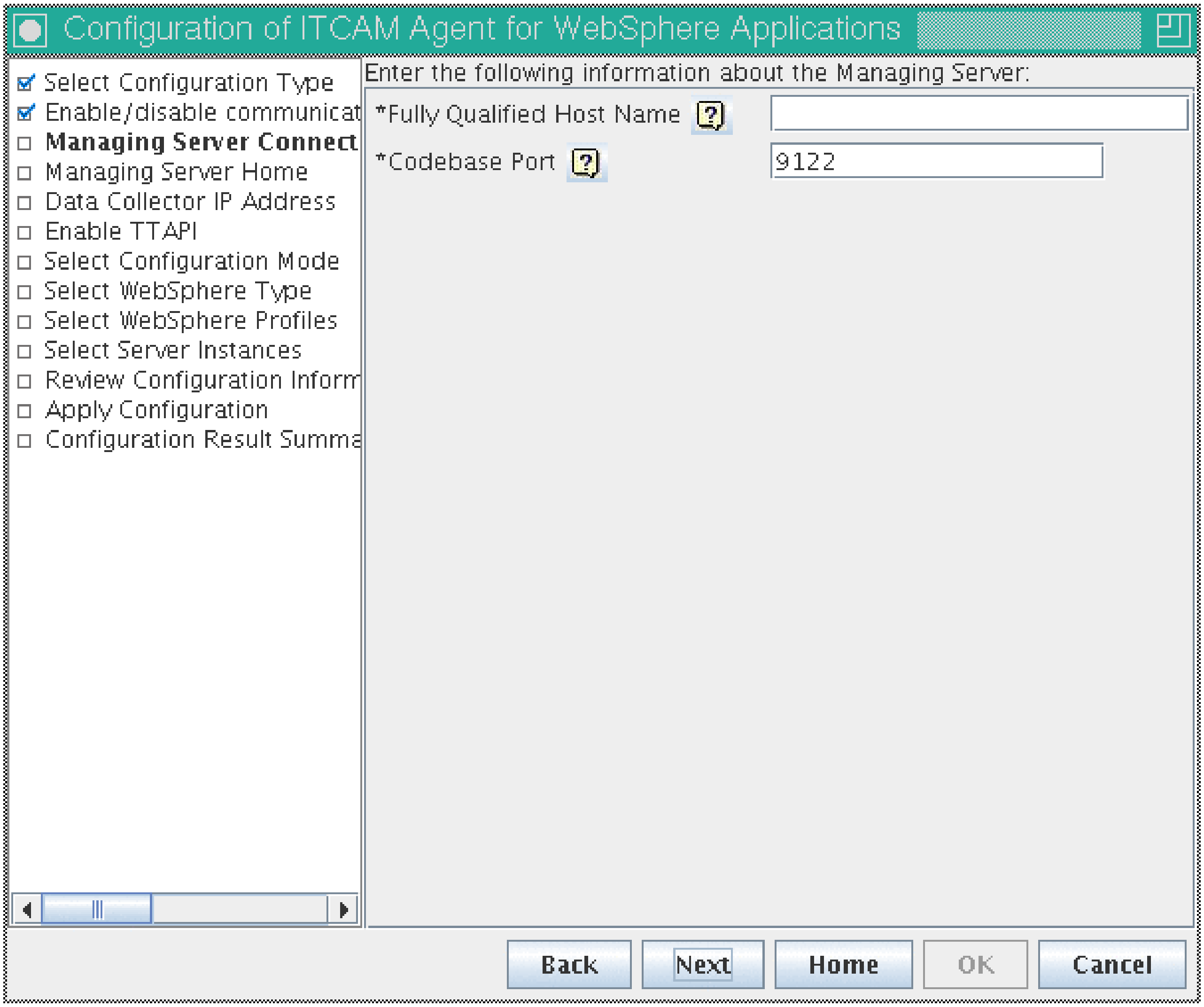
☑ **Enable communication to Managing Server for deep-dive diag**

Figure 74. Configuring the Data Collector to monitor application server instances, window 2

If you want to configure the Data Collector to communicate with the Managing Server, check the **Enable communication to Managing Server for deep-dive diagnostics** box. Then, Click **Next**. If you left the box unchecked, go to step 7 on page 145.

Note: If you leave the box unchecked, you can still configure the Data Collector to communicate with the Managing Server later. See “Configure Data Collector communication with the Managing Server using GUI” on page 161.

4. Enter the fully qualified host name of the Managing Server. If a split Managing Server installation is used, enter the name of the host where the Kernel is located.


Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Enable/disable communicat
□ **Managing Server Connect**
□ Managing Server Home
□ Data Collector IP Address
□ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa

Enter the following information about the Managing Server:

*Fully Qualified Host Name

*Codebase Port 9122

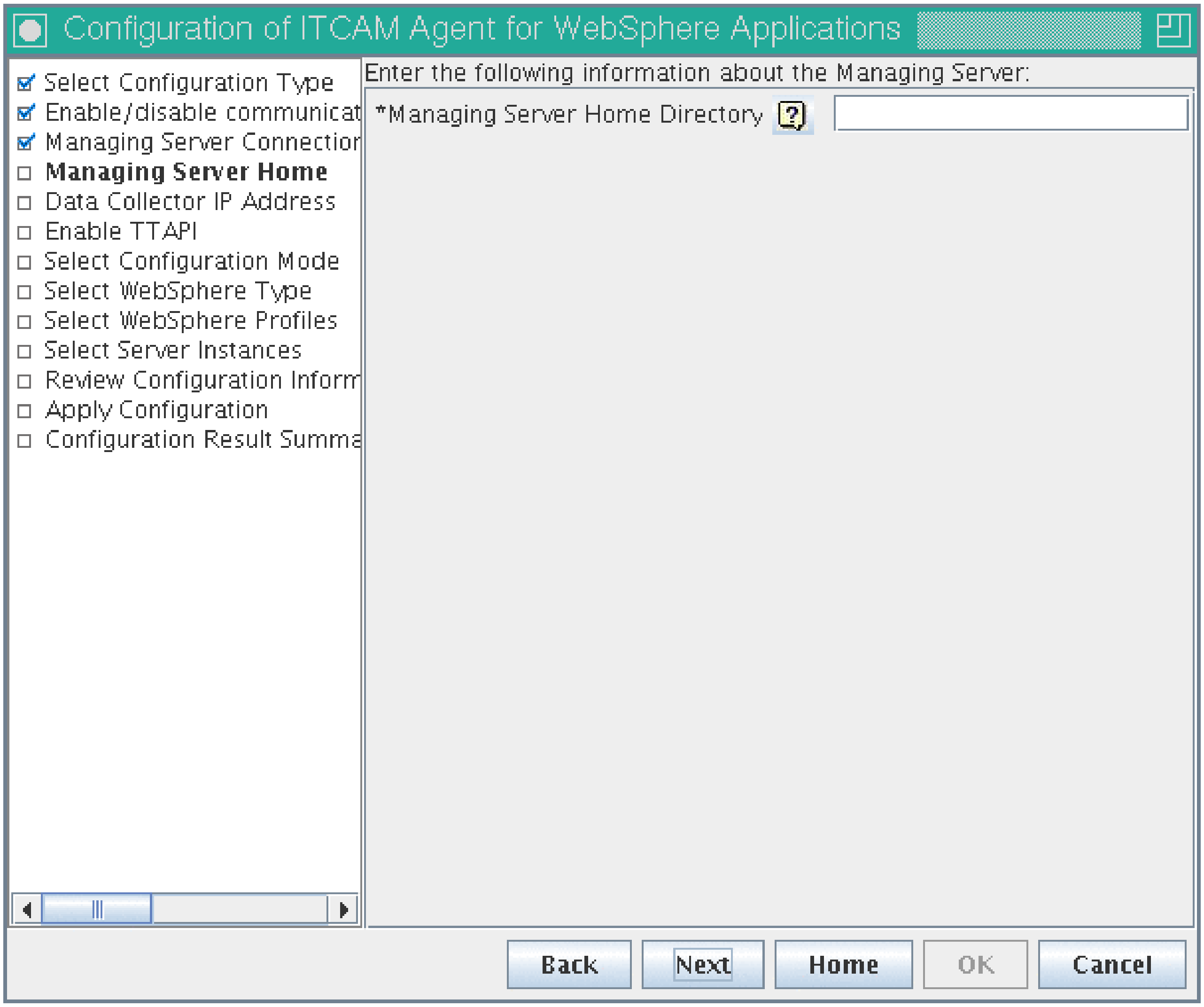
Figure 75. Configuring the Data Collector to monitor application server instances, window 3

If the Managing Server is installed on the same host as the Agent, the address and port for this Managing Server are displayed by default, but you can change them.

After entering the host name, you can also change the port number on which the Managing Server Kernel is listening. Then, click **Next**.

Note: This port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the `.ITCAM61_MS_CONTEXT.properties` file located under the Managing Server Home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

5. Set the Managing Server home directory, which is the destination directory chosen during the installation of the Managing Server.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Enable/disable communicat
☑ Managing Server Connectior
□ **Managing Server Home**
□ Data Collector IP Address
□ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa

Enter the following information about the Managing Server:

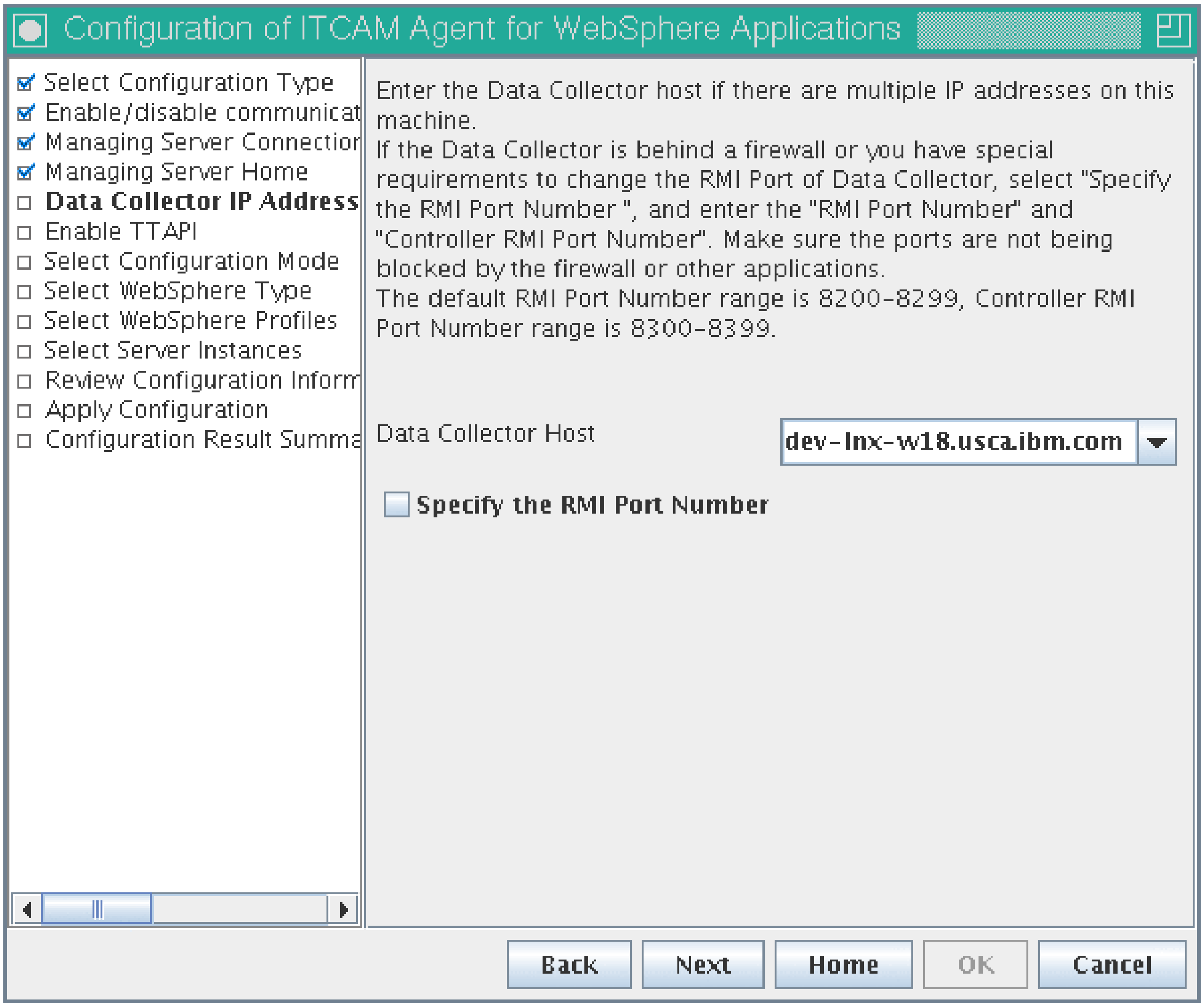
*Managing Server Home Directory

Figure 76. Configuring the Data Collector to monitor application server instances, window 4

If the Managing Server is running and the configuration utility has been able to communicate to it, its home directory will be displayed by default. If the Managing Server is not available at the time of communication, you need to enter the home directory.

If the Managing Server home directory is not displayed, input it. Click **Next**.

6. If there are multiple IP address on this host, select the address that the Data Collector needs to use for communication with the Managing Server. Also, if you need to change the ports that the Data Collector uses to accept incoming connections from the Managing Server (in case of split Managing Server installation, the Publish Server), select "Specify the RMI Port Number", and enter the "RMI Port Number" and "Controller RMI Port Number". Make sure that the ports are not being blocked by the firewall or other applications. The default RMI port Number range is 8200-8299; the Controller RMI Port Number range is 8300-8399.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicat
☑ Managing Server Connectior
☑ Managing Server Home
□ Data Collector IP Address
□ Enable TTAPI
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inforn
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Enter the Data Collector host if there are multiple IP addresses on this machine.
If the Data Collector is behind a firewall or you have special requirements to change the RMI Port of Data Collector, select "Specify the RMI Port Number ", and enter the "RMI Port Number" and "Controller RMI Port Number". Make sure the ports are not being blocked by the firewall or other applications.
The default RMI Port Number range is 8200-8299, Controller RMI Port Number range is 8300-8399.

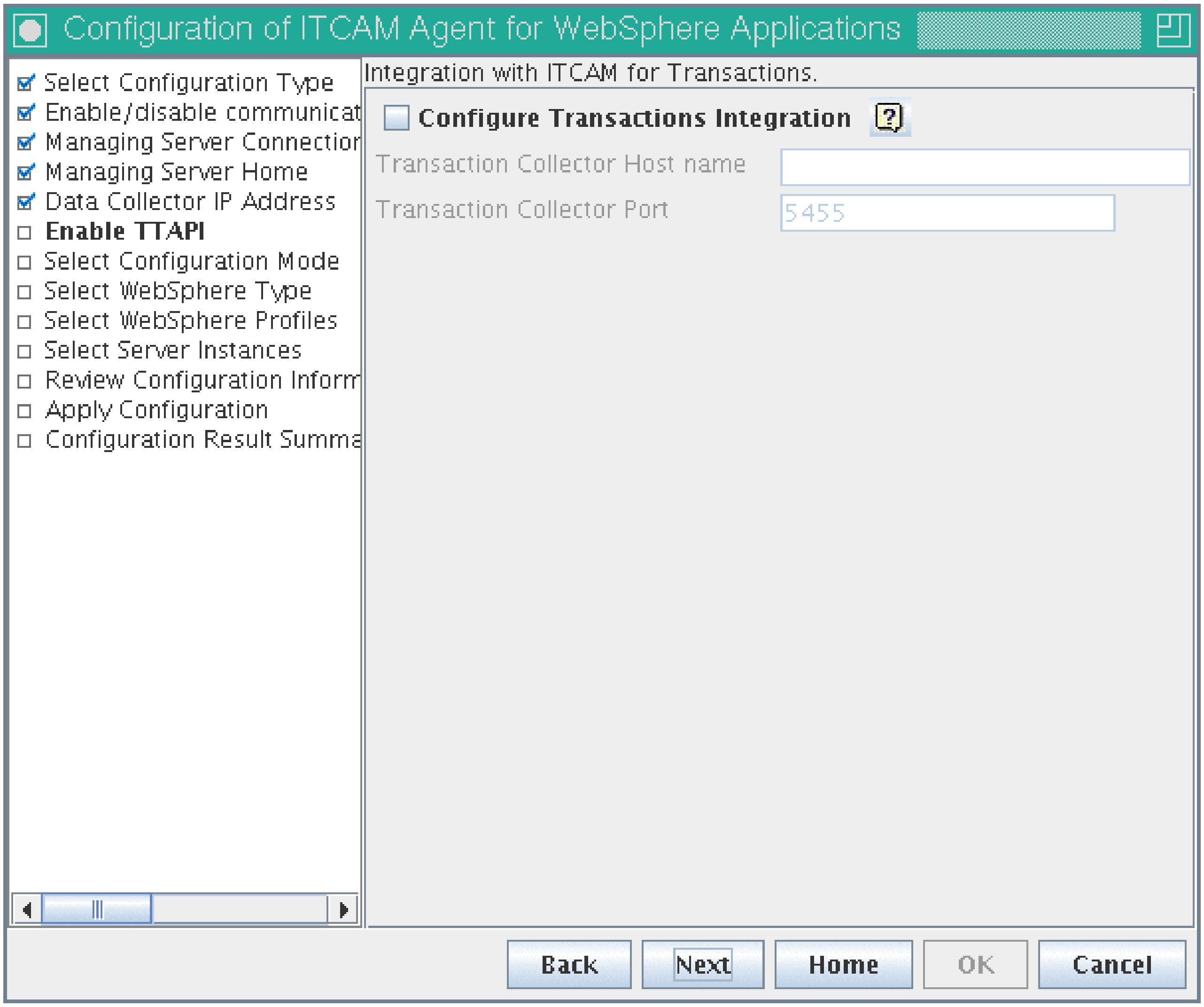
Data Collector Host: dev-lnx-w18.usca.ibm.com

□ Specify the RMI Port Number

Figure 77. Configuring the Data Collector to monitor application server instances, window 5

After making any necessary changes, click **Next**.

7. You can enable the Transaction Tracking API function in the following window. Transaction Tracking Application Programming Interface (TTAPI) enables the integration of ITCAM Agent for WebSphere Applications and ITCAM for Transactions. With TTAPI, the Data Collector can send transaction information to ITCAM for Transactions; also, if ITCAM for Application Diagnostics Managing Server is used, transaction-specific information is available in the Visualization Engine. TTAPI also enables integration of the Data Collector with the Robotic Response Time component (or T6 agent).


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicat
☑ Managing Server Connectior
☑ Managing Server Home
☑ Data Collector IP Address
□ **Enable TTAPI**
□ Select Configuration Mode
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Integration with ITCAM for Transactions.

□ **Configure Transactions Integration**

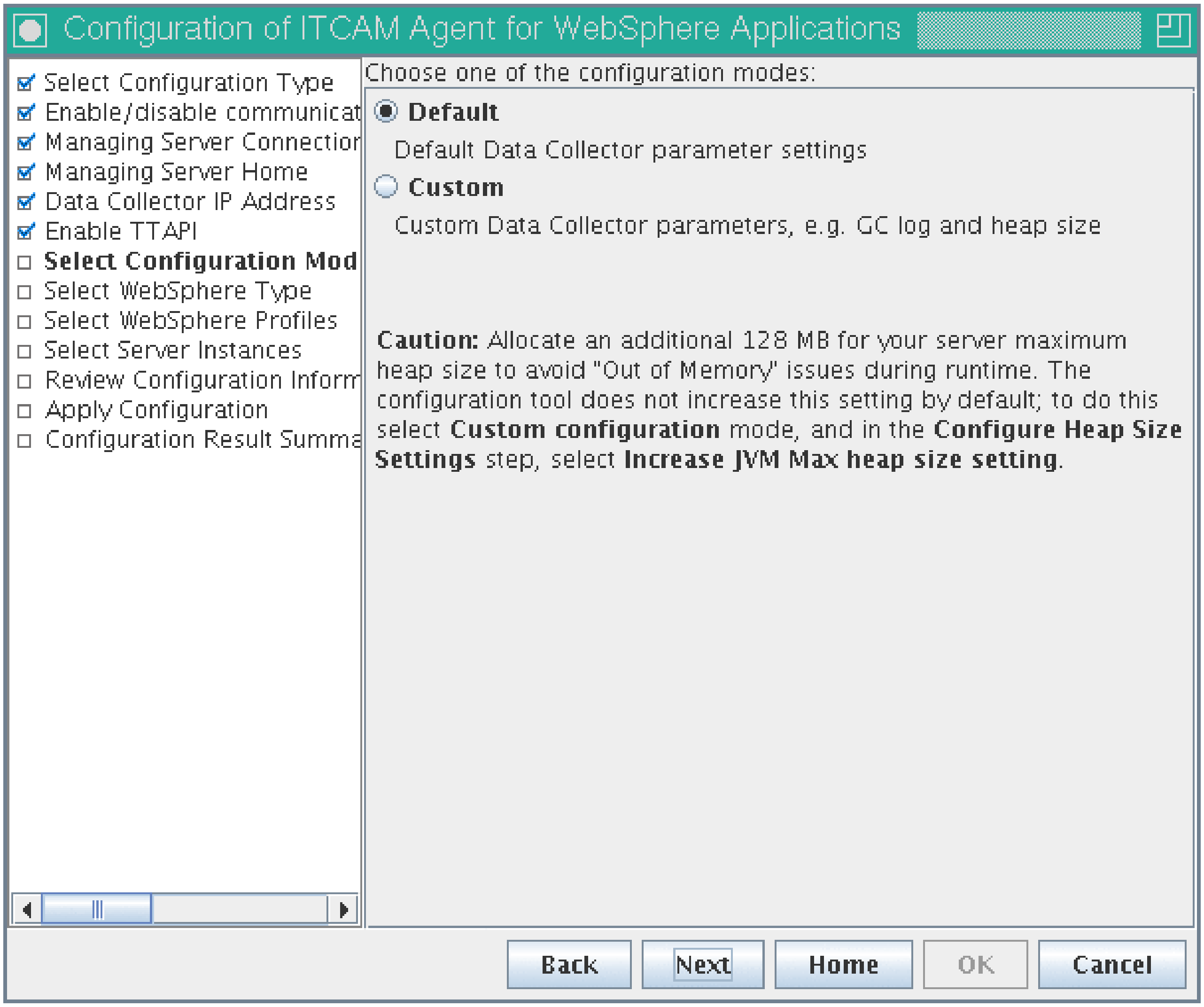
Transaction Collector Host name

Transaction Collector Port 5455

Figure 78. Configuring the Data Collector to monitor application server instances, window 6

To enable TTAPI, check the **Configure Transaction Integration** box, and enter the fully qualified host name or IP address for ITCAM for Transaction Tracking agent and the port number that the Data Collector uses to connect to it. Then, click **Next**. If you do not need to enable the Transaction Tracking API function, leave the box unchecked and click **Next**.

8. A window for selecting the configuration mode is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicat
☑ Managing Server Connectior
☑ Managing Server Home
☑ Data Collector IP Address
☑ Enable TTAPI
□ Select Configuration Mod
□ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose one of the configuration modes:

● **Default**

Default Data Collector parameter settings

○ **Custom**

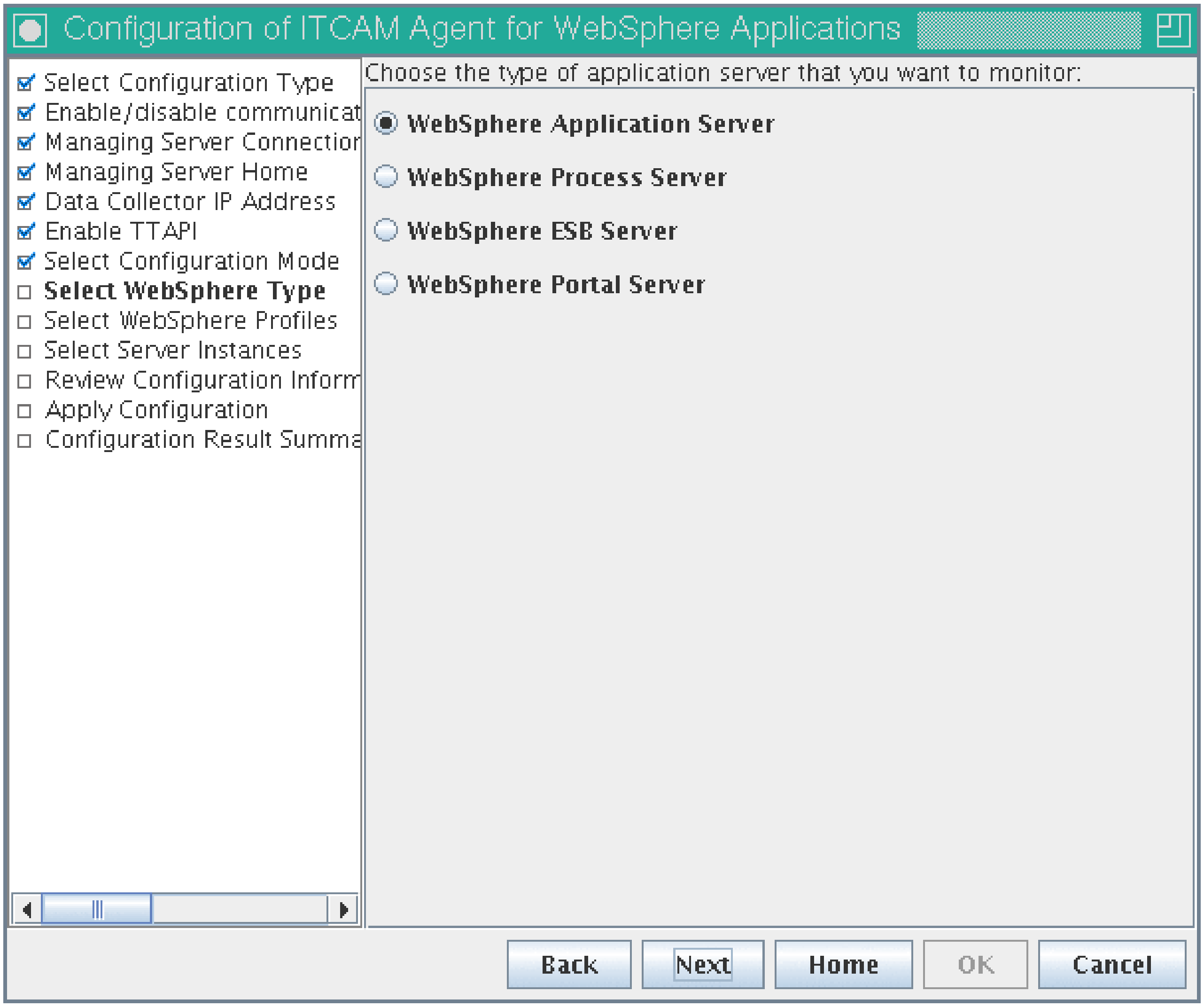
Custom Data Collector parameters, e.g. GC log and heap size

Caution: Allocate an additional 128 MB for your server maximum heap size to avoid "Out of Memory" issues during runtime. The configuration tool does not increase this setting by default; to do this select **Custom configuration** mode, and in the **Configure Heap Size Settings** step, select **Increase JVM Max heap size setting**.

Figure 79. Configuring the Data Collector to monitor application server instances, window 7

If you need to modify Garbage Collection logging settings, increase the Maximum Heap size, or disable backing up the application server configuration, select **Custom**. (In this case, the configuration utility will display additional windows for these settings). Otherwise, choose **Default**. Click **Next**.

9. A window for choosing the type of application server that the Data Collector monitors is displayed.



☑ Select Configuration Type
☑ Enable/disable communicat
☑ Managing Server Connectior
☑ Managing Server Home
☑ Data Collector IP Address
☑ Enable TTAPI
☑ Select Configuration Mode
□ **Select WebSphere Type**
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa

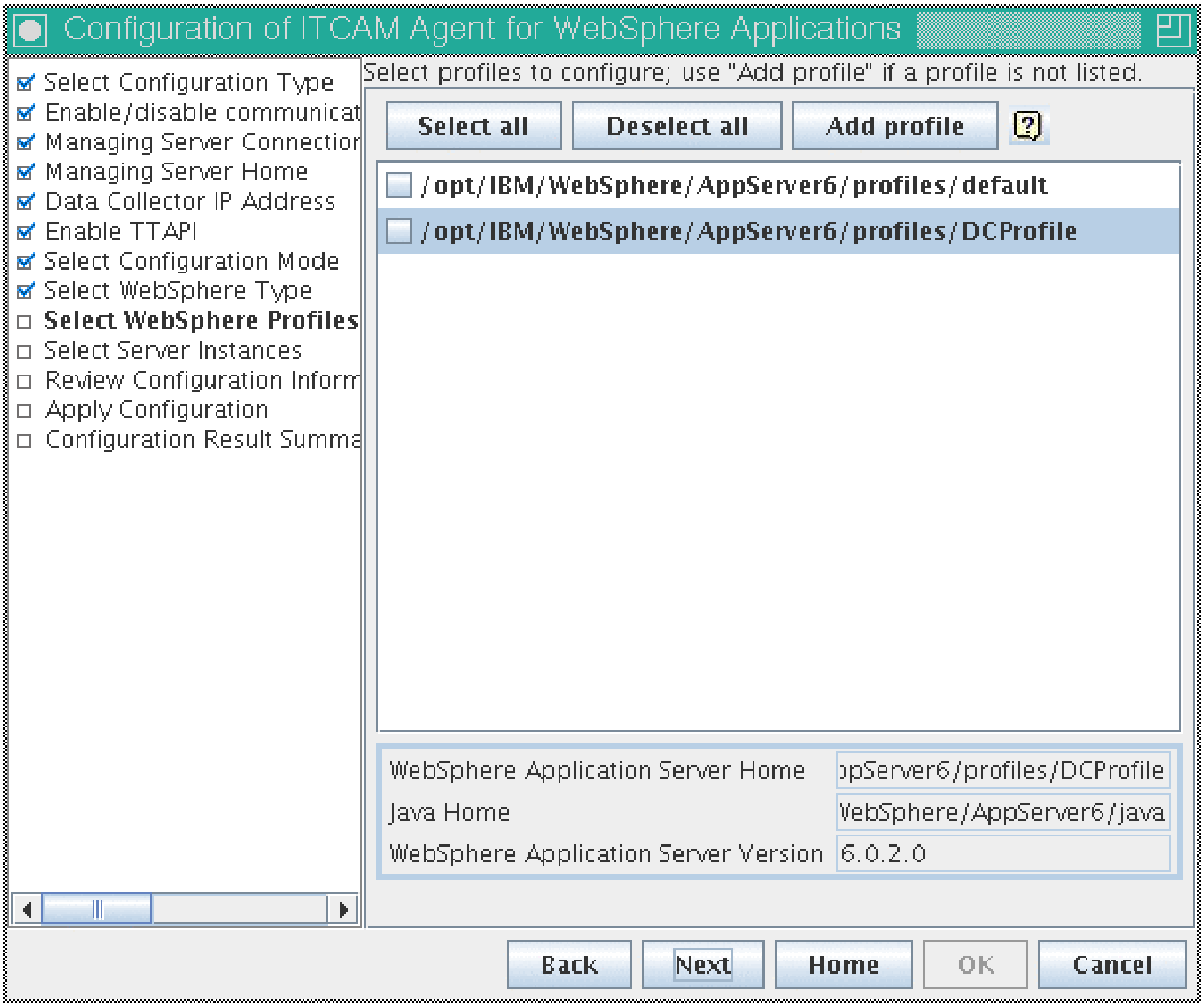
Choose the type of application server that you want to monitor:

● **WebSphere Application Server**
○ **WebSphere Process Server**
○ **WebSphere ESB Server**
○ **WebSphere Portal Server**

Figure 80. Configuring the Data Collector to monitor application server instances, window 8

Select the application server type, and click **Next**.

10. Discovered application server profiles are listed in the following window.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicat
☑ Managing Server Connectior
☑ Managing Server Home
☑ Data Collector IP Address
☑ Enable TTAPI
☑ Select Configuration Mode
☑ Select WebSphere Type
□ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inforn
□ Apply Configuration
□ Configuration Result Summa
Select all
Deselect all
Add profile
?
Back
Next
Home
OK
Cancel

Select profiles to configure; use "Add profile" if a profile is not listed.

□ /opt/IBM/WebSphere/AppServer6/profiles/default

□ /opt/IBM/WebSphere/AppServer6/profiles/DCProfile

WebSphere Application Server Home	ɔpServer6/profiles/DCProfile
Java Home	VebSphere/AppServer6/java
WebSphere Application Server Version	6.0.2.0

Figure 81. Configuring the Data Collector to monitor application server instances, window 9

Check the box for the profile for which you want to configure the Data Collector. You can select multiple profiles from the list; the Data Collector will be configured for each of the selected server profiles. If the application server profile you want to use does not show up in the list, specify the application server profile installation directory by click **Add profile**. If multiple installations are found, make sure the one selected is running. The selected profile information is displayed below the selection box. Select the application server that the Data Collector is to monitor and click **Next**.

11. Select the server instances you want to configure. For a stand alone (not Network Deployment and not Extended Deployment) environment, enter the application server host name or IP address and the SOAP/RMI port of the application server instance you are configuring. For a Network Deployment environment, you must specify the Deployment Manager host name or IP address and SOAP/RMI port.

Important:

- If the application server has more than one instance and the Data Collector is already configured for some of them, only the instances for which it is not configured are initially listed in this window. To display configured instances, select the **Include configured server instances** check box. If you select a configured instance, it will be reconfigured.

- For a stand-alone environment, instances must be running during the configuration.
- For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running.

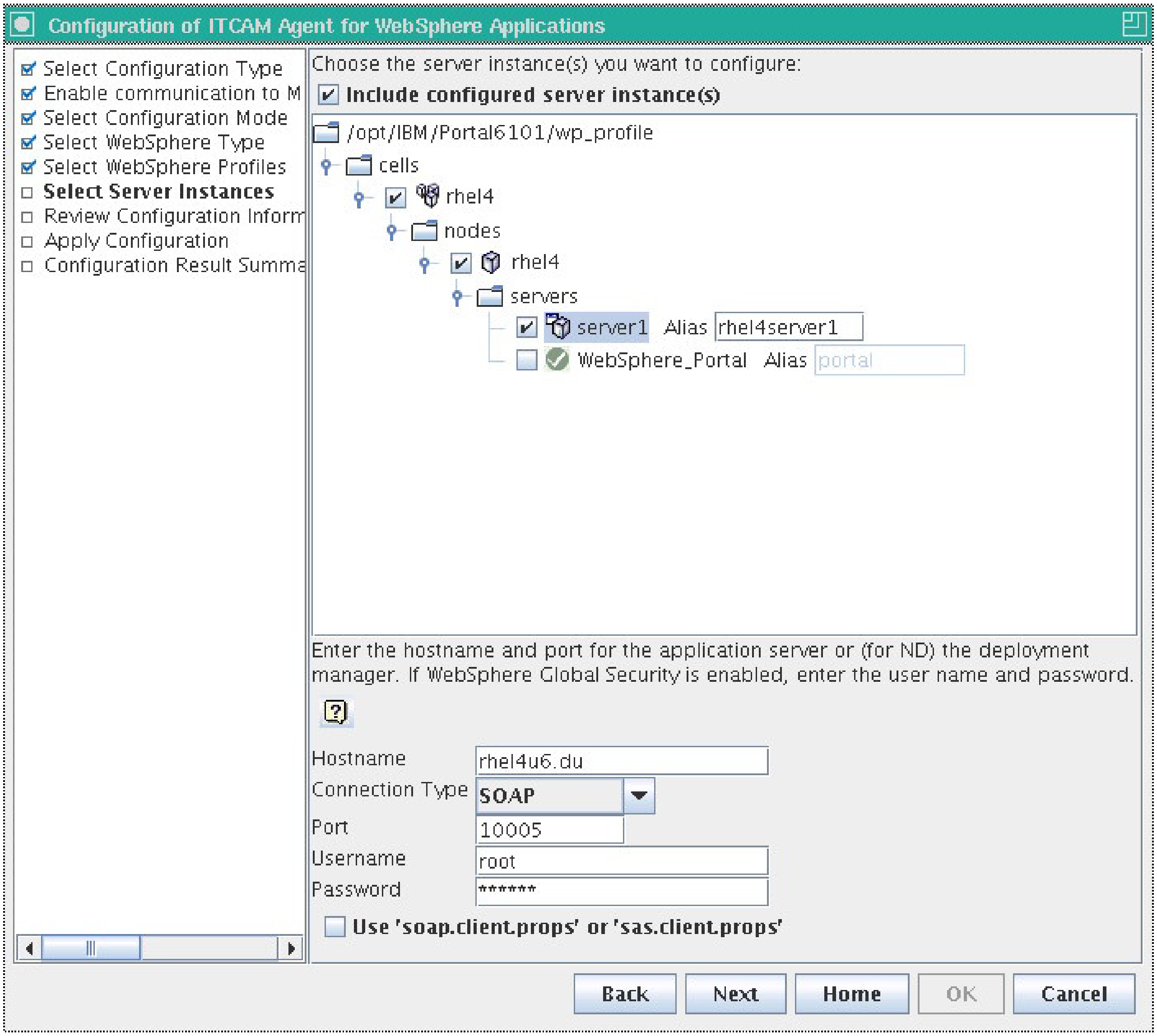
You can refer to the following table to establish Data Collector and application server communication:

Table 11. Fields for establishing Data Collector and application server communication

Field	**What to do**
Host name	Type the fully qualified host name or IP address of the application server instance that the Data Collector monitors. Do not include a protocol in the host name. For example, type `myserver.ibm.tivoli.com`, not `https://myserver.ibm.tivoli.com`. Note: If using a Network Deployment environment, provide the host name of the Deployment Manager instead.
Connector Type	Select the type of connection the Data Collector and application server will use for communication.
Port	If you selected SOAP as the connector type, enter the connector port used by the application server instance to send commands using the Simple Object Access Protocol (SOAP). The SOAP port is identified in the `SOAP_CONNECTOR_ADDRESS` end point definition within the `AppServer_home/profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml` file for the application server instance. **Note:** If using Network Deployment, provide the SOAP port of the Deployment Manager instead. If you selected RMI as the connector type, enter the connector port used by the application server instance to send commands using RMI.
Username (only for Global Security enabled)	Type the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server. If, instead of typing the user ID, you want to retrieve the user ID from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.

Table 11. Fields for establishing Data Collector and application server communication (continued)

Field	What to do
Password (only for Global Security enabled)	Type the password that corresponds to the user specified in the **Username** field. If, instead of typing the password, you want to retrieve the password from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable communication to M
☑ Select Configuration Mode
☑ Select WebSphere Type
☑ Select WebSphere Profiles
□ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the server instance(s) you want to configure:

☑ Include configured server instance(s)

```
/opt/IBM/Portal6101/wp_profile
  cells
    ☑ rhel4
      nodes
        ☑ rhel4
          servers
            ☑ server1   Alias rhel4server1
            □ WebSphere_Portal   Alias portal
```

Enter the hostname and port for the application server or (for ND) the deployment manager. If WebSphere Global Security is enabled, enter the user name and password.

Hostname	rhel4u6.du
Connection Type	SOAP
Port	10005
Username	root
Password	*******

□ Use 'soap.client.props' or 'sas.client.props'

Figure 82. Configuring the Data Collector to monitor application server instances, window 10

Next to every selected instance, you can enter a server alias. This alias determines the name of the Tivoli Enterprise Portal node for this instance. Valid characters for the alias include A-z, a-z, 0-9, underbar (_), dash (-), and period (.); do not use other characters.

Important: if you have selected several application server profiles, the connection information (host name, port, connection type, and username/password) may be different for every profile. Select an instance in each profile and enter the information for the profile. Make sure that information is correct for every profile.

Check the boxes next to the instances that must be monitored by the Data Collector, complete the fields, and click **Next**.

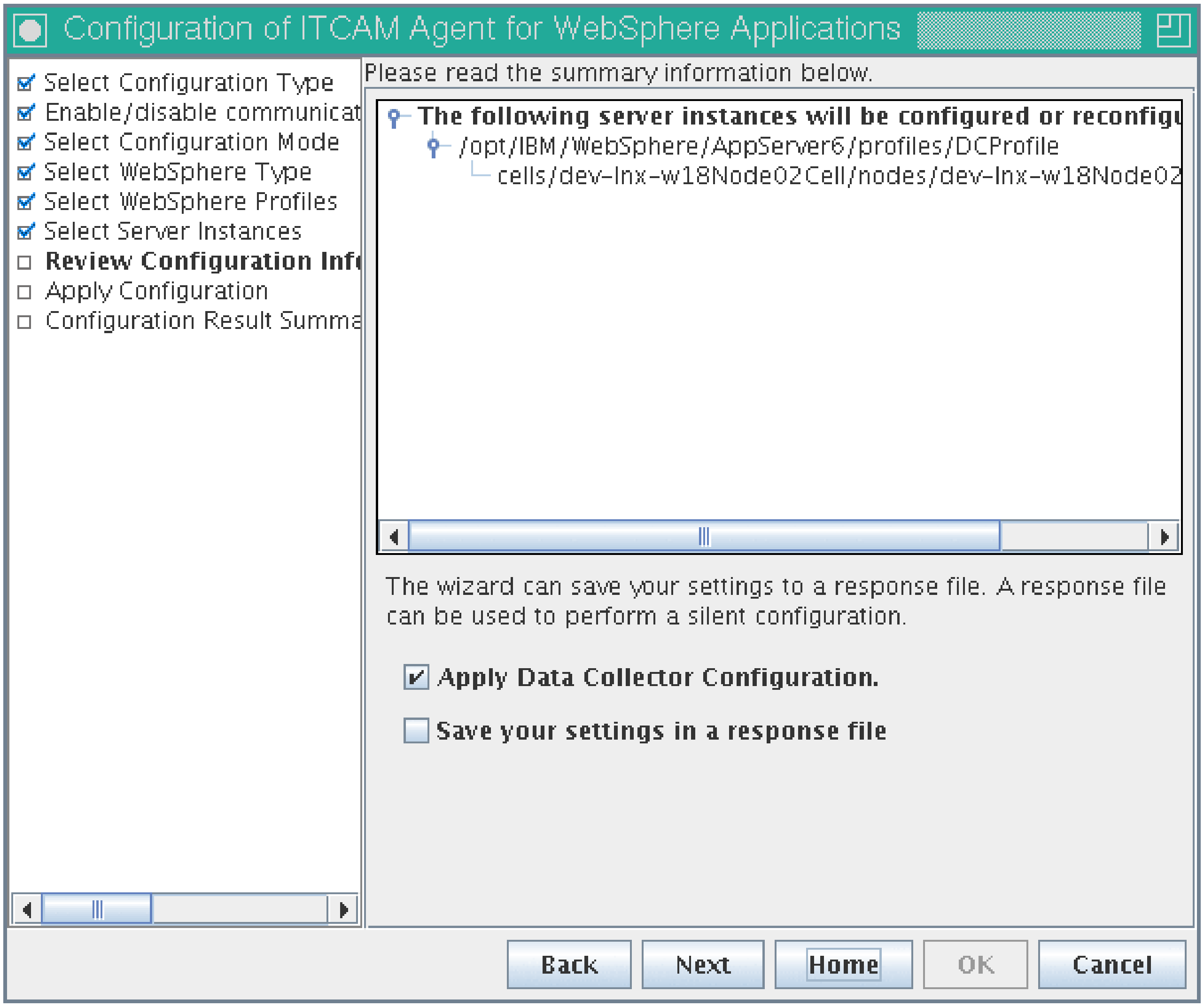
If the configuration utility is not able to communicate with any of the server instances, the selection window is displayed again, and the instances are highlighted in red. Select an instance highlighted in red to see the error message for it.

Important: If you have selected Custom configuration in Step 8 on page 146, the following additional windows will be displayed at this point:

- **Configure GC Log settings**: in this window, you can change the path and cycle settings for the Garbage Collection log for each application server instance. To change the log path, double click the **GC Log Path** table cell. To change the log cycle settings, double click the **GC Cycles** table cell.

  The **GC Cycles** setting is only supported if IBM Developer Kit for Java is used. The format of this setting is `x, y`; `x` and `y` are numbers. The logging will be performed to `x` files in rotation; information for `y` garbage collection cycles will be sent to one file before switching to the next file.
- **Configure Heap Size settings**: in this window, you can increase the maximum heap size for the application server instances. For best performance, increase the heap size for all instances; to do this, select the **Select All** box. You can increase the heap size for individual instances by selecting the **Increase JVM Max heap size setting** box in table rows.

12. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicat
☑ Select Configuration Mode
☑ Select WebSphere Type
☑ Select WebSphere Profiles
☑ Select Server Instances
□ Review Configuration Info
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Please read the summary information below.

```
The following server instances will be configured or reconfigu
  /opt/IBM/WebSphere/AppServer6/profiles/DCProfile
    cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02
```

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

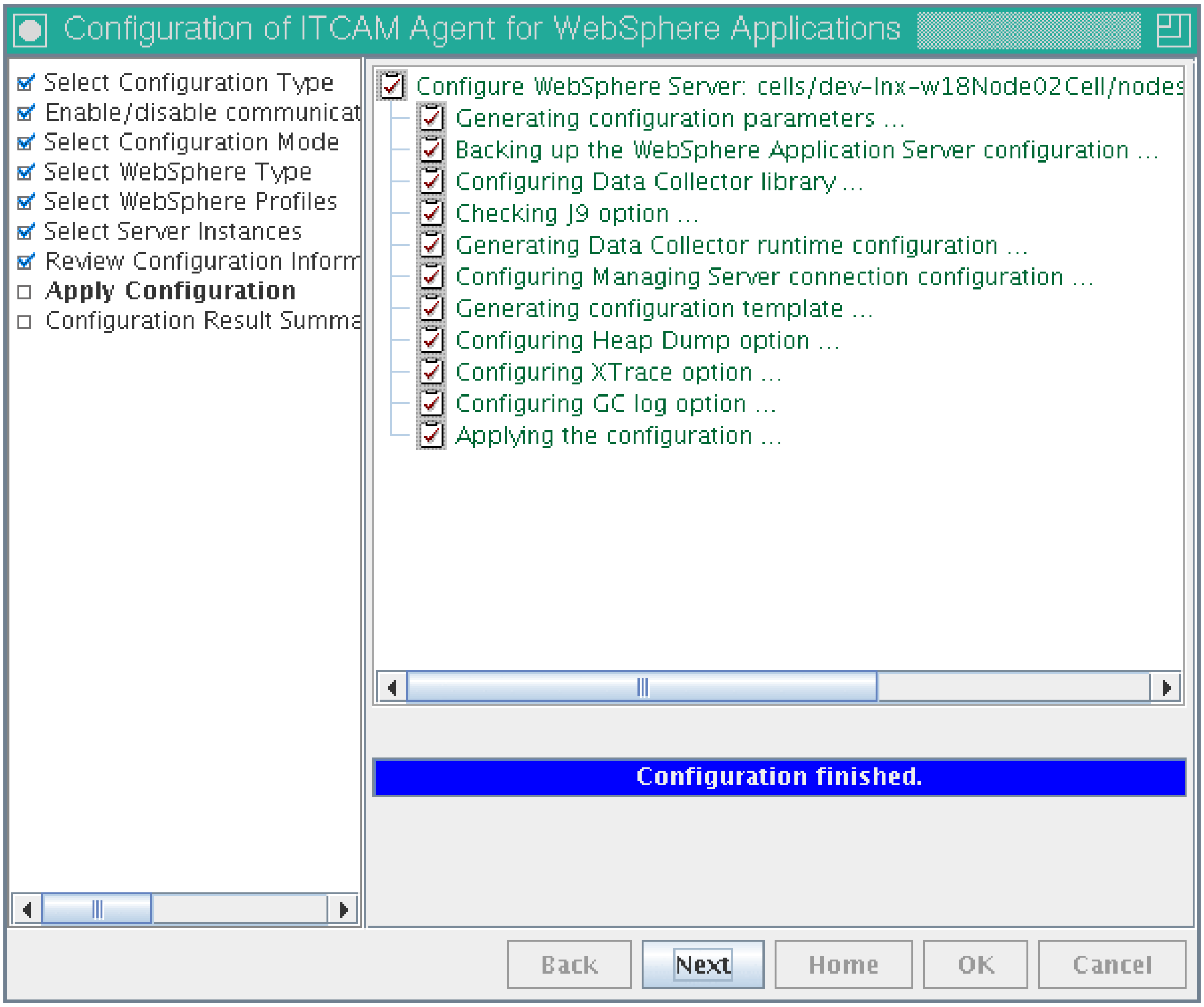
☑ **Apply Data Collector Configuration.**

□ **Save your settings in a response file**

Figure 83. Configuring Communication to the monitoring agent, window 11

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Data Collector Configuration**, the configuration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

13. The configuration utility validates the application server connection and applies the configuration.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Enable/disable communicat
☑ Select Configuration Mode
☑ Select WebSphere Type
☑ Select WebSphere Profiles
☑ Select Server Instances
☑ Review Configuration Inform
□ **Apply Configuration**
□ Configuration Result Summa

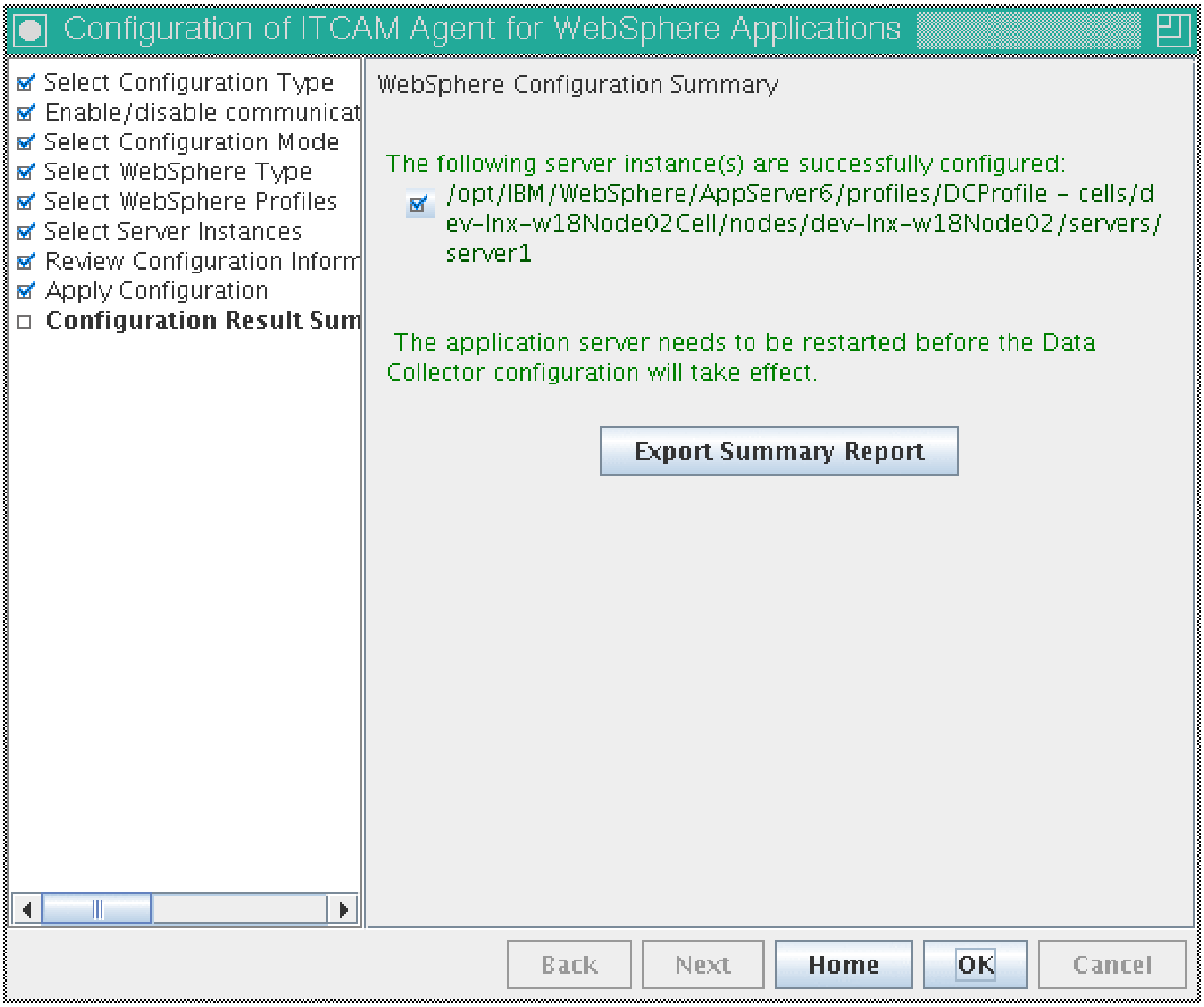
☑ Configure WebSphere Server: cells/dev-lnx-w18Node02Cell/nodes
- ☑ Generating configuration parameters ...
- ☑ Backing up the WebSphere Application Server configuration ...
- ☑ Configuring Data Collector library ...
- ☑ Checking J9 option ...
- ☑ Generating Data Collector runtime configuration ...
- ☑ Configuring Managing Server connection configuration ...
- ☑ Generating configuration template ...
- ☑ Configuring Heap Dump option ...
- ☑ Configuring XTrace option ...
- ☑ Configuring GC log option ...
- ☑ Applying the configuration ...

Configuration finished.

Figure 84. Configuring the Data Collector to monitor application server instances, window 12

Click **Next**

14. WebSphere configuration summary information is displayed.



☑ Select Configuration Type
☑ Enable/disable communicat
☑ Select Configuration Mode
☑ Select WebSphere Type
☑ Select WebSphere Profiles
☑ Select Server Instances
☑ Review Configuration Inform
☑ Apply Configuration
□ **Configuration Result Sum**

WebSphere Configuration Summary

The following server instance(s) are successfully configured:

☑ /opt/IBM/WebSphere/AppServer6/profiles/DCProfile - cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02/servers/server1

The application server needs to be restarted before the Data Collector configuration will take effect.

Figure 85. Configuring the Data Collector to monitor application server instances, window 13

To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window, or click **OK** to complete the configuration process.

15. If you click **OK**, the **TEMS Connection** window is displayed. If IBM Tivoli Monitoring is not used (in a deep dive only installation), make sure **No TEMS** is selected, and click **Save**. Otherwise click **Cancel** to close the window.

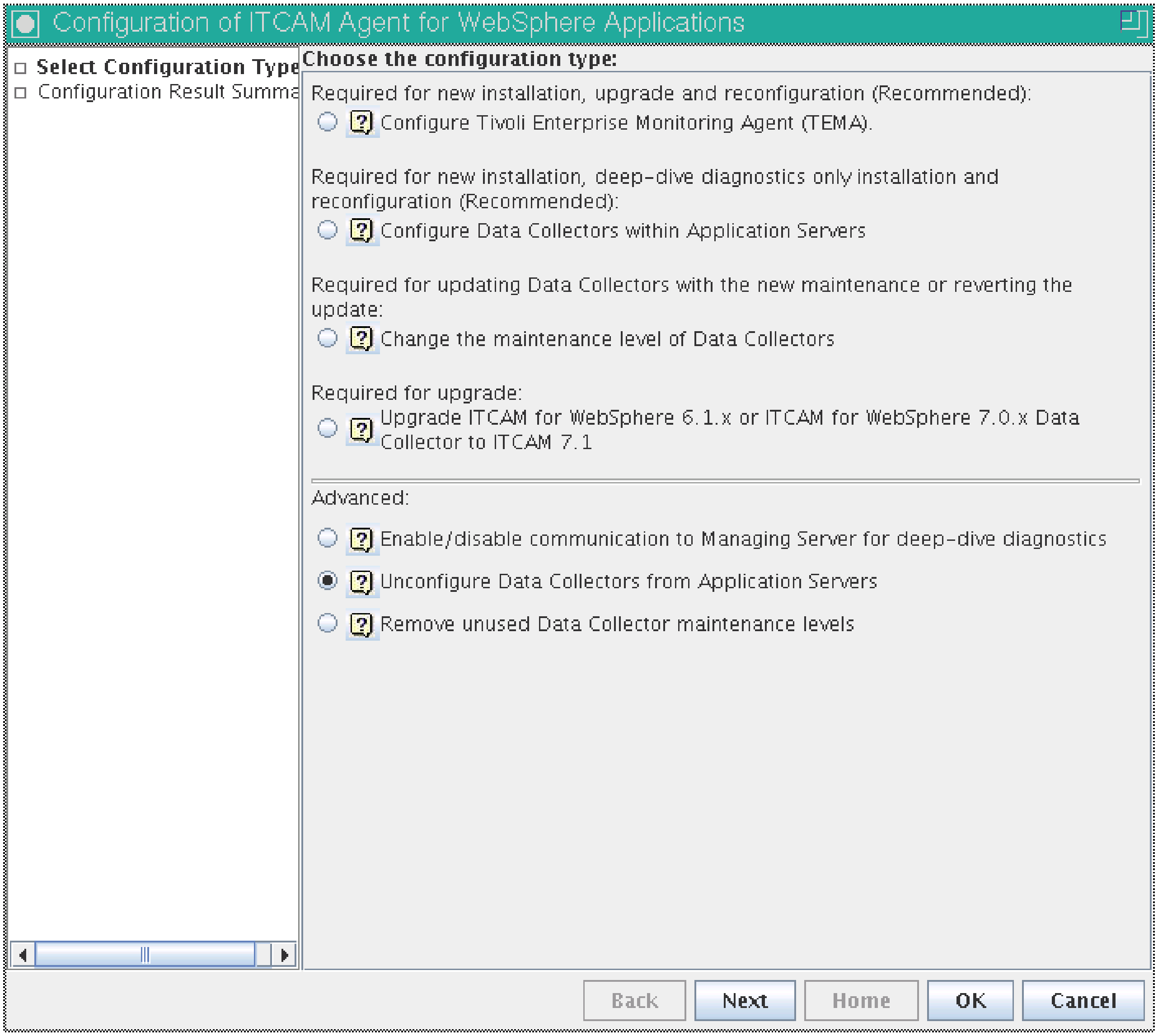
    Important: After configuring the Data Collector to monitor an application server instance, perform the applicable steps in “Additional steps for configuring the Data Collector on Linux and UNIX systems” on page 200, including a restart of the application server. The Data Collector configuration will take effect after the server is restarted.

Unconfigure the Data Collector for application server instances using GUI

If you no longer want the Data Collector to monitor an application server instance, you can unconfigure the Data Collector from it.

To do this, perform the following steps:

1. Enter the Agent Configuration window. See "Entering the Agent Configuration window" on page 133.


Configuration of ITCAM Agent for WebSphere Applications
□ Select Configuration Type
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

○ Enable/disable communication to Managing Server for deep-dive diagnostics

● Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 86. Unconfiguring the Data Collector for application server instances, window 1

2. Select **Unconfigure Data Collectors from Application Servers** and click **Next**.
3. Select the server instance(s) you want to unconfigure. All the instances monitored by this installation of the Agent are listed.

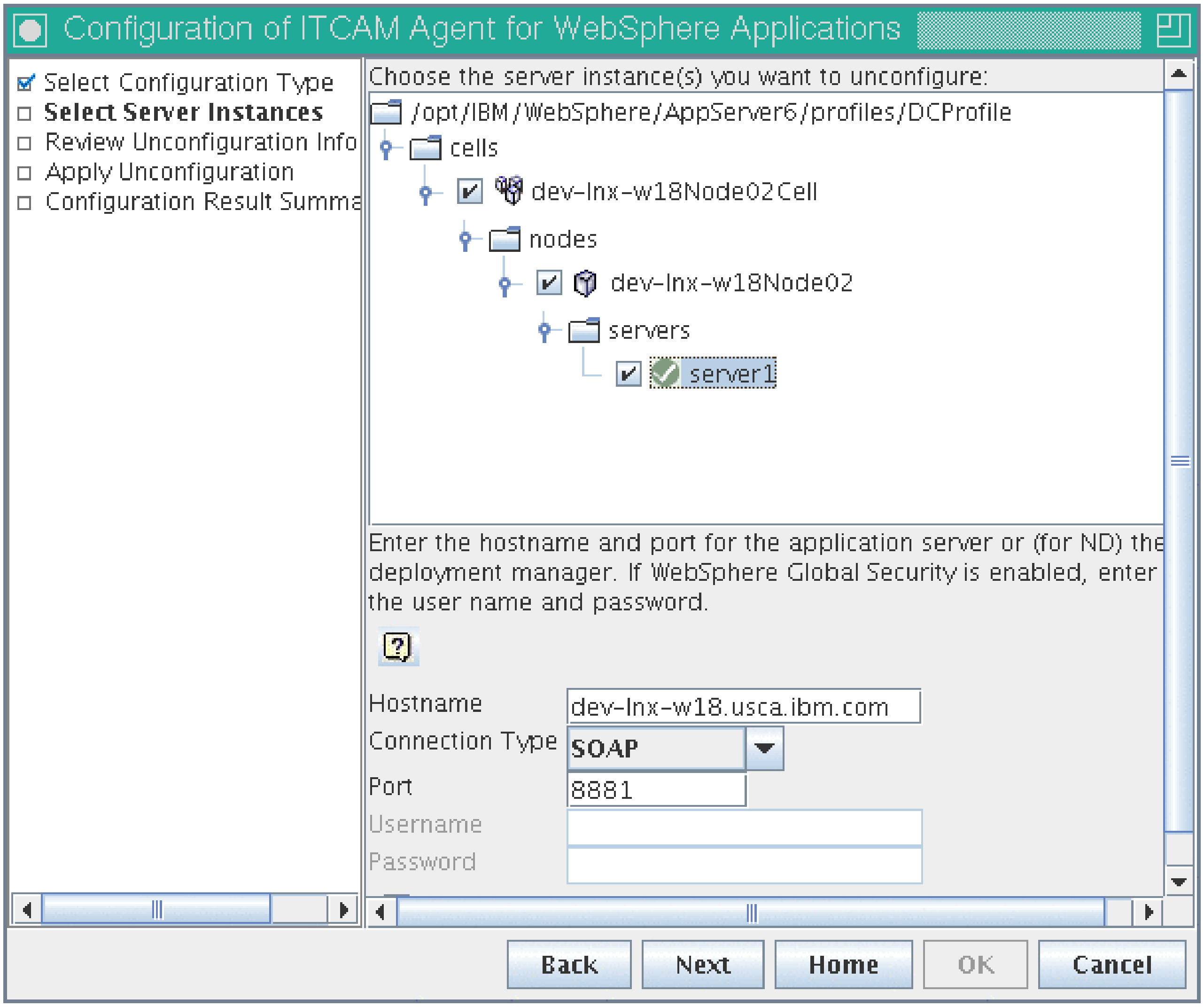
   Note:

   - Instance(s) must be running during the configuration.
   - For Network Deployment environment the Node Agent and Deployment Manager must also be running.

   You also need to set the connection parameters for the application server instances. By default, the information that was set during initial Data Collector configuration for each instance will be displayed (except username and password). The following table lists the fields:

Table 12. Fields for establishing Data Collector and application server communication

Field	What to do
Host Name	Type the fully qualified host name or IP address of the application server instance that the Data Collector monitors. Do not include a protocol in the host name. For example, type `myserver.ibm.tivoli.com`, not `https://myserver.ibm.tivoli.com`. Note: If using a Network Deployment environment, provide the host name of the Deployment Manager instead.
Connector Type	Select the type of connection the Data Collector and application server will use for communication.
Port	If you selected SOAP as the connector type, enter the connector port used by the application server instance to send commands using the Simple Object Access Protocol (SOAP). The SOAP port is identified in the `AppServer_home/profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml` file for the instance of application server that the Data Collector will monitor. **Note:** If using Network Deployment, provide the SOAP port of the Deployment Manager instead. If you selected RMI as the connector type, enter the connector port used by the application server instance to send commands using RMI.
Username (only for Global Security enabled)	Type the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server. If, instead of typing the user ID, you want to retrieve the user ID from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.
Password (only for Global Security enabled)	Type the password that corresponds to the user specified in the **Username** field. If, instead of typing the password, you want to retrieve the password from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ Select Server Instances
□ Review Unconfiguration Info
□ Apply Unconfiguration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the server instance(s) you want to unconfigure:

- /opt/IBM/WebSphere/AppServer6/profiles/DCProfile
  - cells
    - ☑ dev-lnx-w18Node02Cell
      - nodes
        - ☑ dev-lnx-w18Node02
          - servers
            - ☑ server1

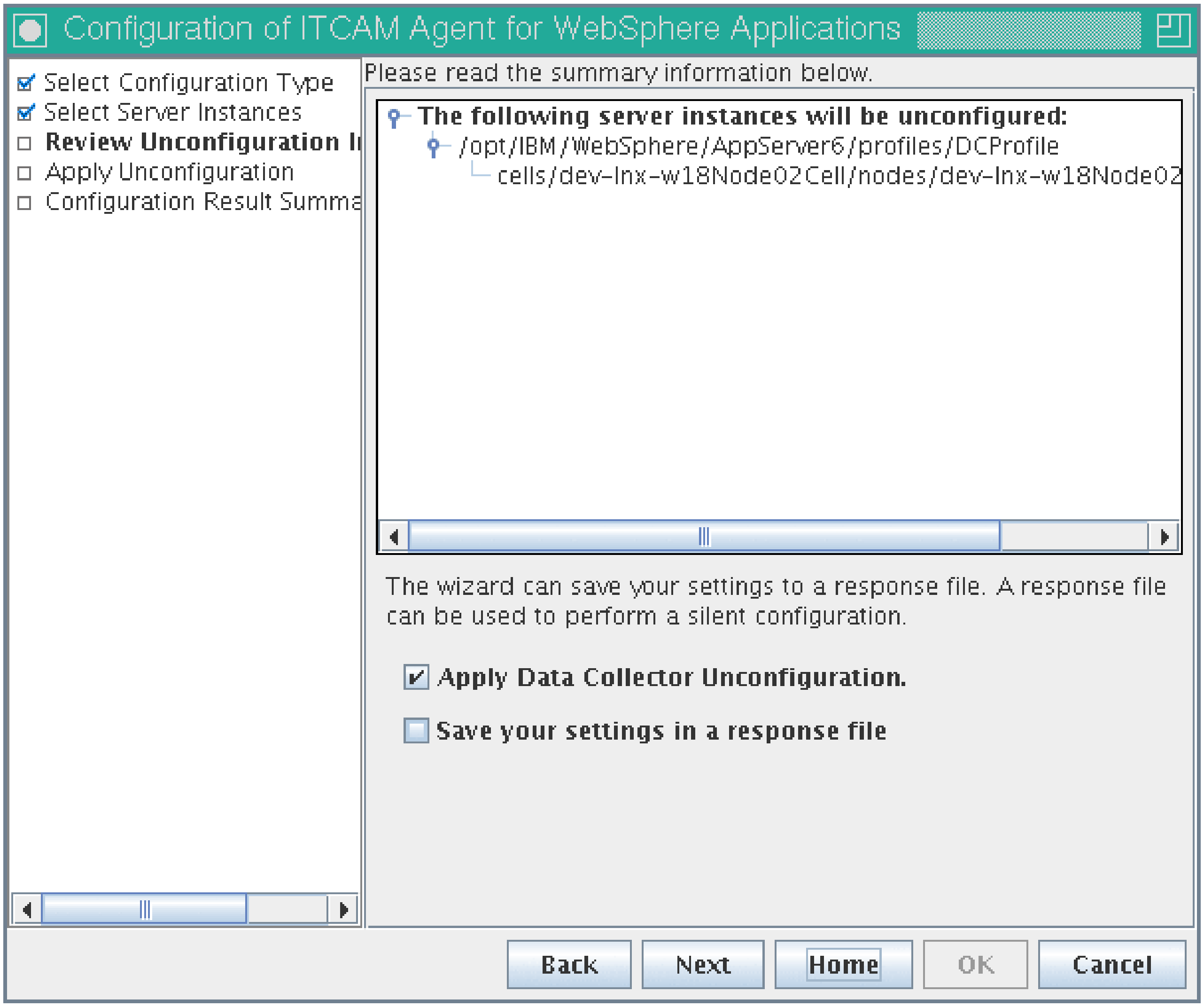
Enter the hostname and port for the application server or (for ND) the deployment manager. If WebSphere Global Security is enabled, enter the user name and password.

Hostname	dev-lnx-w18.usca.ibm.com
Connection Type	SOAP
Port	8881
Username	
Password	

Figure 87. Unconfiguring the Data Collector for application server instances, window 2

Check the boxes next to any instances you no longer want to monitor. Then, click **Next**.

4. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Select Server Instances
□ **Review Unconfiguration I**
□ Apply Unconfiguration
□ Configuration Result Summa

Please read the summary information below.

The following server instances will be unconfigured:
/opt/IBM/WebSphere/AppServer6/profiles/DCProfile
cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

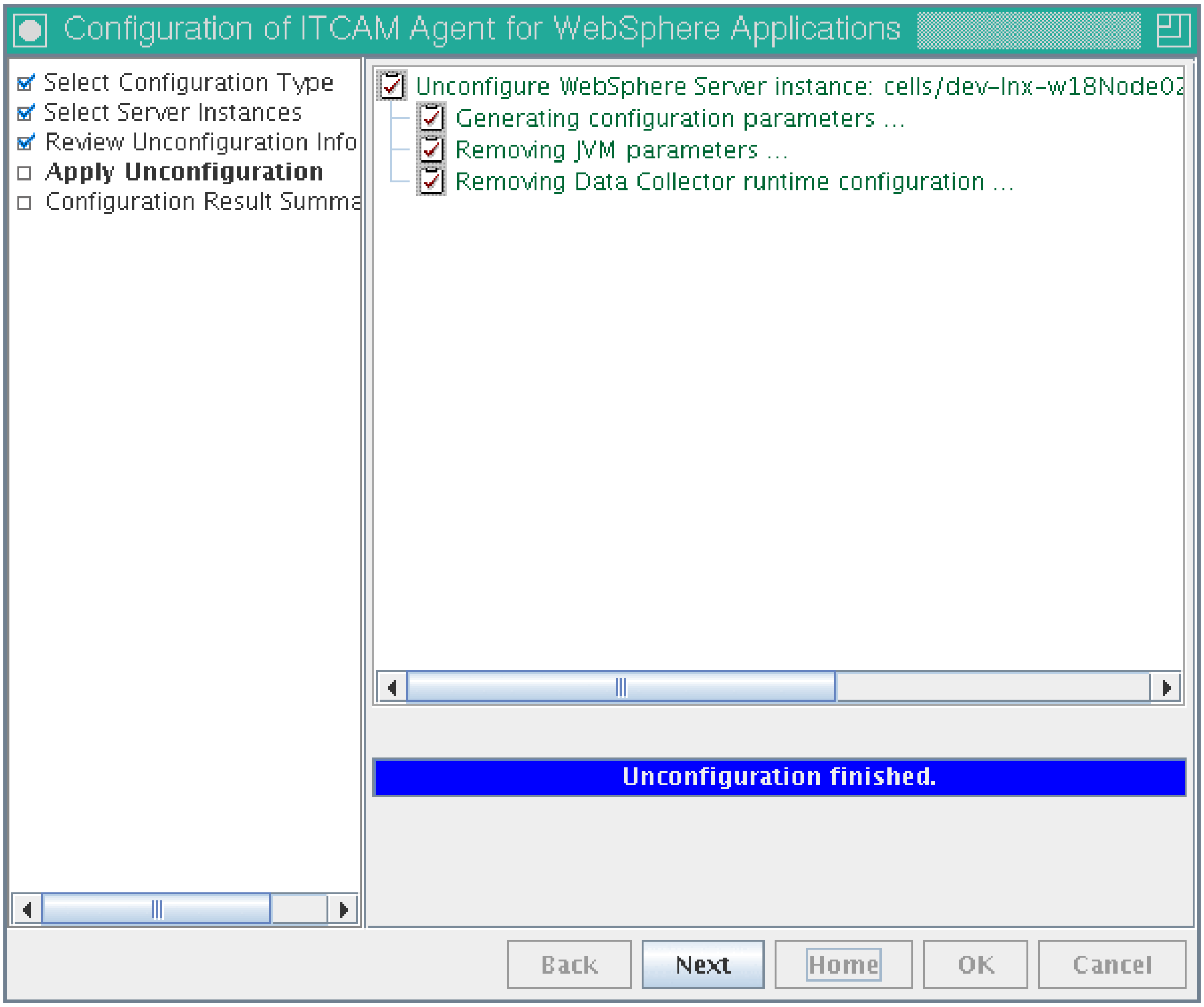
☑ **Apply Data Collector Unconfiguration.**

□ **Save your settings in a response file**

Figure 88. Unconfiguring the Data Collector for application server instances, window 3

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Data Collector Unconfiguration**, the unconfiguration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

5. The configuration utility will validate the applications server connection and apply the unconfiguration.



☑ Select Configuration Type
☑ Select Server Instances
☑ Review Unconfiguration Info
□ **Apply Unconfiguration**
□ Configuration Result Summa

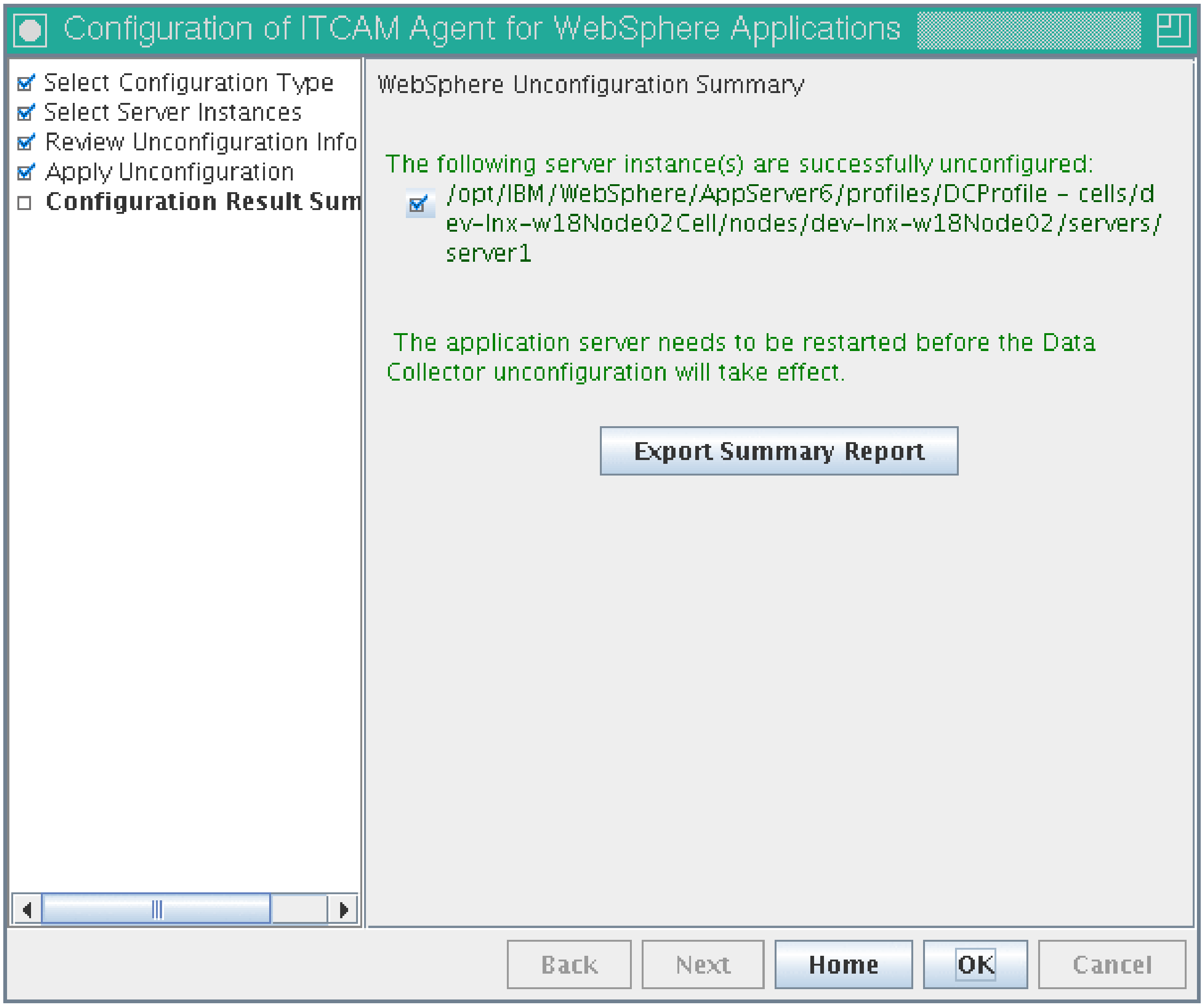
☑ Unconfigure WebSphere Server instance: cells/dev-lnx-w18Node02
- ☑ Generating configuration parameters ...
- ☑ Removing JVM parameters ...
- ☑ Removing Data Collector runtime configuration ...

Unconfiguration finished.

Figure 89. Unconfiguring the Data Collector for application server instances, window 4

Click **Next**.

6. WebSphere unconfiguration summary information is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Server Instances
☑ Review Unconfiguration Info
☑ Apply Unconfiguration
□ Configuration Result Sum
Export Summary Report
Back
Next
Home
OK
Cancel

WebSphere Unconfiguration Summary

The following server instance(s) are successfully unconfigured:

☑ /opt/IBM/WebSphere/AppServer6/profiles/DCProfile - cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02/servers/server1

The application server needs to be restarted before the Data Collector unconfiguration will take effect.

Figure 90. Unconfiguring the Data Collector for application server instances, window 5

To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window, or click **OK** to complete the configuration process. If you click **OK**, the **TEMS Connection** window is displayed. If IBM Tivoli Monitoring is not used (in a deep dive only installation), make sure **No TEMS** is selected, and click **Save**. Otherwise

Configure Data Collector communication with the Managing Server using GUI

If you have configured the Data Collector to monitor an application server instance, you may later change its configuration for communication with the ITCAM for Application Diagnostics Managing Server for this instance. You may also change Transaction Tracking integration configuration.

In this way, you may:

- If you have previously not configured it to communicate to the Managing Server, enable such communication.

- If it was already configured to communicate to the Managing Server, change the address or port number for the Managing Server kernel, or disable such communication.

You may perform such configuration on many configured application server instances at the same time.

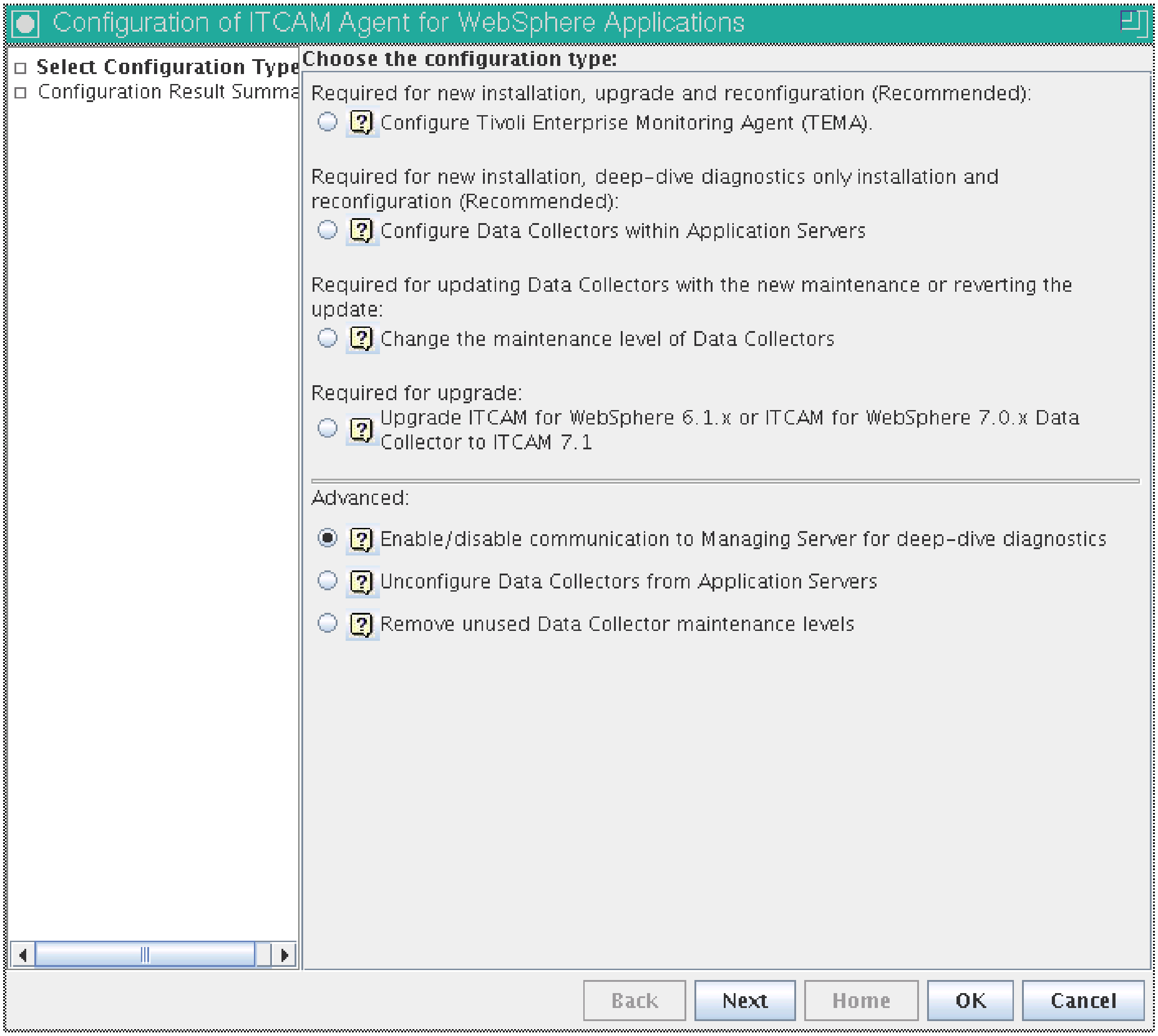
Note: If the Data Collector communicates to the Managing Server, you can also use the Visualization Engine to disable such communication (**Administration** > **Server Management** > **Data Collector Configuration**). See Table 13 for a comparison between these two ways of disabling Data Collector communication to the Managing Server:

Table 13. Comparison of ways to disable Data Collector communication to the Managing Server.

Disable Data Collector communication to the Managing Server using Data Collector configuration	Disable Data Collector communication to the Managing Server using the Visualization Engine
The application server instance is not listed in the Visualization Engine.	The application server instance remains listed in the Visualization Engine.
The Visualization Engine shows no information on the application server instance.	The Visualization Engine shows whether the application server instance is up or down; monitoring information is not available.
No system or network resources are used for Managing Server communication.	Some system and network resources are used to maintain Managing Server communication.
You do not need to apply maintenance fixes for the Agent that only impact Managing Server communication.	You need to apply maintenance fixes for the Agent that only impact Managing Server communication.
In order to re-enable communication, you need to perform Data Collector configuration again, and restart the application server.	In order to re-enable communication using the Visualization Engine, you do not need to restart the application server.

Complete the following steps to enable, disable, or configure Data Collector communication with the Managing Server:

1. Enter the Agent Configuration window. See “Entering the Agent Configuration window” on page 133.



Configuration of ITCAM Agent for WebSphere Applications

□ Select Configuration Type
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):
○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):
○ Configure Data Collectors within Application Servers

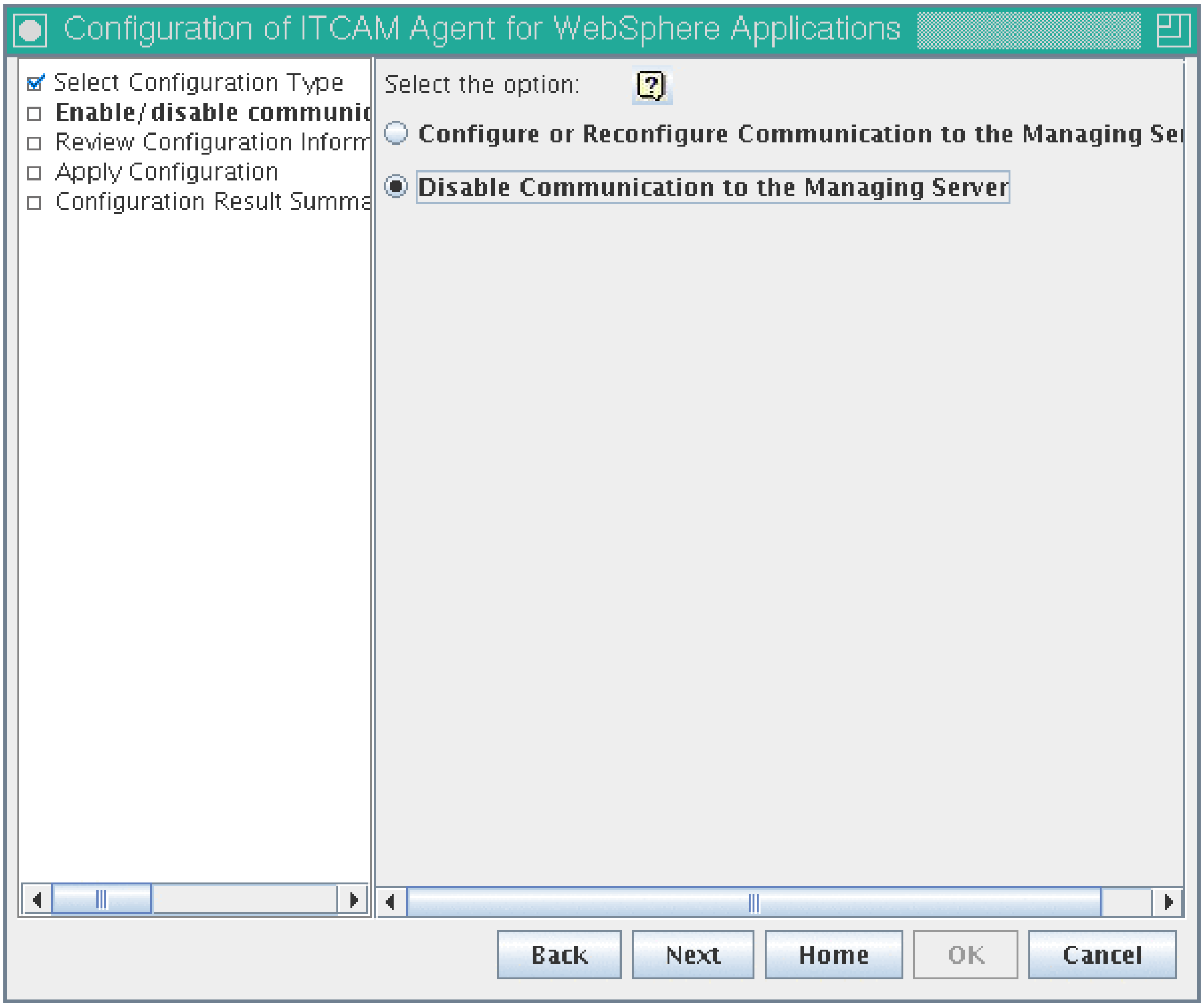
Required for updating Data Collectors with the new maintenance or reverting the update:
○ Change the maintenance level of Data Collectors

Required for upgrade:
○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:
● Enable/disable communication to Managing Server for deep-dive diagnostics
○ Unconfigure Data Collectors from Application Servers
○ Remove unused Data Collector maintenance levels

Figure 91. Configuring the Data Collector to monitor application server instances, window 1

2. Select **Enable/disable communication to Managing Server for deep-dive diagnostics** and click **Next**.
3. In the following window you must choose whether to enable or modify the Managing Server connection settings, or to disable communication with the Managing Server..


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ Enable/disable communic
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Select the option:

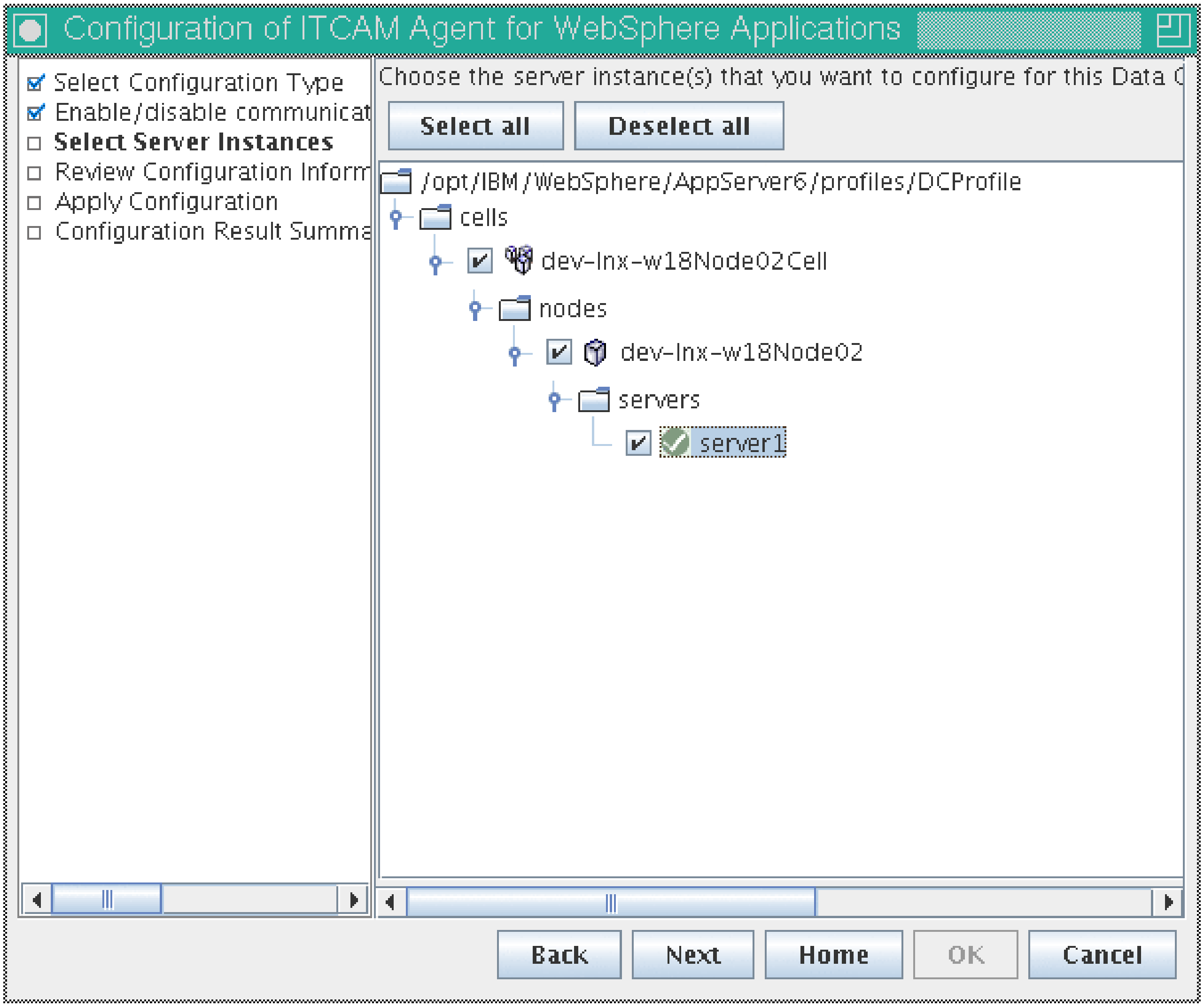
○ Configure or Reconfigure Communication to the Managing Se

● Disable Communication to the Managing Server

Figure 92. Configuring Data Collector communication with the Managing Server, window 2

If you wish to enable Managing Server communication that was previously not configured, or to change the address or port of the Managing Server, or to change Transaction Tracking integration configuration, select **Configure or Reconfigure communication to the Managing Server**. Click **Next**. Then, follow the procedure described in Steps 4 on page 142 to 7 on page 145 to set up the Managing Server and Transaction Tracking integration configuration details. Then, go to Step 6 on page 166.If you wish to disable communication with the Managing Server, select **Disable communication to the Managing Server** and click **Next**.

4. Select the server instances for which you want to disable Managing Server communication. All the instances monitored by this installation of the Agent are listed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicat
□ Select Server Instances
□ Review Configuration Inform
□ Apply Configuration
□ Configuration Result Summa
Select all
Deselect all
Back
Next
Home
OK
Cancel

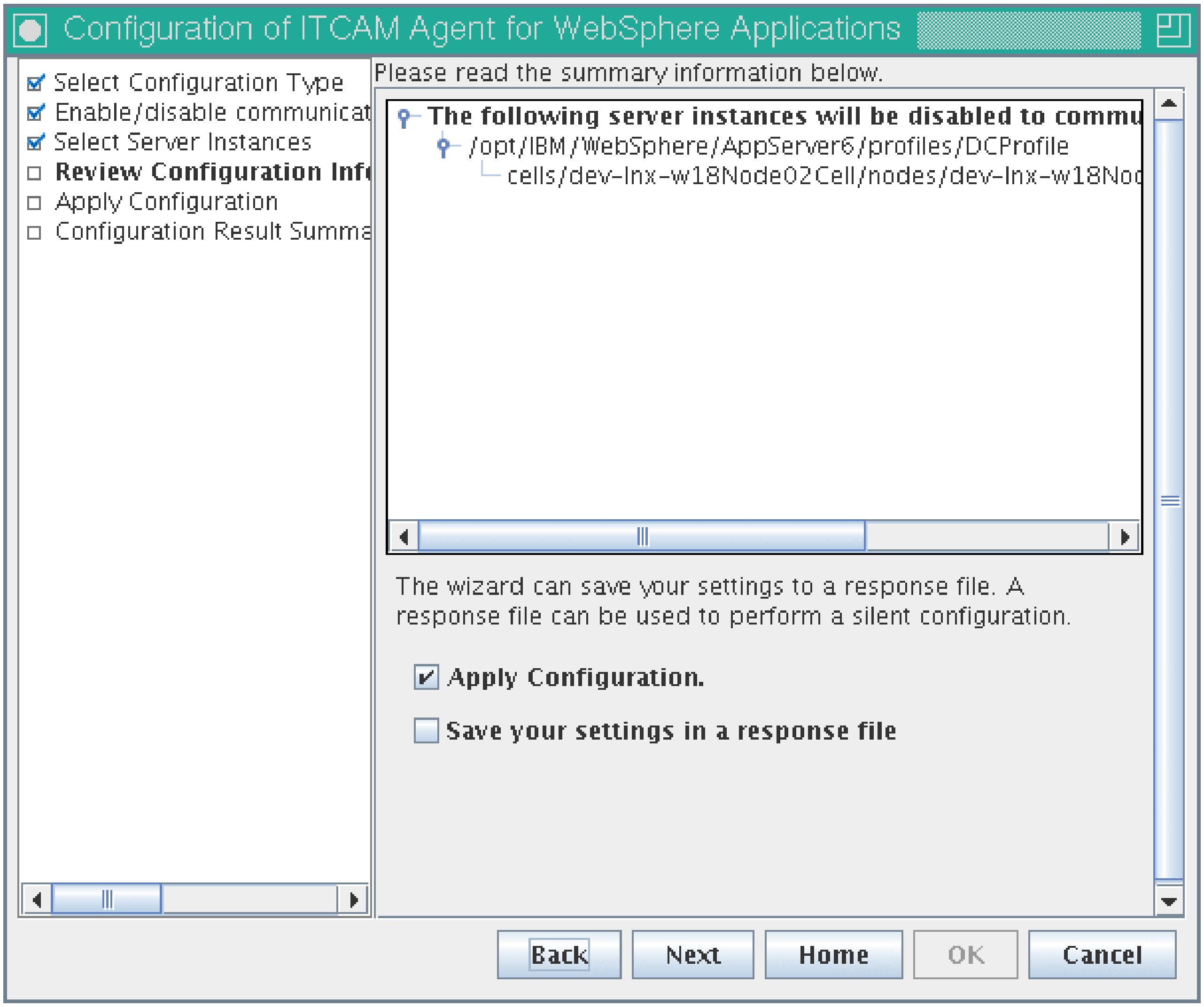
Choose the server instance(s) that you want to configure for this Data C

- /opt/IBM/WebSphere/AppServer6/profiles/DCProfile
  - cells
    - ☑ dev-lnx-w18Node02Cell
      - nodes
        - ☑ dev-lnx-w18Node02
          - servers
            - ☑ server1

Figure 93. Configuring Data Collector communication with the Managing Server, window 3

Check the boxes next to the instances that must no longer be monitored with the Managing Server, and click **Next**.

5. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Enable/disable communicat
☑ Select Server Instances
□ Review Configuration Info
□ Apply Configuration
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Please read the summary information below.

The following server instances will be disabled to commu
/opt/IBM/WebSphere/AppServer6/profiles/DCProfile
cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Noc

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

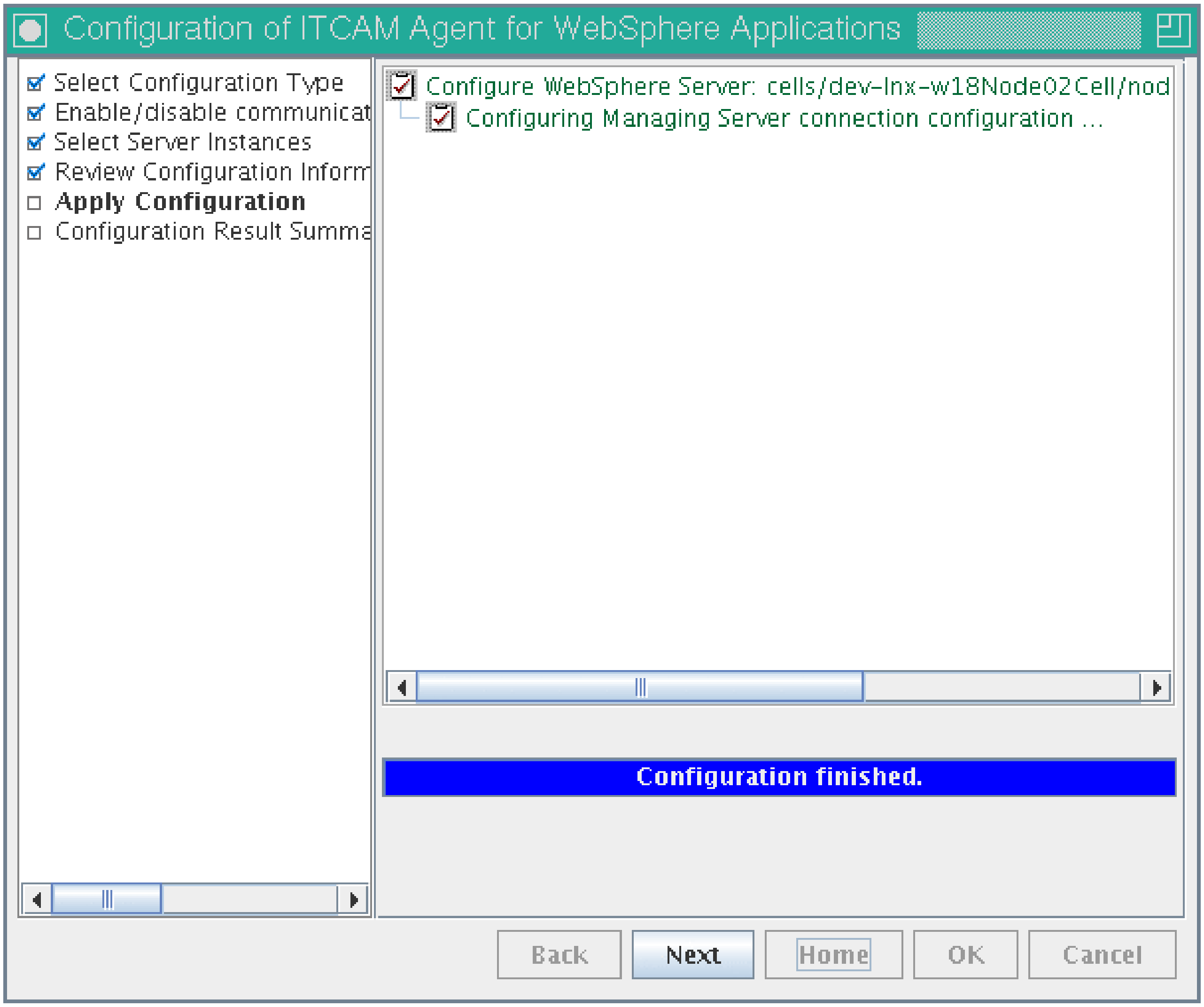
☑ Apply Configuration.

□ Save your settings in a response file

Figure 94. Configuring Data Collector communication with the Managing Server, window 4

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Configuration**, the new configuration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

6. A summary is displayed.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Enable/disable communicat
☑ Select Server Instances
☑ Review Configuration Inform
□ **Apply Configuration**
□ Configuration Result Summa

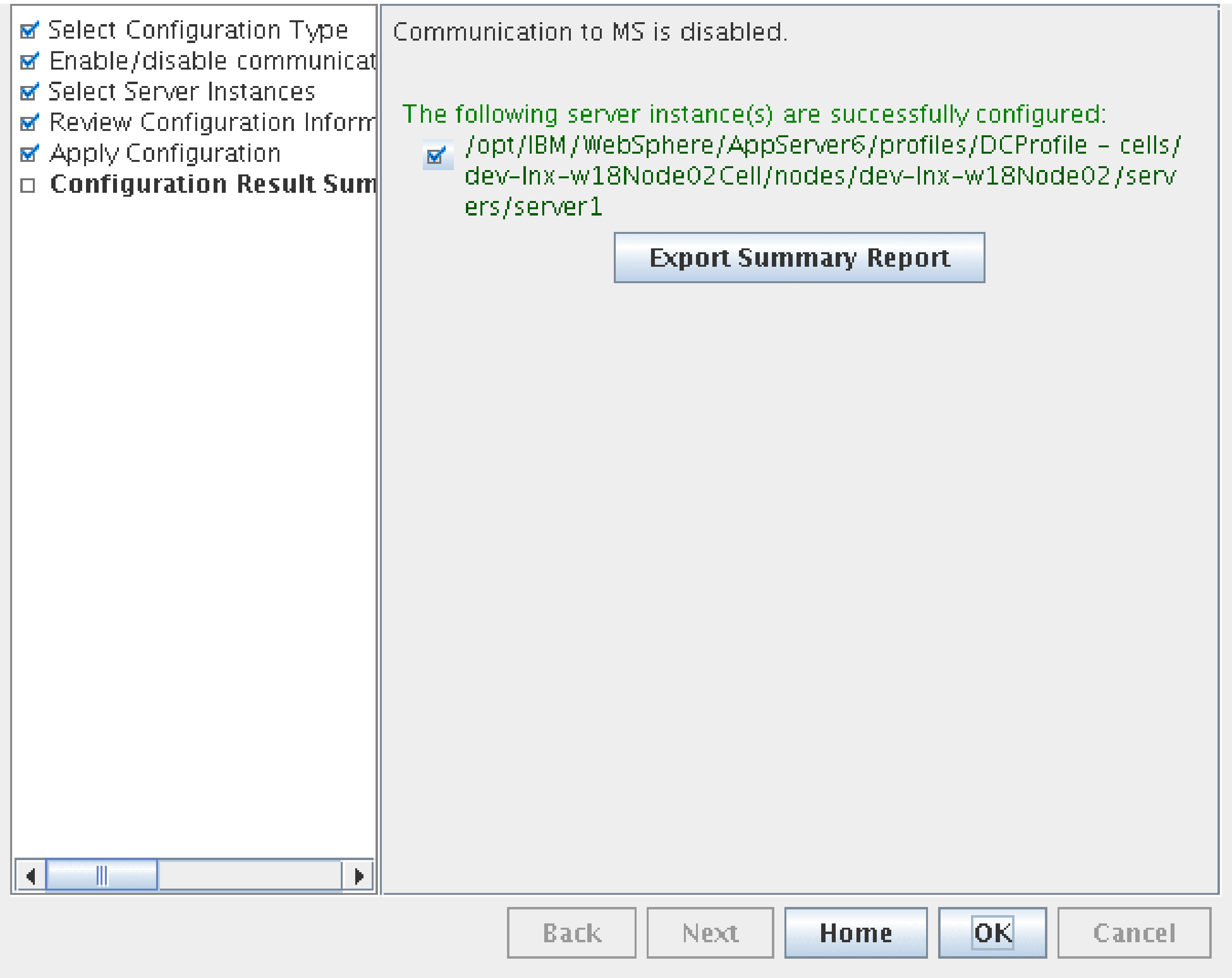
☑ Configure WebSphere Server: cells/dev-lnx-w18Node02Cell/nod
☑ Configuring Managing Server connection configuration ...

Configuration finished.

Figure 95. Configuring Data Collector communication with the Managing Server, window 5

Click **Next**.

7. A summary is displayed.


☑ Select Configuration Type
☑ Enable/disable communicat
☑ Select Server Instances
☑ Review Configuration Inform
☑ Apply Configuration
□ Configuration Result Sum
Export Summary Report
Back
Next
Home
OK
Cancel

Communication to MS is disabled.

The following server instance(s) are successfully configured:

☑ /opt/IBM/WebSphere/AppServer6/profiles/DCProfile - cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02/servers/server1

Figure 96. Configuring Data Collector communication with the Managing Server, window 5

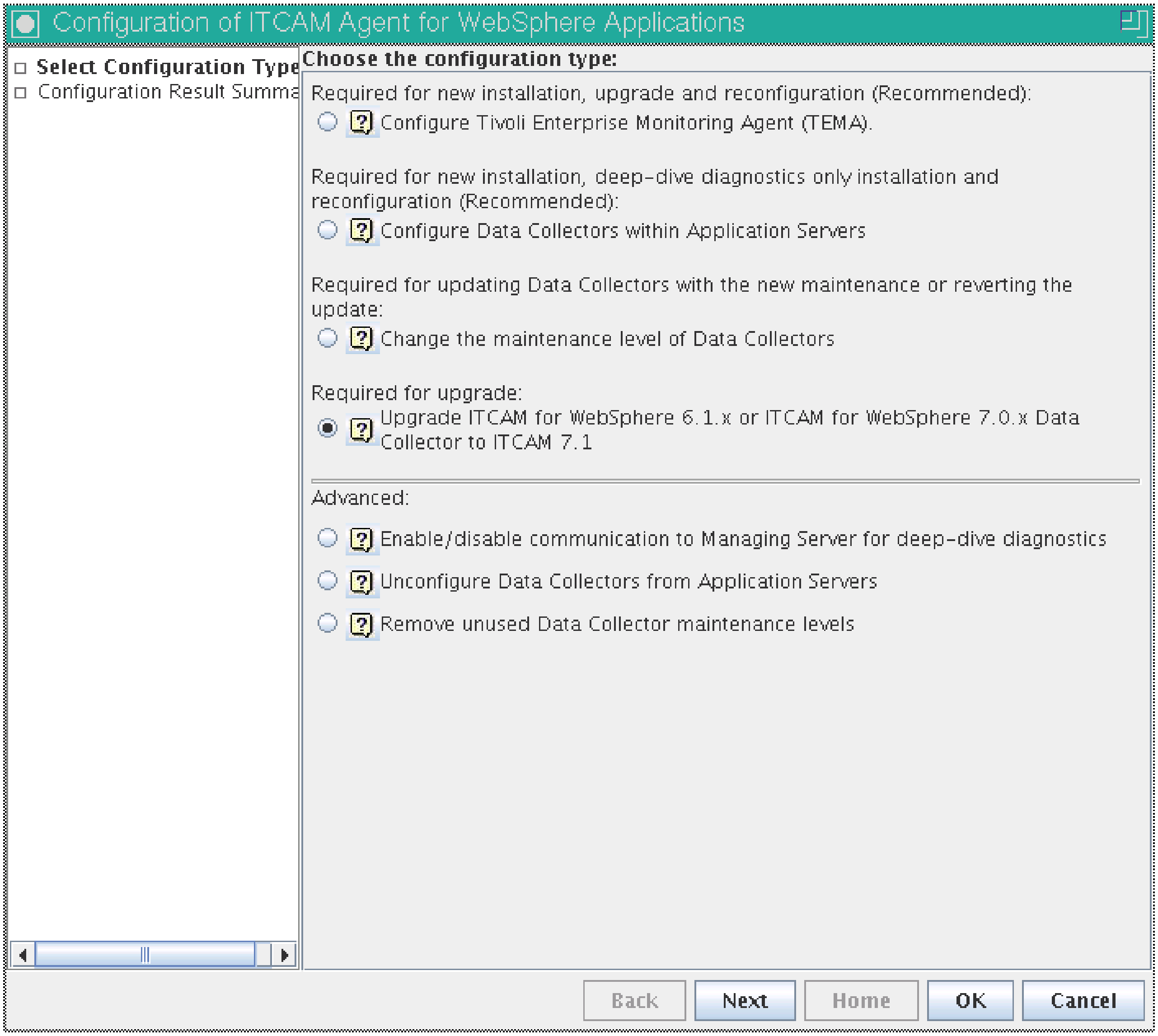
To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window, or click **OK** to complete the configuration process. If you click **OK**, the **TEMS Connection** window is displayed. If IBM Tivoli Monitoring is not used (in a deep dive only installation), make sure **No TEMS** is selected, and click **Save**. Otherwise click **Cancel** to close it.

Upgrading monitoring to Data Collector 7.1 using GUI

If an application server instance is monitored by a previous version of the Data Collector (from ITCAM for WebSphere 6.1, ITCAM for Web Resources 6.2, or ITCAM for WebSphere 7.0), you can upgrade monitoring to version 7.1.

To upgrade monitoring of server instances to Data Collector version 7.1, perform the following procedure:

1. Enter the Agent Configuration window. See “Entering the Agent Configuration window” on page 133.



Configuration of ITCAM Agent for WebSphere Applications

□ Select Configuration Type
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

● Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

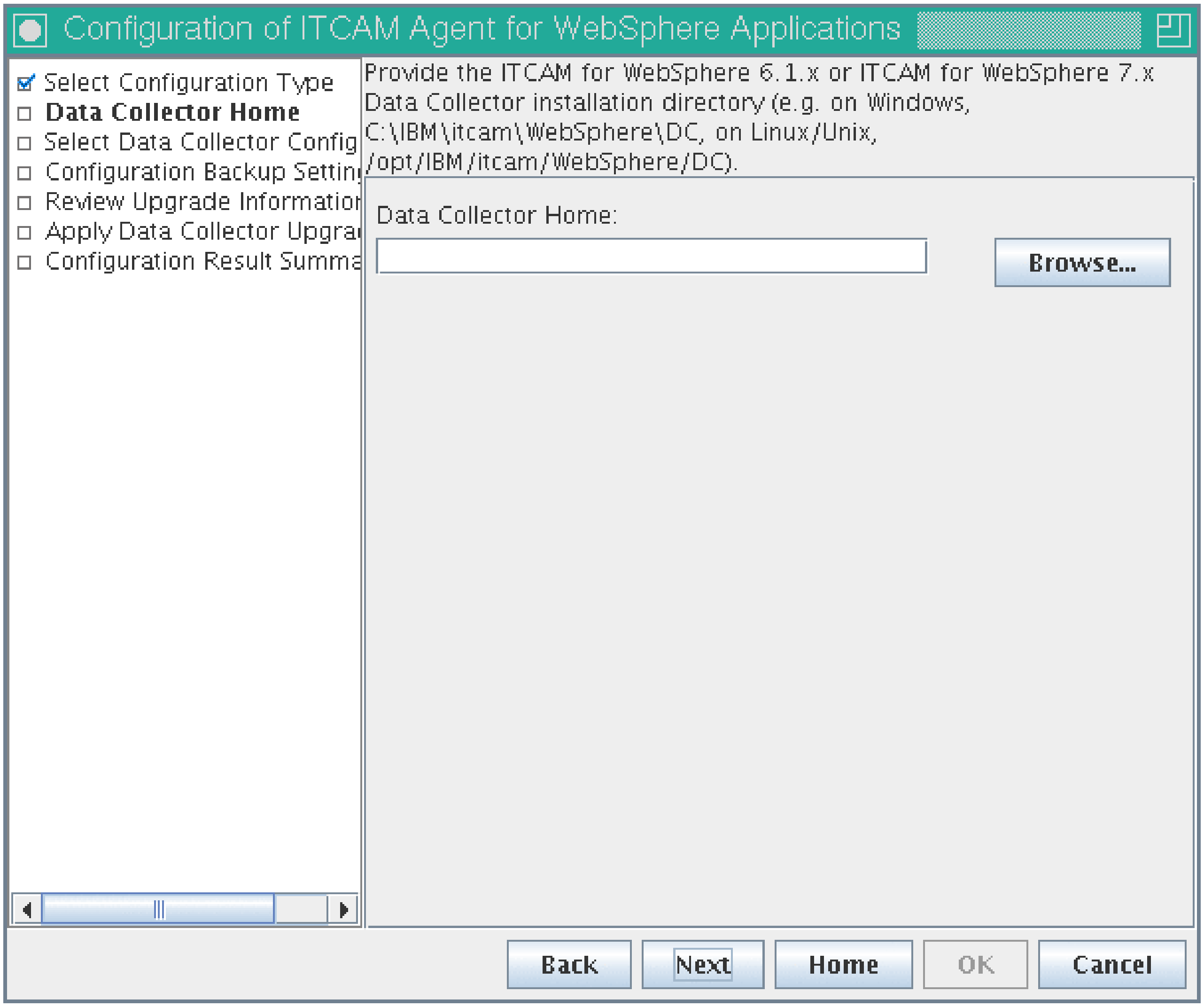
○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 97. Upgrading monitoring to Data Collector 7.1, window 1

2. Select **Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1** and click **Next**.
3. Set the home directory of the previous version of the Data Collector.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ Data Collector Home
□ Select Data Collector Config
□ Configuration Backup Settin
□ Review Upgrade Informatio
□ Apply Data Collector Upgra
□ Configuration Result Summa
Browse...
Back
Next
Home
OK
Cancel

Provide the ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.x Data Collector installation directory (e.g. on Windows, C:\IBM\itcam\WebSphere\DC, on Linux/Unix, /opt/IBM/itcam/WebSphere/DC).

Data Collector Home:

Figure 98. Upgrading monitoring to Data Collector 7.1, window 2

Enter the full path to the directory in which the older version of the Data Collector as installed. If it was configured with the default options, the path is `C:\IBM\itcam\WebSphere\DC`. Then, click **Next**.

4. Select the server instances you want to upgrade. All the instances monitored by this installation of the older Data Collector are listed.

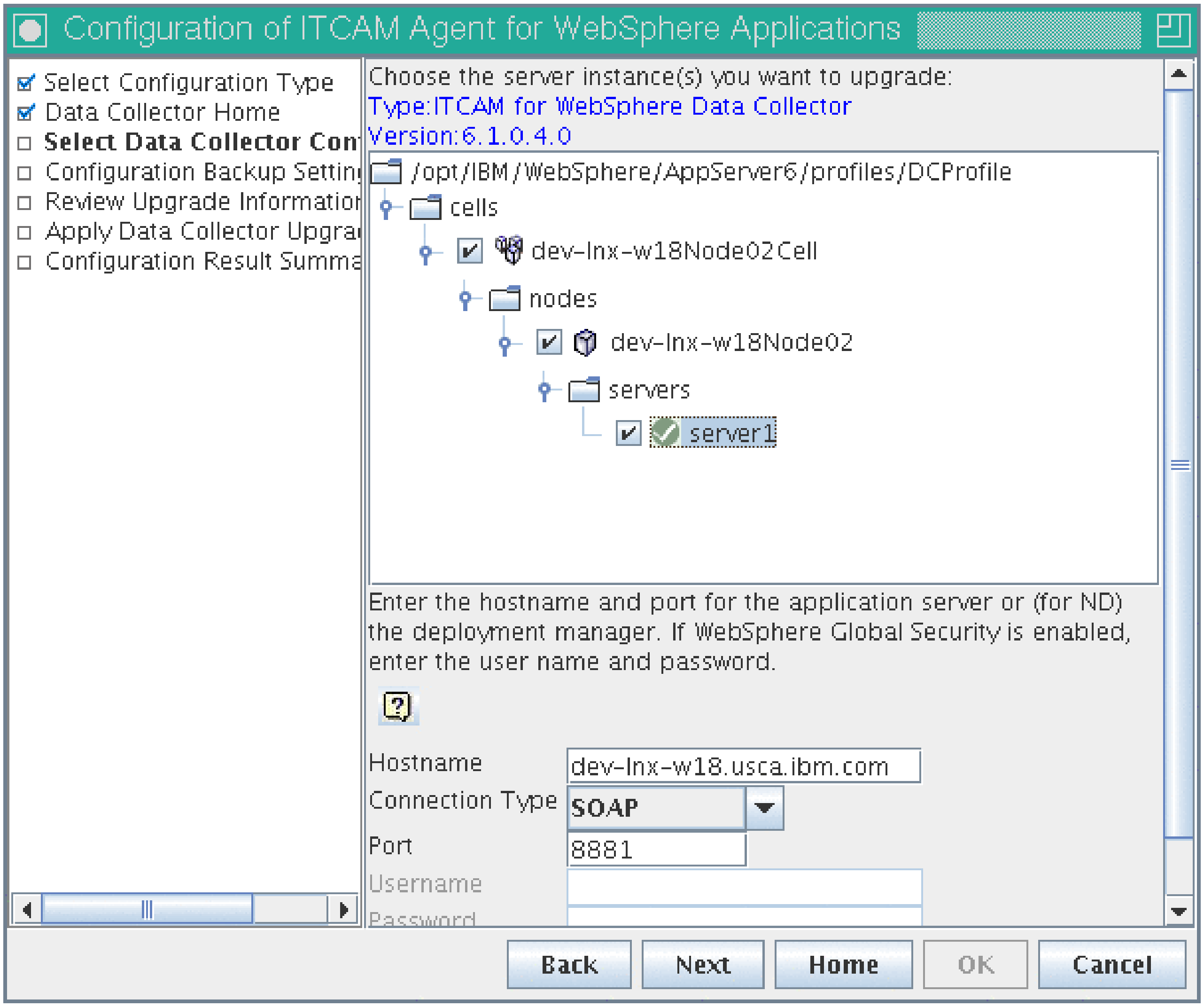
   Note:

   - For a stand alone environment, instances must be running during the configuration.
   - For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running.

   You also need to set the connection parameters for the application server instances. By default, the information that was set during initial Data Collector configuration for each instance will be displayed (except username and password). The following table lists the fields:

Table 14. Fields for establishing Data Collector and application server communication

Field	What to do
Host Name	Type the fully qualified host name or IP address of the application server instance that the Data Collector monitors. Do not include a protocol in the host name. For example, type `myserver.ibm.tivoli.com`, not `https://myserver.ibm.tivoli.com`. Note: If using a Network Deployment environment, provide the host name of the Deployment Manager instead.
Connector Type	Select the type of connection the Data Collector and application server will use for communication.
Port	If you selected SOAP as the connector type, enter the connector port used by the application server instance to send commands using the Simple Object Access Protocol (SOAP). The SOAP port is identified in the `AppServer_home/profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml` file for the instance of application server that the Data Collector will monitor. **Note:** If using Network Deployment, provide the SOAP port of the Deployment Manager instead. If you selected RMI as the connector type, enter the connector port used by the application server instance to send commands using RMI.
Username (only for Global Security enabled)	Type the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server. If, instead of typing the user ID, you want to retrieve the user ID from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.
Password (only for Global Security enabled)	Type the password that corresponds to the user specified in the **Username** field. If, instead of typing the password, you want to retrieve the password from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
□ Select Data Collector Con
□ Configuration Backup Settin
□ Review Upgrade Informatio
□ Apply Data Collector Upgra
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the server instance(s) you want to upgrade:

Type:ITCAM for WebSphere Data Collector

Version:6.1.0.4.0

- /opt/IBM/WebSphere/AppServer6/profiles/DCProfile
  - cells
    - ☑ dev-lnx-w18Node02Cell
      - nodes
        - ☑ dev-lnx-w18Node02
          - servers
            - ☑ server1

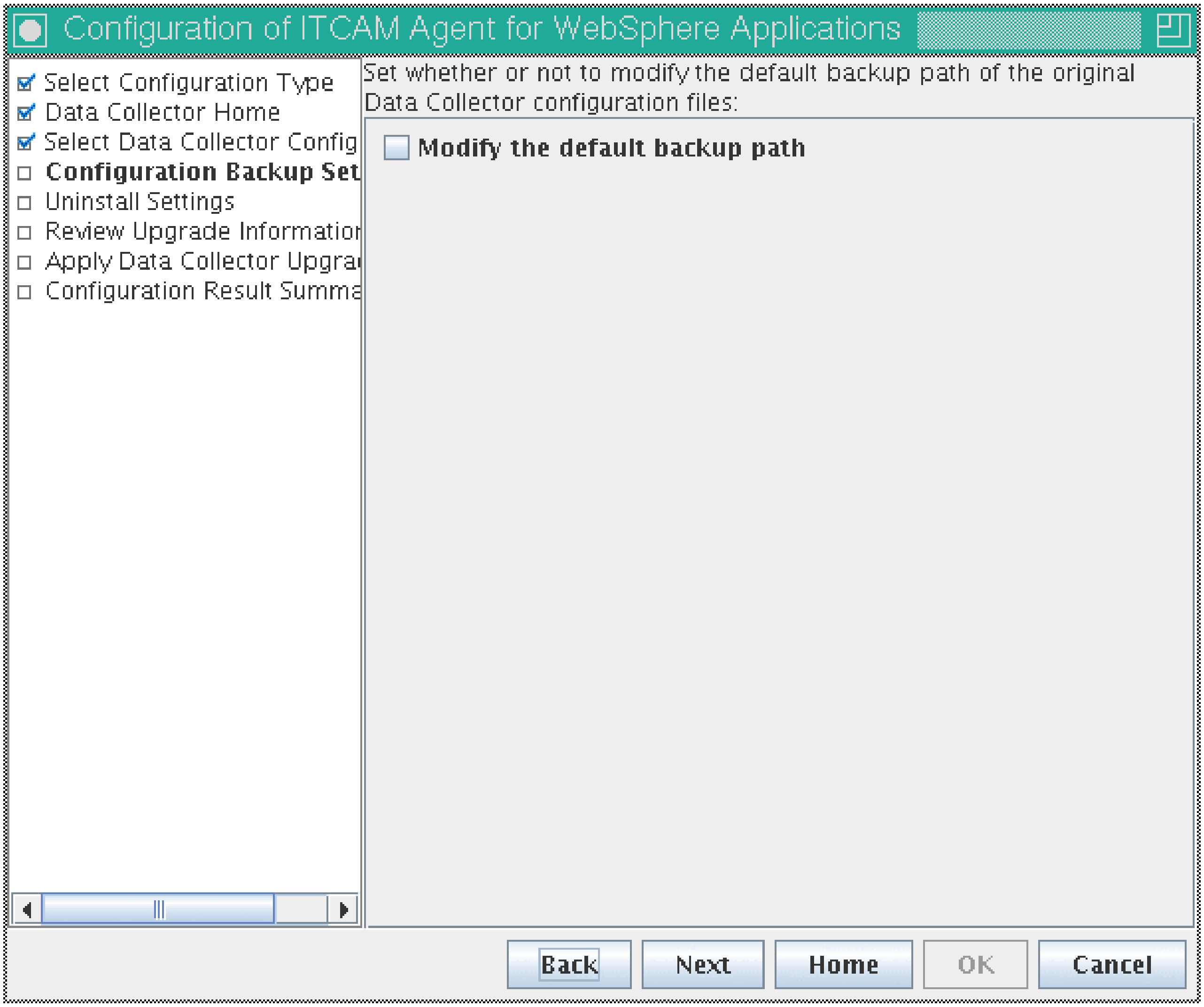
Enter the hostname and port for the application server or (for ND) the deployment manager. If WebSphere Global Security is enabled, enter the user name and password.

Hostname	dev-lnx-w18.usca.ibm.com
Connection Type	SOAP
Port	8881
Username	
Password	

Figure 99. Upgrading monitoring to Data Collector 7.1, window 3

Check the boxes next to the instances you want to configure. Then, click **Next**.

5. In the following window, choose whether you want to modify the path for backing up application server configuration files. Normally you do not need to change it.



Configuration of ITCAM Agent for WebSphere Applications

☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Config
□ **Configuration Backup Set**
□ Uninstall Settings
□ Review Upgrade Informatior
□ Apply Data Collector Upgra
□ Configuration Result Summa

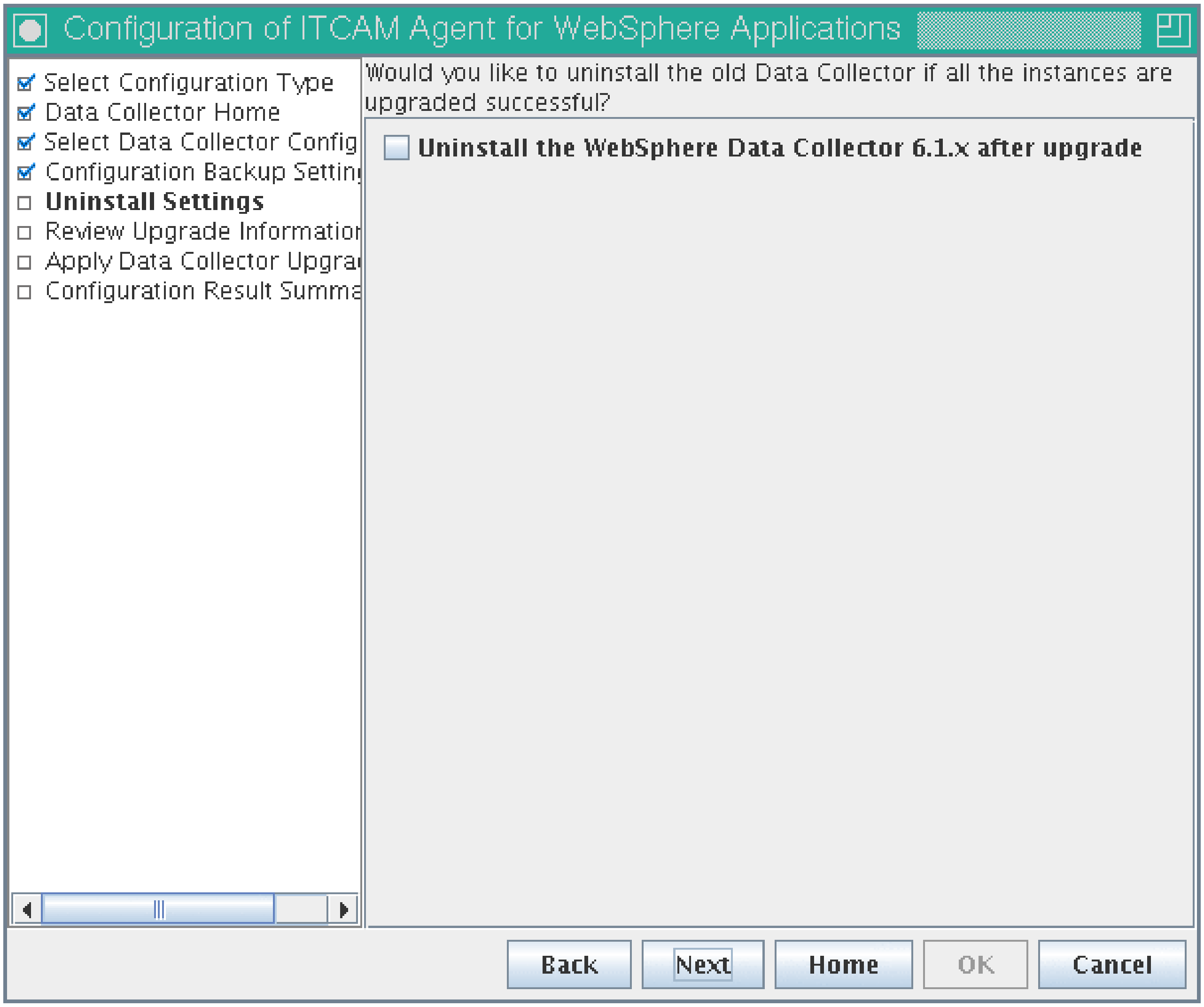
Set whether or not to modify the default backup path of the original Data Collector configuration files:

□ **Modify the default backup path**

Figure 100. Upgrading monitoring to Data Collector 7.1, window 4

If you wish to change the backup path, check the box and click **Browse** to set the new path.Click **Next**.

6. In the following window, choose whether you want to uninstall the old Data Collector after upgrading the instances. If you are upgrading all application server instances monitored by the older Data Collector on this host, you may choose to perform the uninstallation. If there are instances you are not upgrading, unconfigure the old Data Collector for them using its own configuration utility before uninstalling it. There is no requirement to uninstall the old Data Collector.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Config
☑ Configuration Backup Settin
□ Uninstall Settings
□ Review Upgrade Informatio
□ Apply Data Collector Upgra
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

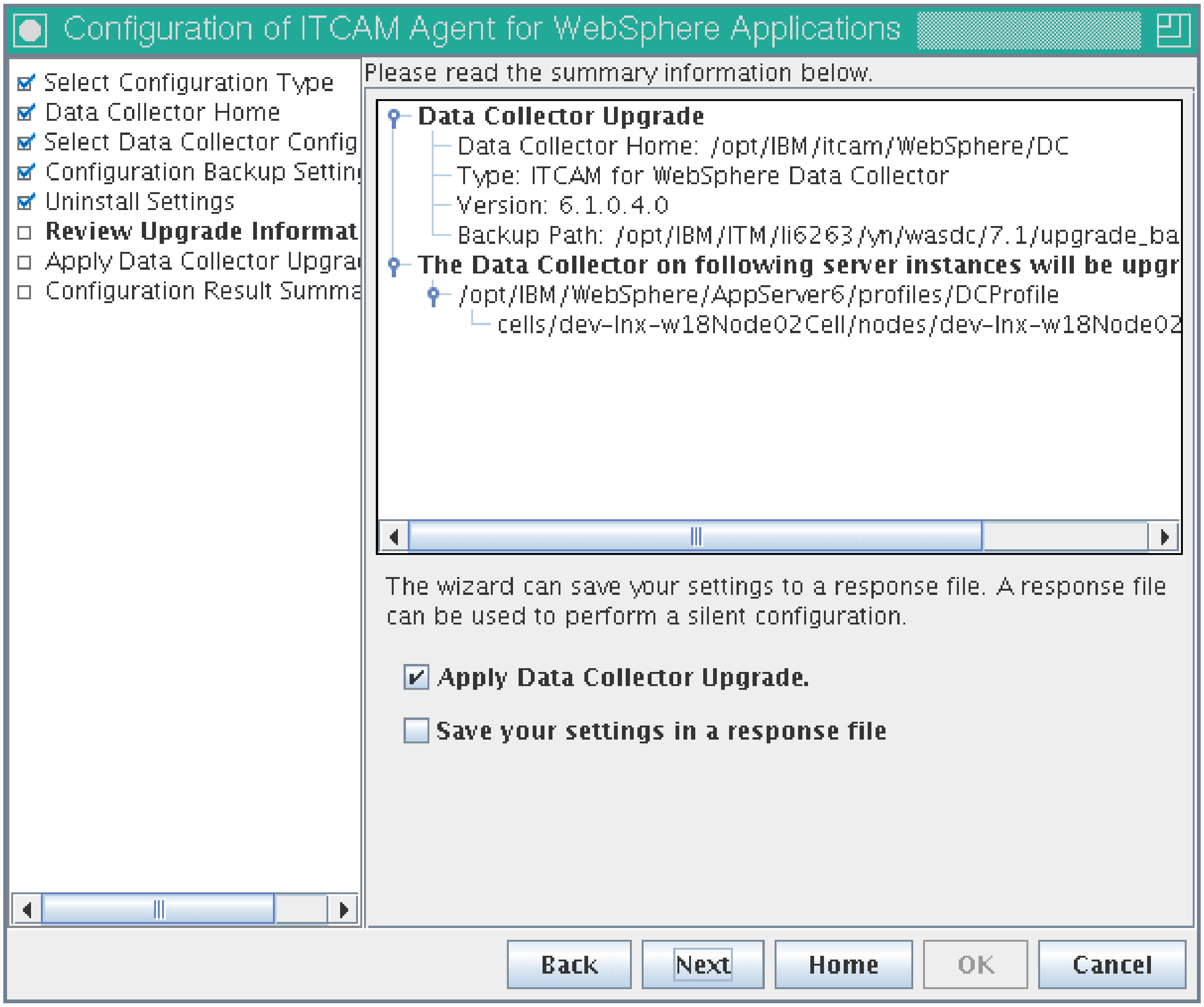
Would you like to uninstall the old Data Collector if all the instances are upgraded successful?

□ Uninstall the WebSphere Data Collector 6.1.x after upgrade

Figure 101. Upgrading monitoring to Data Collector 7.1, window 5

If you wish to uninstall the old Data Collector, check the box.Click **Next**.

7. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.



☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Config
☑ Configuration Backup Settin
☑ Uninstall Settings
□ **Review Upgrade Informat**
□ Apply Data Collector Upgra
□ Configuration Result Summa

Please read the summary information below.

Data Collector Upgrade
Data Collector Home: /opt/IBM/itcam/WebSphere/DC
Type: ITCAM for WebSphere Data Collector
Version: 6.1.0.4.0
Backup Path: /opt/IBM/ITM/li6263/yn/wasdc/7.1/upgrade_ba
The Data Collector on following server instances will be upgr
/opt/IBM/WebSphere/AppServer6/profiles/DCProfile
cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

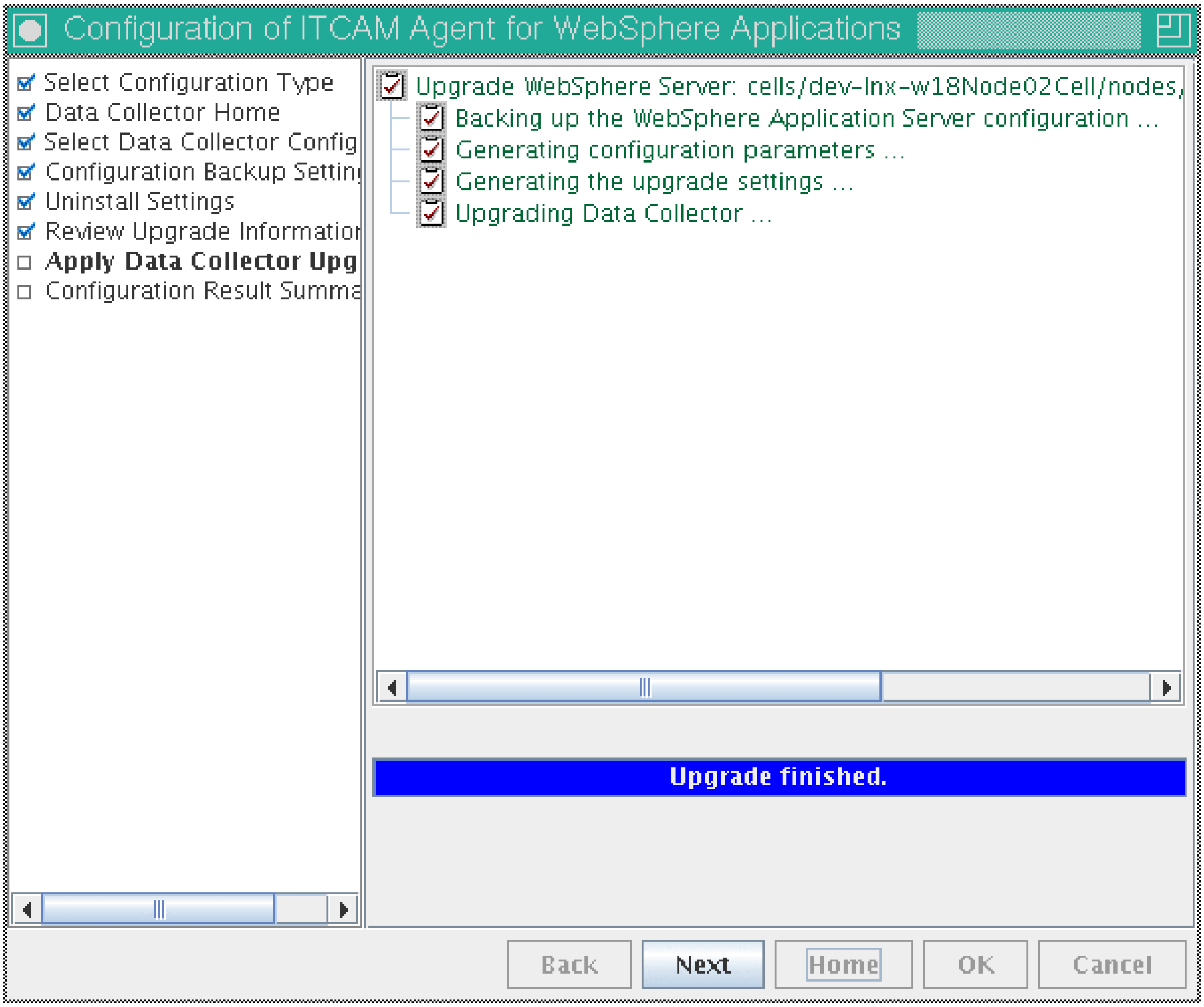
☑ **Apply Data Collector Upgrade.**

□ **Save your settings in a response file**

Figure 102. Upgrading monitoring to Data Collector 7.1, window 6

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Data Collector Upgrade**, the upgrade will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

8. The configuration utility will validate the applications server connection and apply the upgrade.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Config
☑ Configuration Backup Settin
☑ Uninstall Settings
☑ Review Upgrade Informatior
□ Apply Data Collector Upg
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

☑ Upgrade WebSphere Server: cells/dev-lnx-w18Node02Cell/nodes/

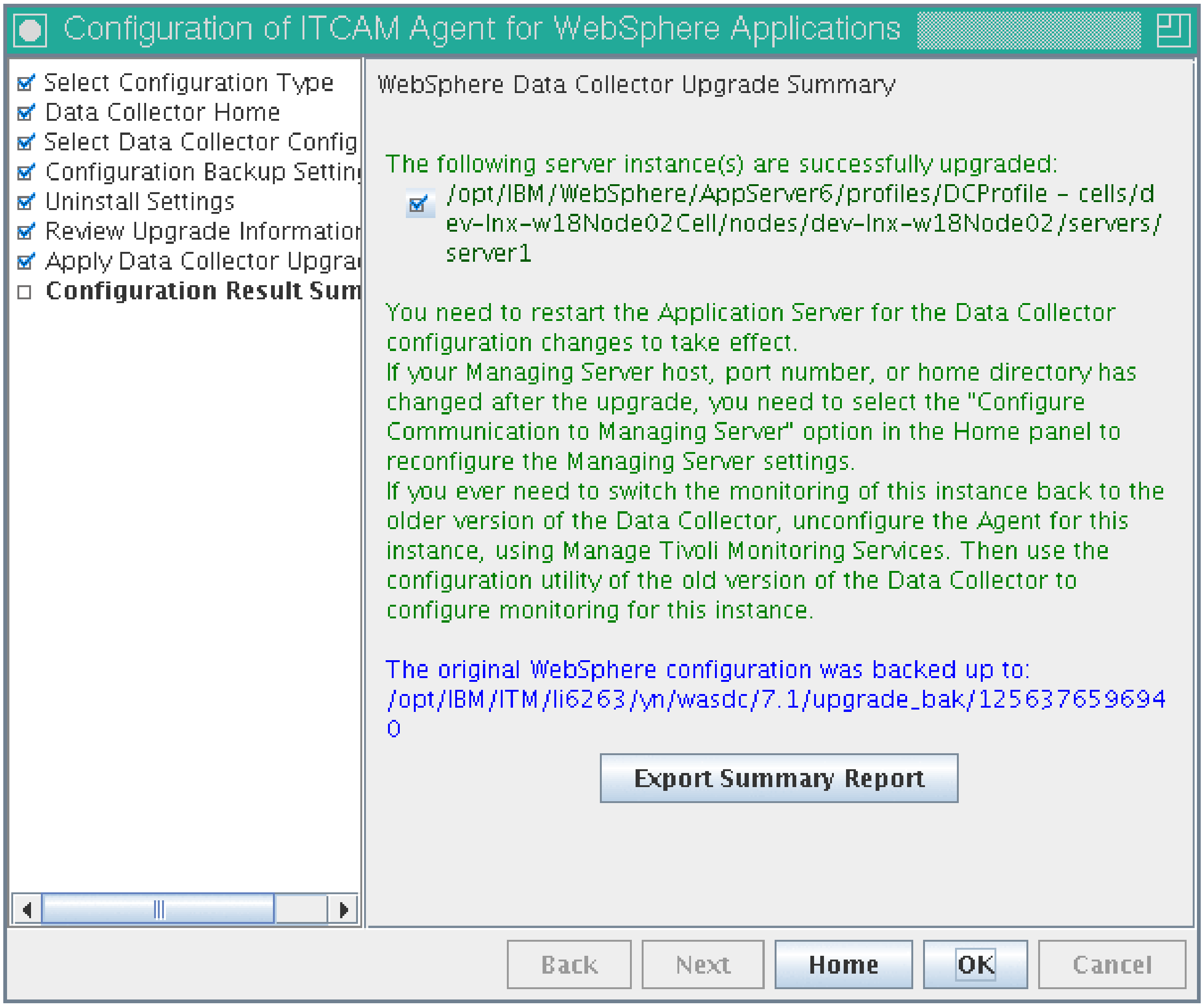
- ☑ Backing up the WebSphere Application Server configuration ...
- ☑ Generating configuration parameters ...
- ☑ Generating the upgrade settings ...
- ☑ Upgrading Data Collector ...

Upgrade finished.

Figure 103. Upgrading monitoring to Data Collector 7.1, window 7

Click **Next**.

9. WebSphere unconfiguration summary information is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Data Collector Home
☑ Select Data Collector Config
☑ Configuration Backup Settin
☑ Uninstall Settings
☑ Review Upgrade Informatio
☑ Apply Data Collector Upgra
□ Configuration Result Sum
Export Summary Report
Back
Next
Home
OK
Cancel

WebSphere Data Collector Upgrade Summary

The following server instance(s) are successfully upgraded:

☑ /opt/IBM/WebSphere/AppServer6/profiles/DCProfile - cells/dev-lnx-w18Node02Cell/nodes/dev-lnx-w18Node02/servers/server1

You need to restart the Application Server for the Data Collector configuration changes to take effect.
If your Managing Server host, port number, or home directory has changed after the upgrade, you need to select the "Configure Communication to Managing Server" option in the Home panel to reconfigure the Managing Server settings.
If you ever need to switch the monitoring of this instance back to the older version of the Data Collector, unconfigure the Agent for this instance, using Manage Tivoli Monitoring Services. Then use the configuration utility of the old version of the Data Collector to configure monitoring for this instance.

The original WebSphere configuration was backed up to:
/opt/IBM/ITM/li6263/yn/wasdc/7.1/upgrade_bak/1256376596940

Figure 104. Upgrading monitoring to Data Collector 7.1, window 8

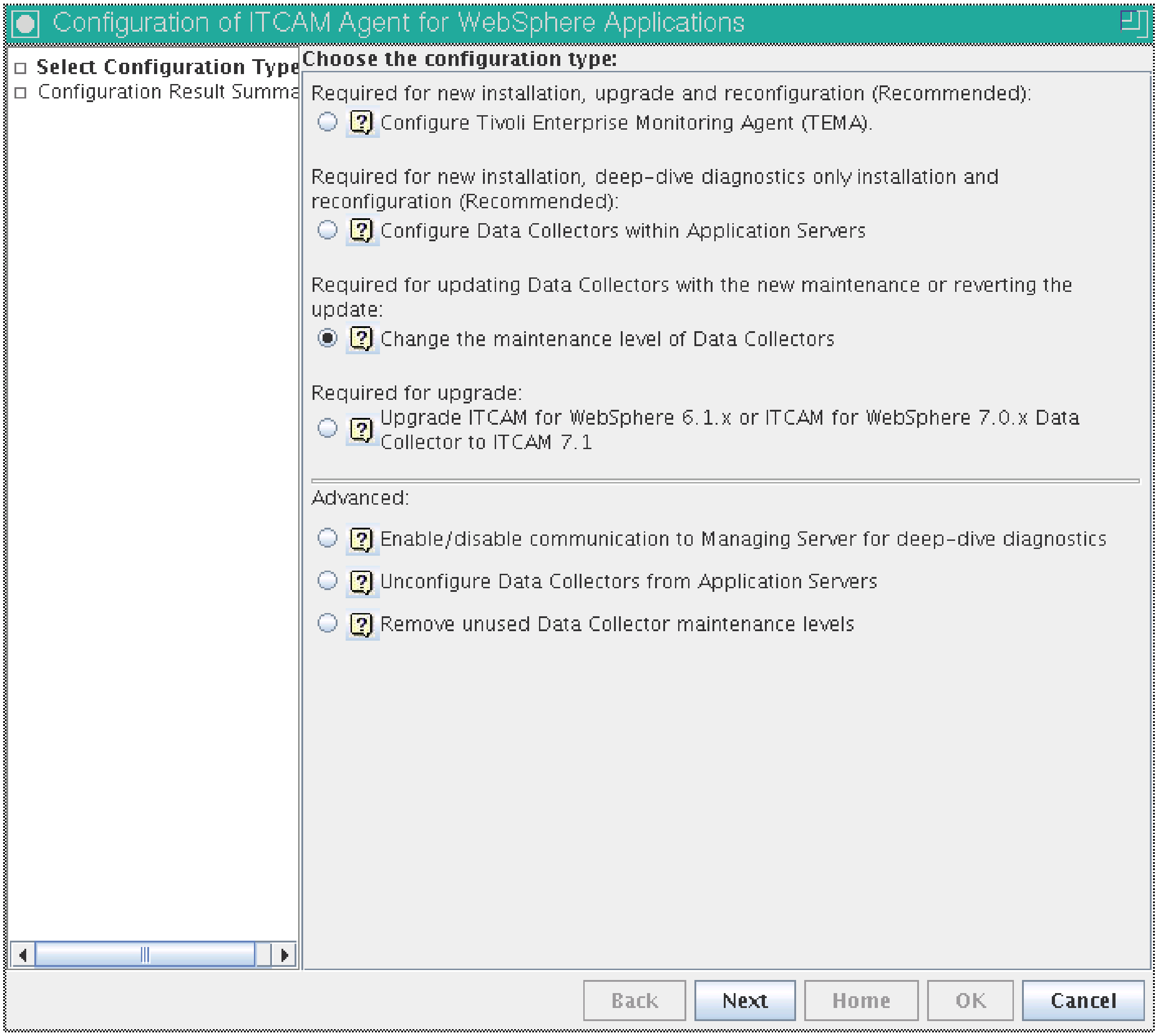
To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window, or click **OK** to complete the configuration process. If you click **OK**, the **TEMS Connection** window is displayed. If IBM Tivoli Monitoring is not used (in a deep dive only installation), make sure **No TEMS** is selected, and click **Save**. Otherwise click **Cancel** to close it.

Changing Data Collector maintenance level using GUI

If an application server instance is monitored by the Data Collector version 7.1, and more than one maintenance level for this version is installed by the host (for example, 7.1.0 and 7.1.0.1), you can change the maintenance level. After installing a new maintenance level, you must perform this change to update the monitoring of application server instances. You can not remove an old maintenance level until all monitored server instances are moved to another level.

To change the Data Collector maintenance level for monitored application server instances, perform the following procedure:

1. Enter the Agent Configuration window. See "Entering the Agent Configuration window" on page 133.


Configuration of ITCAM Agent for WebSphere Applications
□ Select Configuration Type
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

● Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

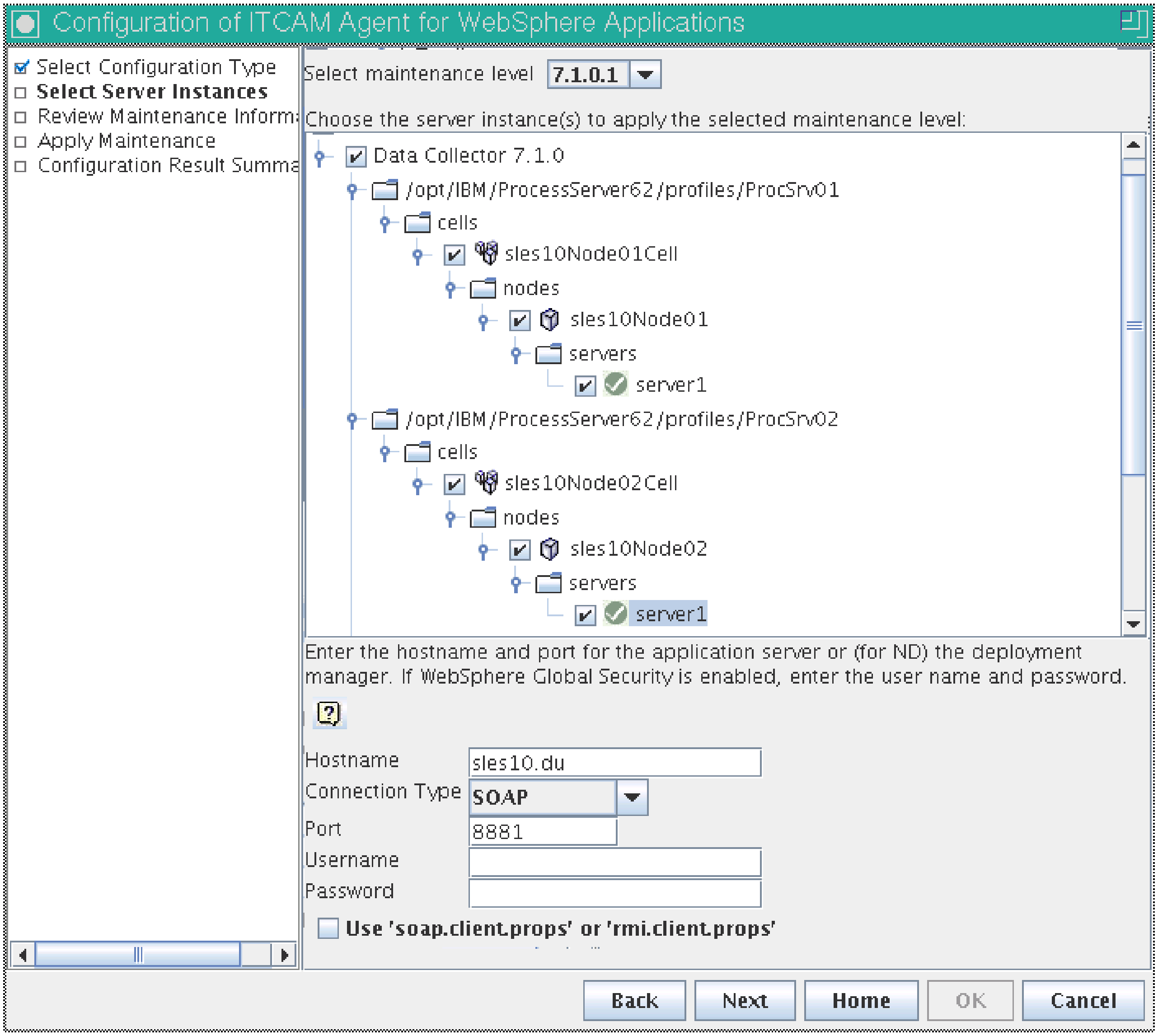
○ Enable/disable communication to Managing Server for deep-dive diagnostics

○ Unconfigure Data Collectors from Application Servers

○ Remove unused Data Collector maintenance levels

Figure 105. Changing Data Collector maintenance level, window 1

2. Select **Change the maintenance level of Data Collectors** and click **Next**.
3. Select the required maintenance level, and the server instances you want to change. All the instances monitored by this installation of the Agent are listed.



Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- □ **Select Server Instances**
- □ Review Maintenance Inform
- □ Apply Maintenance
- □ Configuration Result Summa

Select maintenance level **7.1.0.1**

Choose the server instance(s) to apply the selected maintenance level:

```
☑ Data Collector 7.1.0
  /opt/IBM/ProcessServer62/profiles/ProcSrv01
    cells
      ☑ sles10Node01Cell
        nodes
          ☑ sles10Node01
            servers
              ☑ server1
  /opt/IBM/ProcessServer62/profiles/ProcSrv02
    cells
      ☑ sles10Node02Cell
        nodes
          ☑ sles10Node02
            servers
              ☑ server1
```

Enter the hostname and port for the application server or (for ND) the deployment manager. If WebSphere Global Security is enabled, enter the user name and password.

Hostname	sles10.du
Connection Type	SOAP
Port	8881
Username	
Password	

□ **Use 'soap.client.props' or 'rmi.client.props'**

Figure 106. Changing Data Collector maintenance level, window 2

Note:

- For a stand alone environment, instances must be running during the configuration.
- For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running.

You also need to set the connection parameters for the application server instances. By default, the information that was set during initial Data Collector configuration for each instance will be displayed (except username and password). The following table lists the fields:

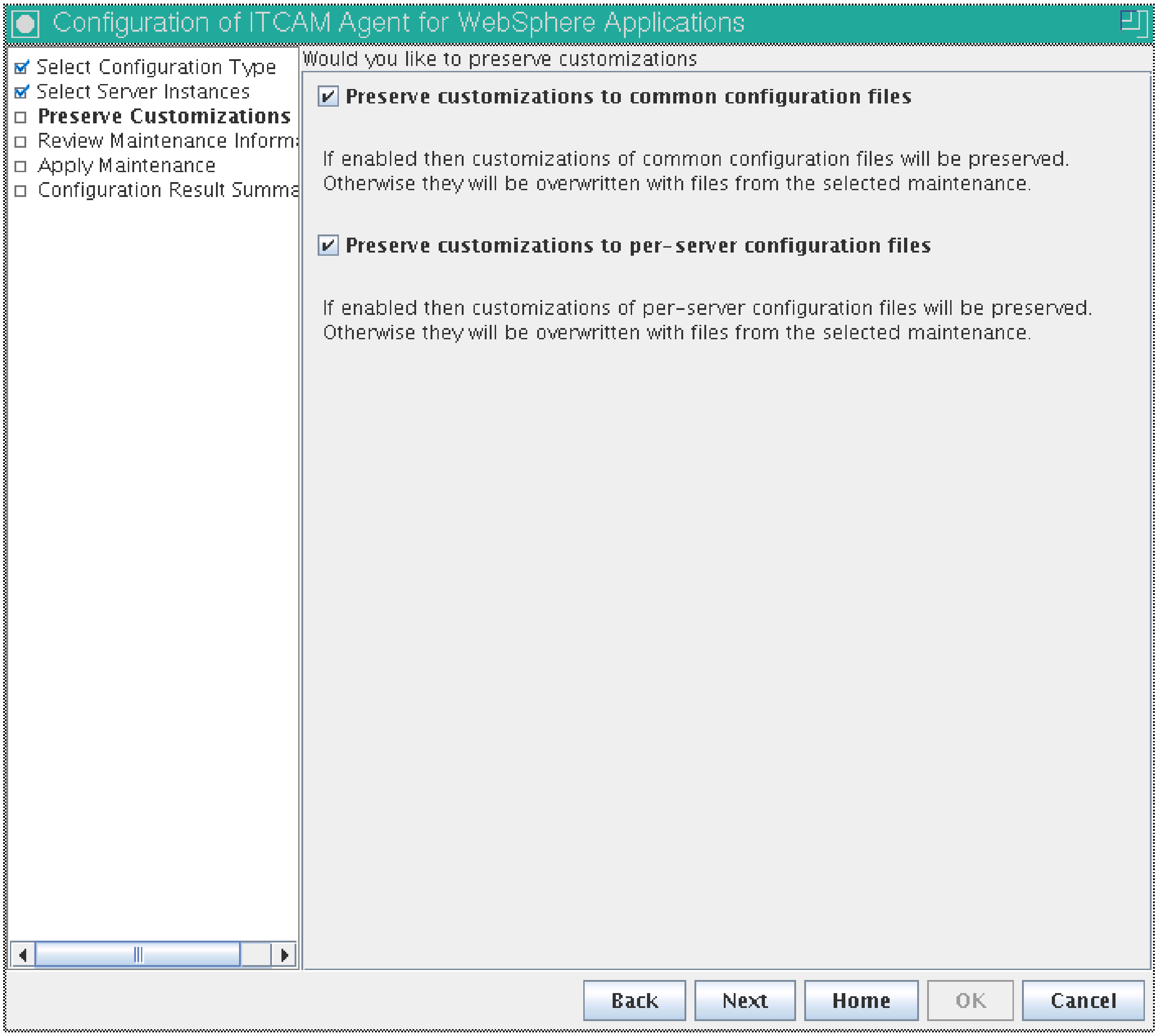
Table 15. Fields for establishing Data Collector and application server communication

Field	What to do
Host Name	Type the fully qualified host name or IP address of the application server instance that the Data Collector monitors. Do not include a protocol in the host name. For example, type myserver.ibm.tivoli.com, not https://myserver.ibm.tivoli.com. Note: If using a Network Deployment environment, provide the host name of the Deployment Manager instead.
Connector Type	Select the type of connection the Data Collector and application server will use for communication.
Port	If you selected SOAP as the connector type, enter the connector port used by the application server instance to send commands using the Simple Object Access Protocol (SOAP). The SOAP port is identified in the `AppServer_home/profiles/profile_name/config/cells/cell_name/nodes/node_name/serverindex.xml` file for the instance of application server that the Data Collector will monitor. **Note:** If using Network Deployment, provide the SOAP port of the Deployment Manager instead. If you selected RMI as the connector type, enter the connector port used by the application server instance to send commands using RMI.
Username (only for Global Security enabled)	Type the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server. If, instead of typing the user ID, you want to retrieve the user ID from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.
Password (only for Global Security enabled)	Type the password that corresponds to the user specified in the **Username** field. If, instead of typing the password, you want to retrieve the password from a properties file, select **Use 'soap.client.props' or 'sas.client.props'**.

Check the boxes next to the instances you want to configure. Then, click **Next**.

4. In the following window, choose whether the update is to preserve modifications that were made to custom Data Collector configuration files (see "Properties files for the Data Collector" on page 217). Unless you have special requirements, preserve the customizations; ensure that both checkboxes are selected.

Attention: You can only choose whether to preserve common configuration files if this is the first time you are changing instances on this host to this maintenance level. At this time the common files will be processed. If you have already changed any instances to the level, this checkbox is unavailable.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Server Instances
□ Preserve Customizations
□ Review Maintenance Informa
□ Apply Maintenance
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Would you like to preserve customizations

☑ **Preserve customizations to common configuration files**

If enabled then customizations of common configuration files will be preserved. Otherwise they will be overwritten with files from the selected maintenance.

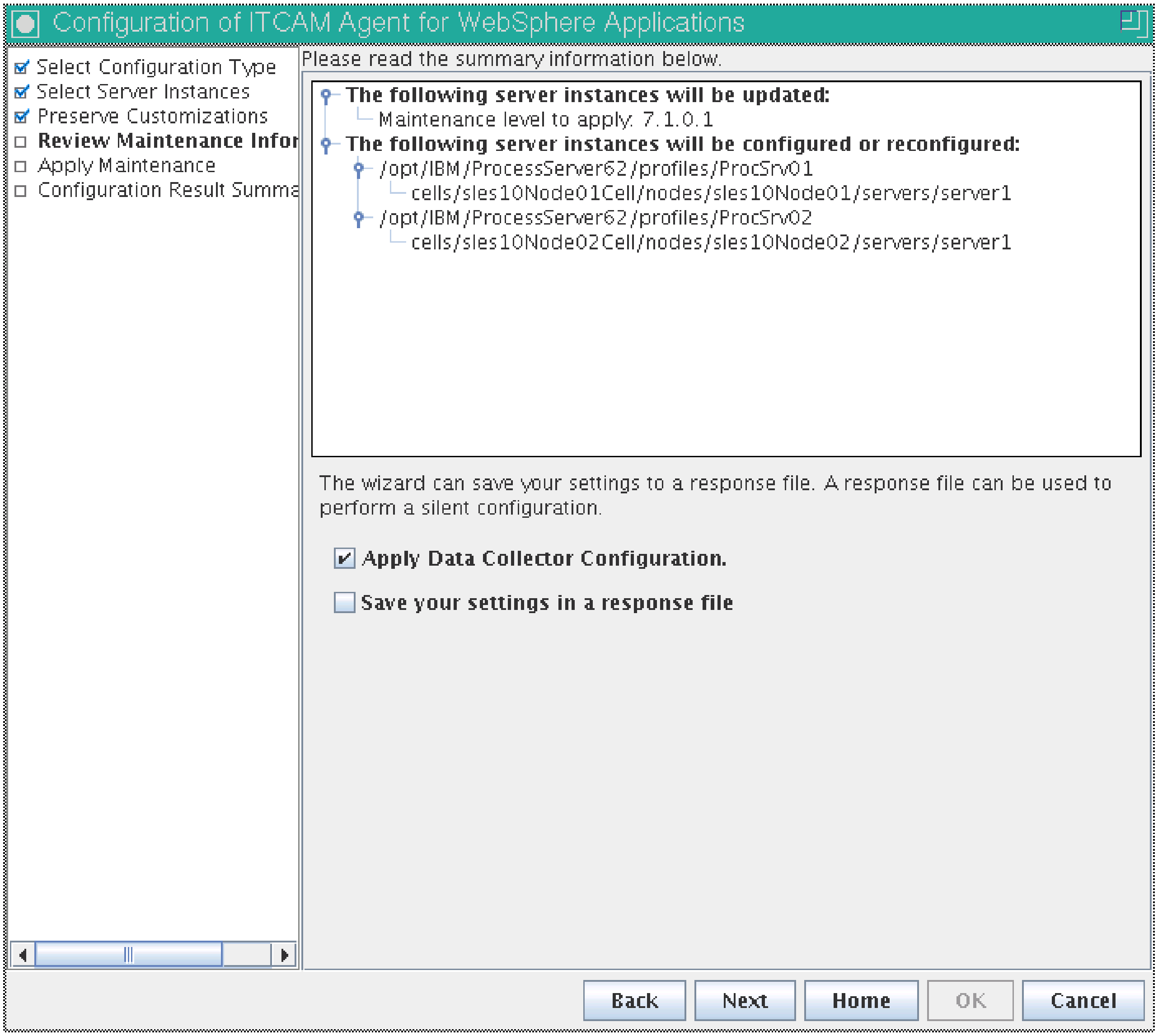
☑ **Preserve customizations to per-server configuration files**

If enabled then customizations of per-server configuration files will be preserved. Otherwise they will be overwritten with files from the selected maintenance.

Figure 107. Changing Data Collector maintenance level, window 3

Click **Next**.

5. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- ☑ Select Server Instances
- ☑ Preserve Customizations
- □ **Review Maintenance Infor**
- □ Apply Maintenance
- □ Configuration Result Summa

Please read the summary information below.

The following server instances will be updated:
Maintenance level to apply: 7.1.0.1
The following server instances will be configured or reconfigured:
/opt/IBM/ProcessServer62/profiles/ProcSrv01
cells/sles10Node01Cell/nodes/sles10Node01/servers/server1
/opt/IBM/ProcessServer62/profiles/ProcSrv02
cells/sles10Node02Cell/nodes/sles10Node02/servers/server1

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

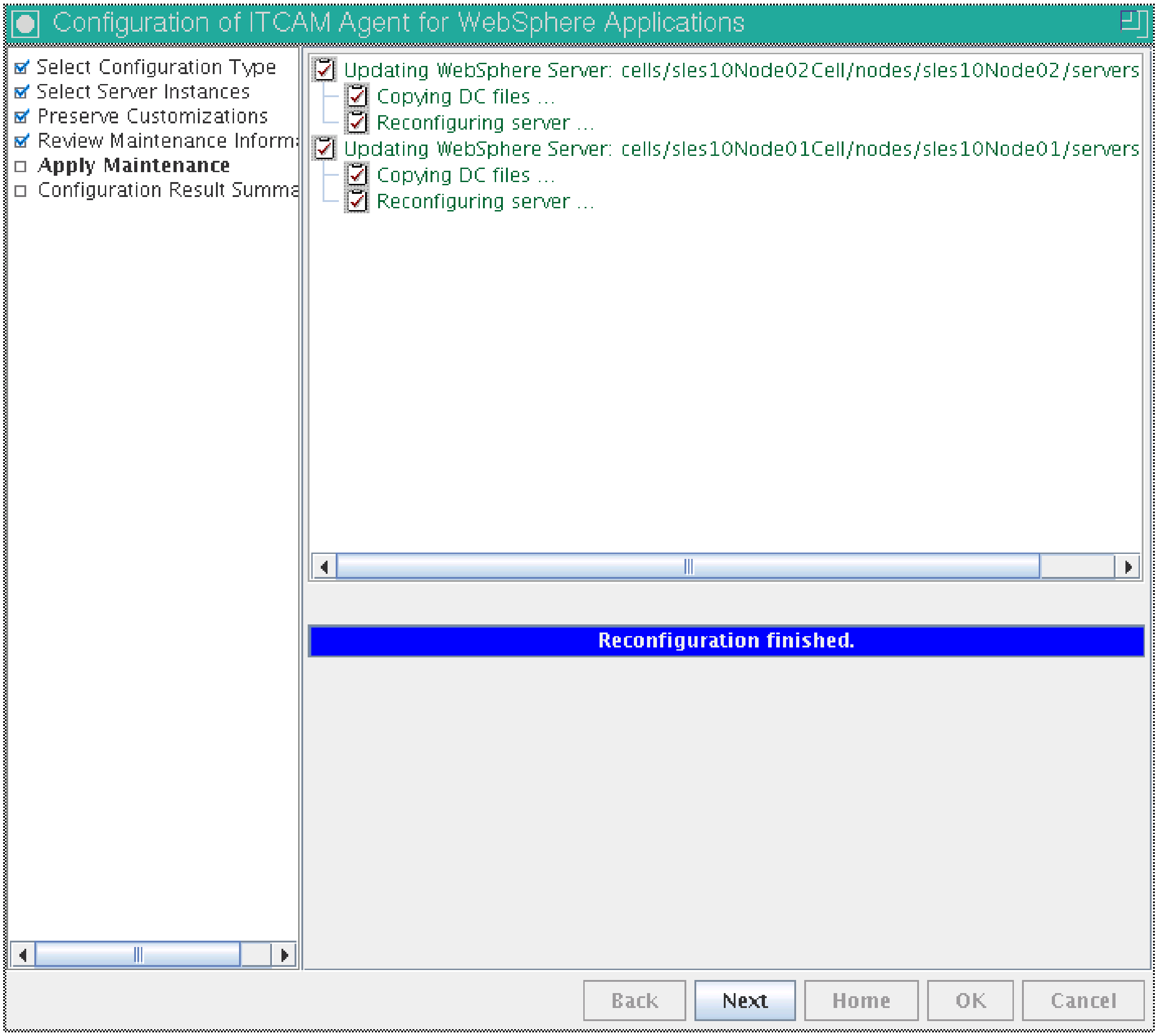
☑ **Apply Data Collector Configuration.**

□ **Save your settings in a response file**

Figure 108. Changing Data Collector maintenance level, window 4

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Configuration**, the new configuration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

6. The configuration utility will validate the applications server connection and apply the change.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Server Instances
☑ Preserve Customizations
☑ Review Maintenance Inform
□ Apply Maintenance
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

☑ Updating WebSphere Server: cells/sles10Node02Cell/nodes/sles10Node02/servers
- ☑ Copying DC files ...
- ☑ Reconfiguring server ...

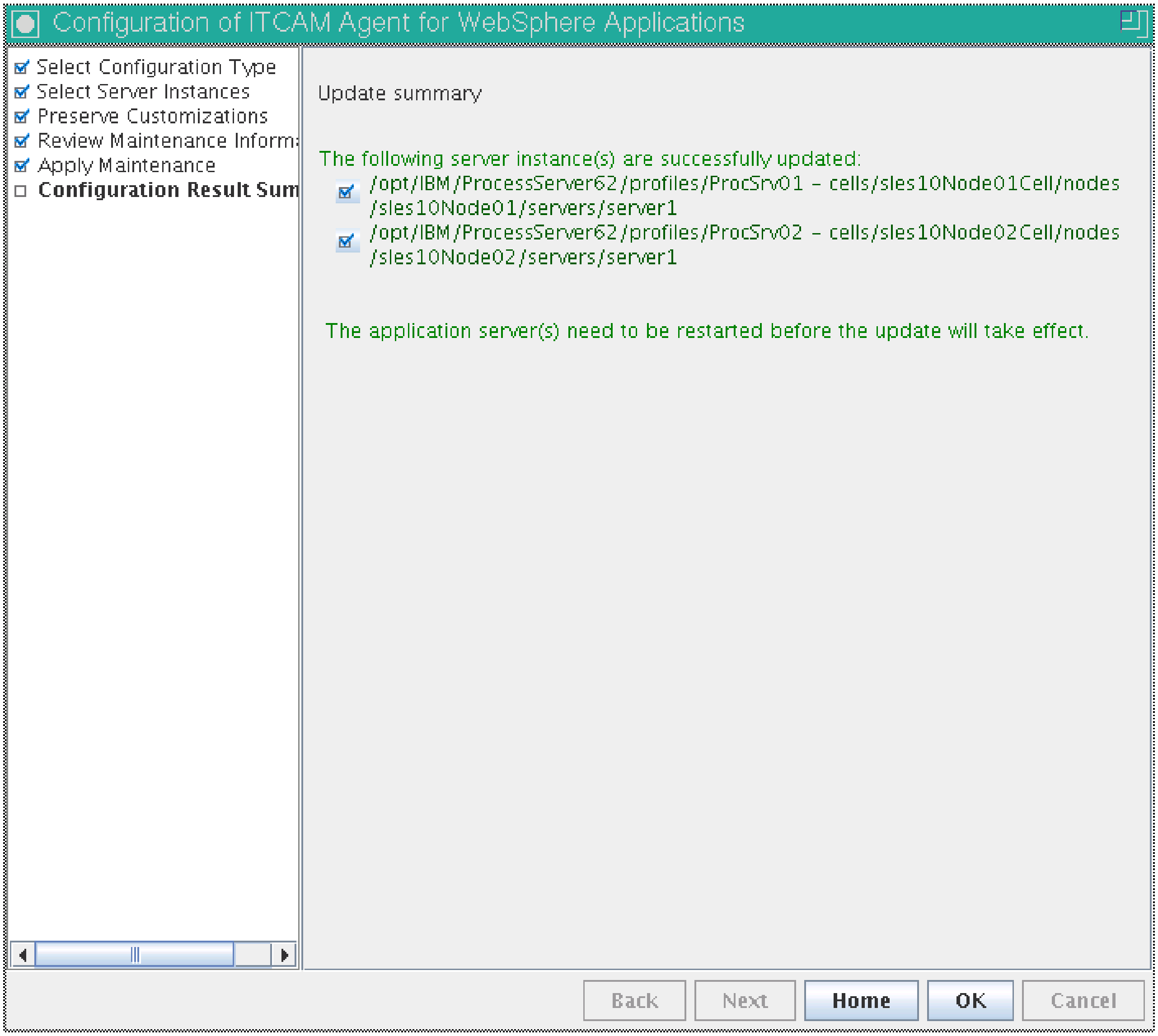
☑ Updating WebSphere Server: cells/sles10Node01Cell/nodes/sles10Node01/servers
- ☑ Copying DC files ...
- ☑ Reconfiguring server ...

Reconfiguration finished.

Figure 109. Changing Data Collector maintenance level, window 5

Click **Next**.

7. Summary information is displayed.



Configuration of ITCAM Agent for WebSphere Applications

- ☑ Select Configuration Type
- ☑ Select Server Instances
- ☑ Preserve Customizations
- ☑ Review Maintenance Informa
- ☑ Apply Maintenance
- □ **Configuration Result Sum**

Update summary

The following server instance(s) are successfully updated:

☑ /opt/IBM/ProcessServer62/profiles/ProcSrv01 - cells/sles10Node01Cell/nodes /sles10Node01/servers/server1

☑ /opt/IBM/ProcessServer62/profiles/ProcSrv02 - cells/sles10Node02Cell/nodes /sles10Node02/servers/server1

The application server(s) need to be restarted before the update will take effect.

Figure 110. Changing Data Collector maintenance level, window 6

To export the summary report to a file, click the **Export Summary Report** button. The application server needs to be restarted before the Data Collector configuration takes effect. Click **Home** to return to the **Agent Configuration** window.

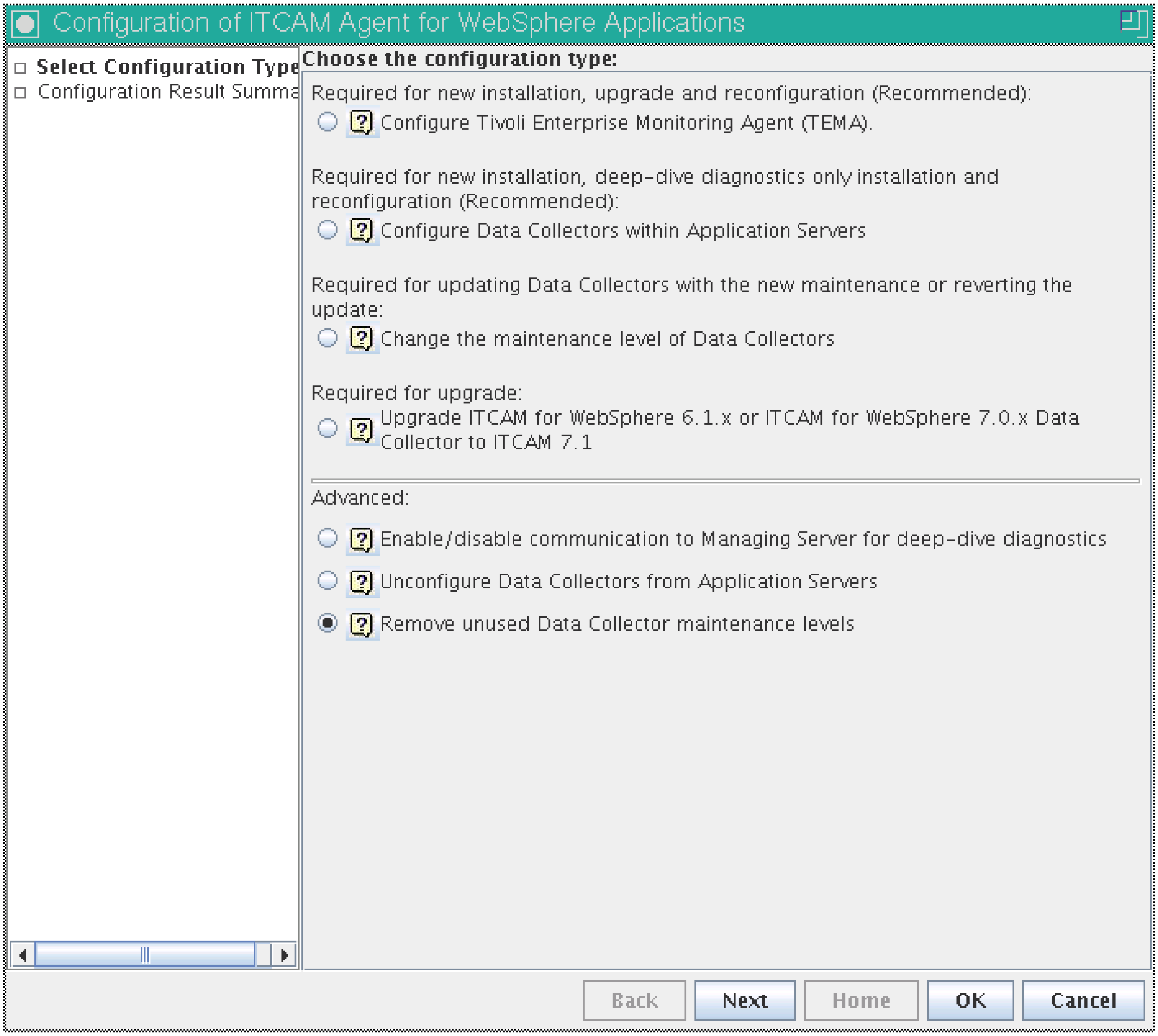
Tip: If an older maintenance level is no longer used, you can remove it. See "Removing a Data Collector maintenance level using GUI."

Removing a Data Collector maintenance level using GUI

If an older maintenance level of the Data Collector version 7.1 is installed, and all the monitored applications server instances were updated to the new maintenance level, you can remove the older maintenance level.

To remove an unused maintenance level Data Collector version 7.1, perform the following procedure:

1. Enter the Agent Configuration window. See "Entering the Agent Configuration window" on page 133.



Configuration of ITCAM Agent for WebSphere Applications

□ **Select Configuration Type**
□ Configuration Result Summa

Choose the configuration type:

Required for new installation, upgrade and reconfiguration (Recommended):

○ Configure Tivoli Enterprise Monitoring Agent (TEMA).

Required for new installation, deep-dive diagnostics only installation and reconfiguration (Recommended):

○ Configure Data Collectors within Application Servers

Required for updating Data Collectors with the new maintenance or reverting the update:

○ Change the maintenance level of Data Collectors

Required for upgrade:

○ Upgrade ITCAM for WebSphere 6.1.x or ITCAM for WebSphere 7.0.x Data Collector to ITCAM 7.1

Advanced:

○ Enable/disable communication to Managing Server for deep-dive diagnostics

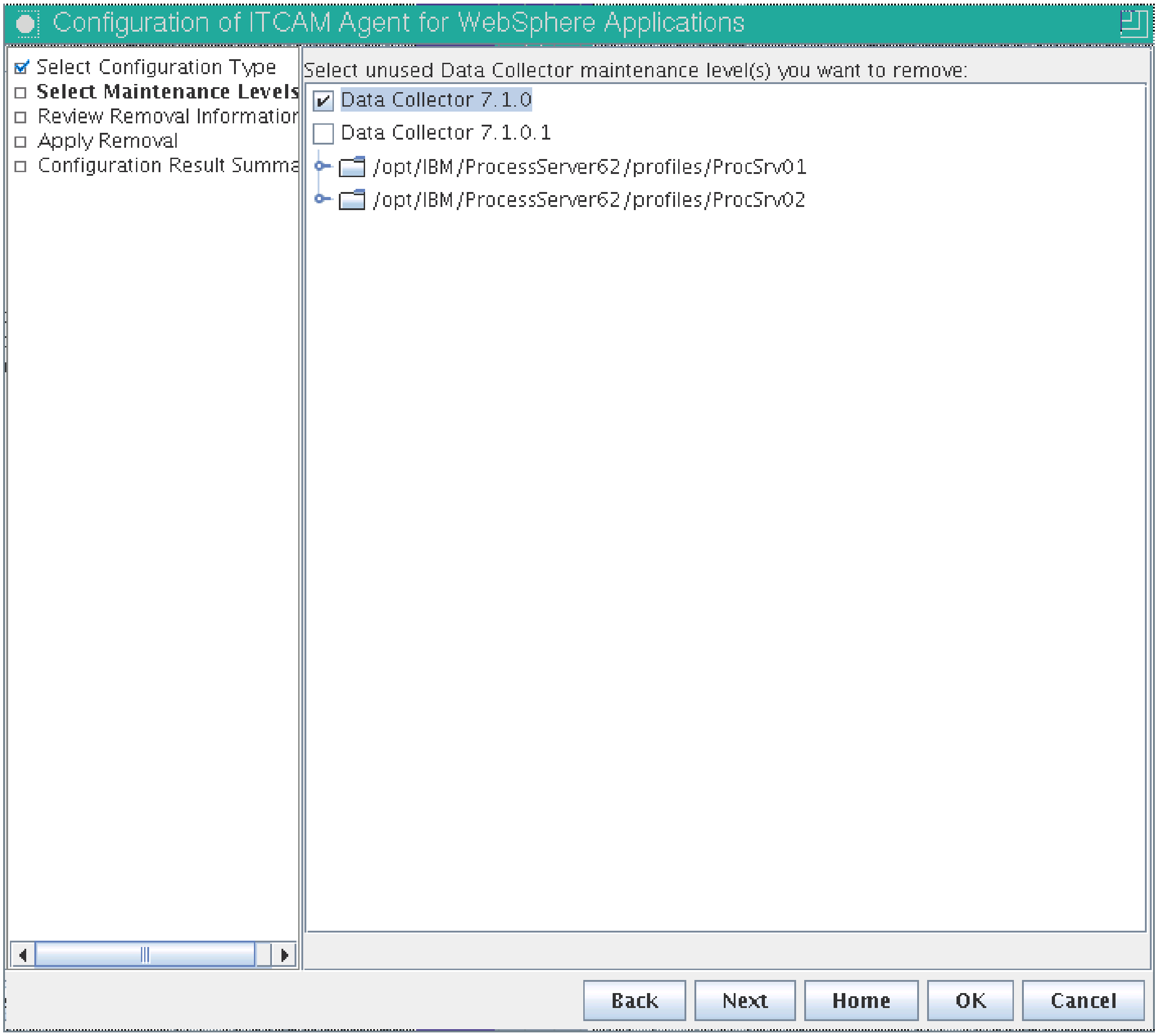
○ Unconfigure Data Collectors from Application Servers

● Remove unused Data Collector maintenance levels

Figure 111. Uninstalling a Data Collector maintenance level, window 1

2. Select **Remove unused Data Collector maintenance levels** and click **Next**.
3. Select the maintenance levels to remove. Only the levels that are not used for any application server instances are available for selection. For other available maintenance level, this window shows a list of application server instances monitored by them.

   Tip: If you want to remove a Data Collector maintenance level, but this window shows it as used for application server instances, change the maintenance level for the instances. See "Changing Data Collector maintenance level using GUI" on page 177.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
□ **Select Maintenance Levels**
□ Review Removal Informatior
□ Apply Removal
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Select unused Data Collector maintenance level(s) you want to remove:

☑ Data Collector 7.1.0

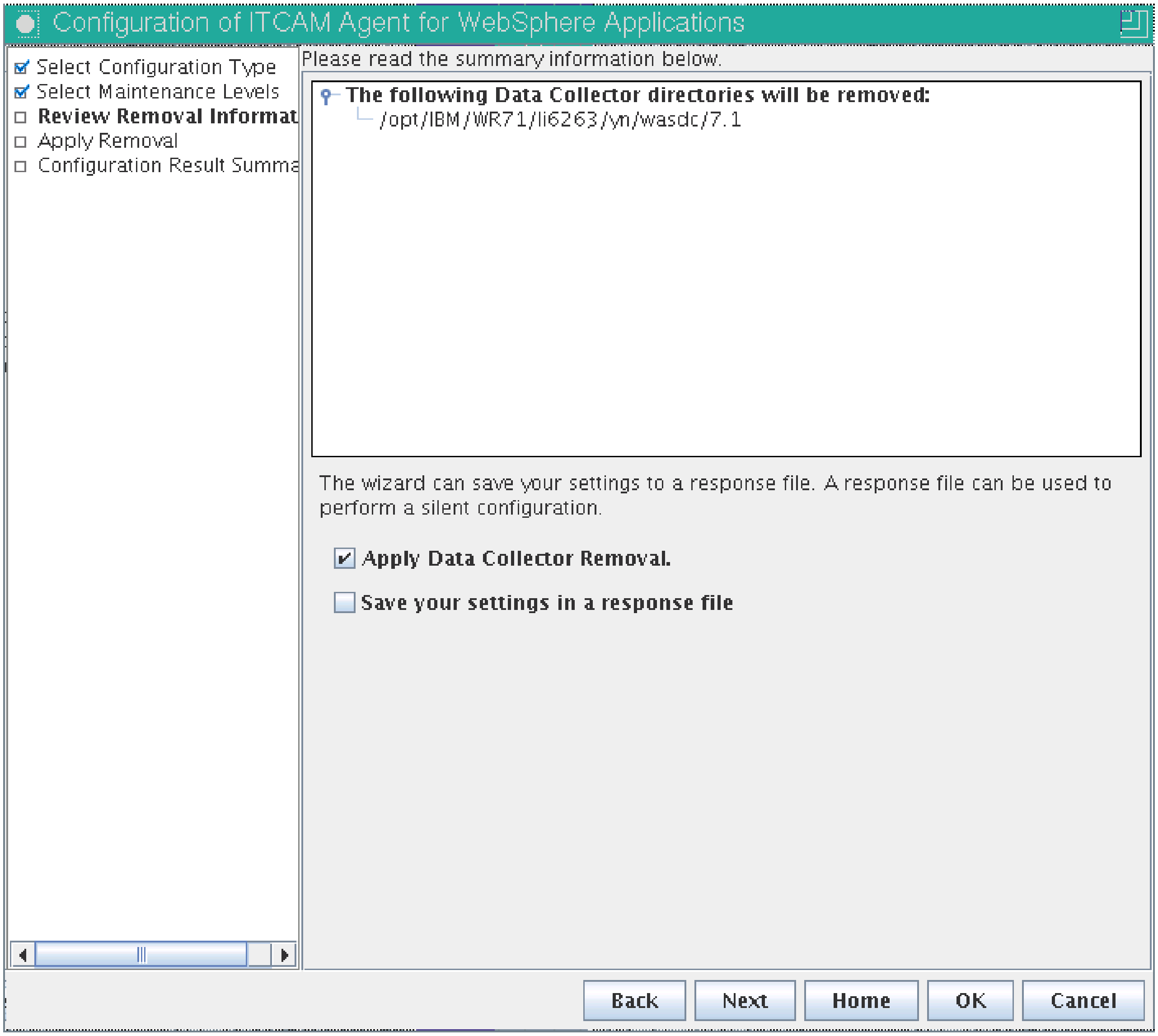
□ Data Collector 7.1.0.1

- /opt/IBM/ProcessServer62/profiles/ProcSrv01
- /opt/IBM/ProcessServer62/profiles/ProcSrv02

Figure 112. Uninstalling a Data Collector maintenance level, window 2

Check the boxes next to the levels you want to uninstall. Then, click **Next**.

4. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Maintenance Levels
□ Review Removal Informat
□ Apply Removal
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

Please read the summary information below.

The following Data Collector directories will be removed:
/opt/IBM/WR71/li6263/yn/wasdc/7.1

The wizard can save your settings to a response file. A response file can be used to perform a silent configuration.

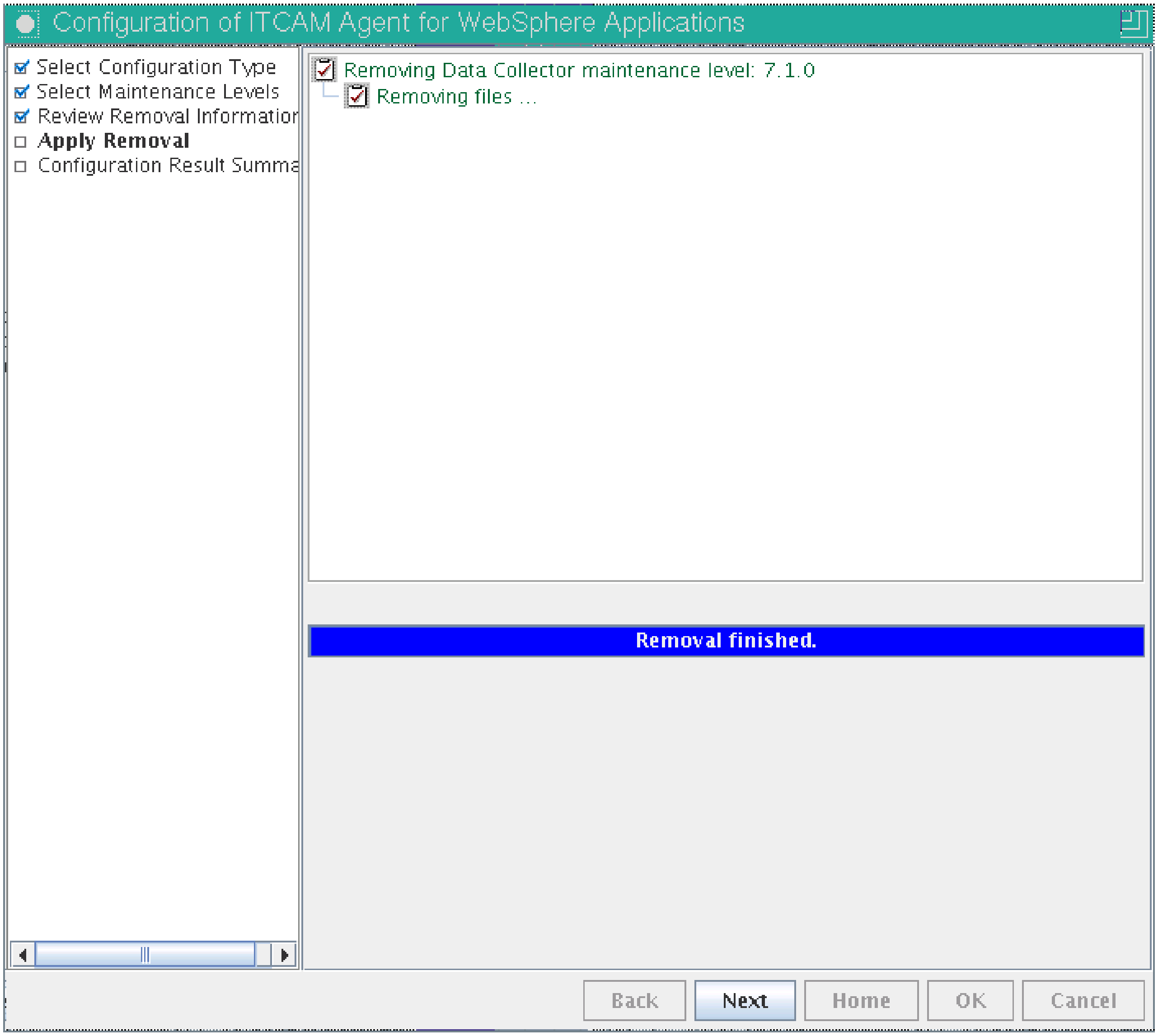
☑ Apply Data Collector Removal.

□ Save your settings in a response file

Figure 113. Uninstalling a Data Collector maintenance level, window 3

If you need to create a response file, check the box **Save your settings in a response file** and click **Browse** to select the file location; otherwise leave the box unchecked. If you uncheck **Apply Configuration**, the new configuration will not be applied; you can still save it in the response file. When the boxes are set correctly, click **Next**.

5. The configuration utility will apply the changes.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Maintenance Levels
☑ Review Removal Information
□ Apply Removal
□ Configuration Result Summa
Back
Next
Home
OK
Cancel

☑ Removing Data Collector maintenance level: 7.1.0

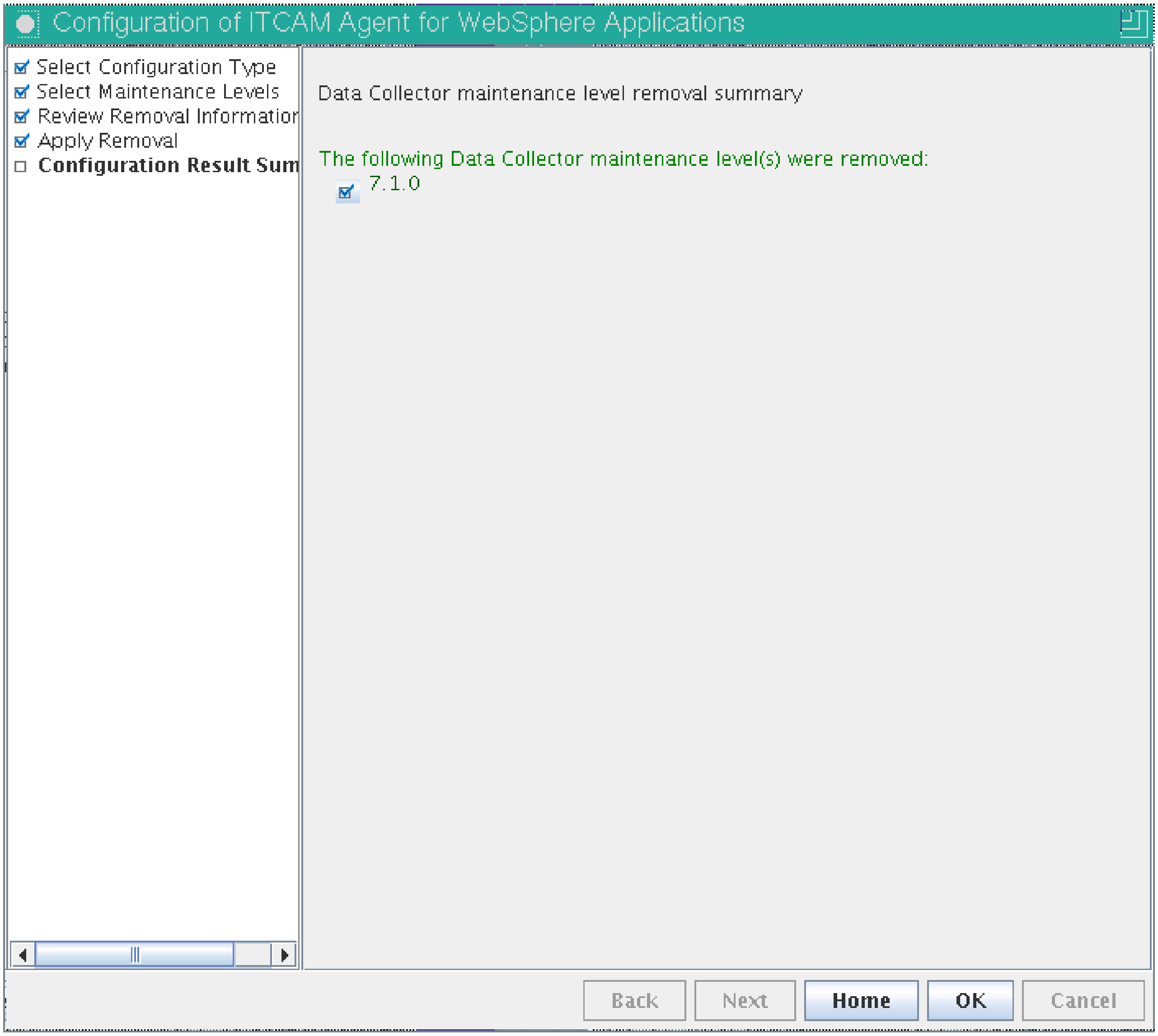
☑ Removing files ...

Removal finished.

Figure 114. Uninstalling a Data Collector maintenance level, window 4

Click **Next**.

6. Summary information is displayed.


Configuration of ITCAM Agent for WebSphere Applications
☑ Select Configuration Type
☑ Select Maintenance Levels
☑ Review Removal Informatior
☑ Apply Removal
□ Configuration Result Sum
Back
Next
Home
OK
Cancel

Data Collector maintenance level removal summary

The following Data Collector maintenance level(s) were removed:

☑ 7.1.0

Figure 115. Uninstalling a Data Collector maintenance level, window 5

To export the summary report to a file, click the **Export Summary Report** button. Click **Home** to return to the **Agent Configuration** window.

Starting ITCAM Agent for WebSphere Applications

To start ITCAM Agent for WebSphere Applications, invoke the following command on the computer where it is installed:

```
./itmcmd agent start yn
```

where `yn` is the 2-character product code for the ITCAM Agent for WebSphere Applications.

The installer also adds the Agent to system startup scripts. To remove it from the scripts, see "Deep dive diagnostics only installation: disabling Monitoring Agent autostart" on page 109.

Installing application support on Linux and UNIX systems

To ensure that ITCAM Agent for WebSphere Applications works within your IBM Tivoli Monitoring infrastructure, you need to install application support files for it on every hub monitoring server, portal server, and portal client. After configuring the Agent on the monitored host, you also need to enable Tivoli monitoring history collection. You do not need to install application support files if IBM Tivoli Monitoring is not used (in a deep dive diagnostics only installation).

Important: You will need to stop the monitoring server, portal server, or portal client when installing the support files.

Attention: you must install support files for ITCAM Agent for WebSphere Applications version 7.1 before installing them for version 7.1.0.1.

Installing application support on the Tivoli Enterprise Monitoring Server

1. Stop the monitoring server by running the following command:

   ```
   ./itmcmd server stop tems_name
   ```
2. Run **./install.sh** from the installation media
3. Press **Enter** to accept the default directory (/opt/IBM/ITM) or type the full path to the installation directory you used when the software asks for the IBM Tivoli Monitoring home directory.

   The software displays the following prompt:

   ```
   Select one of the following:
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS).
   3) Install TEMS support for remote seeding
   4) Exit install.

   Please enter a valid number:
   ```
4. Type **1** and press **Enter**.
5. The software license agreement is displayed after the initialization, enter 1 to accept the agreement and press **Enter**.
6. Type the 32 character encryption key that was specified during the installation of the monitoring server and press **Enter**.

   Note: If you have already installed another IBM Tivoli Monitoring component on this computer or you are installing support for an agent from an agent installation image, this step does not occur.

   The information of installed products is displayed.
7. Press **Enter** to continue the installation and the installer promotes you with the following message:

   ```
   Product packages are available for the following operating systems and
   component support categories:

    1) Tivoli Enterprise Portal Browser Client support
    2) Tivoli Enterprise Portal Desktop Client support
    3) Tivoli Enterprise Portal Server support
    4) Tivoli Enterprise Monitoring Server support

   Type the number for the OS you want, or type "q" to quit selection:
   ```
8. Type **4** and press **Enter** to install the application support on the Tivoli Enterprise Monitoring server and the following message is displayed:

```
You selected number "4" or "Tivoli Enterprise Monitoring Server support"

Is the selection correct [ 1=Yes, 2=No; default is "1"]?
```

9. Type **1** and press **Enter** to confirm the selection and the message about the products to install is displayed:

   ```
   The following products are available for installation:

    1) IBM Tivoli Composite Application Manager Agent for HTTP Servers
      v07.10.00.01
    2) IBM Tivoli Composite Application Manager Agent for WebSphere
      Applications V07.10.00.01
    3) all of the above

   Type the numbers for the products you want to install,
   type "b" to change operating system, or type "q" to quit selection.
   If you enter more than one number, separate the numbers by a comma or a space.

   Type you selections here:
   ```

10. Type **3** and press **Enter** and the installer promotes you with the following message to ask you to confirm your selection:

    ```
    The following products will be installed:

     IBM Tivoli Composite Application Manager Agent for HTTP Servers
       V07.10.00.01
     IBM Tivoli Composite Application Manager Agent for WebSphere
       Applications V07.10.00.01

    Are your selections correct [ 1=Yes, 2=No; default is "1" ]?
    ```

11. Type **1** and press **Enter** to confirm your selection and start the installation.

12. After installing all of the components, the following message is displayed to ask you whether you want to install components for a different operating system:

    ```
    Do you want to install additional products or product support packages
     [ 1=Yes, 2=No; default is "2" ]?
    ```

    Type **2** and press **Enter**.

13. The installation step completes and the information of installed Tivoli Enterprise Monitoring Server product supports is displayed:

    ```
    *) IBM Tivoli Composite Application Manager Agent for HTTP Servers
    *) IBM Tivoli Composite Application Manager Agent for WebSphere Applications
    ```

    And the installer also promotes you with the following message to seed product supports on the Tivoli Enterprise Monitoring Server:

    ```
    Note: This operation causes the monitoring server to restart.
    Do you want to seed product support on the Tivoli Enterprise Monitoring Server?
    [ 1=Yes, 2=No; default is "1" ]?
    ```

14. Enter **Press** to make the default choice.

15. After starting the Tivoli Enterprise Monitoring Server, the message about the application supports to seed is displayed:

    ```
    The following new Tivoli Enterprise Monitoring Server product support packages
    will be seeded:
     *) IBM Tivoli Composite Application Manager Agent for HTTP Servers
     *) IBM Tivoli Composite Application Manager Agent for WebSphere Applications

    Note: Not all situations might have the default distribution list setting,
    for some you might need to manually set the distribution list in TEP.
    Select listed above Tivoli Enterprise Monitoring Server product support
    for which default distribution list will be upgraded:
    [1=new, 2=all, 3=none] (Default is: 1):
    ```

16. Press **Enter** to make the default choice.
17. After the support seeding and stopping the monitoring server, the following message is displayed to remind you about the configuration:

    ```
    You may now configure any locally intalled IBM Tivoli Monitoring product via
    the "/opt/IBM/ITM/bin/itmcmd config" command.
    ```
18. The monitoring server is restarted automatically.

Installing application support on the Tivoli Enterprise Portal Server

On a Tivoli Enterprise Portal Server, you must install application support files both for the server itself and for the browser client.

Stop the portal server before performing this procedure.

1. Run **`./install.sh`** from the installation media
2. Press **Enter** to accept the default directory (`/opt/IBM/ITM`) or type the full path to the installation directory you used when the software asks for the IBM Tivoli Monitoring home directory.

    The software displays the following prompt:

    ```
    Select one of the following:
    1) Install products to the local host.
    2) Install products to depot for remote deployment (requires TEMS).
    3) Install TEMS support for remote seeding
    4) Exit install.

    Please enter a valid number:
    ```
3. Type **1** and press **Enter**.
4. The software license agreement is displayed after the initialization, enter 1 to accept the agreement and press **Enter**.
5. Type the 32 character encryption key that was specified during the installation of the monitoring server and press **Enter**.

    Note: If you have already installed another IBM Tivoli Monitoring component on this computer or you are installing support for an agent from an agent installation image, this step does not occur.

    The information of installed products is displayed.
6. Press **Enter** to continue the installation and the installer promotes you with the following message:

    ```
    Product packages are available for the following operating systems and
    component support categories:

     1) Tivoli Enterprise Portal Browser Client support
     2) Tivoli Enterprise Portal Desktop Client support
     3) Tivoli Enterprise Portal Server support
     4) Tivoli Enterprise Monitoring Server support

    Type the number for the OS you want, or type "q" to quit selection:
    ```
7. Type **3** and press **Enter** to install the application support on the Tivoli Enterprise Portal server and the following message is displayed:

    ```
    You selected number "3" or "Tivoli Enterprise Portal Server support"

    Is the selection correct [ 1=Yes, 2=No; default is "1"]?
    ```
8. Type **1** and press **Enter** to confirm the selection and the message about the products to install is displayed:

```
The following products are available for installation:

 1) IBM Tivoli Composite Application Manager Agent for HTTP Servers
     v07.10.00.01
 2) IBM Tivoli Composite Application Manager Agent for WebSphere
     Applications V07.10.00.01
 3) all of the above

Type the numbers for the products you want to install,
type "b" to change operating system, or type "q" to quit selection.
If you enter more than one number, separate the numbers by a comma or a space.

Type you selections here:
```

9. Type **3** and press **Enter** and the installer promotes you with the following message to ask you to confirm your selection:

```
The following products will be installed:

 IBM Tivoli Composite Application Manager Agent for HTTP Servers
    V07.10.00.01
 IBM Tivoli Composite Application Manager Agent for WebSphere
    Applications V07.10.00.01

Are your selections correct [ 1=Yes, 2=No; default is "1" ]?
```

10. Type **1** and press **Enter** to confirm your selection and start the installation.
11. After installing all of the components, the following message is displayed to ask you whether you want to install components for a different operating system:

```
Do you want to install additional products or product support
   packages [ 1=Yes, 2=No; default is "2" ]?
```

    Type **1** and press **Enter**.
12. The following message is displayed.

```
Product packages are available for the following operating systems and
component support categories:

 1) Tivoli Enterprise Portal Browser Client support
 2) Tivoli Enterprise Portal Desktop Client support
 3) Tivoli Enterprise Portal Server support
 4) Tivoli Enterprise Monitoring Server support

Type the number for the OS you want, or type "q" to quit selection:
```

13. Type **1** and press **Enter** to install the application support on the Tivoli Enterprise Portal browse client and the following message is displayed:

```
You selected number "1" or "Tivoli Enterprise Portal Browse Client support"

Is the selection correct [ 1=Yes, 2=No; default is "1"]?
```

14. Type **1** and press **Enter** to confirm the selection and the message about the products to install is displayed:

```
The following products are available for installation:

 1) IBM Tivoli Composite Application Manager Agent for HTTP Servers
   v07.10.00.01
 2) IBM Tivoli Composite Application Manager Agent for
   WebSphere Applications v07.10.00.01
 3) all of the above

Type the numbers for the products you want to install,
type "b" to change operating system, or type "q" to quit selection.
If you enter more than one number, separate the numbers by a comma or a space.

Type you selections here:
```

15. Type **3** and press **Enter** and the installer promotes you with the following message to ask you to confirm your selection:

```
The following products will be installed:

 IBM Tivoli Composite Application Manager Agent for HTTP Servers
   V07.10.00.01
 IBM Tivoli Composite Application Manager Agent for WebSphere
   Applications V07.10.00.01

Are your selections correct [ 1=Yes, 2=No; default is "1" ]?
```

16. Type **1** and press **Enter** to confirm your selection and start the installation.
17. After installing all of the components, the following message is displayed to ask you whether you want to install other components:

```
Do you want to install additional products or product support packages
 [ 1=Yes, 2=No; default is "2" ]?
```

    Type **2** and press **Enter**.
18. The installation program will complete the installation and exit. After this, re-configure the portal server and browser client by running:

```
itmcmd config -A cq
```

    At any prompts, press **Enter** to accept the default values.

Important: If the Tivoli Enterprise Portal Server provides the browser client, check that the Eclipse help server has been configured. See "Ensure that the Eclipse server has been configured" on page 196.

Installing application support on the Tivoli Enterprise Portal desktop client

Note: Stop the desktop client before performing this procedure.

1. Run **./install.sh** from the installation media
2. Press **Enter** to accept the default directory (/opt/IBM/ITM) or type the full path to the installation directory you used when the software asks for the IBM Tivoli Monitoring home directory.

   The software displays the following prompt:

```
Select one of the following:
1) Install products to the local host.
2) Install products to depot for remote deployment (requires TEMS).
3) Install TEMS support for remote seeding
4) Exit install.

Please enter a valid number:
```

3. Type **1** and press **Enter**.
4. The software license agreement is displayed after the initialization, enter 1 to accept the agreement and press **Enter**.
5. Type the 32 character encryption key that was specified during the installation of the monitoring server and press **Enter**.

   Note: If you have already installed another IBM Tivoli Monitoring component on this computer or you are installing support for an agent from an agent installation image, this step does not occur.

   The information of installed products is displayed.
6. Press **Enter** to continue the installation and the installer promotes you with the following message:

```
Product packages are available for the following operating systems and
 component support categories:

 1) Tivoli Enterprise Portal Browser Client support
 2) Tivoli Enterprise Portal Desktop Client support
 3) Tivoli Enterprise Portal Server support
 4) Tivoli Enterprise Monitoring Server support

Type the number for the OS you want, or type "q" to quit selection:
```

7. Type **2** and press **Enter** to install the application support on the Tivoli Enterprise Portal desktop client and the following message is displayed:

   ```
   You selected number "2" or "Tivoli Enterprise Portal Desktop Client support"

   Is the selection correct [ 1=Yes, 2=No; default is "1"]?
   ```

8. Type **1** and press **Enter** to confirm the selection and the message about the products to install is displayed:

   ```
   The following products are available for installation:

    1) IBM Tivoli Composite Application Manager Agent for HTTP Servers
      v07.10.00.01
    2) IBM Tivoli Composite Application Manager Agent for WebSphere
      Applications V07.10.00.01
    3) all of the above

   Type the numbers for the products you want to install,
   type "b" to change operating system, or type "q" to quit selection.
   If you enter more than one number, separate the numbers by a comma or a space.

   Type you selections here:
   ```

9. Type **3** and press **Enter** and the installer promotes you with the following message to ask you to confirm your selection:

   ```
   The following products will be installed:

    IBM Tivoli Composite Application Manager Agent for HTTP Servers
      V07.10.00.01
    IBM Tivoli Composite Application Manager Agent for WebSphere
      Applications V07.10.00.01

   Are your selections correct [ 1=Yes, 2=No; default is "1" ]?
   ```

10. Type **1** and press **Enter** to confirm your selection and start the installation.
11. After installing all of the components, the following message is displayed to ask you whether you want to install components for a different operating system:

    ```
    Do you want to install additional products or product support packages
     [ 1=Yes, 2=No; default is "2" ]?
    ```

    Type **2** and press **Enter**.
12. The installer prompts you with the following message for the configuration:

    ```
    You may now configure any locally intalled IBM Tivoli Monitoring product via
    the "/opt/IBM/ITM/bin/itmcmd config" command.
    ```

13. The installation program will complete the installation and exit. After this, re-configure the desktop client by running:

    ```
    itmcmd config -A cj
    ```

    At any prompts, press **Enter** to accept the default values.

Important: Check that the Eclipse help server has been configured for the client. See “Ensure that the Eclipse server has been configured” on page 196.

Ensure that the Eclipse server has been configured

After installing application support files on a Tivoli Enterprise Portal Server that provides the browser client or on a Tivoli Enterprise Portal desktop client, you must check the Eclipse help server for the portal client to ensure that it has been configured.

To do this, perform the following procedure:

1. Start Manage Tivoli Enterprise Monitoring Services:

   ```
   ./itmcmd manage
   ```

   The Manage Tivoli Enterprise Monitoring Services window opens.
2. Verify that the Eclipse Help Server entry indicates **Yes** in the Configured column. If it does not, right-click the entry, and select **Configure** from the pop-up menu.
3. You are prompted for the port number that the Eclipse Help Server should use. Verify that this value is set to the same port number you specified when installing IBM Tivoli Monitoring, and click **OK**.

Enabling history collection

Some ITCAM Agent for WebSphere Applications workspaces require collection of history data. You need to enable it by using a script on the Tivoli Enterprise Portal Server.

The `kynHistoryConfigure.sh` script is installed with the Agent support files. It requires the IBM Tivoli Monitoring user interface component (`tacmd` command).

You need to run the script after installing the support files.

To run the script, you need to know the name of the Tivoli Enterprise Monitoring Server, as configured on the Tivoli Enterprise Portal Server. If there is more than one Tivoli Enterprise Monitoring Server to which Agents for WebSphere Applications are connected, you need to run the script for each of the Tivoli Enterprise Monitoring Servers.

The script is located in the *ITM_HOME*/bin directory. Run it with the following command:

```
kynHistoryConfigure.bat username password TEMS_name
```

username is the name of a Tivoli Enterprise Portal user with administrative privileges (for example, SYSADMIN). *password* is the password for this user. *TEMS_name* is the name of the Tivoli Enterprise Monitoring Server, as configured on the Tivoli Enterprise Portal Server.

Silent installation and configuration on Linux and UNIX systems

The installer and the configuration utility support a *silent* mode. In this mode, no user interaction is required for an installation or configuration. Instead, the parameters are taken from a *response file*. You may install and uninstall the Agent; also, all the tasks that you can perform in the configuration utility are also available in silent mode.

Response files have a text format. You can create a response file based on one of the samples provided on the installation DVD.

You may also create a response file during GUI configuration (see “Configuring the Agent using GUI” on page 133), modify it if necessary, and then use it for a silent configuration. In this way, you can quickly reproduce similar configuration many times, for example, on different hosts.

Silent installation

You can use the Installer to install ITCAM Agent for WebSphere Applications in silent mode. To do this, modify the sample file provided on the installation DVD, and then run the installer from the command line.

To perform a silent installation, first you need to prepare the response file. Then, run the installer, supplying the name of the response file. A silent uninstallation does not require a response file.

Attention: you must install ITCAM Agent for WebSphere Applications version 7.1 before installing version 7.1.0.1.

Preparing the response file for the agent installation

To prepare a response file for installing the agent, perform the following procedure:

1. On the product installation DVD, in the top level directory, locate the `silent_install.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify the following property, if necessary. Do not modify any other properties.

Table 16. Agent installation response file properties

Response file property	Meaning
EncryptionKey	The 32-character encryption key used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment. See IBM Tivoli Monitoring: Installation and Setup Guide for details about the encryption key.

4. Save the edited copy in a work directory, for example, as `/tmp/silent.txt`.

Running the Installer in silent mode

After preparing the response file for your installation and uninstallation, run the installer, specifying the path and name for the response file. Perform the following procedure:

1. Change to the directory where the installation DVD is mounted.
2. Invoke `install.sh`:

   ```
   ./install.sh -q -h ITM_home -p response_file_name
   ```

   where *ITM_home* specifies the destination directory where the agent will be installed (by default it is `/opt/IBM/ITM`; you can use different destination directories to install several copies of the agent on the same host); *response_file_name* is the name of the response file you have prepared (with full path). For example:

   ```
   ./install.sh -q -h /opt/IBM/ITM -p /tmp/silent.txt
   ```

Attention: if you are performing an upgrade or maintenance level update, and the Monitoring Agent is currently running, silent installation will be aborted.

Performing a silent uninstallation

To uninstall ITCAM Agent for WebSphere Applications in silent mode, perform the following procedure:

1. Change to the *ITM_home*/bin directory.
2. Run the command:

   ```
   uninstall.sh -f yn platform_code
   ```

You can find complete information about silent Tivoli monitoring installation in "Appendix B. Performing a silent installation of IBM Tivoli Monitoring" of the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Silent configuration

You can use the Configuration utility in Silent mode to perform all configuration tasks for ITCAM Agent for WebSphere Applications. To do this, prepare the response file by modifying a sample provided with the Agent, or use a response file saved during interactive configuration.

All configuration tasks (see "Configuring the Agent using GUI" on page 133) for the Agent can also be performed in Silent mode, without user interaction. This may be especially useful for large-scale deployments.

To perform a configuration task, you need to prepare a response file, and then start the configuration utility.

Preparing a response file

To perform a configuration task using silent mode, you can prepare a response file for configuration in any one of two ways:

- Create a copy of a sample response file for the task. Modify this copy, and save it in a work directory, for example, as `C:\TEMP\SILENT`Sample response files are located in the *ITM_home*/`samples` directory. For file names and instructions, see "Modifying sample response files for configuration tasks" on page 199.
- Perform the configuration procedure using the GUI (see "Configuring the Agent using GUI" on page 133). In this procedure, check the **Save Configuration Setting in a Response File** box, and select the name for the response file. Modify the file if necessary, and use it for similar silent configuration on different instances and/or hosts. (Saving a response file is not available for configuring Monitoring Agent connection to the Monitoring Server).

  Attention: if you need to modify any paths in the response file, make sure to modify the \ characters to \\, : characters to \:, and prefix spaces with \ (for example, `C\:\\Program\ Files\\IBM\\WebSphere`). If you need to modify the profile home path for Data Collector Configuration, or the instance name in Data Collector unconfiguration or upgrade, make sure to replace all occurrences. For more detail on the information in the file, see "Modifying sample response files for configuration tasks" on page 199 and the comments in the sample response files.

Running the Configuration utility in silent mode

After preparing the response file for a configuration task, run the configuration utility, specifying the path and name for the response file. Perform the following procedure:

1. Change to the *ITM_home*/bin directory.

2. Invoke the configuration utility as follows. Specify the parameters in the exact order shown:

   ```
   itmcmd -A -p response_file_name yn
   ```

   where *response_file_name* is the name of the response file you have prepared (with full path). For example:

   ```
   itmcmd -A -p /tmp/silent.txt yn
   ```

Modifying sample response files for configuration tasks

For each of the configuration tasks for ITCAM Agent for WebSphere Applications, a sample response file is available in the `ITM_home/samples` directory. Make a copy of the file and edit it as required, using the information provided in the comments within the file. For more information on specific configuration options, see "Configuring the Agent using GUI" on page 133.

- **Configuring Monitoring Agent connection to the Monitoring Server and Data Collector connection to the monitoring agent**, as in the GUI or command line configuration (see "Configuring Monitoring Agent settings and communication with the Monitoring Server using GUI" on page 134), are performed with one response file. If the Agent is to communicate with the IBM Tivoli Monitoring infrastructure, you must perform this configuration task before configuring the Data Collector to monitor any application server instances. Do not perform this task if Tivoli Monitoring is not used (in a deep dive diagnostics only installation). The sample file name is `ynv_silent_config_wasdc.txt`.
- **Configuring the Data Collector to monitor an application server instance**: the sample file name is `ynv_silent_config_wasdc.txt`.
- **Unconfiguring the Data Collector from an application server instance**: the sample file name is `ynv_silent_unconfig_wasdc.txt`.
- **Configure the Data Collector communication with the Managing Server**: the sample file name is `ynv_silent_config_ms.txt`.
- **Upgrade an application server instance from an older version of the Data Collector**: the sample file name is `ynv_silent_upgrade_wasdc.txt`.
- **Change the Data Collector maintenance level for monitoring an application server instance**: the sample file name is `ynv_silent_reconfig_wasdc.txt`
- **Remove unused Data Collector maintenance levels**: the sample file name is `ynv_silent_remove_unused_wasdc.txt`

The response file is a text file, containing parameter names and values in the format *parameter=value*, for example:

```
KERNEL_HOST01=servername.domain.com
```

Comment lines begin with a number sign (#). Blank lines are ignored.

Any \ character must be escaped as \\, `:` as `\:`, and spaces must be prefixed with \, for example:

```
MS_AM_HOME=C\:\\Program\ Files\\ITCAM\\MS
```

In the file sections marked as "repeatable", parameters are specific to a profile path or an application server instance name. For these parameters, use the path or name as a key, in the format *parameter.key=value*. For example:

```
KYN_WAS_HOME./opt/IBM/WebSphere/profiles/AppSrv01=/opt/IBM/WebSphere
KYN_WAS_SERVERS./opt/IBM/WebSphere/profiles/AppSrv01=
   cells/ITCAMCell/nodes/ITCAMNode/servers/server1,
   cells/ITCAMCell/nodes/ITCAMNode/servers/server2
```

```
KYN_WAS_HOME./opt/IBM/WebSphere/profiles/AppSrv02=/opt/IBM/WebSphere
KYN_WAS_SERVERS./opt/IBM/WebSphere/profiles/AppSrv02=
   cells/ITCAMCell/nodes/ITCAMNode/servers/server3
```

Additional steps for configuring the Data Collector on Linux and UNIX systems

For every application server instance where the Data Collector was configured, perform the following steps, as applicable:

1. Restart the instance of the application server that will be monitored by the Data Collector. See "Restarting the application server" on page 263.

   If the application server fails to start up, Data Collector configuration has failed. See 2.
2. You know the Data Collector configuration has failed if any of the following problems occur:
   - After the configuration, the application server fails to restart.
   - During a GUI configuration, the summary panel for the Configuration Tool indicates the configuration has failed.
   - During a silent configuration, the command line indicates a message that the configuration has failed.
   - After the configuration, there are messages in the Tivoli common log file that indicates configuration has failed.

   If Data Collector configuration has failed, see Appendix D, "Manual changes to application server configuration for the Data Collector," on page 271.
3. Perform the tasks described in each of the following sections, if applicable.
4. Start the portal interface and verify that you can see monitored data.

Data Collector installed on IBM WebSphere Application Server 6.0.2 on SLES 9 (64-bit): enabling heap dumps

For Data Collectors installed on IBM WebSphere Application Server 6.0.2 on SuSe Linux Enterprise Server (SLES) 9 (64-bit), you must perform the following procedure in order for heap dumps to be displayed in the Heap Dump Management page in the Visualization Engine (Application Monitor) user interface:

1. Upgrade IBM WebSphere Application Server 6.0.2 with the latest available fix pack. For example, upgrade to IBM WebSphere Application Server 6.0.2.15.
2. Upgrade the JVM with the latest available fix pack. For example, upgrade to J9VM - 20060427_1214_LHdSMr.
3. Log into the IBM WebSphere Application Server administrative console for the instance of the application being monitored by the Data Collector, and navigate as follows:
   a. Click **Server** → **Application Servers** and select the server name.
   b. In the **Configuration** tab, navigate to **Server Infrastructure** → **Java and Process Management** → **Process Definition** → **Additional Properties: Java Virtual Machine**.
   c. In the **Generic JVM arguments** field, add the following strings of text:

   ```
   -Xdump:heap:events=throw,filter=com/cyanea/command/mdd/HeapDump
       -Dcyanea.mdd.brokenJ9Ras=true
   ```
4. Click **Apply**.
5. In the Messages dialog box, click **Save**.

6. In the Save to Master Configuration dialog box, complete one of the following steps:
   - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.

JDK 1.4.2 J9: enabling Java core dumps and heap dumps

If you have JDK 1.4.2 J9, you need to perform the procedure in this section to enable Java core dumps and heap dumps. On all other JDK versions, Java core dumps and heap dumps are enabled by default.

J9 is typically used on the following platforms:

- 1.4.2 JDK, 64-bit AMD64 on **Windows** and **Linux**
- 1.4.2 JDK, 32-bit i386. (J9 JVM is used only if the -Xj9 JVM option is specified.)

One way to check whether you have J9 is to check the system out log (typically SystemOut.log) for a line that contains `J2RE 1.4.2 IBM J9`.

If you have IBM JDK 1.4.2 J9, to enable Java core dumps and heap dumps perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server being monitored by the Data Collector.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
4. In the **Generic JVM arguments** field, add the following string of text:
   ```
   -Xtrace
   ```
5. Click **Apply**.
6. In the Messages dialog box, click **Save**.
7. In the Save to Master Configuration dialog box:
   - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.

Note: if you find the following message in the application server native_stderr.log file:

```
The JVM option is invalid: -Xtrace Could not create the Java virtual machine.
```

Or,

```
[ Unrecognized option: -Xtrace ] [ JVMCI123: Unable to parse 1.2 format supplied
options - rc=-6 ] Could not create JVM.
```

this means you do not have IBM JDK 1.4.2 J9. In this case, you need to remove the `-Xtrace` JVM argument.

IBM JDK 1.4.2: removing the -Xnoclassgc argument

If an older version of the Data Collector (prior to 6.1 fix pack 1 6.1.0-TIV-ITCAMfWAS_MP-FP0001) was earlier configured for this application server instance, the `-Xnoclassgc` JVM parameter may be present, as that version required it. Remove this argument, as its presence may lead to a slowdown in performance.

Perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server being monitored by the Data Collector.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
4. If `-Xnoclassgc` is still specified in the **Generic JVM arguments**, remove the setting.
5. Click **Apply**.
6. In the Messages dialog box, click **Save**.
7. In the Save to Master Configuration dialog box:
   - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.

Generating your own .jks key files and trust files

This product provides default Secure Socket Layer (SSL) certificates so you can set up a secure environment without customization. These .jks files are meant for test purposes only and expire shortly after deployment. These files are not recommended for use in a production environment. See Appendix A, "Setting up security," on page 251 for more information on setting up SSL.

If you used the root ID for the Data Collector installation and the application server is not owned and operated by the root ID

The installer will have the authority to use whatever directories and files it requires. The installer will be able to find most application server installations on the computer. But, if the application server is not owned and operated by root ID, you will need to finish the following tasks, in order for the Data Collector to work correctly:

1. Use the chown command to turn over the Data Collector installation from root to the application server owner ID:
   ```
   chown -R wasOwnerId:wasGroupId DC_home
   ```
2. Make sure that the application server owner ID can write to the /var/ibm/tivoli/common/CYN directory:
   ```
   chown -R wasOwnerId:wasGroupId /var/ibm/tivoli/common/CYN
   ```

Completing and verifying Data Collector configuration

To finish and verify configuration of the Data Collector for an application server instance, complete the following steps::

1. Restart the instance of the application server that will be monitored by the Data Collector. See "Restarting the application server" on page 263.
2. You know the Data Collector configuration has failed if any of the following problems occur:
   - After the configuration, the application server fails to restart.
   - During a GUI configuration, the summary panel for the Configuration Tool indicates the configuration has failed.

- During a command line or silent configuration, the displayed text indicates that the configuration has failed.
- After the configuration, there are messages in the Tivoli common log file that indicates configuration has failed.

If the Data Collector configuration has failed:

- Restore the application server configuration that you had before attempting the failed configuration. See “Restoring the application server configuration after a failed Data Collector configuration” on page 271.
- Run the GUI, command line, or silent configuration again.
- If the configuration fails repeatedly, contact IBM Support. If directed by IBM Support, configure the application server instance manually; see “Manually configuring the Data Collector to monitor an application server instance” on page 272.

3. If you are using the IBM Tivoli Monitoring infrastructure, start a Tivoli Enterprise Portal client and verify that you can see monitored data for the application server instance.
4. If you are using the ITCAM for Application Diagnostics Managing Server infrastructure, access the Visualization Engine and verify that you can see monitored data for the application server instance.

Uninstalling ITCAM Agent for WebSphere Applications on Linux and UNIX systems

To remove ITCAM Agent for WebSphere Applications on UNIX and Linux systems, first unconfigure the Data Collector from all application server instances. See “Unconfiguring the Data Collector from application server instances using command line” on page 119 and “Unconfigure the Data Collector for application server instances using GUI” on page 155.

After this, perform the following procedure:

1. From a command prompt, run the following command to change to the appropriate /bin directory:
   ```
   cd ITM_home/bin
   ```
2. Run the following command:
   ```
   ./uninstall.sh
   ```
   A numbered list of product codes, architecture codes, version and release numbers, and product titles is displayed for all installed products.
3. Type the number for the monitoring agent. Repeat this step for each additional installed product you want to uninstall.

Installing and uninstalling a Language Pack on Linux and UNIX systems

A Language Pack enables user interaction with the agent in a language other than English. For example, when a Spanish language pack is installed, the Tivoli Enterprise Portal workspaces and the internal messages of the Agent are displayed in Spanish.

To enable full support for a language, you must install the Language Pack on the agent host and all hosts where the Tivoli monitoring support files for the agent are installed (hub Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and all Tivoli Enterprise Portal desktop clients).

If you no longer want to use a language, uninstall the language pack for it.

Before installing or uninstalling a Language Pack, ensure that:

- The agent and the Tivoli Enterprise Portal Support Files are installed.
- The Java runtime environment (JRE) is available on every host where you are planning to install the Language Pack. (The JRE is required by IBM Tivoli Monitoring).
- You know the installation directories (*ITM_home*) for the Agent and all other Tivoli monitoring components on which you are planning to install the agent. The default installation directory is `/opt/IBM/ITM`.

Installing a Language Pack on Linux and UNIX systems

To install a Language Pack on Linux and UNIX systems you need to use the installer on the Language Pack DVD. The procedure is the same on the Agent host, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client.

Perform the following procedure:

1. Mount the Language Pack DVD. Make sure the full path to the mount directory does not include spaces.
2. Use the following commands to start the installer from the Language Pack DVD:
   ```
   cd dir_name
   ./lpinstaller.sh -c ITM_home
   ```
3. Select the language of the installer and click OK.

   Note: In this step, you select the language for the installer user interface, not the language pack that will be installed.
4. Click **Next** on the Introduction window.
5. Select **Add/Update** and click **Next**.
6. Select the directory where the the National Language Support package (NLSPackage) files are located. This is the `nlspackage` directory on the Language Pack DVD.
7. Select **ITCAM Agent for WebSphere Applications**.
8. Select the languages to install and click **Next**.

   Note: You can hold down the **Ctrl** key for multiple selections.
9. Examine the installation summary page and click **Next** to begin installation.
10. Click **Next**.
11. Click **Finish** to exit the installer.
12. If you are installing the Language Pack on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart the server or client. If the Eclipse Help Server is running, restart it as well.

Uninstalling a Language Pack on Linux and UNIX systems

To uninstall a Language Pack on Linux and UNIX systems you need to use the installer on the Language Pack DVD. The procedure is the same on the Agent host, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client.

Perform the following procedure:

1. Mount the Language Pack DVD. Make sure the full path to the mount directory does not include spaces.
2. Use the following commands to start the installer from the Language Pack DVD:

   ```
   cd dir_name
   ./lpinstaller.sh -c ITM_home
   ```
3. Select the language of the installer and click OK.

   Note: In this step, you select the language for the installer user interface, not the language pack that will be installed.
4. Click **Next** on the Introduction window.
5. Select **Remove** and click **Next**.
6. Select **ITCAM Agent for WebSphere Applications**.
7. Select the languages to uninstall and click **Next**.

   Note: You can hold down the **Ctrl** key for multiple selections.
8. Examine the installation summary page and click **Next** to begin installation.
9. Click **Next**.
10. Click **Finish** to exit the installer.
11. If you are installing the Language Pack on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart the server or client. If the Eclipse Help Server is running, restart it as well.

Part 4. Installing and Configuring ITCAM Agent for WebSphere Applications on a Remote Computer

Chapter 6. Installing and configuring ITCAM Agent for WebSphere Applications remotely

IBM Tivoli Monitoring support remote installation and configuration of Agents, including ITCAM Agent for WebSphere Applications. This section contains instructions for remote installation and configuration specifict to this Agent.

For details on remote agent deployment in IBM Tivoli Monitoring, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

This capability requires IBM Tivoli Monitoring. If Tivoli Monitoring is not used (in a deep dive diagnostics only installation), remote installation and configuration is not supported.

Installing, upgrading and configuring ITCAM Agent for WebSphere Applications remotely using command line

You can use the `tacmd` command on a hub Tivoli Enterprise Monitoring Server (TEMS) host to install the Agent remotely on any host running the IBM Tivoli Monitoring OS Agent, You can also use this command to upgrade the remote Agent (from the Tivoli Enterprise Monitoring Agent of ITCAM for WebSphere 6.1, or the WebSphere Tivoli Enterprise Monitoring Agent of ITCAM for Web Resources 6.2), and to configure Tivoli Enterprise Monitoring Agent settings.

Before installing or upgrading the Agent, you need to add its installation bundles to the TEMS.

For details on using `tacmd`, and for other available options (including installation from a remote TEMS), see *IBM Tivoli Monitoring Command Reference*.

Note: This section describes commands in a syntax valid on Linux and UNIX systems. On a Windows TEMS host, use `tacmd` instead of `./tacmd`, and use \ instead of / in paths.

Adding the installation bundles

In most cases, it is best practice to add both the Windows bundle and the Linux and UNIX systems bundle to a TEMS host. In this way you will be able to deploy the Agent on hosts with both platform types. However, you can choose to add only the Windows bundle or only the Linux and UNIX systems bundle.

Perform the following procedure:

1. Copy or mount the Agent installation images on the TEMS host.
2. Change to the *`ITM_HOME`*`/bin` directory.
3. Use the following command to log on:

   ```
   ./tacmd login -s localhost -u sysadmin -p password
   ```

   Use the password for the `SYSADMIN` user of IBM Tivoli Monitoring.
4. To add the installation bundle for Windows target hosts, enter the command:

   ```
   ./tacmd addBundles -i path_to_Windows_image/WINDOWS/Deploy -t yn
   ```

5. To add the installation bundle for Linux or UNIX system target hosts:

   ```
   ./tacmd addBundles -i path_to_Linux_UNIX_package/unix -t yn
   ```

Installing the Agent on a remote host

To install the Agent on a remote host, perform the following procedure on the TEMS host:

1. Change to the *ITM_HOME*/bin directory.
2. Use the following command to log on:

   ```
   ./tacmd login -s localhost -u sysadmin -p password
   ```

   Use the password for the SYSADMIN user of IBM Tivoli Monitoring.
3. To list the available Operating System agents on remote hosts, enter the command:

   ```
   ./tacmd listSystems -t UX LZ NT
   ```

   Find the necessary remote host in the list, and note the name of the Operating System agent on it.

   Important: The Operating System agent must be running. This is indicated by Y in the list. If the Operating System agent on the target host is not running, start it before performing the installation.
4. To install ITCAM Agent for WebSphere Applications on a remote host, enter the command:

   ```
   ./tacmd addSystem -t yn -n OS_agent_name
   ```

   OS_agent_name is the name of the Operating System agent, for example, lrtx228:LZ. The node identifier displayed in the Tivoli Enterprise Portal navigation tree will be set to "Primary", and the port for incoming Data Collector connections will be set to 63335.

   Alternatively, you can install ITCAM Agent for WebSphere Applications on a remote host and configure custom settings for the node identifier and port at the same time. To do this, enter the command:

   ```
   ./tacmd addSystem -t yn -n OS_agent_name  --properties
     CONFIGURATION_TYPE.configure_type="tema_configure"
     KYN_Tema_Config.KYN_ALT_NODEID="node_id"
     KYN_Tema_Config.KYN_PORT=port_number
   ```

   OS_agent_name is the name of the Operating System agent, for example, lrtx228:LZ.

   node_id is an alternative Node ID for identifying the agent. This identifier that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is "Primary", used with the host name of the computer where the Agent is installed is used.

   port_number is the TCP socket port that the monitoring agent will use to listen for connection requests from the Data Collectors. The default is 63335. The port will only be used for local communication on the host (except if you use the monitoring agent to support Data Collectors on IBM i hosts, see *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Data Collector Installation and Configuration Guide for IBM i*).

If you want to monitor the remote deployment status, enter the command:

```
./tacmd getDeployStatus
```

When the Agent is successfully installed, it will automatically connect to the Tivoli Enterprise Monitoring Server, and the Tivoli Enterprise Portal will show it.

Upgrading the Agent on a remote host

To upgrade the Agent on a remote host (from the Tivoli Enterprise Monitoring Agent of ITCAM for WebSphere 6.1, or the WebSphere Tivoli Enterprise Monitoring Agent of ITCAM for Web Resources 6.2), perform the following procedure on the TEMS host:

1. Change to the *ITM_HOME*/bin directory.
2. Use the following command to log on:

   ```
   ./tacmd login -s localhost -u sysadmin -p password
   ```

   Use the password for the SYSADMIN user of IBM Tivoli Monitoring.
3. To list the available Operating System agents on remote hosts, enter the command:

   ```
   ./tacmd listSystems -t UX LZ NT
   ```

   Find the necessary remote host in the list, and note the name of the Operating System agent on it.

   Important: The Operating System agent must be running. This is indicated by Y in the list. If the Operating System agent on the target host is not running, start it before performing the installation.
4. To install ITCAM Agent for WebSphere Applications on a remote host, enter the command:

   ```
   ./tacmd updateagent -t yn -n OS_agent_name
   ```

   OS_agent_name is the name of the Operating System agent, for example, lrtx228:LZ.

If you want to monitor the remote deployment status, enter the command:

```
./tacmd getDeployStatus
```

When the Agent is successfully installed, it will automatically connect to the Tivoli Enterprise Monitoring Server, and the Tivoli Enterprise Portal will show it.

Configuring the Agent on a remote host

To configure Monitoring Agent settings on a remote host where the Agent is installed, perform the following procedure on the TEMS host:

1. Change to the *ITM_HOME*/bin directory.
2. Use the following command to log on:

   ```
   ./tacmd login -s localhost -u sysadmin -p password
   ```

   Use the password for the SYSADMIN user of IBM Tivoli Monitoring.
3. To list the available Agents on remote hosts, enter the command:

   ```
   ./tacmd listSystems -t yn
   ```

   Find the necessary remote host in the list, and note the name of the Agent on it.

Important: The Agent must be running. This is indicated by `Y` in the list. If the Operating System agent on the target host is not running, start it before performing the installation.

4. To configure ITCAM Agent for WebSphere Applications on a remote host, enter the command:

```
./tacmd configureSystem --system Agent_name --properties
  CONFIGURATION_TYPE.configure_type="tema_configure"
  KYN_Tema_Config.KYN_ALT_NODEID="node_id"
  KYN_Tema_Config.KYN_PORT=port_number
```

   Agent_name is the name of ITCAM Agent for WebSphere Applications on the remote host, for example, `Primary:tivm40:KYNA`;

   node_id is an alternative Node ID for identifying the agent. This identifier that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is "Primary", used with the host name of the computer where the Agent is installed is used.

   port_number is the TCP socket port that the monitoring agent will use to listen for connection requests from the Data Collectors. The default is 63335. The port will only be used for local communication on the host (except if you use the monitoring agent to support Data Collectors on IBM i hosts, see *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Data Collector Installation and Configuration Guide for IBM i*).

   Alternatively, you can create a response file with the settings, and then run the tacmd command on the response file. The content of the response file is:

```
--system
Agent_name
--properties
CONFIGURATION_TYPE.configure_type="tema_configure"
KYN_Tema_Config.KYN_ALT_NODEID="node_id"
KYN_Tema_Config.KYN_PORT=port_number
```

   For example:

```
--system
Primary:tivm40:KYNA
--properties
CONFIGURATION_TYPE.configure_type="tema_configure"
KYN_Tema_Config.KYN_ALT_NODEID="mynode"
KYN_Tema_Config.KYN_PORT=63336
```

   To use the response file, enter the following command:

```
./tacmd configureSystem response_file_name
```

When the Agent is successfully configured, it will automatically connect to the Tivoli Enterprise Monitoring Server using the new settings, and the Tivoli Enterprise Portal will show it.

To perform other configuration tasks on a remote Agent installation, see “Configuring ITCAM Agent for WebSphere Applications remotely using Tivoli Enterprise Portal” on page 214.

Installing ITCAM Agent for WebSphere Applications remotely using Tivoli Enterprise Portal

You can use Tivoli Enterprise Portal to install ITCAM Agent for WebSphere Applications remotely. Before this installation, the Agent support files must be installed on the Tivoli Enterprise Portal Server (including browser client support files), hub Tivoli Enterprise Monitoring Servers, and Tivoli Enterprise Portal desktop clients.

Adding the Agent to the remote installation depot

To make remote installation available, you must first add ITCAM Agent for WebSphere Applications to the remote deployment depot on the hub Tivoli Enterprise Monitoring Server.

On Windows, see “Installing application support on the Tivoli Enterprise Monitoring Server” on page 82; be sure to select the Agent for the remote deployment depot in Step 7 on page 82.

Performing a remote installation

You may need to prepare the host computer for installation of the Agent. See Chapter 2, “Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Windows,” on page 11 and Chapter 4, “Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Linux and UNIX systems,” on page 99.

To install ITCAM Agent for WebSphere Applications remotely using IBM Tivoli Monitoring, perform the following procedure:

1. Select the node for installation in Tivoli Enterprise Portal. (The node must already be a part of IBM Tivoli Monitoring infrastructure; for details on setting up a node in IBM Tivoli Monitoring, see *IBM Tivoli Monitoring: Installation and Setup Guide*).
2. Right-click the name of the node, and select **Add Managed System...**
3. In the **Select a monitoring Agent** window, select **IBM Tivoli Composite Application Manager Agent for WebSphere Applications** and click **OK**.
4. The agent configuration window is displayed. Select **Configure Tivoli Enterprise Monitoring Agent**, and configure the Monitoring Agent settings. See “Configure Monitoring Agent settings” on page 28. Other configuration options are not available before installation is complete.

   Note: while you can choose to create a response file, the **Browse** button will not be available. You will need to enter the pathname for the response file manually. The file will be saved on the host where the Agent is installed.
5. Click **Finish**. The Agent installation process will be started; you can track its progress in the **Deployment Status** workspace.

Configuring ITCAM Agent for WebSphere Applications remotely using Tivoli Enterprise Portal

You can use Tivoli Enterprise Portal to configure ITCAM Agent for WebSphere Applications remotely. You can configure and unconfigure the Data Collector for application server instances, configure the communication of the Data Collector to the Managing Server, and upgrade application server instances from previous versions of the Data Collector.

To configure ITCAM Agent for WebSphere Applications remotely using IBM Tivoli Monitoring, select the Agent in the Tivoli Enterprise Portal. Right click it, and select **Configure**.

The **Managed System Configuration** window is displayed.

This window is the same as the Agent Configuration window available on the host where the Agent is installed. Using this window, you can perform Agent configuration. See "Configuring ITCAM Agent for WebSphere Applications on Windows" on page 25 for the configuration procedures.

The following configuration procedures are available:

- Configuring Data Collector communication to the monitoring agent. See "Configure Monitoring Agent settings" on page 28.
- Configuring the Data Collector to monitor application server instances. See "Configure the Data Collector to monitor application server instances" on page 32.
- Unconfiguring the Data Collector from application server instances. See "Unconfigure the Data Collector for application server instances" on page 47.
- Enable, disable, or configure Data Collector communication to the Managing Server. See "Configure Data Collector communication with the Managing Server" on page 53
- Upgrade monitoring from a previous version of the Data Collector. See "Upgrading monitoring to Data Collector 7.1" on page 60.
- Change the maintenance level of the Data Collector. See "Changing Data Collector maintenance level" on page 69.
- Remove an unused Data Collector maintenance level. See "Removing a Data Collector maintenance level" on page 76.

Note: while you can choose to create a response file, the **Browse** button will not be available. You will need to enter the pathname for the response file manually. The file will be saved on the host where the Agent is installed.
If you configure the Data Collector to monitor application server instances, the instances will be restarted automatically, so that the changes can take effect. However, you may still need to perform additional tasks on the host computer after this configuration. See "Additional steps for configuring the Data Collector on Windows" on page 91 and "Additional steps for configuring the Data Collector on Linux and UNIX systems" on page 200.

Part 5. Advanced configuration of the Agent

Chapter 7. Customization and advanced configuration for the Data Collector

This section contains instructions for customizing your configuration of the Data Collector.

Perform the procedures in each of the following sections, if they apply.

Properties files for the Data Collector

Several properties files control Data Collector configuration and behavior.

These files, as well as other files used by the Data Collector, are located under the *DC_home* directory. The location of *DC_home* is *ITM_home*\TMAITM6\wasdc\7.1.0.1 on Windows, *ITM_home*/*architecture_code*/yn/wasdc/7.1.0.1 on Linux and UNIX systems.

For most common changes to this configuration, you will need to edit the Data Collector properties file and the Toolkit properties file. Several other properties files also exist.

The Data Collector properties file

The Data Collector properties file is automatically created by the installer, and is unique for every application server instance monitored by the Data Collector. Its name is *DC_home*/runtime/*appserver_version.node_name.server_name*/datacollector.properties.

However, to facilitate future upgrades, **do not change** this file.

Instead, add the settings you want to modify to the Data Collector custom properties file. This file is named *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/datacollector_custom.properties ; this will override the values in the Data Collector properties file.

Note: If the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/datacollector_custom.properties file does not exist, create it when you need to make changes. You may also need to create the custom directory.

The Toolkit properties file

The Toolkit properties file is automatically created by the Data Collector at startup, using various input files. It is unique for every application server instance monitored by the Data Collector. Its name is *DC_home*/runtime/*appserver_version.node_name.server_name*/toolkit.properties.

Because this file is re-created at each Data Collector startup, **do not make any changes** to this file as they will be overwritten.

Instead, add the settings you want to modify to the Data Collector custom properties file. This file is named *DC_home*/runtime/

app_server_version.*node_name*.*server_name*/custom/toolkit_custom.properties ; this will override the values in the Toolkit properties file.

You may also set toolkit properties for all the application server instances monitored by this installation of the Data Collector. To do this, add the settings to the global toolkit custom properties file: *DC_home*/runtime/custom/ toolkit_global_custom.properties . However, if a property is set in the instance specific toolkit_custom.properties file, it will override the value in the global file for this instance.

Note: If the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/ toolkit_custom.properties or *DC_home*/runtime/custom/ toolkit_custom.properties file does not exist, create it when you need to make changes. You may also need to create the custom directory.

Other properties files

The following properties files are unique for every application server instance monitored by the Data Collector:

- *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/ cynlogging.properties defines the log file names and logging details for the Java portion of the Data Collector.
- *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/cyn-cclog.properties defines the log file names and logging details for the C++ portion of the Data Collector.
- *DC_home*/runtime/*appserver_version.node_name.server_name*/kwjdc.properties defines communication with the monitoring agent, including the host name and port for the monitoring agent host.

Tuning Data Collector performance and monitoring scope

The Data Collector monitors the performance of the application server in several ways. This monitoring introduces a performance overhead. The scope and accuracy of the monitoring can vary; but, when more information is gathered, the performance overhead is increased.

The monitoring scope is broadly determined by the monitoring level, which the user can set as necessary.

In the Tivoli Enterprise Portal, the available monitoring levels are L1 and L2. In the Visualization Engine, monitoring levels (known as Monitoring On Demand, or MOD, levels) are L1, L2, and L3.

This level is set independently for IBM Tivoli Monitoring and the Managing Server. For example, the user may set monitoring level L1 for IBM Tivoli Monitoring from the Tivoli Enterprise Portal, and at the same time set MOD L2 in the Managing Server Visualization Engine. In this case, only L1 data will be available in the Tivoli Enterprise Portal, but L2 information will be displayed in the Visualization Engine.

You can also set the *sampling rate* for the Managing Server and Monitoring Agent independently. For the Managing Server, the sampling rate determines the percentage of monitored requests that are archived in the database; irrespective of the sampling rate, all data is sent to the Managing Server, so the resource usage of the Data Collector is not affected by it. The sampling rate is set separately for every Data Collector installation. Having a low sampling rate does not prevent the user from seeing requests that have hung in-flight, nor does it prevent Managing Server traps and Tivoli Enterprise Portal situations from working on all requests. Generally, a 2% sampling rate is suggested for MOD L1 Tivoli monitoring data collection in a production environment where data is often stored for 15 to 30 days or more.

Note: For Managing Server data collection, the sampling rate does not apply to Custom Request and Nested Request monitoring.

You can also fine tune the Data Collector monitoring process using the properties files. This impacts the performance overhead, as well as the scope and accuracy of the monitoring. While the default configuration is broadly acceptable for common situations, you can use the properties files to reach the performance and monitoring that closely match the requirements of your environment.

Data Collector internal buffering and turbo mode settings

The following parameters afect buffering in communication between the Data Collector and ITCAM for Application Diagnostics Managing Server. In most cases, the default settings are appropriate. Do not change these parameters unless directed by IBM Software Support. These settings do not affect communication with the Monitoring Agent.

Internal Buffering settings

The following parameters in the Data Collector properties file (see “The Data Collector properties file” on page 217) control internal buffering in the Data Collector.

internal.memory.limit
: The default value is `100` (MB). This property limits the amount of memory the Data Collector may use for all its buffering needs. Reducing this setting can lower the memory overhead introduced by the Data Collector; however, it can also increase the probability of buffer overflow at MOD L2 or L3 during periods of very high transaction volume. You can also reduce buffer load by limiting the monitoring scope for MOD L2 and L3, using the settings in the rest of this chapter, especially “Controlling instrumentation of application classes for lock analysis, memory leak analysis, and method profiling and tracing” on page 223.

internal.memory.accept.threshold
: The default value is `2` (MB). Once the amount of memory specified in `internal.memory.limit` is reached, a buffer overflow state happens, and data will not be buffered. This property specifies the minimum amount of free memory to be reached before buffering is resumed.

internal.url.limit
: The default value is `1000`. This property controls the maximum URL length accepted by the Data Collector. If your URL length typically exceeds this value, it should be increase to avoid display truncation.

internal.sql.limit
: The default value is `5000`. This property controls the maximum SQL length accepted by the Data Collector. If your SQL statement length is typically greater than this value, the value should be increased to avoid display trunaction.

internal.probe.event.queue.size.limit
The default value is `900000`. This property controls the maximum size of the queue of events maintained by the Data Collector.

internal.probe.event.packet.size
The default value is `5000` Kbytes. Changing the default is not recommended. Valid values are `1` to `4000000` (or up to available process memory on the server). This property specifies the size of the Data Collector internal send buffer. The send buffer controls how much data the Data Collector can be sent to the Publish Server at a given time. In normal situations, this property does not have to be changed, as the default send buffer size is more than adequate.

Turbo Mode

If the Data Collector cannot send data to the Managing server fast enough, Data collector buffer space may be exhausted. The Data Collector may react in two ways, depending on whether *turbo mode* is enabled or disabled.

Turbo mode is controlled by the **dc.turbomode.enabled** setting in the Data Collector properties file (see "The Data Collector properties file" on page 217). Set it to `true` to enable turbo mode, or to `false` to disable it. By default, turbo mode is disabled.

If turbo mode is enabled, the Data Collector will enter turbo mode when three quarters of the maximum memory size (set in `internal.memory.limit`) is used. In turbo mode, the Data Collector raises the priority of the threads that send data to the Managing Server and the Monitoring Agent. Application threads remain at a lower priority, and may freeze until the buffer shortage is relieved. This ensures maximum reporting accuracy but can have a significant impact on application performance.

In turbo mode, the Data Collector also continues to monitor any existing requests, but any new incoming requests will not be monitored until the buffer shortage is relieved. The application will process them, and the Data Collector will notify the Managing Server of a "dropped" request.

If turbo mode is disabled, the Data Collector will drop any monitoring data in the event of a buffer shortage. Therefore, information in the Tivoli Enterprise Portal and Visualization Engine may be incomplete, but application performance will not be impacted.

Disable turbo mode on "mission critical" production systems, where any application thread freeze is not acceptable in any situation. However, a danger of buffer shortage (and, therefore, engagement of turbo mode) usually happens only in MOD L2 or L3; on production systems, users need to enable these levels only when investigating an issue. Turbo mode may be of use in such an investigation. So, if a significant performance impact in the event of an investigation is acceptable, you can enable turbo mode.

Enabling instrumentation and monitoring of RMI/IIOP requests between application servers

If the Data Collector will communicate with ITCAM for Application Diagnostics Managing Server, and two or more application servers are using Remote Method Invocation over Internet InterORB Protocol (RMI/IIOP), you need to enable instrumentation and monitoring of RMI/IIOP requests in order to view composite requests (via correlation icons) in the Visualization Engine.

All the servers must be instrumented by Data Collectors connected to the same Managing Server.

For all the application servers, in the Toolkit custom properties file (see "The Toolkit properties file" on page 217), add or uncomment the following property:

```
org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.toolkit.
   ai.orbinterceptor.Initializer=true
```

Disabling various types of Byte Code Instrumentation for J2EE APIs

In Byte Code Instrumentation (BCI), the Data Collector intercepts method entry and exit calls for various types of Java APIs in order to create an execution flow of each application request. Some resources are used for the monitoring. You can tune the Data Collector so that some of the APIs are not monitored, reducing resource use. For some APIs, you can also disable collection of BCI information for MOD L1, reducing resource use for this level (typically enabled most of the time on production systems).

To disable BCI monitoring for J2EE APIs, set (or uncomment) the following properties in the toolkit custom properties file (see "The Toolkit properties file" on page 217). These properties are set to `true` by default. After changing the file, restart the application server instance.

Table 17. Adding lines to toolkit_custom.properties

Type of J2EE API	Line to add to toolkit_custom.properties file
Enterprise JavaBeans™ (EJB)	`com.ibm.tivoli.itcam.toolkit.ai.enableejb=false`
Java Connector Architecture (JCA)	`com.ibm.tivoli.itcam.toolkit.ai.enablejca=false`
Java Database Connectivity (JDBC)	`com.ibm.tivoli.itcam.toolkit.ai.enablejdbc=false`
Java Naming and Directory Interface (JNDI)	`com.ibm.tivoli.itcam.toolkit.ai.enablejndi=false`
Java Message Service (JMS)	`com.ibm.tivoli.itcam.toolkit.ai.enablejms=false`
Web containers for Servlets/ JavaServer Pages (JSP)	`com.ibm.tivoli.itcam.dc.was.webcontainer=false`
HTTP session count tracking	`com.ibm.tivoli.itcam.toolkit.ai.enablesessioncount=false`
CICS® Transaction Gateway (CTG)	`com.ibm.tivoli.itcam.dc.ctg.enablectg=false`
IMS™	`com.ibm.tivoli.itcam.dc.mqi.enableims=false`
Java Data Objects (JDO)	`com.ibm.tivoli.itcam.dc.mqi.enablejdo=false`

Table 17. Adding lines to toolkit_custom.properties (continued)

Type of J2EE API	Line to add to toolkit_custom.properties file
Message Queue Interface (MQI)	`com.ibm.tivoli.itcam.dc.mqi.enablemqi=false`
Axis web service	`com.ibm.tivoli.itcam.toolkit.ai.axis.enablewebservice=false`
Remote Method Invocation (RMI)	`am.ejb.rmilistener.enable=false`
IBM WebSphere Application Server EJB container	`com.ibm.tivoli.itcam.dc.was.enableEJBContainer=false`

WebSphere Portal Server 5.1	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureWPSServlet=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureAuthorization=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.WPSDistributedMapCache=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureGatewayServlet=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureLogin=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureModelBuilding=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePageLoading=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePageRendering=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePortal=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePortalActionLegacy=false`
	`com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePortalActionStd=false`

WebSphere Portal Server 6	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureWPSServlet=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureAuthorization=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.WPSDistributedMapCache=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureGatewayServlet=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureLogin=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureModelBuilding=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePageLoading=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePageRendering=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePortal=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePortalActionLegacy=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePortalActionStd=false`
	`com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureStandardPortal=false`

For most API types, BCI information is only collected for MOD levels L2 and L3. If the MOD Level is set to L1, BCI data is not sent to IBM Tivoli Monitoring or the Managing Server, although the method entry and exit is still intercepted. (The MOD Level set for IBM Tivoli Monitoring does not affect the data sent to the Managing Server, and vice versa).

For the following API types, BCI information (if it is not disabled completely, as shown above) is also collected at MOD L1. For performance reasons, you can also disable it only for L1 monitoring, while keeping it enabled for L2 and L3. To do this, add (or uncomment) the following lines in the toolkit custom properties file (see "The Toolkit properties file" on page 217):

Table 18. Modifying lines in toolkit_custom.properties

Type of J2EE API	Line to add to toolkit_custom.properties file
JCA	`com.ibm.tivoli.itcam.toolkit.ai.jca.callback.unconditional=false`
JDBC	`com.ibm.tivoli.itcam.toolkit.ai.jdbc.callback.unconditional=false`
JNDI	`com.ibm.tivoli.itcam.toolkit.ai.jndi.callback.unconditional=false`
JMS	`com.ibm.tivoli.itcam.toolkit.ai.jms.callback.unconditional=false`

Attention: Setting any of these properties to `false` may result in some missing data when MOD Level is switched from L1 to L2. For example, the Data Collector may not be able to determine the Data Source names for JDBC requests.

Controlling instrumentation of application classes for lock analysis, memory leak analysis, and method profiling and tracing

The Data Collector can use Byte Code Instrumentation (BCI) to collect lock analysis information, memory leak analysis information (at MOD L3), method profiling (at MOD L2) and application method entry and exit (at MOD L3). Instrumentation for this data is disabled by default, and you must enable it if the information is required. This information is only displayed in the Visualization Engine of ITCAM for Application Diagnostics Managing Server.

To enable BCI for lock analysis, Level 3 memory leak analysis, and Level 3 method entry and exit tracing, you must make adjustments to the toolkit custom properties file (see "The Toolkit properties file" on page 217).

Making these adjustments will activate the use of one or more configuration files in the *DC_home*`/itcamdc/etc` directory, which contain the default settings to control BCI. The configuration files and default settings are described in the following table:

Table 19. Byte Code Instrumentation configuration files

File name	Purpose	Default behavior
lock_analysis.xml	Defines application lock analysis BCI. **Note:** Specific behavior in each MOD level is determined by settings in the Data Collector properties file.	Lock acquire and release requests for all application classes are Byte-Code-Instrumented. Lock event, lock contention, and lock reporting information is provided in MOD L2 and MOD L3. (You can enable lock analysis for MOD L1 as well; see "Customizing lock analysis" on page 224).
memory_leak_diagnosis.xml	Defines application Memory Leak Diagnosis BCI.	Heap allocations for all classes instantiated by all application classes are Byte-Code-Instrumented. Leak Analysis data is collected at MOD L3.
method_entry_exit.xml	Defines application method entry and exit BCI.	All non-trivial methods for all application classes, subject to certain thresholds and limits, are Byte-Code-Instrumented. Method profiling data is collected at MOD L2; method entry and exit analysis data is collected at MOD L3.

If you want to enable one or more of the BCI features with the default settings, see "Enabling Byte Code Instrumentation features with default settings" on page 224.

If you want to customize the default settings and make more granular choices for what classes and methods to modify, see the following sections:

- "Customizing lock analysis" on page 224
- "Customizing memory leak diagnosis" on page 226
- "Customizing method profiling and method entry and exit tracing" on page 228

Attention: Enabling Byte Code Instrumentation for any of these features will slightly increase resource usage even on monitoring levels where no data is collected for them.

Enabling Byte Code Instrumentation features with default settings

Perform the following procedure to enable one or more of the BCI features (lock analysis, Level 3 memory leak analysis, and method profiling and entry and exit tracing,) with the default settings. Method profiling at MOD L2 and method entry and exit tracing at MOD L3 are enabled by the same properties.

1. In the toolkit custom properties file (see "The Toolkit properties file" on page 217), uncomment one or more of the following lines by removing the number sign (#) at the beginning of the line:

   ```
   am.camtoolkit.gpe.customxml.lock=DC_home/itcamdc/etc/lock_analysis.xml
   am.camtoolkit.gpe.customxml.leak=DC_home/itcamdc/etc/memory_leak_diagnosis.xml
   am.camtoolkit.gpe.customxml.L3=DC_home/itcamdc/etc/method_entry_exit.xml
   ```

   See Table 19 on page 223 for a description of the default behaviors when each of these configuration files is activated.
2. Set one or more of the following properties to `true`:

   ```
   com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis=true
   com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
   com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
   ```

Customizing lock analysis

By default, if lock analysis is enabled, lock acquire and release requests for all application classes are Byte-Code-Instrumented. With default settings, lock contention information is provided in MOD L2 and MOD L3. You may configure the Data Collector to modify the lock information provided on the different MOD levels, and to exclude some classes from BCI for lock analysis.

Configuring lock analysis information for MOD levels

The following properties in the Data Collector properties file (see "Properties files for the Data Collector" on page 217) control the lock analysis information provided by the Data Collector.

internal.lockanalysis.collect.L*n*.lock.event

This property whether lock acquisition/release events are collected and passed to the Managing Server. (If the Managing Server is not used, this parameter is ignored). The variable *n* can represent MOD L1, L2 or L3. Possible values are `true` or `false`. In most cases, the recommended setting at all levels is `false` as there is little benefit in displaying lock acquisition events if they do not involve contention; lock contention events are collected separately. However, you may wish to enable lock event collection for some development tasks.

Example:

```
internal.lockanalysis.collect.L1.lock.event = true
```

internal.lockanalysis.collect.L*n*.contend.events

This property controls whether lock contention events are collected and passed to the Managing Server. (If the Managing Server is not used, this parameter is ignored). The variable *n* can represent MOD L1, L2 or L3. Possible values are `true`, `false` or `justone`.

`True` indicates contention records are collected. For each lock acquisition request that results in contention, a pair of contention records are written for each thread that acquired the lock ahead of the requesting thread. False indicates contention records are not written. Justone indicates contention records are written, however, a maximum of one pair of contention records are written for each lock acquisition request that encounters contention, regardless of how many threads actually acquired the lock prior to the requesting thread.

Setting this property to true enables you to determine whether a single thread is holding a lock for an excessive time, or if the problem is due to too many threads all attempting to acquire the same lock simultaneously.

The recommended setting at L1 is false. The recommended setting at L2 is justone, this enables you to collect just one pair of contention records for each lock acquisition that encountered contention. The recommended setting at L3 is true, in order to identify every thread that acquired the lock ahead of the requesting thread; this setting has a high performance cost, which is common for L3 monitoring, and the user should only enable L3 for a limited time to reduce performance impact.

Example:

```
internal.lockanalysis.collect.L2.contend.events = justone
```

internal.lockanalysis.collect.L*n*.contention.inflight.reports

This parameter controls whether data is collected for the Lock Contention report, available in the Visualization Engine of the Managing Server. (If the Managing Server is not used, this parameter is ignored). The variable *n* can represent Mod L1, L2 or L3. Possible values are true or false. The recommended setting at L1 is false. The recommended setting at L2 and L3 is true.

Example:

```
internal.lockanalysis.collect.L3.contention.inflight.reports = true
```

Setting classes for lock analysis instrumentation

To set classes for lock analysis instrumentation, perform the following procedure:

1. Make a copy of the *DC_home*/itcamdc/etc/lock_analysis.xml in a temporary location. Open the copy in a text editor.
2. Modify the lockingClasses specification in the file.

   This element defines the classes for which lock requests will be Byte-Code-Instrumented. By default, all lock requests in all application classes are selected. By modifying this tag, you can implement a more granular selection, although within a class all lock requests are Byte-Code-Instrumented. Multiple lockingClasses tags can be specified.

   The lockingClasses element can include wildcard characters. The following section describes how the wildcard characters work:

   - Asterisk (*) stands for zero or more occurrences of any character when used by itself. When embedded within a sequence of characters (for example, java.*.String), it matches zero or more occurrences of any character except the package separator (.).
   - Two periods (..) can be used to specify all sub-packages. It matches any sequence of characters that starts and ends with the package separator (.).

     For example, java..String matches java.lang.String and com.ibm..* matches any declaration beginning with com.ibm.
   - If the locking class name begins with an exclamation point (!), any classes matching the classes identified in the tag are specifically excluded from BCI

for lock analysis. This is useful for indicating that all classes are to be Byte-Code-Instrumented except for those classes that are specifically excluded.

In the following example, an application with a package name of com.mycompany.myapp has the following requirements:

- Only classes that begin with Cus or Sup should be Byte-Code-Instrumented for lock analysis.
- The Supplier class should not be Byte-Code-Instrumented for lock analysis.

The following example shows the contents of the customized lock_analysis.xml file that accomplishes this:

```
 <aspect>
   <type>application</type>
   <name>com.ibm.tivoli.itcam.toolkit.ai.aspectj.apptrace.CaptureLock</name>
   <enabledProperty>
          com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis</enabledProperty>
   <defaultEnabled>true</defaultEnabled>
   <lockingClass>com.mycompany.myapp.Cus*</lockingClass>
   <lockingClass>com.mycompany.myapp.Sup*</lockingClass>
   <lockingClass>!com.mycompany.myapp.Supplier</lockingClass>
</aspect>
```

3. Complete one of the following steps:
   - Save the file in the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom directory, then complete the following steps:
     a. In the toolkit custom properties file (see "The Toolkit properties file" on page 217), set the property am.camtoolkit.gpe.customxml.lock to the name (without path) of the file you modified in Step 2 on page 225.
     b. In the same toolkit custom properties file, set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis=true
        ```
   - Save the file in any directory on the monitored host, then complete the following steps:
     a. In the toolkit custom properties file (see "The Toolkit properties file" on page 217), set the property am.camtoolkit.gpe.customxml.lock to the path and name for the file you modified in Step 2 on page 225.
     b. In the same toolkit custom properties file, set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis=true
        ```

Customizing memory leak diagnosis

By default, if memory leak analysis is enabled, all application classes are Byte-Code-Instrumented for memory leak analysis and all information is collected in MOD L3. You may configure the Data Collector to exclude some classes from BCI for memory leak analysis.

Perform the following procedure to set classes for Memory Leak Diagnosis:

1. Make a copy of the *DC_home*/itcamdc/etc/memory_leak_diagnosis.xml file in a temporary location. Open the copy in a text editor.
2. Modify the parameters in the file. The following table describes the tags you can modify:

Table 20. Parameters for the memory leak diagnosis configuration file

Tag name	Description
heapAllocationTarget	Defines the allocating and allocated classes for which heap allocations will be Byte-Code-Instrumented. By default, all allocating and allocated classes are selected. By modifying the allocatingClassName and allocatedClassName tags within the heapAllocationTarget tag, you can implement a more granular selection. Each heapAllocationTarget tag must contain exactly one allocatingClassName tag, and one or more allocatedClassName tags. Multiple heapAllocationTarget tags can be specified.
allocatingClassName	Identifies the name of a class or classes to be modified. Each heapAllocationTarget tag must contain exactly one allocatingClassName tag.
allocatedClassName	Identifies the specific heap allocation requests within the class or classes identified by the allocatingClassName tag that are to be Byte-Code-Instrumented. Each heapAllocationTarget tag must contain one or more allocatedClassName tags.

Both allocatingClassName and allocatedClassName tags can include wildcard characters. The following is a summary of how the wildcard characters work:

- Asterisk (*) stands for zero or more occurrences of any character when used by itself. When embedded within a sequence of characters (for example, java.*.String), it matches zero or more occurrences of any character except the package separator (.).
- Two periods (..) can be used to specify all sub-packages. It matches any sequence of characters that starts and ends with the package separator (.).

  For example, java..String matches java.lang.String and com.ibm..* matches any declaration beginning with com.ibm.
- If the allocated class name begins with an exclamation point (!), any heap allocations for classes that match the allocated class name are specifically excluded from BCI for Memory Leak Diagnosis. This is useful for indicating that all heap allocations within a class or group of classes are to be Byte-Code-Instrumented except for those allocations that are specifically excluded.

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Within the Customer class, all heap allocations should be Byte-Code-Instrumented.
- Within the Supplier class, all heap allocations should be Byte-Code-Instrumented except for allocations for classes beginning with java.lang.String.

The following example shows the contents of the customized memory_leak_diagnosis.xml file that accomplishes this:

```
<aspect>
    <type>application</type>
    <name>com.ibm.tivoli.itcam.toolkit.ai.aspectj.apptrace.CaptureHeap</name>
    <enabledProperty>
                com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis</enabledProperty>
    <defaultEnabled>true</defaultEnabled>
    <-- Modify the heapAllocationTarget tag to select or deselect the allocating and
          allocated classes for Memory Leak Diagnosis -->
    <heapAllocationTarget>
        <allocatingClassName>
                   com.mycompany.myapp.Customer</allocatingClassName>
        <allocatedClassName>*</allocatedClassName>
    </heapAllocationTarget>
    <heapAllocationTarget>
```

```
        <allocatingClassName>
                    com.mycompany.myapp.Supplier</allocatingClassName>
        <allocatedClassName>!java.lang.String*</allocatedClassName>
    </heapAllocationTarget>
</aspect>
```

3. Complete one of the following steps:
   - Save the file in the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom directory, then complete the following steps:
     a. In the toolkit custom properties file (see “The Toolkit properties file” on page 217), set the property am.camtoolkit.gpe.customxml.leak to the name (without path) of the file you modified in Step 2 on page 226.
     b. In the same toolkit custom properties file, set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
        ```
   - Save the file in any directory on the monitored host, then complete the following steps:
     a. In the toolkit custom properties file (see “The Toolkit properties file” on page 217), set the property am.camtoolkit.gpe.customxml.leak to the path and name for the file you modified in Step 2 on page 226.
     b. In the same toolkit custom properties file, sets the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
        ```

Customizing method profiling and method entry and exit tracing

Method profiling and method entry and exit tracing are enabled together and use the same call interceptions. Method profiling is performed at MOD L2, and method entry and exit tracing is performed at MOD L3. You may configure the Data Collector to change the thresholds and limits for method profiling, and to exclude some classes and methods for method entry and exit tracing.

Customizing thresholds for Level 2 method profiling

The Data Collector will only instrument method profiling data when the method exceeds certain thresholds of CPU time and real ("wall clock") time usage. There are also limits on the total number of methods, stack size, and running thread size. You can customize the thresholds and limits.

The following properties in the Data Collector properties file (see “The Data Collector properties file” on page 217) control the thresholds and limits for method profiling.

am.mp.cpuThreshold
The default is 30 milliseconds. Only the methods which take at least the minimum amount of CPU time specified in this property are captured for method profiling data. This avoids unnecessary clutter. Generally, methods with greater than the value specified in this property are considered useful. Customers can reduce or increase this value if needed.

am.mp.clockThreshold
The default is 30 milliseconds. Only the methods which take at least the minimum amount of wall clock time specified in this property are captured for method profiling data. This avoids unnecessary clutter. Generally, methods with greater than the value specified in this property are considered useful. Customers can reduce or increase this value if needed.

am.mp.leagueTableSize
The default is 1000. This is the maximum number of methods that are monitored for method profiling data. Customers can reduce or increase this value if needed. Decreasing it will help in reducing memory requirements.

am.mp.methodStackSize
The default is 100. This is the maximum stack size of any running thread that is recorded in method profiling.

Setting classes and methods for Level 3 method entry and exit tracing

By default, method entry and exit tracing on MOD L3 is performed for all classes and methods. To set specific classes and methods for method entry and exit analysis, perform the following procedure:

1. Make a copy of the *DC_home*/itcamdc/etc/method_entry_exit.xml file in a temporary location. Open the copy in a text editor.
2. Modify the parameters in the file. The following table describes the parameters you can modify:

Table 21. Parameters for the Level 3 method entry and exit analysis configuration file

Tag name	Description
methodSelection	Defines the classes and methods to be modified. By default, all classes and methods are selected. By modifying the className and methodName tags within the methodSelection tag, you can implement a more granular selection. Each methodSelection tag must contain exactly one className tag, and one or more methodName tags. Multiple methodSelection tags can be specified.
className	Identifies the name of a class or classes to be modified. Each methodSelection tag must contain exactly one className tag.
methodName	Identifies a method or method within the class or classes identified by the className tag to be modified for entry/exit tracing. Each methodSelection tag must contain one or more methodName tags.

Both className and methodName tags can include wildcard characters. The following section describes how the wildcard characters works:

- Asterisk (*) stands for zero or more occurrences of any character when used by itself. When embedded within a sequence of characters (for example, java.*.String), it matches zero or more occurrences of any character except the package separator (.).
- Two periods (..) can be used to specify all sub-packages. It matches any sequence of characters that starts and ends with the package separator (.).

  For example, java..String matches java.lang.String and com.ibm..* matches any declaration beginning with com.ibm.
- If the method name begins with an exclamation point (!), any methods that match the method name are specifically excluded from BCI for entry and exit tracing. This is useful for indicating that all methods within a class or group of classes are to be Byte-Code-Instrumented except for those methods that are specifically excluded.

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Within the Customer class, all methods should be Byte-Code-Instrumented.
- Within the Supplier class, all methods should be Byte-Code-Instrumented except for those methods beginning with the get or set.

The following example shows the contents of the customized method_entry_exit.xml file that accomplishes this:

```
<aspect>
  <type>application</type>
  <name>com.ibm.tivoli.itcam.toolkit.ai.aspectj.apptrace.EntryExitAspect</name>
  <enabledProperty>
         com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace</enabledProperty>
   <defaultEnabled>true</defaultEnabled>
   <methodSelection>
        <className>com.mycompany.myapp.Customer</className>
        <methodName>*</methodName>
   </methodSelection>
   <methodSelection>
        <className>com.mycompany.myapp.Supplier</className>
        <methodName>!get*</methodName>
        <methodName>!set*</methodName>
   </methodSelection>
</aspect>
```

3. Complete one of the following steps:
   - Save the file in the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom directory, then complete the following steps:
     a. In the toolkit custom properties file (see "The Toolkit properties file" on page 217), set the property am.camtoolkit.gpe.customxml.L3 to the name (without path) of the file you modified in Step 2 on page 229.
     b. In the same toolkit custom properties file, set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
        ```
   - Save the file in any directory on the monitored host, and then complete the following steps:
     a. In the toolkit custom properties file (see "The Toolkit properties file" on page 217), set the property am.camtoolkit.gpe.customxml.L3 to the path and name for the file you modified in Step 2 on page 229.
     b. Set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
        ```

Defining custom requests

By default, only certain types of Java classes and methods are monitored as requests by the Data Collector. Servlets, JSPs, EJB business methods, and certain standard J2EE APIs are recognized as requests. You can designate additional classes and methods as *custom requests*.

For example, ITCAM will not recognize Struts Action classes as requests by default, however you may set up custom request definitions and cause the Actions to be recognized as Nested Requests.

Perform the following procedure to enable monitoring of custom requests and designate one or more methods as custom requests:

1. Make a copy of the *DC_home*/itcamdc/etc/custom_requests.xml file in a temporary location. Open the copy in a text editor.
2. Modify the parameters in the file. The following table describes the parameters you can modify:

Table 22. Parameters for the custom requests configuration file

Tag name	Description
edgeRequest	Identifies one or more application methods that are to be Byte-Code-Instrumented for custom request processing. By modifying the requestName, Matches, type, and methodName tags within the edgeRequest tag, you can customize the selection. Each edgeRequest tag must contain exactly one methodName tag, and one or more Matches tags. Multiple edgeRequest tags can be specified.
requestName	Defines a unique name for this request. The request name is displayed to the user when the method entry and exit is traced.
Matches	Identifies a class or classes that contain the methods that are to be Byte-Code-Instrumented for custom request processing. Multiple Matches tags can be present within a single edgeRequest tag.
type	Indicates whether or not a class must be a system or application class in order to match the edgeRequest tag.
methodName	Identifies the names of the methods within one of the classes identified by the Matches tag that are to be Byte-Code-Instrumented for custom request processing. Exactly one methodName tag can be specified in each edgeRequest tag.

The Matches and methodName tags can include wildcard characters. The following section describes how the wildcard characters works:

- Asterisk (*) stands for zero or more occurrences of any character when used by itself. When embedded within a sequence of characters (for example, java.*.String), it matches zero or more occurrences of any character except the package separator (.).
- Two periods (..) can be used to specify all sub-packages. It matches any sequence of characters that starts and ends with the package separator (.).

  For example, java..String matches java.lang.String and com.ibm..* matches any declaration beginning with com.ibm.

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Within the Customer class, the creditCheck() method should be treated as a custom request called CreditCheck.
- Within the Supplier class, the inventoryCheck() method should be treated as a custom request called SupplyCheck.

The following example shows the contents of the customized custom_requests.xml file that accomplishes this:

```
<customEdgeRequests>
      <edgeRequest>
              <requestName>CreditCheck</requestName>
              <Matches>com.mycompany.myapp.Customer</Matches>
              <type>application</type>
              <methodName>creditCheck</methodName>
      </edgeRequest>
      <edgeRequest>
              <requestName>SupplyCheck</requestName>
              <Matches>com.mycompany.myapp.Supplier</Matches>
              <type>application</type>
              <methodName>inventoryCheck</methodName>
      </edgeRequest>
</customEdgeRequests>
```

3. Complete one of the following steps:
   - Save the file in the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom directory. Then, in the

toolkit custom properties file (see "The Toolkit properties file" on page 217), set the property am.camtoolkit.gpe.customxml.custom to the name (without path) of the file you modified in Step 2 on page 230.

- Save the file in any directory on your computer. Then, in the toolkit custom properties file (see "The Toolkit properties file" on page 217), set the property am.camtoolkit.gpe.customxml.custom to the path and name for the file you modified in Step 2 on page 230.

Enabling Asynchronous Bean request monitoring

If your applications use asynchronous bean requests, and the requests are not displayed in the Tivoli Enterprise Portal or the Visualization Engine, you will need to enable Asynchronous Bean request monitoring using the Toolkit custom properties file..

First, check whether custom requests have been defined on the Data Collector (see "Defining custom requests" on page 230). Open the toolkit custom properties file and, if it exists, the global toolkit custom properties file (see "The Toolkit properties file" on page 217). Check both of these files for the following property (not commented out):

```
am.camtoolkit.gpe.customxml.custom=xml_filename
```

If this property exists, custom requests have been defined. In this case, edit the XML file named in the property. If both the instance specific toolkit custom properties file and the global toolkit custom properties file have this property, use the filename from the instance specific file. If the filename does not have a path, the file is located in the the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom directory. Find the tag </customEdgeRequests>, and add the following text immediately before this line:

```
<edgeRequest>
 <requestName>AsyncWorkBean</requestName>
 <Implements>com.ibm.websphere.asynchbeans.Work</Implements>
 <type>application</type>
 <methodName>run</methodName>
</edgeRequest>
<edgeRequest>
 <requestName>AsyncTimerBean</requestName>
 <Implements>commonj.timers.TimerListener</Implements>
 <type>application</type>
 <methodName>timerExpired</methodName>
</edgeRequest>
<edgeRequest>
 <requestName>AsyncAlarmBean</requestName>
 <Implements>com.ibm.websphere.asynchbeans.AlarmListener</Implements>
 <type>application</type>
 <methodName>fired</methodName>
</edgeRequest>
```

If the property does not exist (or is commented out), custom requests have not been defined. In this case, perform the following procedure:

1. create a new file: *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/custom_requests_async.xml, with the following text:

```
<gpe>
 <bci>
  <customEdgeRequests>
   <edgeRequest>
    <requestName>AsyncWorkBean</requestName>
    <Implements>com.ibm.websphere.asynchbeans.Work</Implements>
    <type>application</type>
    <methodName>run</methodName>
   </edgeRequest>
   <edgeRequest>
    <requestName>AsyncTimerBean</requestName>
    <Implements>commonj.timers.TimerListener</Implements>
    <type>application</type>
    <methodName>timerExpired</methodName>
   </edgeRequest>
   <edgeRequest>
    <requestName>AsyncAlarmBean</requestName>
    <Implements>com.ibm.websphere.asynchbeans.AlarmListener</Implements>
    <type>application</type>
    <methodName>fired</methodName>
   </edgeRequest>
  </customEdgeRequests>
 </bci>
</gpe>
```

2. In the toolkit custom properties file (see “The Toolkit properties file” on page 217), set the property:

   ```
   am.camtoolkit.gpe.customxml.custom=custom_requests_async.xml
   ```

After performing the changes described in this section, restart the application server instance monitored by the Data Collector.

Customizing monitoring of custom MBeans

By default, the Data Collector will monitor WebSphere Application Server MBeans. If the environment includes custom MBeans, you may configure the Data Collector to monitor some of them (according to specific definitions), or all of them.

Configuring data collection for specific custom MBeans

You may define specific MBeans. Data collection will be enabled for these MBeans only.

Note: Data collection for the J2EE Domain MBean is not available in an IBM WebSphere Application Server environment.

Perform the following procedure to customize the generic configuration for JMX data collection:

1. Make a copy of the *DC_home*/itcamdc/etc/was/*app_server_version*/mbeanconfig_*app_server_version*.xml file in a temporary location. Open the copy in a text editor.
2. Modify the parameters to fit your custom MBean. The following table describes the parameters you can modify:

Table 23. Parameters for the JMX MBean configuration file

Element	Nested within	Description
Version	DomainList	Defines the version of the application server
Name	Domain	Defines a domain. If the asterisk (*) is defined, all MBeans that match the query ObjectName will be returned; otherwise, only the MBeans that belong to this domain name will be returned.
Description	Domain	Describes the domain. This can be any text string.
MBean	Domain	Defines the MBeans to be collected.

Table 23. Parameters for the JMX MBean configuration file (continued)

Element	Nested within	Description
ObjectName	MBean	Defines the MBean object name for collection. If the MBean element is used within an Attr element (which indicates the embedded MBean), then the object name is any symbolic name, such as $ATTRIBUTE_VALUE. This symbolic name will be replaced with the actual object name internally.
Category	MBean	Defines a unique key for the MBean. Each MBean must have a unique key, which is used in the JMXAcquireAttribute to get the MBean attributes.
RetrieveAllAttrs	MBean	A value of true indicates that all the attributes for the MBean must be collected. If you set this to false, you must define the attributes in the Attr element.
Attr	MBean	Defines the attributes to be collected. There may be multiple Attr elements, defining multiple attributes.
Name	Attr	The attribute name.
MappedKey	Attr	Defines a unique key for the attribute. Each attribute must have a unique key, which is used in the JMXAcquireAttribute to get the specific attribute.
MBean	Attr	Defines the embedded MBean within this attribute. This tag is used when an attribute has an embedded MBean, which points to another MBean with the object name.
JavaBean	Attr	Defines the embedded MBean within this attribute. This tag is used when an attribute has an embedded MBean, which refers to another java object. The references java object has the elements of a JavaBean (setter, getter).
TargetType	Attr	Defines the type of the attribute. This is usually specified for the JavaBean type to determine the attribute type.

3. Complete one of the following steps:
   - Save the file in the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom directory. Then, in the toolkit custom properties file (see "The Toolkit properties file" on page 217), set the property am.camtoolkit.jmxe.custom to the name (without path) of the file you modified in Step 2 on page 233.
   - Save the file in any directory on the monitored host. Then, in the toolkit custom properties file (see "The Toolkit properties file" on page 217), set the property am.camtoolkit.jmxe.custom to the path and name for the file you modified in Step 2 on page 233.

Enabling and customizing data collection for all custom MBeans

You may enable data collection for all custom MBeans and customize the way they are identified to the user.

To enable it, set the following property in the Toolkit properties file (see "The Toolkit properties file" on page 217):

```
am.getallmbeans=y
```

This property is in effect only if the custom MBeans property is commented out in the Toolkit properties file, as shown in the following example:

```
#  Uncomment the line  to enable custom mbeans
#am.camtoolkit.jmxe.custom=
   C:/PROGRA~1/IBM/itcam/WEBSPH~1/DC/itcamdc/etc/custom_mbeanconfig.xml
```

Tip: Check that the am.camtoolkit.jmxe.custom property is also not present in the Toolkit global properties file (see "The Toolkit properties file" on page 217).

The following properties provide additional options for display of the MBean data:

```
am.jmxkeyword=type_identifier
am.jmxusecanonical=y
am.jmxtruncate=n
am.jmxlength=30
```

The properties and their definitions are:

am.getallmbeans

Set this property to y to enable data collection for all MBeans. If it is set to n, data collection for all MBeans is disabled. If the custom MBeans property (am.camtoolkit.jmxe.custom) is set, am.getallmbeans has no effect.

am.jmxkeyword

The Visualization Engine presents data on monitored MBeans by organizing them into categories. The category name is formed from the Domain and type keywords in the MBeans Object Name If the type keyword does not exist, the name keyword is used to create the category. If the name keyword does not exist, then the object name is used as the category. If this default behavior does not provide enough granularity to distiguish MBean categories, you can use the am.jmxkeyword property to define more keywords to be included in the category name.

For example, if you specify am.jmxkeyword=identifier, then the value of the identifier keyword from the object name is included in the category name, in addition to value of the type keyword. More than one keyword can be specified in the property. The keywords must be separated by a comma (,).

am.jmxusecanonical

If you need to see all of the keywords from the object name in the category, assign the am.jmxusecanonical=y property. This setting will result in including all keyword values for the category name, separated by an underscore (_) character.

am.jmxtruncate

In some cases, especially if am.jmxusecanonical=y, the category name can be quite long. By default, the Data Collector will truncate the category name to the length specified by the am.jmxlength property, or to 30 characters if the am.jmxlength property is not specified. If you do not want the category name to be truncated, specify the am.jmxtruncate=n property.

am.jmxlength

This property specifies the maximum length of the category name. The default is 30. This property is ignored if the am.jmxtruncate=n property is specified.

Modifying Performance Monitoring Infrastructure settings

If the Data Collector communicates with ITCAM for Application Diagnostics Managing Server, the level of instrumentation for Performance Monitoring Infrastructure (PMI) is determined by the current MOD level set in the

Visualization Engine. You can customize the PMI level for each MOD level. The collection level set in Tivoli Enterprise Portal does not affect the PMI level.

By default, the following PMI setting will be enabled at each Managing Server MOD level:

Table 24. Default Performance Monitoring Infrastructure instrumentation settings

Monitoring (MOD) level	PMI setting
1	`Basic`
2	`Extended`
3	`All`

To customize these settings, perform the following procedures in the Data Collector custom properties file (see "The Data Collector properties file" on page 217):

Table 25. Procedures to customize instrumentation of the Performance Monitoring Infrastructure

Type of customization	Procedure

Change the PMI setting that will be set for a particular Managing Server monitoring (MOD) level.	Add or uncomment one or more of the following lines and give it a different setting. The possible values are `none`, `basic`, `extended`, or `all`:
	`am.was6pmi.settings.1=basic`
	`am.was6pmi.settings.2=extended`
	`am.was6pmi.settings.3=all`

Perform fine-grained customization of the instrumentation for a particular PMI module at a particular monitoring level. See the following Web site for a description of the numeric IDs that you will need when customizing PMI instrumentation at this detailed level: http://www.ibm.com/support/docview.wss?uid=swg21221308	Add a line to set fine-grained customization for a particular module at a particular monitoring level. It has the format `module_type=number1,number2,...`, for example:
	`am.was6custompmi.settings.1=beanmodule=1,2,3,4,5,6,7,8,`
	`  9,10,14,15,19,20,21,22,23,24,25,28,29,30,31,32,33,34`
	Use `*` to monitor all IDs in the module, or `none` to monitor none:
	`am.was6custompmi.settings.3=beanModule=*`
	`am.was6custompmi.settings.3=webAppModule=none`

Attention: The `am.was6pmi.*` property names are also valid for monitoring Version 7 application servers.

If you do not want the level of instrumentation for PMI to change as the Managing Server MOD level changes, add the following line to the Data Collector custom properties file (see "The Data Collector properties file" on page 217):

```
am.pmi.settings.nochange=true
```

Enabling Performance Monitoring Infrastructure settings for the Service Integration Bus

You can configure the Data Collector to collect Service Integration Bus (SIB) Performance Monitoring Infrastructure (PMI) data.

To do this, perform the following procedure:

1. Add the following lines to the Data Collector custom properties file (see "The Data Collector properties file" on page 217):

   ```
   am.was6custompmi.settings.1=SIB Service=*
   am.was6custompmi.settings.2=SIB Service=*
   am.was6custompmi.settings.3=SIB Service=*
   ```

These lines set custom PMI settings for Level 1, Level 2 and Level 3 monitoring levels respectively.

2. Restart the instance of the application server that is being monitored by the Data Collector. See "Restarting the application server" on page 263.

Enabling and disabling instrumentation of Web Services as new request types

By default, the Data Collector monitors JAX-RPC 1.1 and Axis 1.x Web Services. To enable monitoring of JAX-WS Web Services, you need to perform additional steps. You can also disable monitoring of all Web Services.

To enable instrumentation of JAX-WS Web Services, you need to deploy the JAX-WS handler for the Data Collector. To do this, perform the following procedure on every application server that is a requester (client) or provider (server) of JAX-WS Web Services, and is monitored by the Data Collector:

1. Copy the file `DC_home/itcamdc/lib/com.ibm.tivoli.itcam.dc.jaxws-handlers.jar` into the `AppServer_home/plugins` directory.
2. Change to the *AppServer_home* directory, and run the following command:
   - on Windows, `osgiCfgInit.bat`
   - on Linux or UNIX systems, `./osgiCfgInit.sh`
3. Restart the application server instances monitored by the Data Collector.

To disable instrumentation of Web Services, set the following property in the Data Collector custom properties file (see "The Data Collector properties file" on page 217):

```
ws.instrument=false
```

Important: To enable Web Services composite request monitoring and correlation in the Visualization Engine and in ITCAM for Transactions, you need to monitor both the Web services requester (client) and the Web services provider (server) using ITCAM Agent for WebSphere Applications Data Collectors, and the Data Collectors must be connected to the same Managing Server.

Enabling and disabling memory monitoring

The Data Collector can monitor native memory usage and save results to a log file. This capability is disabled by default.

If you enable Data Collector memory monitoring, the Data Collector will save memory usage statistics to the trace log file (`trace-dc-native.log`). For the location of the Data Collector trace log file, see *IBM Tivoli Composite Application Manager for Application Diagnostics Troubleshooting Guide*.

The statistics reflect Data Collector memory consumption on the native side. The Java side memory consumption is not reflected in the logged numbers.

To enable memory monitoring, set the following property in the Data Collector custom properties file (see "The Data Collector properties file" on page 217):

```
log.statistics=true
```

By default, the statistics are logged once every 30 seconds. You can set a different period, in milliseconds, in the `log.statistics.frequency` property in the Data

Collector custom properties file. For example, to log memory usage statistics once every 10 seconds, use the following setting:

```
log.statistics.frequency=10000
```

To disable memory monitoring, set the following property in the Data Collector custom properties file:

```
log.statistics=false
```

Configuring the Data Collector after changing the application server version

If you upgrade the application server being monitored by the Data Collector from a 6.x version to a 7.x version, you must reconfigure the Data Collector to point to the updated instance of the application server.

Complete the following steps:

1. For a non-Network Development environment, unconfigure the Data Collector from all application server instances before the upgrade. See “Unconfigure the Data Collector for application server instances” on page 47, “Unconfiguring the Data Collector from application server instances using command line” on page 119, and “Unconfigure the Data Collector for application server instances using GUI” on page 155.
2. Perform the upgrade of the application server.
3. For a non-Network Development environment, make sure the application server instance is upgraded and started. For a Network Deployment environment, make sure the Deployment Manager and Node Agent are upgraded and started; do not start the instances.
4. Use the Configuration Tool to configure the Data Collector for each application server instance. See “Configuring ITCAM Agent for WebSphere Applications on Windows” on page 25 and “Configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems” on page 110.
5. Start or restart the monitored application server instance. See “Restarting the application server” on page 263.

Steps to perform if the IP address of the application server host is to be changed

If the IP address of the application server host is to be changed, perform the following procedure:

1. Use the Configuration Tool to unconfigure the Data Collector for this application server instance. See “Configuring ITCAM Agent for WebSphere Applications on Windows” on page 25 and “Configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems” on page 110.
2. Stop the instance of the application server that is being monitored by the Data Collector. See “Stopping the application server” on page 266.
3. Perform the IP address change at the operating system and network level.
4. Start the instance of the application server that is being monitored by the Data Collector. See “Starting the application server” on page 265.
5. Use the Configuration Tool to configure the Data Collector again for this application server instance. See “Configuring ITCAM Agent for WebSphere Applications on Windows” on page 25 and “Configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems” on page 110.

Moving the Data Collector to a different host computer

If the Data Collector communicates to ITCAM for Application Diagnostics Managing Server, you may move it to a different host computer while maintaining the same Managing Server identity (Probe ID and Controller ID). The Managing Server will see the new host as the continuation of the old, preserving history, analysis, etc.

The following section describes some prerequisites for moving the Data Collector to a different host computer while keeping the same Probe ID and Controller ID:

- Host A and host B have the same configuration at the operating system level.
- You must move the same version of the Data Collector from host A to host B.

To maintain the Probe ID and Controller ID when moving to another physical host, perform the following procedure:

1. On host A, stop the instance of the application server that is being monitored by the Data Collector. See "Stopping the application server" on page 266.
2. On host B, install the Data Collector and configure it using the Visualization Engine (Application Monitor) user interface. Configuring the Data Collector will generate the *DC_home*/runtime/*appserver_version.node_name.server_name*/id file and other Data Collector runtime property files.
3. Using the Visualization Engine (Application Monitor) user interface, unconfigure the Data Collector on host B. This step deletes all information about this Data Collector from the ITCAM for Application Diagnostics database. Do not unconfigure the Data Collector using the Configuration tool.
4. On host B, stop the instance of the application server that is being monitored by the Data Collector. See "Stopping the application server" on page 266.
5. Copy the contents of the *DC_home*/runtime/*appserver_version.node_name.server_name*/id file on host A to the *DC_home*/runtime/*appserver_version.node_name.server_name*/id file on host B.
6. On host B, save the *DC_home*/runtime/*appserver_version.node_name.server_name*/id file.
7. On host B, start the instance of the application server that is being monitored by the Data Collector. See "Starting the application server" on page 265.

The Data Collector on host B assumes the identity of the Data Collector on host A and is configured by the Managing Server with the runtime configuration of the Data Collector on host A. This does not affect monitoring in Tivoli Enterprise Portal.

Installing Memory Dump Diagnostic for Java with IBM Support Assistant

Memory Dump Diagnostic for Java (MDD for Java) either analyzes a single heap dump or analyzes and compares two heap dumps and searches for evidence of a memory leak. In order to download MDD for Java, you will need to first install IBM Support Assistant (ISA). ISA provides extra help with diagnosing problems and provides extra tools and components for troubleshooting as well as providing a place to write problems (PMRs).

MDD for Java analyzes manual or scheduled heap dumps performed by ITCAM's Heap Dump Management feature.

ITCAM's Heap Dump Management feature enables you to schedule or immediately initiate the collection of an IBM Heap Dump for a particular application server. Then this dump must be downloaded and post-processed outside the Visualization Engine (Application Monitor) user interface using MDD for Java. (The other Memory Diagnosis tools provided by ITCAM, such as Memory Analysis, Heap Analysis and Memory Leak Diagnosis, provide analysis through the Visualization Engine (Application Monitor) user interface.)

MDD for Java only analyzes heap dumps from IBM JDKs. For non-IBM JDKs use the ITCAM Memory Leak Diagnosis feature.

Searching capabilities for ITCAM Agent for WebSphere Applications are not supported in ISA.

Where to install IBM Support Assistant and Memory Dump Diagnostic for Java

The following section describes two common configurations:

- Install ISA and MDD for Java on a standalone server that is not running an application server. After the IBM heap dump has been collected on the application server, it must be transferred to the MDD for Java computer for post-processing.

  This configuration is recommended for production environments where you do not want the post-processing of the dump to impact the performance of the application server.
- Install ISA and MDD for Java on each application server host computer, so that you can analyze the heap dump locally without having to transfer it.

  This configuration might be suitable for a development or test environment where the overhead of analyzing the heap dump is not a concern.

The decision on where to install might also be influenced by the platforms supported by ISA.

Downloading, installing, configuring, and launching IBM Support Assistant and Memory Dump Diagnostic

See the online helps in the Visualization Engine (Application Monitor) user interface for instructions on how to download, install, configure, and launch ISA, including the ISA plug-in for the Agent, and Memory Dump Diagnostic for Java. Go to **Help > Welcome > Using IBM Support Assistant to diagnose problems**.

Note: ISA can be installed on both the Data Collector and Managing Server computers, but only the ISA installed on the Managing Server computer can be invoked from the Visualization Engine (Application Monitor) user interface.

Setting the Heap Dump scan interval

The Heap Dump Management function of ITCAM Agent for WebSphere Applications can create Heap Dumps of the monitored IBM WebSphere Application Server by user request. This function is available only with ITCAM for Application Diagnostics Managing Server.

Once in a defined time interval, ITCAM Agent for WebSphere Applications will scan the existing Heap Dumps, in order to inform the user of their existence and to delete heap dump files that are over 48 ours old.

By default, this interval is every 12 hours. To change the interval, set the `am.mddmgr.poll.delay` property in the toolkit custom properties file (see "The Toolkit properties file" on page 217) to the new interval in seconds.

Configuring a Data Collector for multiple network interfaces

If the application server host has multiple IP addressed at the time of Data Collector configuration, the Configuration tool will set the preferred IP address for communication with the Managing Server. If more than one IP address is added later, set the preferred IP address manually, as described in this section.

If theData Collector needs to expose a specific IP to the Managing Server, complete one of the following steps:

1. In the Data Collector custom properties file (see "The Data Collector properties file" on page 217), set the `am.socket.exportip` and `am.socket.bindip` properties to the IP address to be exposed.
2. In the file *DC_home*/runtime/*appserver_version.node_name.server_name*/ dc.java.properties, set the `appserver.rmi.host` property to the IP address to be exposed.
3. Make sure that the Managing server can access the required IP address of the Data Collector (You can verify this by doing a ping).
4. If the Data Collector is using Port Consolidator:
   a. In the Data Collector custom properties file (see "The Data Collector properties file" on page 217), set the `proxy.host` property to the IP address to be exposed.
   b. In the file *DC_home*/itcamdc/etc/proxy.properties, set the `am.socket.exportip` and `am.socket.bindip` properties to the IP address to be exposed.
   c. In the Port Consolidator start script (*DC_home*/itcamdc/bin/ proxyserverctrl_ws.bat or *DC_home*/itcamdc/bin/proxyserverctrl_ws.sh), set the property JAVA_RMI_SERVER_HOSTNAME to the IP address to be exposed.

Customizing RMI garbage collection interval

If the Data Collector communicates with ITCAM for Application Diagnostics Managing Server, it uses RMI over TCP/IP for this communication. One effect of using RMI is that garbage collection occurs every minute. If you don't want this to happen, you can specify the garbage collection interval explicitly to a preferred interval.

The Data Collector communicates with the Managing Server using TCP/IP sockets and RMI. One effect of using RMI is that garbage collection occurs every minute. If you don't want this to happen, you can specify the garbage collection interval explicitly to a preferred interval by specifying the parameters in the **Generic JVM arguments** field. These parameters must be implemented as a pair.

To do this, complete the following steps:

1. Log into the IBM WebSphere Application Server administrative console.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.

4. In the **Generic JVM arguments** field, append the following parameters if such parameters don't exist, or update their values if they already exist.

   ```
   -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000
   ```

   Note: These values require a dash (-) in front of each parameter, and a single space between parameters. You must specify both parameters if you specify them at all. The value is in milliseconds; 3,600,000 represents one hour.

Customizing CICS transaction correlation

CICS is a transaction framework, primarily used to run mature applications. To communicate with CICS, Java applications can use the CICS Transaction Gateway (CTG).

If CICS translation correlation is enabled, the Data Collector callback code will add composite tracking data, called Global Publish Server (GPS) tokens, into the communications area (COMMAREA) used to carry transaction request data to CICS. This data can be used by ITCAM for Transactions, which instruments the CICS transaction framework. ITCAM for Transactions will correlate every CICS transaction with the corresponding CTG call using the GPS token. The user can then view a detailed breakdown of transaction response time in the ITCAM Visualization Engine.

However, the presence of the GPS token in COMMAREA may not always be desirable. If ITCAM for CICS Data Collector or ITCAM for CICS Client is not installed on the CICS server, the GPS token might reach the server application, which may (in some cases) not process it correctly. For this reason, transaction correlation is disabled by default.

You can enable GPS tokens for specific transactions based on CTG gateway address or protocol; by CICS system; by CICS program or by the CICS transaction ID. Enable correlation with CICS systems that have the ITCAM for CICS Data Collector installed, configured, and enabled. To do this, edit the file *DC_home*/runtime/*app_server_version.node_name.server_name*/custom/ctg.filters . This file can contain any number of lines with the following syntax:

```
Type=E|I[,Gateway=<CTG URL>][,Server=<CICS Server>][,Program=<CICS Program>]
   [,Transid=<Mirror tran ID>]
```

Each line defines a filter, which disables or enables GPS tokens for some transactions.

The `Type` parameter is mandatory for each line. A value of "E" sets up an Exclude filter; transactions matching it will not have a GPS token inserted into the COMMAREA. "I" denotes an Include filter; any transactions matching an include filter will have a GPS token, overriding any Exclude filter applying to them.

All other parameters are optional, but at least one of them must be present on every line. To match a filter, a transaction must match all of the parameters set on the line:

- `Gateway` is any part of the CTG URL, including the protocol, host name and/or port
- `Server` is the host name of the CICS server (this may be different from the CTG host name)
- `Program` is the CICS program name (a field in a CICS transaction request)

- Transid is the CICS Mirror Transaction ID. Except Multi Regional Operation (MRO) CICS/CTG environments, this parameter is of little use as all CTG transactions will have the same Mirror Transaction ID

For example, to disable addition of GPS tokens to the COMMAREA of all transactions routed through the local protocol, add the following line to *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/ctg.filters:

```
Type=E,Gateway=local://*
```

To disable addition of GPS tokens to transactions for programs starting'CYN$' to be run on the CICS3101 server, but enable them for transactions for the CYN$ECI2 program on the same server, use the following lines:

```
Type=E,Program=CYN$*,Server=CICS3101
Type=I,Program=CYN$ECI2,Server=CICS3101
```

The default configuration is to disable all correlation through the following line:

```
Type=E,Gateway=*
```

Modifying the garbage collection log path

The Data Collector configuration set the path for the garbage collection log file (itcam_dc_gclog.log or native_stderr.log) to *AppServer_home*/profiles/*profile_name*/logs/*server_instance_name*. For example, C:\Program~1\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1. For version 1.3 JDKs, you cannot modify this. For other JDKs, if you want to change the location or name of this log file, perform the following procedure:

1. In the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/kwjdc.properties file, make the following modification:

   Change the following parameter to point to the new garbage collection log file location:

   ```
   TEMAGCCollector.gclog.path=gc_logfile_path_and_name
   ```

   You can also optionally limit the size of the Garbage Collector logs. To do this you need to set the parameter to the following value:

   ```
   TEMAGCCollector.gclog.path=gc_logfile_path_and_name, x, y
   ```

   Where *x* and *y* are numbers. In this case, the logging will be performed to *x* files in rotation; information for *y* garbage collection cycles will be sent to one file before switching to the next file.
2. Log into the IBM WebSphere Application Server administrative console for the instance of the application server for the Data Collector installed on the RMI server.
3. Click **Server > Application Servers** and select the *server_name*.
4. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
5. In the **Generic JVM arguments** field, change the following parameters to point to the new garbage collection log file location:

Table 26. JVM options for garbage collection logging

JDK version	Parameter
IBM 1.4 and 1.5	`-verbosegc -Xverbosegclog:${SERVER_LOG_ROOT}/itcam_gc.log,5,3000`
Sun and HP 1.4 and 1.5	-Xloggc:*gc_logfile_path_and_name* -XX:+PrintGCTimeStamps

Make sure the *gc_logfile_path_and_name* matches the value you specified in Step 1 on page 243.

6. Click **Apply**.
7. In the Messages dialog box, click **Save**.
8. In the Save to Master Configuration dialog box, complete the following steps:
   - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.
9. Restart the instance of the application server that is being monitored by the Data Collector. See "Restarting the application server" on page 263.

Suppressing verbose garbage collection output in Data Collectors with a Sun JDK

For Sun JDKs, the Data Collector configuration enables verbose garbage collection output using the -Xloggc generic JVM argument. By default, the -Xloggc causes the JVM to generate class loading and unloading events to the native standard output stream. The process might fill the log files and consume excessive disk space.

To suppress class loading and unloading events, add the -XX:-TraceClassUnloading -XX:-TraceClassLoading options to the JVM arguments of the application server. Perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
4. In the **Generic JVM arguments** field, add the following string of text:
   ```
   -XX:-TraceClassUnloading -XX:-TraceClassLoading
   ```
5. Click **Apply**.
6. In the Messages dialog box, click **Save**.
7. In the Save to Master Configuration dialog box, complete the following steps:
   - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.
8. Restart the instance of the application server that is being monitored by the Data Collector. See "Restarting the application server" on page 263.

What to do when deleting an application server profile

If you do not unconfigure the Data Collector before you delete an application server profile, Data Collector installation log and runtime data remains in the system, and running the WebSphere update command will fail (typically with a `JACL failed` error message).

Unconfigure the Data Collector for all monitored application server instances in a profile before deleting it.

Integrating the Data Collector with ITCAM for Transactions

Transaction Tracking Application Programming Interface (TTAPI) enables the integration of ITCAM Agent for WebSphere Applications and ITCAM for Transactions. ITCAM for Application Diagnostics Managing Server is required for this.

The Data Collector can generate TTAPI events for the following requests:

- All composite requests that generate events to Global Publishing Server (GPS), including:
  - RMI/IIOP
  - Web Services
  - MQI
  - CICS
  - IMS
- Top level EJB requests (including Message-Driven Beans)
- Top level Servlet and JSP requests
- Custom edge requests
- JDBC nested requests
- JNDI nested requests

Enabling and disabling TTAPI on the Data Collector

Enable TTAPI when configuring or reconfiguring the Data Collector for an application server instance.

To enable reporting failed JDBC nested requests under a separate name from the successful ones, set the following property in the toolkit custom properties file (see “The Toolkit properties file” on page 217):

```
com.ibm.tivoli.itcam.dc.ttapi.jdbc.status.enabled=true
```

To disable Data Collector and TTAPI integration, set the following property in the toolkit custom properties file (see “The Toolkit properties file” on page 217):

```
com.ibm.tivoli.itcam.dc.ttapi.enable=false
```

To disable integration of the Data Collector with ITCAM for Transactions Web Response Time (T5) agent, set the following property in the toolkit custom properties file (see “The Toolkit properties file” on page 217):

```
com.ibm.tivoli.itcam.dc.ttapi.wrm.servlet.enabled=false
```

To enable Optim™ Performance Manager integration, set the following property in the toolkit custom properties file (see “The Toolkit properties file” on page 217 file:

```
com.ibm.tivoli.itcam.dc.ttapi.jdbc.opm.enabled=true
```

If any monitored J2EE application changes the JDBC connection client attributes during an active session, also set the following property:

```
com.ibm.tivoli.itcam.dc.ttapi.jdbc.opm.clientinfo.reset=true
```

If exceptions (failed requests) for JNDI and JDBC nested requests happen within a reporting period, they are reported via TTAPI, and the status of the transaction is set to Fail. The user is able to inspect individual exceptions. To limit the amount of

JDBC and JNDI exceptions displayed for a top level transaction, set the following property in the toolkit custom properties file (see "The Toolkit properties file" on page 217:

```
com.ibm.tivoli.itcam.dc.ttapi.maxExceptions=number
```

To disable collecting JNDI information, set the following property in the toolkit custom properties file (see "The Toolkit properties file" on page 217):

```
com.ibm.tivoli.itcam.dc.ttapi.jndi.enabled=false
```

Tracing the integration of TTAPI with the Data Collector

You can trace the Transaction Tracking Application Programming Interface (TTAPI) and the Data Collector (DC) integration and put all the tracing information in a log file. To do that you need to modify the*DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/cynlogging.properties file. Follow this procedure to enable the integration tracing:

1. Open the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/cynlogging.properties file for editing.
2. Add the following lines to the cynlogging.properties file:

   ```
   # ttapi tracing
    CYN.trc.shared.datacollector.ttapi.TTAPIUtil.level=DEBUG_MAX
    CYN.trc.shared.datacollector.ttapi.TTAPIUtil.logging=true
   ```
3. Save the cynlogging.properties file and exit editing mode.

After you have enabled the integration tracing the tracing information is saved in a log file. The log file, by default, is located in the *DC_home*/logs/CYN/logs directory.

The information contained in the log will help IBM support staff troubleshoot any potential problems with the TTAPI integration with the DC.

Overriding the Data Collector autoconfiguration

By default, if the Data Collector communicates with ITCAM for Application Diagnostics Managing Server, it will be automatically configured by the Managing Server with the default configuration profile at the time of first connection. You may disable automatic configuration or select a different profile. These settings only take effect if you perform them before the Data Collector connects to the Managing Server for the first time.

To disable automatic configuration of the Data Collector in the Managing Server, set the following property in the Data Collector custom properties file (see "The Data Collector properties file" on page 217):

```
dc.autoconfigure=false
```

To change the profile name for automatic configuration of the Data Collector in the Managing Server, set the following property in the Data Collector custom properties file (see "The Data Collector properties file" on page 217):

```
dc.autoconfigure.configname=config_name
```

Note: If the Data Collector has already been configured by the Managing Servers, changing these settings will not have any effect.

To configure or unconfigure a Data Collector from the Managing Server, or to change the Data Collector configuration profile, use the Visualization Engine. From the top navigation, select **Administration** > **Server Management** > **Data Collector**

Configuration. For more information on Data Collector configuration by the Managing Server, see the Visualization Engine online help.

Properties for communication with a Deployment Manager

The following properties define Data Collector communication with the Deployment Manager in a Network Deployment or Extended Deployment. They are normally set by the configuration utility.

The properties are in the Data Collector properties file (see "The Data Collector properties file" on page 217).

deploymentmgr.rmi.port

Defines the port for RMI communication to the Deployment Manager.

Example:

```
deploymentmgr.rmi.port=Deployment_Manager_RMI_(bootstrap)_port
```

deploymentmgr.rmi.host

Defines the host name or IP address for RMI communication to the Deployment Manager.

Example:

```
deploymentmgr.rmi.host=dmgr.domain.com
```

Part 6. Appendixes

Appendix A. Setting up security

Setting up optional security for ITCAM for Application Diagnostics is described in this chapter.

For information on optional security for ITCAM for z/OS refer to the *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide for z/OS*

Because security for ITCAM for Application Diagnostics often involves integration of the various components, this chapter contains information pertaining to both Managing Servers and Data Collectors on distributed platforms.

Perform the procedures in each of the following sections, if they apply.

Node Authentication

Node Authentication is the technique used to ensure that the managing server and data collectors communicate with each other in a secure manner. In Node Authentication related configuration, the Kernel, Data Collectors or Port Consolidator operate in secure mode either individually or in combination. The configuration changes are common for all the modes except that a particular component can be made to operate in a different mode by changing the property security.enabled on that particular component. You can use the following combinations:

- Managing server in secure mode and the data collector in non secure mode.
- Data collector in secure mode and the managing server in non secure mode.
- Managing server and data collector in secure or non secure mode.

Script to run if your SSL certificates have expired

All SSL certificates have an expiration time. For some certificates, the expiration time is 4 years, after which the product will not function if you have enabled Node Authentication and SSL. If this is the case, to increase the expiration time, perform the procedure at “Script to run if your SSL certificates have expired” on page 258.

Node Authentication on the Managing Server

The following procedures are Node Authentication related configuration that occurs on the Managing Server component.

Kernel-related changes

In the managing server in the $MSHOME/bin directory there is setenv.sh file that is shared by all managing server components. All changes made to the setenv.sh file apply to all managing server components. All the managing server components initialize their respective security modules based on the properties in this setenv.sh file. The installer configures all managing server components with security enabled configuration by default with the exception of kernel-related changes which are enabled by changing the .kl1 and .kl2 property files on the managing server.

In the Kernel properties file (*MS_home*/etc/kl1.properties) complete the following steps:

1. To enable a Kernel to operate in secure mode, set the following property:

```
security.enabled=true
```

2. If you have a multiple Network Interface Card (NIC) environment or are upgrading the Managing Server from version 6.0 to version 7.1.0.1, in the Kernel properties file (*MS_home*/etc/kl1.properties), set `codebase.security.enabled=false`.

   If you have more than one instance of the Kernel, set `codebase.security.enabled=false` in kl2.properties as well.
3. Restart the Managing Server. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

Data Collector custom properties file changes

The following procedure is Node Authentication related configuration that occurs by modifying the datacollector_custom.properties file.

Enabling the Data Collector to operate in secure mode

In the Data Collector custom properties file (*DC_home*/runtime/*app_server_version.node_name.server_name*/custom/datacollector_custom.properties) complete the following steps:

1. Set `security.enabled=true`
2. Restart the application server.

Node Authentication related properties in the Port Consolidator

The following procedure is Node Authentication related configuration that occurs by modifying the proxy.properties file.

In the Port Consolidator properties file (*DC_home*/itcamdc/etc/proxy.properties) complete the following steps.

1. To enable the Port Consolidator to operate in secure mode:

   ```
   security.enabled=true
   ```
2. Restart the application server. See “Restarting the application server” on page 263.

See Appendix F, “Port Consolidator reference and configuration,” on page 281 for instructions on configuring the Data Collector to use the Port Consolidator.

Keystore management and populating certificates

You do not have to use the following commands unless you want to create unique certificates with a new storepass and keypass. You can run keystore management on the managing server and the data collector. These commands will populate a new store with those certificates.

For populating all new keystores : there are 3 stores used by ITCAM for Application Diagnostics: CyaneaMgmtStore to run on the managing server, CyaneaDCStore to run on the data collectors, and CyaneaProxyStore to run on the data collector when you want to enable the data collector port consolidator.

CyaneaMgmtStore contains: mgmttomgmt.cer (cn=cyaneamgmt)dctomgmt.cer (cn=cyaneadc)proxytomgmt.cer (cn=cyaneaproxy)

CyaneaDCStore contains: proxytodc.cer (cn=cyaneaproxy) mgmttodc.cer (cyaneamgmt)

CyaneaProxyStore contains: mgmttoproxy.cer (cn=cyaneamgmt) dctoproxy.cer (cn=cyaneadc)

To run the keytool commands, you must be in the java/bin directory or have keytool in your PATH. This is the command with the necessary parameters:

keytool -genkey -alias *alias_name* -keyalg RSA -keysize 1024 -sigalg MD5withRSA -validity 2000 -keypass *keypass* -keystore ./*storename* -storepass *storepass* -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

Use the following details to create all the necessary stores and certificates:

Note: Replace "oakland1" with your custom keypass and "oakland2" with your custom storepass. Replace "CyaneaMgmtStore", "CyaneaDCStore", and "CyaneaProxyStore" with your custom store names.

```
keytool -genkey -alias mgmttomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./CyaneaMgmtStore
  -storepass oakland2 -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland,
  ST=CA, C=US"
```

```
keytool -genkey -alias dctomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./CyaneaMgmtStore -storepass oakland2
  -dname "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"
```

```
keytool -genkey -alias proxytomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./CyaneaMgmtStore -storepass oakland2
  -dname "cn=cyaneaproxy, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"
```

```
keytool -genkey -alias proxytodc -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./CyaneaDCStore -storepass oakland2
  -dname "cn=cyaneaproxy, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"
```

```
keytool -genkey -alias mgmttodc -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./CyaneaDCStore
  -storepass oakland2 -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea,
  L=Oakland, ST=CA, C=US"
```

```
keytool -genkey -alias mgmttoproxy -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./CyaneaProxyStore -storepass oakland2
  -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"
```

```
keytool -genkey -alias dctoproxy -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./CyaneaProxyStore
  -storepass oakland2 -dname "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland,
  ST=CA, C=US"
```

Extracting Certificates:

When you have created the three 3 Stores, extract the certificates by completing the following steps:

1. Extract all certificates from CyaneaMgmtStore by running the following commands:

   ```
   keytool -export -alias mgmttomgmt -keypass oakland1 -keystore ./CyaneaMgmtStore
     -storepass oakland2 -file mgmttomgmt.cer
   ```

   ```
   keytool -export -alias dctomgmt -keypass oakland1 -keystore ./CyaneaMgmtStore
     -storepass oakland2 -file dctomgmt.cer
   ```

   ```
   keytool -export -alias proxytomgmt -keypass oakland1 -keystore ./CyaneaMgmtStore
     -storepass oakland2 -file proxytomgmt.cer
   ```
2. Extract all certificates from CyaneaDCStore by running the following commands:

   ```
   keytool -export -alias proxytodc -keypass oakland1 -keystore ./CyaneaDCStore
     -storepass oakland2 -file proxytodc.cer
   ```

```
keytool -export -alias mgmttodc -keypass oakland1 -keystore ./CyaneaDCStore
  -storepass oakland2 -file mgmttodc.cer
```

3. Extract all certificates from CyaneaProxyStore by running the following commands:

   ```
   keytool -export -alias mgmttoproxy -keypass oakland1
     -keystore ./CyaneaProxyStore -storepass oakland2 -file mgmttoproxy.cer
   ```

   ```
   keytool -export -alias dctoproxy -keypass oakland1
     -keystore ./CyaneaProxyStore -storepass oakland2 -file dctoproxy.cer
   ```

When you have extracted your files, copy the following certificates and Stores to the following locations:

MS_home/etc:CyaneaMgmtStore mgmttoproxy.cer mgmttomgmt.cer mgmttodc.cer

DC_home/itcamdc/etc:CyaneaDCStore CyaneaProxyStore
proxytomgmt.cerproxytodc.cerdctoproxy.cer dctomgmt.cer

Configuring components to use new keystores and certificates

Configure components to use new keystores and certificates:

1. Modify *MS_home*/bin/setenv.sh. At the end of the script you will need to modify the following lines with the new keystore name, storepass, and keypass:

   ```
   KEYSTR_LOC=MS_home/etc/IBMMSStore
   KEYSTR_PASS=oakland2
   KEYSTR_KEYPASS=oakland1
   ```

2. Modify the Visualization Engine (Application Monitor) user interface with the new keystore name, storepass and keypass. Perform the following procedure:
   a. Start the Managing Server.
   b. Log into the IBM WebSphere Application Server administrative console.
   c. Click **Server > Application Servers** and select the *server_name*.
   d. In the **Configuration** tab, navigate to **Server Infrastructure: Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine > Additional Properties: Custom Properties**.
   e. For the following name and value pairs, click **New**, enter the Name and Value, and click **Apply**:
      1) Set the path of the certificate to use when security is enabled for the Visualization Engine (Application Monitor) user interface:

         ```
         certificate.path=MS_home/etc/mgmttomgmt.cer
         ```

      2) Set the keystore location of the Managing Server:

         ```
         keystore.location=MS_home/etc/CyaneaMgmtStore
         ```

      3) Set the keystore password of Managing Server:

         ```
         keystore.storepass=oakland2
         ```

      4) Set the keystore key password of Managing Server:

         ```
         keystore.keypass=oakland1
         ```

      5) Set the user ID passed to the other end for authentication:

         ```
         nodeauth.userid=cyaneamgmt
         ```

   f. Restart the application server.
3. Modify *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/datacollector_custom.properties file with the new storename, storepass and keypass.
   a. Stop the instance of the application server that is being monitored by the Data Collector.

b. Go to DC_home/runtime/app_server_version.node_name.server_name/custom/ datacollector_custom.properties.

c. Set the following property definitions:

   Note: All the following properties are set during the installation or at configuration time. By default you do not need to do anything. You only need to change the following properties if you have changed items that the following properties are referring to. All the keywords in angle (< >) brackets need to be replaced by the appropriate value.

   - The path of the certificate to use when communicating with the data collector. This is only needed when the data collector is operating in secure mode. The delimiter must be a semicolon on all platforms certificate.path=<AM_HOME>/etc/dctomgmt.cer;<AM_HOME>/etc/dctoproxy.cer.
   - The keystore location of the data collector keystore.location=@{AM_HOME}/etc/CyaneaDCStore.
   - The keystore password of data collector server keystore.storepass=oakland94612.
   - The keystore key password of data collector server keystore.keypass=oakland94612.

d. Start the instance of the application server that is monitored by the data collector for the property changes to take effect.

4. Restart the Managing Server to implement the changes made to the Managing Server and Data Collector. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

Secure Socket Layer communications

On distributed platforms, ITCAM for Application Diagnostics uses the SSL security protocol for integrity and confidentiality. You have the option of configuring all monitoring components to utilize SSL for communications. The following steps describe a sample HTTP-based SSL transaction using server-side certificates:

1. The client requests a secure session with the server.
2. The server provides a certificate, its public key, and a list of its ciphers to the client.
3. The client uses the certificate to authenticate the server (verify that the server is who it claims to be).
4. The client picks the strongest common cipher and uses the server's public key to encrypt a newly-generated session key.
5. The server decrypts the session key with its private key.
6. From this point forward, the client and server use the session key to encrypt all messages.

The monitoring software uses the Java Secure Sockets Extensions (JSSE) API to create SSL sockets in Java applications.

Note: If you performed an embedded installation of the IBM WebSphere Application Server with the Managing Server, use the IBM WebSphere Application Server default key. For more information on IBM WebSphere Application Server default keys, refer to the IBM WebSphere Application Server documentation.

This section describes how to customize the default settings for SSL authentication in ITCAM for Application Diagnostics.

Password encryption and Kernel property file encryption

The amcrypto.sh script comes with the Managing Server and is present in *MS_home*/bin to encrypt the passwords related to Node Authentication and SSL.

Password encryption

To encrypt a password, complete the following steps:

1. Enter:

   ```
   amcrypto.sh -encrypt password
   ```

   The password is written to stdout.
2. Copy this encrypted password and place it in the appropriate config files.

   Currently password encryption is supported only for the following property values on both the Managing Server and Data Collectors:

   - KEYSTR_PASS and KEYSTR_KEYPASS in *MS_home*/bin/setenv.sh
   - JDBC_PASSWORD in *MS_home*/bin/setenv.sh. See *ITCAM Managing Server Installation and Customization Guide* for full instructions for changing the Java Database Connectivity (JDBC) user ID and password for the database Schema user.
   - keystore.storepass, keystore.keypass using the same method mentioned in the Step 2 on page 254.
   - keystore.storepass and keystore.keypass in *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/datacollector_custom.properties file.
3. Restart the Managing Server to activate the password encryption changes:
   a. If it is not already stopped, stop the Managing Server.
   b. Start the Managing Server.
4. Restart the VE application server.

Properties file encryption

Complete the following steps:

1. To encrypt a properties file, use:

   ```
   amcrypto.sh -encyptPropertyFile file
   ```

   The *file* is kl1.properties or kl2.properties in *MS_home*/etc. This command encrypts the given input file and stores it in a file with different name. The user can back up the existing properties file and have it replaced by the encrypted file for more security.
2. To decrypt a properties file, use:

   ```
   amcrypto.sh -decryptPropertyFile file
   ```

   The *file* is kl1.properties or kl2.properties in *MS_home*/etc. This command decrypts the given file and writes the decrypted file to another file with a different name.
3. Restart the Managing Server to activate the changes:
   a. If it is not already stopped, stop the Managing Server.
   b. Start the Managing Server.

Enabling Secure Socket Layer at the Data Collector level

To enable SSL, enable Node Authentication first (See “Node Authentication” on page 251). SSL works only with Node Authentication enabled.

Configuration with default options involves setting one property to `true` to operate the Data Collector in SSL mode:

1. In the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/ datacollector_custom.properties file, set the following property to `true` by removing the comment symbol (#) in front of the property definition (by default, this property is commented out).

   ```
   comm.use.ssl.dc=true
   ```

2. Restart the application server.

Note: On the managing server only the Kernel-related changes need to be enabled other managing server components are enabled automatically.

Verifying secure communications

To verify SSL is properly configured, look for the message labeled CYND4051I in one of the following files:

Table 27. Location of the CYND4051I message

Windows	C:\Program Files\IBM\tivoli\common\CYN\logs\node_name.server_name\java_msg_log_file. For example: `C:\Program Files\IBM\tivoli\common\CYN\logs\IBMNode01.server1\msg-dc-Ext.log`
UNIX and **Linux**	/var/ibm/tivoli/common/CYN/logs/*node_name.server_name*/*java_msg_log_file*. For example: `/var/ibm/tivoli/common/CYN/logs/IBMNode01.server1/msg-dc-Ext.log`
z/OS	[ITCAM_CONFIG]/runtime/wasXX.node.server/logs/CYN/logs
IBM i	/QIBM/UserData/tivoli/common/CYN/logs/*node_name.server_name*/*java_msg_log_file*. For example: `/QIBM/UserData/tivoli/common/CYN/logs/IBMNode01.server1/msg-dc-Ext.log`

That message includes the text `Join Proxy Server and Kernel successfully`.

Only the CommandAgent port uses SSL. Other ports opened by the Data Collector (the ProbeController port and the Data Collector - Publish Server port do not use SSL. Therefore, when SSL is enabled, only the data on the channels connected to the CommandAgent port is encrypted.

All the data processed on the CommandAgent channel is encrypted when SSL is enabled. The data can be classified as follows:

Table 28. Classification of the data processed on the CommandAgent channel

Classification	Data
Command and control data	Configuring and unconfiguring the Data Collector
User actions related to threads	• Starting and stopping JVM threads • Changing thread priorities • Getting thread priorities and thread status • Requesting drill down information to see cookies, etc ... • Generating thread dumps • Getting thread stack traces

Table 28. Classification of the data processed on the CommandAgent channel (continued)

Classification	Data
System information	• information • Operating system platform information • JVM information
Application information	• All the applications installed on the monitored • Application binaries and location information • Thread pool information related to JMS, JCA, JTA, Servlet, EJB, etc ... • Data source information
Performance data	All Performance Monitoring Infrastructure data
Transport data	• ORB data • SOAP ports
Memory Information	• Obtaining JVM Heap Snapshot data • Performing memory leak analysis • Performing heap dump

Privacy filtering

The following procedures describe how to enable and verify privacy filtering.

Enabling privacy filtering

Privacy filtering is used to filter out SQL, cookie, and HTTP request query strings and other private data, for example drivers license numbers. When this property is set to `true`, this data is not collected by the Data Collector.

1. Stop the instance of application server that is being monitored by the Data Collector.
2. Go to *DC_home*/runtime/*app_server_version.node_name.server_name*/custom/datacollector_custom.properties.
3. Set the following property definition:

   ```
   secure.filter.on=true
   ```
4. Start the instance of application server that is being monitored by the Data Collector.

Verifying privacy filtering

The following statement is printed out to the Data Collector log when privacy filtering is properly configured:

```
Privacy Filter is On. Http Request Query String, SQL String and Http Cookie data is
not trasmitted.
```

The log file is trace-dc.log.

Script to run if your SSL certificates have expired

All SSL certificates have an expiration time. For some certificates, the expiration time is 4 years, after which the product will not function if you have enabled Node Authentication and SSL. If this is the case, to increase the expiration time, perform the following procedure:

1. Open the script located at *MS_home*/bin/security_cert.sh with a text editor. This is the content of the script:

```
#!/bin/sh

# (C) Copyright IBM Corp. 2005  All Rights Reserved.
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#

# Note: This script requires $JDK_HOME to be defined and it requires
# JDK_HOME/bin/keytool to be present. This keytool is available in FULL JDK
# versions and may not be available in JRE versions of the install

# PLEASE DEFINE JDK HOME

JDK_HOME=/opt/IBM/WebSphere/AppServer6/java

PATH=${JDK_HOME}/bin:$PATH

# This script generates ALL the certificates and certificate stores required for
# ITCAMfWAS Product (DC/MS/Port Consolidator). Currently it populates
# certificates with validity of 7000 days. If you feel its too high replace
# validity period to a lower number according to your needs. Please Note: once
# limit is reached, Product will stop working when NodeAuthentication/SSL is ON
# Its your responsibility to re-generate the certificates and stores.
# Please replace ALL the certificates at DC, MS and PortCosolidator level.
# Partial replacement will NOT work


keytool -genkey -alias mgmttomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA -validity 7000
 -keypass cyanea94612 -keystore ./CyaneaMgmtStore -storepass cyanea94612 -dname
 "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias dctomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA -validity 7000
 -keypass cyanea94612 -keystore ./CyaneaMgmtStore -storepass cyanea94612 -dname
 "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias proxytomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
 -validity 7000 -keypass cyanea94612 -keystore ./CyaneaMgmtStore -storepass cyanea94612
 -dname "cn=cyaneaproxy, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias proxytodc -keyalg RSA -keysize 1024 -sigalg MD5withRSA
 -validity 7000 -keypass oakland94612 -keystore ./CyaneaDCStore -storepass oakland94612
 -dname "cn=cyaneaproxy, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias mgmttodc -keyalg RSA -keysize 1024 -sigalg MD5withRSA
 -validity 7000 -keypass oakland94612 -keystore ./CyaneaDCStore -storepass oakland94612
 -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias mgmttoproxy -keyalg RSA -keysize 1024 -sigalg MD5withRSA
 -validity 7000 -keypass oakland94612 -keystore ./CyaneaProxyStore -storepass oakland94612
 -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias dctoproxy -keyalg RSA -keysize 1024 -sigalg MD5withRSA
 -validity 7000 -keypass oakland94612 -keystore ./CyaneaProxyStore -storepass oakland94612
 -dname "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -export -alias mgmttomgmt -keypass cyanea94612 -keystore ./CyaneaMgmtStore
 -storepass cyanea94612 -file mgmttomgmt.cer

keytool -export -alias dctomgmt -keypass cyanea94612 -keystore ./CyaneaMgmtStore
 -storepass cyanea94612 -file dctomgmt.cer

keytool -export -alias proxytomgmt -keypass cyanea94612 -keystore ./CyaneaMgmtStore
 -storepass cyanea94612 -file proxytomgmt.cer

keytool -export -alias proxytodc -keypass oakland94612 -keystore ./CyaneaDCStore -storepass
 oakland94612 -file proxytodc.cer
```

```
keytool -export -alias mgmttodc -keypass oakland94612 -keystore ./CyaneaDCStore -storepass
 oakland94612 -file mgmttodc.cer

keytool -export -alias mgmttoproxy -keypass oakland94612 -keystore ./CyaneaProxyStore
 -storepass oakland94612 -file mgmttoproxy.cer

keytool -export -alias dctoproxy -keypass oakland94612 -keystore ./CyaneaProxyStore
 -storepass oakland94612 -file dctoproxy.cer

cp ./CyaneaMgmtStore ./CyaneaMgmtStore_Comm
cp ./CyaneaDCStore ./CyaneaDCStore_Comm
cp ./CyaneaProxyStore ./CyaneaProxyStore_Comm

keytool -keystore ./CyaneaMgmtStore_Comm -storepass cyanea94612 -import -alias mgmttodc
 -file ./mgmttodc.cer

keytool -keystore ./CyaneaMgmtStore_Comm -storepass cyanea94612 -import -alias mgmttoproxy
 -file ./mgmttoproxy.cer

keytool -keystore ./CyaneaDCStore_Comm -storepass oakland94612 -import -alias dctomgmt
 -file ./dctomgmt.cer

keytool -keystore ./CyaneaDCStore_Comm -storepass oakland94612 -import -alias dctoproxy
  -file ./dctoproxy.cer

keytool -keystore ./CyaneaProxyStore_Comm -storepass oakland94612 -import -alias proxytodc
 -file ./proxytodc.cer

keytool -keystore ./CyaneaProxyStore_Comm -storepass oakland94612 -import -alias proxytomgmt
  -file ./proxytomgmt.cer
```

2. Specify the path for the location of the Java home directory for the JDK_HOME parameter. For example,

   ```
   JDK_HOME=D:\IBM\AppServer\java
   ```
3. If the increase in expiration time to 20 years (7000 days) is too much, modify the script. Change the value of `-validity 7000` to a lower number of days, in all instances it occurs in the script. For example, change all instances of `-validity 7000` to `-validity 3500`.
4. Save the changes and run the script.

Settings for the Data Collector if Java 2 security is enabled

By default, Data Collector configuration enables Java 2 security on the application server, and sets a permissive policy. This policy ensures that the Data Collector can run properly, and provides no other security protection. If you need a more restrictive policy, perform the following procedure to ensure that the policy becomes active and the Data Collector can still work properly.

The Data Collector sets the Java security policy file location for all monitored application server instances (`java.security.policy` system property) to *`DC_home`*`/itcamdc/etc/datacollector.policy`. You must edit this file in the following way:

- Remove all existing content.
- Copy the sample security policy for the Data Collector from the file *`DC_home`*`/itcamdc/etc/datacollector.security.policy`.
- If ITCAM for Transactions is installed on the server, add a grant statement for the ITCAM for Transactions code base to the security policy file. Follow the model for the grant statements provided in the sample

datacollector.security.policy file, but use the ITCAM for Transactions installation root directory in the codeBase statement.

- Add your required security policy settings.

Save the file, and create a backup copy.

Attention: Each time you configure or reconfigure the Data Collector for an application server instance, the file `*DC_home*/itcamdc/etc/datacollector.policy` might be overwritten. To ensure that your security policy remains active, restore this file from the backup copy after configuring or reconfiguring the Data Collector for any application server instance.

Appendix B. Starting and stopping the monitoring environment

This chapter contains procedures for starting and stopping ITCAM for Application Diagnostics's various components, databases, and application servers.

Disabling and re-enabling a Data Collector

If you need to disable a Data Collector without unconfiguring or uninstalling it, perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console.
2. Click **Server > Application Servers** and select the *server_name*.
3. Navigate to **Process Definition > Java Virtual Machine > Custom Properties**.
4. Find a property with the name `ITCAM_DC_ENABLE`. If this property is not present, add it.
5. Set the value of this property to `false`.
6. Click **OK** or **Apply**. Then click **Save**.
7. Restart the application server (see “Restarting the application server”)

To re-enable a Data Collector that was disabled in this way, perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console.
2. Click **Server > Application Servers** and select the *server_name*.
3. Navigate to **Process Definition > Java Virtual Machine > Custom Properties**.
4. Find the property with the name `ITCAM_DC_ENABLE`.
5. Set the value of this property to `true`.
6. Click **OK** or **Apply**. Then click **Save**.
7. Restart the application server (see “Restarting the application server”)

Restarting the application server

There are separate procedures for restarting the application server in Network Deployment and non-Network Deployment environments.

Restarting the application server in a non-Network Deployment environment

To restart the application server, complete the following steps:

Table 29. Restarting the application server

Windows	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere >** ***application_server_and_version*> Profiles >** ***profile_name*** **> First steps**.
	2. Click **Stop the server**.
	Wait for the First steps output window to display a message similar to the following message:
	`Server` *`server_name`* `stop completed`
	3. Click **Start the server**.
	The First steps output window should display a message similar to the following message:
	`Server` *`server_name`* `open for e-business`
	• From a command line:
	`cd` *`AppServer_home`*`\profiles\`*`profile_name`*`\bin`
	`stopServer` *`server_name`* `[options]`
	`startServer` *`server_name`*

Linux or UNIX systems	`cd` *`AppServer_home`*`/profiles/`*`profile_name`*`/bin`
	`./stopServer` *`server_name`* `[options]`
	`./startServer` *`server_name`*

The *`server_name`* is the name of the configuration directory of the server you want to restart. The default is `server1`.

The *`profile_name`* specifies the profile name. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *`name`* or `-user` *`name`* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Attention: If you are running in a secure environment but have not provided a user ID and password, you will receive an error message.

Restarting the application server in a Network Deployment environment

Complete the following steps to restart the application server:

1. Change to the *`AppServer_home`*`/bin` directory.
2. Stop all servers on the node, and the node itself. Run the `stopNode -stopservers` command
3. Stop the Deployment Manager process. Run the `stopManager` command.
4. Start the Deployment Manager process. Run the `startManager` command.

5. Start the node. Run the `startNode` command.
6. For each application server on the node, start the application server using the procedure in "Starting the application server in a non-Network Deployment environment."

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *`name`* or `-user` *`name`* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Attention: If you are running in a secure environment but have not provided a user ID and password, you will receive an error message.

Starting the application server

There are separate procedures for starting the application server in Network Deployment and non-Network Deployment environments.

Starting the application server in a non-Network Deployment environment

Complete the following steps to start the application server:

Table 30. Starting the application server.

Windows	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere >** ***application_server_and_version*>** **Profiles >** ***profile_name*** **> First steps**.
	2. Click **Start the server**.
	The First steps output window should display a message similar to the following message:
	`Server` *`server_name`* `open for e-business`
	• From a command line:
	`cd` *`AppServer_home`*`\profiles\`*`profile_name`*`\bin`
	`startServer` *`server_name`*

Linux or UNIX systems	`cd` *`AppServer_home`*`/profiles/`*`profile_name`*`/bin`
	`./startServer` *`server_name`*

The *`server_name`* is the name of the configuration directory of the server you want to start. The default is `server1`.

The *`profile_name`* specifies the profile name for version 6 application servers. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *`name`* or `-user` *`name`* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Attention: If you are running in a secure environment but have not provided a user ID and password, you will receive an error message.

Starting the application server in a Network Deployment environment

Complete the following steps to start the application server:

1. Change to the *`AppServer_home`*`/bin` directory.
2. Start the Deployment Manager process. Run the `startManager` command.
3. Start the node. Run the `startNode` command.
4. For each application server on the node, start the application server using the procedure in "Starting the application server in a non-Network Deployment environment" on page 265.

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *`name`* or `-user` *`name`* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Attention: If you are running in a secure environment but have not provided a user ID and password, you will receive an error message.

Stopping the application server

There are separate procedures for stopping the application server in Network Deployment and non-Network Deployment environments.

Stopping the application server in a non-Network Deployment environment

Complete the following steps to stop the application server:

Table 31. Stopping the application server.

Windows	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere >** ***application_server_and_version*****> Profiles >** ***profile_name*** **> First steps**.
	2. Click **Stop the server**.
	Wait for the First steps output window to display a message similar to the following message:
	`Server` *`server_name`* `stop completed`
	• From a command line:
	`cd` *`AppServer_home`*`\profiles\`*`profile_name`*`\bin`
	`stopServer` *`server_name`* `[options]`

Linux or UNIX systems	`cd` *`AppServer_home`*`/profiles/`*`profile_name`*`/bin`
	`./stopServer` *`server_name`* `[options]`

The *`server_name`* is the name of the configuration directory of the server you want to stop. The default is `server1`.

The *`profile_name`* specifies the profile name for version 6 application servers. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *`name`* or `-user` *`name`* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Attention: If you are running in a secure environment but have not provided a user ID and password, you will receive an error message.

Stopping the application server in a Network Deployment environment

Complete following steps to stop the application server:

1. Change to the *`AppServer_home`*`/bin` directory.
2. Stop all servers on the node, and the node itself. Run the `stopNode -stopservers` command
3. Stop the Deployment Manager process. Run the `stopManager` command.

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *`name`* or `-user` *`name`* option specifies the user name for authentication if security is enabled in the server.

- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Attention: If you are running in a secure environment but have not provided a user ID and password, you will receive an error message.

Appendix C. Using regular expressions

Regular expressions are sets of symbols and characters that are used to match patterns of text. You can use regular expressions to search specific IP addresses across your Web environment. Regular expressions also enable you to search a simple, fixed URI or a complex URI pattern that matches one or more groups of transactions.

Regular expression library

An extensive library of regular expression characters and operators is available for your URI filters and IP address specifications. The International Components for Unicode (ICU) open-source development project provides this library for your use. The next section provides the most frequently used expressions for this product. However, you can refer to the following Web page for a full description of the ICU regular expression library and an explanation of how to use the characters and operators for complex expressions: http://oss.software.ibm.com/icu/userguide/regexp.html

Frequently used regular expressions

The following list highlights characters and operators most frequently used in regular expressions:

\

Quotes the character that follows it, which treats that character as a literal character or operator (not a regular expression). When you want the following characters to be treated as literal, you must precede them with a backslash:

```
* ? + [ ( ) { } ^ $ | \ . /
```

In other words, use a backslash followed by a forward slash (`\/`) to include a forward slash in a URI filter. Use a backslash followed by a period (`\.`) to include a period in a URI filter.

Example: to specify the URI pattern `http://www.ibm.com/`, use the following regular expression:

```
http:\/\/www\.ibm\.com\/
```

To specify all URIs that begin with `http://www.ibm.com/`, use the following regular expression:

```
http:\/\/www\.ibm\.com\/.*
```

.

Matches any one character.

Example: to match both `ibm2` and `ibm3` within a string, use `ibm.` such as in the following example: **`http:\/\/www\.ibm.\.com\/`**

(?: ...)

Non-capturing parentheses. Groups the included pattern, but does not provide capturing of matching text. Somewhat more efficient than capturing parentheses.

Example: you can use the non-capturing parenthesis to group expressions to form more complicated regular expressions. To match a URI that starts with one of the following URLs: `http://www.ibm.com/marketing/` or `http://www.ibm.com/sales/`, you would do a grouping with a pipe sign (|) (represents *or*):

`http://www.ibm.com/(?:marketing)|(?:sales)/`

* Matches the preceding element zero or more times. You must quote this character.

Example: the expression, **`ca*t`**, matches `cat`, `caat`, `ct`, and `caaaaat`. The term `cabt`, would not return as a match.

Specifying exclusions with the bang (!) operator (Quality of Service listening policies only)

Note: This section applies to the entry of URI and client IP filters for Quality of Service listening policies only.

You can use an exclamation point (**!**), also called the *bang* operator, to filter out transactions that might match the regular expressions already entered, but that are not to be considered valid transactions for this listening policy. These exclusions are considered negative filters. You can enter these exclusions as additional URI or client IP filters. The formatting of these additional filters is as follows:

URI Filter Exclusions

Use only fixed strings. For example, you can use the following strings:

!http://www.ibm.com/
!http://www.ibm.com/hr/index.html
!http://www.ibm.com/it/errorpage.html

Client IP Exclusions

The following are valid:

!*.24.45.46
!12.*.45.56
!12.24.*.56
!12.24.45.*
!12.24.45.56

You can replace any "octet" (there are four in an IP address: octet . octet . octet . octet) with a wildcard (*). Note that this is not the regular expression wildcard (.*) from the positive filters.

Appendix D. Manual changes to application server configuration for the Data Collector

Automatic Data Collector configuration may fail because of unexpected circumstances. In this case, you need to restore the application server configuration that is backed up by the automatic process. You may also need to configure and unconfigure Data Collector monitoring for an application server instance manually.

Restoring the application server configuration after a failed Data Collector configuration

This section applies only to the **Windows**, **UNIX**, and **Linux** platforms.

If the Data Collector configuration fails, for example if the application server fails to start up, you can use the restoreConfig command to restore the application server configuration. Perform one of the following procedures:

- In a non-Network Deployment environment:
  1. Locate the backup configuration file that was created in the `DC_home/config_dc/backup` directory. If several backup files are present, check the modification date and time of the file; it must be the date and time of the failed configuration. If you did not perform any other Data Collector configurations on the same host after the failed one, use the most recent file in the directory.
  2. Stop all instances of theapplication server. Perform the steps in "Stopping the application server" on page 266.
  3. Run the `restoreConfig` command from the `Appserver_home/profiles/profile_name/bin` directory. The syntax is:

Table 32. Syntax of the restoreConfig command in a non-Network Deployment environment

Operating system	Syntax	Example
Windows	`restoreConfig.bat DC_home/config_dc/backup/backup_file`	`restoreConfig.bat "C:\Program Files\IBM\itcam\WebSphere \DC\config_dc\backup\ WebSphereConfig_2006-04-22.zip"`
UNIX or **Linux**	`./restoreConfig.sh DC_home/config_dc/backup/backup_file`	`./restoreConfig.sh /opt/IBM/itcam /WebSphere/DC/config_dc/backup/ WebSphereConfig_2006-04-22.zip`

  4. Start the instances of the application server. See "Starting the application server" on page 265.
- In a Network Deployment environment:
  1. Locate the backup configuration file that was created in the `DC_home/config_dc/backup` directory. If several backup files are present, check the modification date and time of the file; it must be the date and time of the failed configuration. If you did not perform any other Data Collector configurations on the same host after the failed one, use the most recent file in the directory.
  2. Stop all instances of application servers. Perform the steps in "Stopping the application server" on page 266.

3. Create a temporary directory in any convenient path (*temp_directory*). On a UNIX or Linux host, create it under `/tmp`.
4. Run the `restoreConfig` command from the `*Appserver_home*/profiles/*profile_name*/bin` directory. The syntax is:

Table 33. Syntax of restoreConfig command, Network Deployment environment

Operating system	Syntax	Example
Windows	`restoreConfig.bat DC_home/config_dc/backup/backup_file -location temp_directory`	`restoreConfig.bat "C:\Program Files\IBM\itcam\WebSphere \DC\config_dc\backup\ WebSphereConfig_2006-04-22.zip" -location temp_directory`
UNIX or **Linux**	`./restoreConfig.sh DC_home/config_dc/backup/backup_file -location temp_directory`	`./restoreConfig.sh /opt/IBM/itcam/WebSphere/DC/config_dc /backup/WebSphereConfig_2006-04-22.zip -location temp_directory`

Running the restoreConfig command restores the original application server configuration to the temporary directory.

5. Copy the `server.xml`, `variables.xml`, and `pmi-config.xml` files from the following path:

```
temp_directory/restored_configuration_home/cells/cell_name/
nodes/node_name/servers/server_name
```

to the following path on the **Deployment Manager** host:

```
Appserver_home/profiles/profile_name/config/cells/cell_name/
nodes/node_name/servers/server_name
```

6. Perform a node sync from the Deployment Manager's administrative console for the node.
7. In the Deployment Manager's administrative console, save changes to the master configuration.
8. Start the instances of the application server. See “Starting the application server” on page 265.

Note: If you want to split the Data Collector installation into two parts you can do so by completing the following steps:

1. Generate the Data Collector run time directory
2. Modify the WebSphere parameters.

For more information on how to split Data Collector installation into two parts, refer to the OPAL website, http://www-01.ibm.com/software/brandcatalog/portal/opal/ .

In the search field, type in the following search criteria, "Composite Application Manager for WebSphere Data Collector Configuration Solution for Large Scaled WebSphere".

Manually configuring the Data Collector to monitor an application server instance

You can configure the Data Collector to monitor an application server instance without using the configuration utility. To do this, you need to create a settings file, and then manually add settings using WebSphere Administrative Console. The runtime directory will be created automatically when the Data Collector is started for the application server instance.

Step 1. Create a settings file

The settings file contains the values needed for initial configuration of the Data Collector.

To create this file, copy the file *DC_home*/itcamdc/etc/dcInputs_manual.txt into *DC_home*/runtime/dcInputs.txt. Then, edit *DC_home*/runtime/dcInputs.txt, setting the configuration parameters according to the comments in the file.

Tip: you can use a different name if needed. In this case, you need to use a different value for the -Ditcamdc.inputs property in the next step.

You must set the parameters in Section 1. Change parameters in Section 2 if the defaults are not suitable. Do not change anything below the end of Section 2.

Set the appserver.platform parameter according to the product that is to be monitored:

Table 34. Values for the application server platform designation

Product name and version	Value of appserver.platform
WebSphere Application Server 6.0	was60
WebSphere Enterprise Service Bus (ESB) 6.0, based on WebSphere Application Server 6.0	was60.esb60
WebSphere Process Server 6.0, based on WebSphere Application Server 6.0	was60.prs60
WebSphere Application Server 6.1	was61
WebSphere Enterprise Service Bus (ESB) 6.1, based on WebSphere Application Server 6.1	was61.esb61
WebSphere Process Server 6.1, based on WebSphere Application Server 6.1	was61.prs61
WebSphere Enterprise Service Bus (ESB) 6.2, based on WebSphere Application Server 6.1	was61.esb62
WebSphere Process Server 6.2, based on WebSphere Application Server 6.1	was61.prs62
WebSphere Application Server 7.0	was70
WebSphere Portal Server 6.0, based on WebSphere Application Server 6.0	wps60
WebSphere Portal Server 6.1, based on WebSphere Application Server 6.1	wps61

Step 2. Add settings using WebSphere Administrative Console

Complete the following steps:

1. Log into the IBM WebSphere Application Server administrative console.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
4. In the **Generic JVM arguments** field, add the following entries. All of them must be on a single line; separate different arguments by spaces before the - sign, do not use spaces anywhere else.

Replace *DC_home* with *ITM_home*/TMAITM6/wasdc/7.1.0.1 on Windows, *ITM_home*/*architecture_code*/yn/wasdc/7.1.0.1 on Linux and UNIX systems. On Windows, use / as directory separator (for example, C:/IBM/ITM/TMAITM6/wasdc/7.1.0.1.

For the value of *appserver_version*, see Table 34 on page 273.

For *node_name* and *server_name*, use the node and server name of the application server instance.

For *number*, use 14 for WebSphere Application Server 6.0 and products based on it, 15 for WebSphere Application Server 6.1 and products based on it, or 16 for WebSphere Application Server 7.0 and products based on it.

```
-Xbootclasspath/p:DC_home/toolkit/lib/bcm-bootstrap.jar;
DC_home/itcamdc/lib/ppe.probe-bootstrap.jar
-agentlib:am_ibm_number=DC_home/runtime/
appserver_version.node_name.server_name/
-Ditcamdc.inputs=dcInput.txt
```

Tip: if you have used a different file name instead of dcInput.txt, use the name for the -Ditcamdc.inputs parameter.

Also, for IBM Virtual Machines, add:

```
-Xverbosegclog:${SERVER_LOG_ROOT}/itcam_gc.log,5,3000
```

For Sun Java Virtual Machines (typically used on Solaris and HP/UX systems), add:

```
-XX:+PrintGCTimeStamps -verbosegc -Xloggc:${SERVER_LOG_ROOT}/itcam_gc.log
```

5. Click **Apply**.
6. In the Messages dialog box, click **Save**.
7. In the Save to Master Configuration dialog box, complete the following steps:
   - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.
8. Click **Server > Application Servers** and select the *server_name*.
9. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Environment Entries**.
10. Depending on the operating system and hardware platform, set the following environment entry:

Table 35.

Platform	Entry name	Entry value
AIX4_R1	LIBPATH	*DC_home*/toolkit/lib/aix533
AIX_64	LIBPATH	*DC_home*/toolkit/lib/aix536
HPUX10	SHLIB_PATH	*DC_home*/toolkit/lib/hp11
HPUX_64	SHLIB_PATH	*DC_home*/toolkit/lib/hp116
HPUX_IA64	SHLIB_PATH	*DC_home*/toolkit/lib/hpi116
HPUX_IA64N	SHLIB_PATH	*DC_home*/toolkit/lib/hpi113
LINUX_IX64	LD_LIBRARY_PATH	*DC_home*/toolkit/lib/lx8266
LINUX_IX86	LD_LIBRARY_PATH	*DC_home*/toolkit/lib/li6263
LINUX_PPC	LD_LIBRARY_PATH	*DC_home*/toolkit/lib/lpp263
LINUX_PPC64	LD_LIBRARY_PATH	*DC_home*/toolkit/lib/lpp266
LINUX_S390	LD_LIBRARY_PATH	*DC_home*/toolkit/lib/ls3263

Table 35. (continued)

Platform	Entry name	Entry value
LINUX_S390_64	`LD_LIBRARY_PATH`	*DC_home*`/toolkit/lib/ls3266`
SOLARIS2	`LD_LIBRARY_PATH`	*DC_home*`/toolkit/lib/sol293`
SOLARIS2_IX86	`LD_LIBRARY_PATH`	*DC_home*`/toolkit/lib/sol603`
SOLARIS2_IX86_64	`LD_LIBRARY_PATH`	*DC_home*`/toolkit/lib/sol606`
SOLARIS_64	`LD_LIBRARY_PATH`	*DC_home*`/toolkit/lib/sol296`
W32_IX86 (Windows 32-bit)	`PATH`	*DC_home*`/toolkit/lib/win32`
W64_X64 (Windows 32-bit)	`PATH`	*DC_home*`/toolkit/lib/win64`

11. Click **Apply**.
12. In the Messages dialog box, click **Save**.
13. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
14. Restart the application server instance. The Data Collector will read the settings file and create the runtime directory.

Manually removing Data Collector configuration from an application server instance

If the Agent has been uninstalled but the Data Collector was still configured to monitor any application server instances, these instances may fail to start. In this case, you need to manually remove Data Collector configuration from each instance.

Perform the following procedure:

1. Log on to the WebSphere Administration Server Console.
2. Click **Server** > **Application Servers** and select the server name.
3. In the **Configuration** tab, navigate to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Additional Properties: Java Virtual Machine**.
4. Remove any of the following JVM Custom Properties, if they are present:
   - `am.home`
   - `java.security.policy`
   - `com.ibm.tivoli.jiti.injector.ProbeInjectorManagerChain.primaryInjectorFile` (if it is present)
5. Remove the custom service named `com.cyanea.ws6.ITCAMNotifierCustomService`, if it is present.
6. In **Generic JVM Arguments**:
   - Remove any JVM arguments that include the *DC_home* directory if they are present. There can be a `-Xbootclasspath` argument and a `-agentlib` argument.
   - Remove the `-Xshareclasses:none` and `-verbosegc` arguments if they are present. Remove the `-Xtrace` argument if it is present.
7. Click **Apply** or **OK**.
8. In the **Messages** dialog box, click **Save**.

9. In the **Save to Master Configuration** dialog box, complete one of the following steps:
   - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.
10. In the Navigation Pane, click **Environment > Shared Libraries**.
11. Change the scope to the specific application server instance.
12. In the shared library named `WPSlib`, remove `${ITCAMDCHOME}/itcamdc/lib/wpsaspect.jar` (the environment variable name may be different) from the classpath if it is present. If this was the only entry in the classpath, remove the `WPSlib` shared library.
13. Click **Apply** or **OK**.
14. In the **Messages** dialog box, click **Save**.
15. In the **Save to Master Configuration** dialog box, complete one of the following steps:
   - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
   - If you are not under a Network Deployment environment, click **Save**.
16. Back up the file: *DC_home*`/installer/configured/WasConfiguredServers.xml`
17. Open the file for editing: *DC_home*`/installer/configured/WasConfiguredServers.xml`
18. Look for an entry similar to the following text and referring to the application server instance for which the Data Collector was unconfigured:

```
<instance id="C:\was7\profiles\AppSrv02|cells/CellIT71/nodes/NodeIT71
  /servers/server1">
<node>CONFIG_FILE_STORE_DIR=C:/IBM/ITM/TMAITM6/wasdc/
  7.1.0.1\installer\configured\was70.NodeIT71.server1</node>
  <node>WAS_BASEDIR=C:\was7</node>
</instance>
```

19. If the entry was found, remove it.
20. Save the file. Do **not** delete the file, even if no entries for application server instances remain.
21. Restart the application server instance that was monitored by the Data Collector.

Appendix E. Attribute groups and sizing information for historical warehousing

You can find the record size and recording frequency information for ITCAM Agent for WebSphere Applications in Table 36. This information helps you size the amount of disk space needed for any historical logging.

Table 36. Information for historical warehousing

Table Name	Object Name	Record size	Recording Frequency
KYNPREV	WebSphere Agent Events	616	1 record for each product event. These records are written when problems occur. It is impossible to say how often this may occur
KYNAPSST	Application Server Status	1260	1 record per interval per server instance
KYNLOGANAL	Log Analysis	1072	1 record per interval for each entry written into the application server log stream or file. This table is renamed from the XEWAS KWWERRLG
KYNAPSRV	Application Server	800	1 record per interval per application server. In XEWAS this approximates app server instance kwwappsv
KYNCONTNR	EJB Containers	880	1 record per interval per application server, plus 1 record per interval per EJB container
KYNEJB	Enterprise Java Beans	1040	1 record per interval for each EJB method
KYNCNTROP	Container Object Pools	812	1 record per interval per application server, plus 1 record per interval per EJB container. In XEWAS table name was KWEEBOP.
KYNAPP	Web Applications	1060	1 record per interval per Web application
KYNSERVLT	Servlets JSPs	1320	1 record per interval per servlet
KYNTRANS	Container Transactions	812	1 record per interval per application server plus 1 record per interval per EJB container.
KYNCACHE	Dynamic Cache	588	1 record per cache per cycle
KYNCACHT	Dynamic Cache Templates	952	1 record per cache template per cycle
KYNJ2C	J2C Connection Pools	972	1 record per J2EE connection pool per cycle
KYNSERVS	Servlet Sessions	1064	1 record per servlet session per interval
KYNTHRDP	Thread Pools	864	1 record per thread pool per interval
KYNWLMCL	Workload Management Client	592	1 record per WLM client per interval

Table 36. Information for historical warehousing (continued)

Table Name	Object Name	Record size	Recording Frequency
KYNWLMSR	Workload Management Server	632	1 record per WLM server per interval
KYNGCACT	Garbage Collection Analysis	744	1 record per interval per application server. In XEWAS this approximates kwwgc.
KYNGCAF	Allocation Failure	620	1 record per interval for each allocation failure block. In XEWAS this approximates kwwafb
KYNGCCYC	Garbage Collection Cycle	660	1 record per garbage-collection cycle per interval
KYNREQUEST	Request Analysis	1484	1 record per interval for each workload in each application server. This table is renamed from XEWAS KWWWLDS2
KYNREQSEL	Selected Request	1248	1 record per interval for each workload degradation in each application server. This table is renamed from XEWAS KWWWKLDD
KYNDATAS	Datasources	1164	1 record per interval per data source in each application server
KYNJMSSUM	JMS Summary	860	1 record per interval per MQ queue in each application server
KYNREQHIS	Request Times and Rates	992	1 record per interval per WAS. This table is not in the prior XEWAS product
KYNDBCONP	DB Connection Pools	1096	1 record per datasource per interval plus 1 record per application server per interval
KYNDCMSG	DC Messages – WebSphere	1388	1 record per each entry written into DC log message file
KYNDCSSTK	DCS Stack	1032	1 record per DCS stack per interval plus 1 record per application server per interval
KYNHAMGMT	High Availability Manager	724	1 record per application server per interval
KYNWEBSGW	Web Services Gate Way	968	1 record per Web Services Gateway per interval plus 1 record per application server per interval
KYNWEBSVC	Web Services	1004	1 record per Web Service per interval plus 1 record per application server per interval
KYNALARMM	Alarm Manager	980	1 record per WorkManager per interval plus 1 record per application server per interval
KYNSCHED	Scheduler	1000	1 record per Scheduler per interval plus 1 record per application server per interval
KYNCLICOM	Client Communications	1220	1 record per application server per interval
KYNDURSUB	Durable Subscriptions	1504	1 record per Durable Subscription per interval

Table 36. Information for historical warehousing (continued)

Table Name	Object Name	Record size	Recording Frequency
KYNMECOM	Messaging Engine Communications	1004	1 record per application server per interval
KYNMSGENG	Messaging Engines	972	1 record per Message Engine per interval plus 1 record per application server per interval
KYNMSGQUE	Queue	1040	1 record per Queue per interval
KYNSVCOMEL	Service Component Elements	1752	1 record per Service Component Element per interval plus 1 record per application server per interval
KYNSVCCOMP	Service Components	704	1 record per Service Component plus 1 record per application server
KYNTOPICSP	Topic Spaces	1288	1 record per Topic Space per interval
KYNWMQCL	WMQ Client Link Communications	988	1 record per application server per interval
KYNWMQLINK	WMQ Link Communications	1004	1 record per application server per interval
KYNWPMSV	Workplace Mail Service	776	1 record per application server per interval
KYNWPMQM	Workplace Mail Queues	712	1 record per Mail Queue per interval
KYNWPMIP	Workplace Mail IMAP/POP	720	1 record per protocol (IMAP/POP) per interval
KYNWPTALS	Portal Summary	768	1 record per application server per interval
KYNWPPAGE	Portal Page Summary	832	1 record per Portal Page per interval plus 1 record per application server
KYNWPLETS	Portlet Summary	836	1 record per Portlet per interval plus 1 record per application server
KYNAPHLTH	Application Health Status	1020	1 record per interval per application for each application server
KYNAPMONCF	Application Monitoring Configuration	n/a	not historical table
KYNRQMONCF	Requests Monitoring Configuration	n/a	not historical table
KYNBASELN	Baseline	n/a	not historical table

Appendix F. Port Consolidator reference and configuration

The Port Consolidator is used to reduce network resources. It is used on the Data Collector to limit the number of ports used by the Data Collector when communicating with the Managing Server. The Port Consolidator only consolidates the traffic in one direction: from the Managing Server to the Data Collector. All traffic from the Managing Server to the Data Collector will be routed through the Port Consolidator. However, the traffic from the Data Collector to the Managing Server is direct.

Note: Typically, all Data Collectors and Port Consolidators are installed on the same physical computer. However, it is possible to run the Port Consolidator on a different computer. Contact IBM Software Support for setup assistance in this case.

Configuring a Data Collector to use the Port Consolidator

If you have a firewall, you can avoid allocation of an excessive number of ports in the firewall for multiple Data Collectors by configuring and using the Port Consolidator.

Perform the following procedure to configure a Data Collector to use the Port Consolidator:

1. Edit the `DC_home/runtime/app_server_version.node_name.server_name/custom/datacollector_custom.properties` file. Add the following lines to the end of the file:

   ```
   proxy.host=IP_address
   ```

   This is usually the same IP address as the Data Collector computer, but it could be different in a multiple IP or virtual host scenario. In any case, specify the same IP address as the one specified in the `am.socket.bindip` property in `DC_home/itcamdc/etc/proxy.properties`.

   ```
   proxy.port=port
   ```

   This is usually 8800. In any case, specify the same port specified in the `PROXY_PORT` property in `DC_home/itcamdc/bin/proxyserverctrl_*`.

   Note:

   a. Do not use the loopback address for the IP address. Use a valid IP address for the local system.
   b. `proxy.port` must match the port number for `PROXY_PORT` that is specified in the startup script you run in Step 4.
2. Restart the instance of the application server that is being monitored by the Data Collector. See "Restarting the application server" on page 263.
3. From a command prompt, move to the directory `DC_home/itcamdc/bin`.
4. Start the Port Consolidator using one of the following commands:

Table 37. Command for starting the Port Consolidator

Windows	`proxyserverctrl_ws.bat start`
UNIX and **Linux**	`./proxyserverctrl_ws.sh start`

Do not close the command prompt window.

Note: The value for `PROXY_PORT` that is specified in the script must match the value that you specified for `proxy.port` in Step 1 on page 281.

5. Open the Self-Diagnosis page of the Visualization Engine (Application Monitor) user interface, and check to see that the following components are listed:
   - `COMMANDAGENTPROXY`
   - `KERNELPROXY`
   - `PROBECONTROLLERPROXY`
6. Verify that the Data Collector is using the Port Consolidator:
   a. Look for the message labeled CYND4051I in one of the following files:

Table 38. Location of the CYND4051I message

Windows	*DC_home*\logs\CYN\logs\*node_name.server_name**java_msg_log_file*. For example: C:\IBM\ITM\TMAITM6\wasdc\7.1.0.1\logs\CYN\logs\tivx44Node02.server1\msg-dc-ParentLast.log
UNIX and **Linux**	*DC_home*/logs/CYN/logs/*node_name.server_name*/*java_msg_log_file*. For example: /opt/IBM/AD7101_0505/li6263/yn/wasdc/7.1.0.1/logs/CYN/logs/tivx44Node02.server1/msg-dc-ParentLast.log

   That message includes the text `Join Proxy Server and Kernel successfully`.

   b. From a new command prompt, move to the directory *DC_home*/itcamdc/bin, and enter one of the following commands:

Table 39. Entering the proxyserverctrl_ws command

Windows	`proxyserverctrl_ws.bat list`
UNIX and **Linux**	`./proxyserverctrl_ws.sh list`

   You will see the Data Collector listed as one Service type, `PPECONTROLLER`. Keep this command prompt window open for future use.

7. Verify the Data Collector connection to the Port Consolidator (again) by entering one of the following commands:

Table 40. Entering the proxyserverctrl_ws command

Windows	`proxyserverctrl_ws.bat list`
UNIX and **Linux**	`./proxyserverctrl_ws.sh list`

   You will now see the Data Collector listed as two Service types, PPECONTROLLER and PPEPROBE.

   The Data Collector is configured to use the Port Consolidator.

Reconfiguring the Data Collector to bypass the Port Consolidator

If after configuring the Data Collector to use the Port Consolidator, you want the Data Collector to bypass the Port Consolidator, perform the following procedure:

1. Unconfigure the Data Collector in the Visualization Engine (Application Monitor) user interface:

a. Start the Managing Server.

b. From the top navigation, click **Administration > Server Management > Data Collector Configuration**.

   The Data Collector Management page opens.

c. Go to the Configured Data Collectors at the top of the page.

d. To unconfigure the Data Collector, select the check box that is next to the Data Collector, and click **Apply**.

The unconfigured Data Collector is added to the Unconfigured Data Collectors page.

Notes:

a. If the data collection has reports associated with it, you are prompted to delete those reports before unconfiguring the Data Collector.

b. For further information about unconfiguring a Data Collector in the IBM WebSphere Application Server administrative console, see the section on unconfiguring a Data Collector in the *IBM Tivoli Composite Application Manager for Application Diagnostics: User's Guide*.

2. Stop the Port Consolidator. From a command prompt, enter one of the following values:

Table 41. Entering the proxyserverctrl_ws command

Windows	`proxyserverctrl_ws.bat stop`
UNIX and **Linux**	`./proxyserverctrl_ws.sh stop`

3. Verify that the Port Consolidator is stopped by entering one of the following commands:

Table 42. Entering the proxyserverctrl_ws command

Windows	`proxyserverctrl_ws.bat list`
UNIX and **Linux**	`./proxyserverctrl_ws.sh list`

   You will now see the message `KERNELPROXY is down`.

4. Reconfigure the Data Collector to bypass the Port Consolidator:

   a. Stop the application server. See "Stopping the application server" on page 266.

   b. Edit the `*DC_home*/runtime/*app_server_version.node_name.server_name*/custom/datacollector_custom.properties` file. Remove the following lines from the end of the file:

   ```
   proxy.host=IP address of Data Collector
   proxy.port=port
   ```

   c. Check for the same lines in the `*DC_home*/runtime/*appserver_version.node_name.server_name*/*appserver_version.node_name.server_name*.datacollector.properties` file; if they are present, remove them.

   d. Restart the instance of the application server that is being monitored by the Data Collector. See "Restarting the application server" on page 263.

5. In the Self-Diagnosis page of the Visualization Engine (Application Monitor) user interface, check to see that the Data Collector is listed. The Data Collector will show up as unconfigured.

6. Check the configuration of your Data Collector. In the Visualization Engine (Application Monitor) user interface, click **Administration > Server Management > Data Collector Configuration**.

   The Data Collector will be listed. However, it will be showing as unavailable.

7. View **Unconfigured Data Collectors**.

   Your Data Collector will be listed.

Appendix G. Support information

This chapter describes options for obtaining support for IBM products.

Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

Finding Release Notes

You can find Release Note information online by viewing IBM Technotes. Technotes replace the Release Notes® manual for this product. *Technotes* are short documents that cover a single topic. You can search the Technote collection for common problems and solutions, as well as known limitations and workarounds. Technotes are continuously updated to provide current product information.

The following two procedures describe how to view Technotes and subscribe to have future Technotes e-mailed to you. Alternatively, you can watch demos of these procedures at the following Web site:

http://www.ibm.com/software/support/sitetours.html

Viewing Technotes

Perform the following actions to access Technotes for this product:

1. Launch the IBM Software Support Web site: http://www.ibm.com/software/support
2. Follow the instructions on the screen to search for the Technotes related to the issue encountered.

Subscribing to new Technotes

You can subscribe to an RSS feed of the product support page or subscribe to receive e-mail notification about product tips and newly published fixes through My support. To subscribe to an RSS news feed of the product support page, click the orange **RSS** button under the **Stay up to date** pane.

My Support is a personalized portal that enables you to:

- Specify the products for which you want to receive notifications
- Create a personalized page that provides product information for the products you use
- Choose from flashes, downloads, and Technotes
- Receive an e-mail update in your inbox

Perform the following actions to subscribe to My support e-mails:

1. Launch an IBM support Web site such as the following site: http://www.ibm.com/support/
2. Click **My support** in the upper-right section of the page.
3. If you have not yet registered, click **register** in the upper-right corner of the support page to create your user ID and password.
4. Sign in to **My support**.

5. On the My support page, click **Add products**.
6. Make the following selections from the lists to add this product to your personal page:
   a. Software
   b. Systems Management
   c. Application Performance & Availability
7. Click **Add products**.
8. Click **Subscribe to email**.
9. Set your preferences to specify the information you want in your e-mails.
10. Click **Update**.
11. Click **Submit**.

Searching the information center on your local system or network

IBM provides extensive documentation that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

Searching the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select **Web search**. From this topic, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks®
- IBM DeveloperWorks
- Forums and newsgroups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. To determine what fixes are available for your IBM software product, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Click **Downloads** in the **Software** section.
3. Under the **Updates, drivers, and fixes** section, select **Fixes, fixpacks and utilities**.
4. Navigate to ITCAM for WebSphere or ITCAM for J2EE to obtain a list of available fixes.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

Receiving Weekly support updates

To receive e-mail notifications about software support news and updates, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. On the right hand side, click **My Notifications**.
3. If you have already registered for **My Notifications**, login. If you have not registered, click **register now**. Complete the registration form using your e-mail address as your IBM ID. When you have logged in, the **My notifications for IBM technical support** home page is displayed.
4. Select the **Subscribe** tab.
5. Under the **Software** list, select **Tivoli**.
6. Select **Tivoli Composite Application Manager for J2EE** and/or **Tivoli Composite Application Manager for WebSphere**. Click **Continue**.
7. In the **Options** section, enter a folder name, update notifications will be saved in this folder.
8. In the **Notify me by** section, choose if you want to me notified of updates daily or weekly.
9. In the **Notify me by** section, choose if you want to receive notifications in plain text or html.
10. In the **Document Types** section, customize the types of information you want to be updated on, for example, white papers, drivers etc. Click **Submit**.

If you experience problems with the **My Notifications** feature, you can obtain help in one of the following ways:

Online
Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

By phone
Call 1-800-IBM-4You (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, IBM Tivoli, IBM Lotus®, and IBM Rational® products, as well as IBM DB2 and IBM WebSphere Application Server products that run on Windows, UNIX, or Linux operating systems), enroll in IBM Passport Advantage® in one of the following ways:
  - **Online**: go to the IBM Passport Advantage Web page (http://www.ibm.com/software/passportadvantage) and click **How to Enroll**
  - **By phone**: for the phone number to call in your country, go to the IBM Software Support Web site (http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html) and click the name of your geographic region.
- For IBM eServer™ software products (including, but not limited to, IBM DB2 and IBM WebSphere Application Server products that run in IBM zSeries, IBM

pSeries, and IBM iSeries® environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (http://www.ibm.com/servers/eserver/techsupport.html).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html) and click the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. Determine the business impact of your problem.
2. Describe your problem and gather background information.
3. Submit your problem to IBM Software Support.

Determining the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

Table 43. Criteria for assessing the business impact of your problem

Severity 1	**Critical** business impact: you are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: the program is usable but is severely limited.
Severity 3	**Some** business impact: the program is usable with less significant features (not critical to operations) unavailable.
Severity 4	**Minimal** business impact: the problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describing your problem and gathering background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

Submitting your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online**: go to the "Submit and track problems" page on the IBM Software Support site (http://www.ibm.com/software/support/probsub.html). Enter your information into the appropriate problem submission tool.
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see Searching knowledge bases and Obtaining fixes.

Tivoli Support Technical Exchange

You can become a participant in the new Tivoli Support Technical Exchange, where you can expand your technical understanding of your current Tivoli products in a convenient format hosted by Tivoli support engineers. This program provides support discussions about product information, troubleshooting tips, common issues, problem solving resources and other topics. As Exchange leaders, Tivoli engineers provide subject matter expert direction and value. Participating in the Exchange helps you manage your Tivoli products with increased effectiveness.

What do you do to participate? Review the schedule of Exchange sessions. Find a topic of interest and select **register**. Provide your name, phone number, company name, number of attendees, the Exchange Topic and IBM Customer number. You will be invited to attend a 1-hour to 2-hour conference call where the information is presented. The new Tivoli Support Technical Exchange can help with the following areas:

- Increased product knowledge
- Ways to avoid common pitfalls
- Support recommendations
- Proactive customer support
- Helpful hints and tips
- Knowledge transfer
- Expansion of your knowledge base

For more information or to suggest a future Exchange session, contact Support Technical Exchange (xchange@us.ibm.com). To learn more, visit the following Web site: http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html

Appendix H. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. These are the major accessibility features you can use with ITCAM for Application Diagnostics when accessing it through the *IBM Personal Communications* terminal emulator:

- You can operate all features using the keyboard instead of the mouse.
- You can read text through interaction with assistive technology.
- You can use system settings for font, size, and color for all user interface controls.
- You can magnify what is displayed on your screen.

For more information on viewing PDFs from Adobe, go to the following Web site: http://www.adobe.com/enterprise/accessibility/main.html

Index

A

- accessibility xiv, 291
- AIX
  - APAR required 102
- application server
  - changing version 238
  - deleting profile 244
  - restarting 264
  - starting 265
  - stopping 267
- application server monitoring
  - configuring
    - Linux and UNIX systems 113, 140
    - manually 273
    - Windows 32
  - unconfiguring
    - Linux and UNIX systems 119, 156
    - manually 275
    - Windows 47
  - upgrading
    - Linux and UNIX systems 125, 128, 131, 168
    - Windows 60, 69, 76, 177, 184
- application support 110
- application support files
  - installing
    - Linux and UNIX systems 190
    - Windows 81
- Application support files 6
- AppServer_home xvi
- Asynchronous Bean requests 232
- autoconfiguration 246

B

- books xi
- Byte Code Instrumentation, disabling types of 221

C

- CICS 242
- command line configuration
  - Linux and UNIX systems 110
- communications protocols
  - Windows 27
- configuring
  - on Linux and UNIX systems 110, 198
  - on Windows 25, 89
  - Port Consolidator 281
  - remote 209
  - remote configuration 209
  - remote installation 209
- configuring application server monitoring
  - Linux and UNIX systems 113, 140
  - manually 273
  - Windows 32
- configuring Data Collector
  - Linux and UNIX systems 113, 140
  - manually 273

configuring Data Collector *(continued)*

  - Windows 32
- configuring Managing Server communication
  - Linux and UNIX systems 122, 161
  - Windows 53
- conventions
  - typeface xv
- CTG 242
- custom MBeans 233, 234
- custom requests 230
- customer support 287

D

- Data Collector 5
  - configuring
    - Linux and UNIX systems 113, 140
    - manually 273
    - Windows 32
  - disabling 263
  - moving to a different host computer 239
  - unconfiguring
    - Linux and UNIX systems 119, 156
    - manually 275
    - Windows 47
  - upgrading
    - Linux and UNIX systems 105, 125, 128, 131, 168
    - Windows 15, 60, 69, 76, 177, 184
- Data Collector buffering 219
- Data Collector properties 217
- datacollector_custom.properties 217
- datacollector.properties 217
- DC_home xvi
- destination folder
  - Windows 18
- destination location
  - Windows 18
- directories, variables for xv
- disabling Data Collectors 263

E

- Eclipse help server
  - Windows 84
- enabling history collection
  - Linux and UNIX systems 196
  - Windows 86
- encryption 256
- encryption key
  - UNIX 107
- encryption key for your IBM Tivoli Monitoring environment, defining
  - UNIX 107
  - Windows 19, 88
- encryption key for your ITM environment, defining
  - Windows 197

F

- features
  - Windows 21
- firewall 11, 100
- fixes, obtaining 286

G

- garbage collection 101
  - interval 241
  - verbose output 244
- garbage connection
  - log path 243

H

- heap dump 239, 240
- heap dumps, enabling 91, 201
  - WebSphere Application Server 6.0.2
    - SLES 9 (64-bit) 200
- historical data collection
  - Linux requirements 103
- history 277
- history collection
  - Linux and UNIX systems 196
  - Windows 86
- HotSpot JVM garbage collection 101
- hub TEMS
  - hot standby
    - Windows 27

I

- IBM Support Assistant 239
- information centers, searching to find software problem resolution 286
- install.sh, invoking 106
- installation prerequisites 6
- installing
  - on Linux and UNIX systems 105, 197
  - on Windows 15, 87
  - remote 209
- instrumentation 223
- integration with ITCAM for Transactions 245
- Internet, searching to find software problem resolution 286
- IP address 238
- ISA xv, 239
- ITM_home xvi

J

- Java core dumps, enabling 91, 201
- jks key files 91, 202

K

keystore management 252
knowledge bases, searching to find software problem resolution 285

L

Language pack
- installing
  - on Linux and UNIX systems 204
  - on Windows 94
- uninstalling
  - on Linux and UNIX systems 205
  - on Windows 95

license agreement, product
- UNIX 107
- Windows 17

lock analysis 223, 224

M

Manage Tivoli Enterprise Monitoring Services 196
Managing Server communication
- configuring
  - Linux and UNIX systems 122, 161
  - Windows 53

manual configuration 273
manual unconfiguration 275
manuals xi
MBeans 233
Memory Dump Diagnostic for Java 239
memory leak analysis 226
memory leak diagnosis 223
memory monitoring 237
method entry and exit analysis 223, 228
method tracing 223, 228
Monitoring Agent 6
- autostart 109
- starting 189

Monitoring Agent settings
- Linux and UNIX systems 110, 134
- Windows 28

N

NATs 241
Network Deployment 247
network interfaces 241
Node Authentication 251
- Data Collector 252
- Managing Server 251
- Port Consolidator 252

O

ordering publications xiv

P

password 12, 102
Performance Monitoring Infrastructure
- customizing 236

Performance Monitoring Infrastructure *(continued)*
- Service Integration Bus 236

permissions
- Linux and UNIX systems 99
- Windows 11

physical disability 291
populating certificates 252
Port Consolidator
- configuring 281
- unconfiguring 282

privacy filtering 258
problem determination
- describing problem for IBM Software Support 288
- determining business impact for IBM Software Support 288
- submitting problem to IBM Software Support 288

program folder
- Windows 21

properties files 217
publications xi
- ordering xiv

Q

Quality of Service
- using regular expressions 270

R

reader requirements xi
regular expressions 269
- bang (!) operator 270
- frequently used 269
- library 269
- Quality of Service 270

Release Notes 285
remote agent deployment
- UNIX 107

requirements for readers xi
restarting application servers 264
restoring configuration 271
RMI/IIOP requests, enabling instrumentation 221
root user 202

S

secure communications, verifying 257
security 251
security environment, defining
- Windows 19

selected features
- Windows 22

Service Integration Bus
- Performance Monitoring Infrastructure settings 236

setup.exe, invoking
- Windows 16

silent configuration
- on Linux and UNIX systems 198
- on Windows 89

silent product installation
- Linux and UNIX systems 196

silent product installation *(continued)*
- Windows 87

Software Support
- contacting 287
- describing problem for IBM Software Support 288
- determining business impact for IBM Software Support 288
- receiving weekly updates 287
- submitting problem to IBM Software Support 288

SSL 255
- Data Collector 256

starting
- application servers 265

stopping
- application servers 267

T

tacmd 209
Technotes
- e-mail subscriptions 285
- viewing 285

TEMS connection
- Linux and UNIX systems 110, 134
- Windows 26

The IBM Support Assistant xv
Tivoli Enterprise Portal
- benefits 3

Tivoli Support Technical Exchange 289
toolkit properties 217
toolkit_custom.properties 217
toolkit_global_custom.properties 217
toolkit.properties 217
trust files 91, 202
TTAPI 245
Turbo Mode 220
typeface conventions xv

U

unconfiguring
- Port Consolidator 282

unconfiguring application server monitoring
- Linux and UNIX systems 119, 156
- manually 275
- Windows 47

unconfiguring Data Collector
- Linux and UNIX systems 119, 156
- manually 275
- Windows 47

uninstalling
- on Linux and UNIX systems 203
- on Windows 93

upgrading
- on Linux and UNIX systems 105
- on Windows 15

upgrading application server monitoring
- Linux and UNIX systems 125, 128, 131, 168
- Windows 60, 69, 76, 177, 184

upgrading Data Collector
- Linux and UNIX systems 125, 128, 131, 168

upgrading Data Collector *(continued)*
  Windows 60, 69, 76, 177, 184

V
variables for directories xv

W
Web Services 237

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript® and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Intel, Intel logo, Intel Inside®, Intel Inside logo, Intel® Centrino®, Intel Centrino logo, Celeron®, Intel® Xeon®, Intel SpeedStep®, Itanium®, and Pentium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT®, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Printed in USA

SC27-2818-00